Cours de M2 *Groupes algébriques linéaires* [1]

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

$$\mathrm{Hom}_{\mathrm{C}}(\mathrm{X},\mathrm{Y}) \times \mathrm{Hom}_{\mathrm{C}}(\mathrm{Y},\mathrm{Z}) \to \mathrm{Hom}_{\mathrm{C}}(\mathrm{X},\mathrm{Z}), \quad (f,g) \mapsto g \circ f,$$

de telle sorte que les axiomes suivants soient vérifiés

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

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

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 $\mathrm{X} \xrightarrow{f} \mathrm{Y}$ est un *isomorphisme* s'il existe une flèche $\mathrm{Y} \xrightarrow{g} \mathrm{X}$ telle que $g \circ f = 1_{\mathrm{X}}$ et $f \circ g = 1_{\mathrm{Y}}$. 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.

(i) 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.

(ii) 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.

(iii) 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

[1] Version du 25 décembre 2008

tout objet X, 1_X est l'homomorphisme identité. Les isomorphismes sont les homomorphismes bijectifs.

(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, $\mathbf{Vect}(k)$ 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 $(E, \leqslant)$:
- les objets sont les éléments de E ;
- étant donnés des éléments x et y de E,

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

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 $\mathrm{Hom}_C(x,x)$.

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 $0, 1, \ldots$;
- étant donnés des nombres entiers n et m, $\mathrm{Hom}_{\Delta_k}(n,m)$ est l'ensemble $\mathrm{M}_{m,n}(k)$ des matrices à m lignes et n colonnes à coefficients dans k ;
- pour tous entiers m, n et p, la composition $\mathrm{M}_{n,m}(k) \times \mathrm{M}_{p,n}(k) \to \mathrm{M}_{p,m}(k)$ 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,

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

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* $\mathrm{F} : \mathrm{C} \to \mathrm{C}'$ est la donnée :
- pour tout objet X de C, d'un objet F(X) de C′ ;
- pour toute flèche $\mathrm{X} \xrightarrow{f} \mathrm{Y}$ dans C, d'une flèche $\mathrm{F(X)} \xrightarrow{\mathrm{F}(f)} \mathrm{F(Y)}$ dans C′,

de telle sorte que les axiomes suivants soient vérifiés :

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

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

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

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 $\mathrm{F}(g \circ f) = \mathrm{F}(f) \circ \mathrm{F}(g)$,

on obtient la notion de foncteur *contravariant* ; de manière équivalente, il s'agit d'un foncteur $\mathrm{C}^{\mathrm{op}} \to \mathrm{C}'$ ou $\mathrm{C} \to \mathrm{C}'^{\mathrm{op}}$.

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

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

3. Soit k un corps. On définit un foncteur de *dualité* $\mathrm{D} : \mathbf{Vect}(k) \to \mathbf{Vect}(k)^{\mathrm{op}}$ en associant à un k-espace vectoriel V (resp. à une application k-linéaire u) l'espace vectoriel dual $\mathrm{D}(\mathrm{V}) = \mathrm{Hom}_k(\mathrm{V}, k)$ (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 $\mathrm{L} : \Delta_k \to \mathbf{Vect}(k)$ en associant à tout entier n le k-espace vectoriel $\mathrm{L}(n) = k^n$ et à toute matrice $\mathrm{M} \in \mathrm{Hom}_{\Delta_k}(n, m) = \mathrm{M}_{m,n}(k)$ l'application k-linéaire correspondante de k^n dans k^m.

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

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

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

(1.1.3) Si $\mathrm{F}, \mathrm{G} : \mathrm{C} \to \mathrm{D}$ 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 $\varphi_{\mathrm{X}} : \mathrm{F}(\mathrm{X}) \to \mathrm{G}(\mathrm{X})$ dans D, de telle sorte que la condition suivante soit vérifiée : pour toute flèche $\mathrm{X} \xrightarrow{f} \mathrm{Y}$ dans C, le diagramme

$$\begin{array}{ccc} \mathrm{F}(\mathrm{X}) & \xrightarrow{\varphi_{\mathrm{X}}} & \mathrm{G}(\mathrm{X}) \\ {\scriptstyle \mathrm{F}(f)}\downarrow & & \downarrow{\scriptstyle \mathrm{G}(f)} \\ \mathrm{F}(\mathrm{Y}) & \xrightarrow[\varphi_{\mathrm{Y}}]{} & \mathrm{G}(\mathrm{Y}) \end{array}$$

est commutatif, i.e. $\varphi_{\mathrm{Y}} \circ \mathrm{F}(f) = \mathrm{G}(f) \circ \varphi_{\mathrm{X}}$.

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

2. Par la suite, nous rencontrerons à maintes reprises des morphismes de foncteurs qui seront fabriqués sur le modèle suivant. Soit $n \geqslant 1$ un entier. Tout homomorphisme d'anneaux commutatifs $f : \mathrm{A} \to \mathrm{B}$ donne naturellement naissance à un homomorphisme de monoïdes (multiplicatifs) $\mathrm{M}_n(f) : \mathrm{M}_n(\mathrm{A}) \to \mathrm{M}_n(\mathrm{B})$ associant à une matrice (x_{ij}) la matrice $\mathrm{M}_n(f)(x_{ij}) = (f(x_{ij}))$; on définit ainsi un foncteur M_n de la catégorie des anneaux commutatifs dans la catégorie **Mon** des monoïdes. Le déterminant d'une matrice s'exprimant polynomialement en ses coefficients, $\det(\mathrm{M}_n(f)(\mathrm{M})) = f(\det(\mathrm{M}))$ pour toute matrice $\mathrm{M} \in \mathrm{M}_n(\mathrm{A})$ et donc le déterminant fournit un morphisme de foncteurs $\det : \mathrm{M}_n \to \mathrm{M}_1$.

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

(i) il existe un morphisme de foncteurs $\psi : \mathrm{G} \to \mathrm{F}$ tel que $\psi \circ \varphi = 1_{\mathrm{F}}$ et $\varphi \circ \psi = 1_{\mathrm{G}}$;

(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 **Gr** et les foncteurs de C dans **Ens**.

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

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

pour tout objet X et toute flèche f dans C.

On désigne d'autre part par 1 le foncteur $\mathrm{C} \to \mathbf{Ens}$ tel que $1(\mathrm{X})$ 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 $\mathrm{G} : \mathrm{C} \to \mathbf{Ens}$,

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

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

(i) un foncteur $\mathrm{G} : \mathrm{C} \to \mathbf{Gr}$ *;*

(ii) un foncteur $\widetilde{\mathrm{G}} : \mathrm{C} \to \mathbf{Ens}$ *et des morphismes de foncteurs*

$$m : \widetilde{\mathrm{G}} \times \widetilde{\mathrm{G}} \to \widetilde{\mathrm{G}}, \quad e : 1 \to \widetilde{\mathrm{G}}, \quad \mathrm{inv} : \widetilde{\mathrm{G}} \to \widetilde{\mathrm{G}}$$

vérifiant les axiomes suivants :

(Ass) *le diagramme*

$$\begin{array}{ccccc}
(\widetilde{\mathrm{G}} \times \widetilde{\mathrm{G}}) \times \widetilde{\mathrm{G}} & \xrightarrow{m \times 1_{\widetilde{\mathrm{G}}}} & \widetilde{\mathrm{G}} \times \widetilde{\mathrm{G}} & & \\
\| & & & \searrow^{m} & \\
 & & & & \widetilde{\mathrm{G}} \\
 & & & \nearrow_{m} & \\
\widetilde{\mathrm{G}} \times (\widetilde{\mathrm{G}} \times \widetilde{\mathrm{G}}) & \xrightarrow[1_{\widetilde{\mathrm{G}}} \times m]{} & \widetilde{\mathrm{G}} \times \widetilde{\mathrm{G}} & &
\end{array}$$

est commutatif

(Uni) *les diagrammes*

$$\begin{array}{ccc}
1 \times \widetilde{\mathrm{G}} & \xrightarrow{e \times 1_{\widetilde{\mathrm{G}}}} & \widetilde{\mathrm{G}} \times \widetilde{\mathrm{G}} \\
 & \searrow^{\cong} & \downarrow{\scriptstyle m} \\
 & & \widetilde{\mathrm{G}}
\end{array} \qquad \textit{et} \qquad
\begin{array}{ccc}
\widetilde{\mathrm{G}} \times 1 & \xrightarrow{1_{\widetilde{\mathrm{G}}} \times e} & \widetilde{\mathrm{G}} \times \widetilde{\mathrm{G}} \\
 & \searrow^{\cong} & \downarrow{\scriptstyle m} \\
 & & \widetilde{\mathrm{G}}
\end{array}$$

sont commutatifs

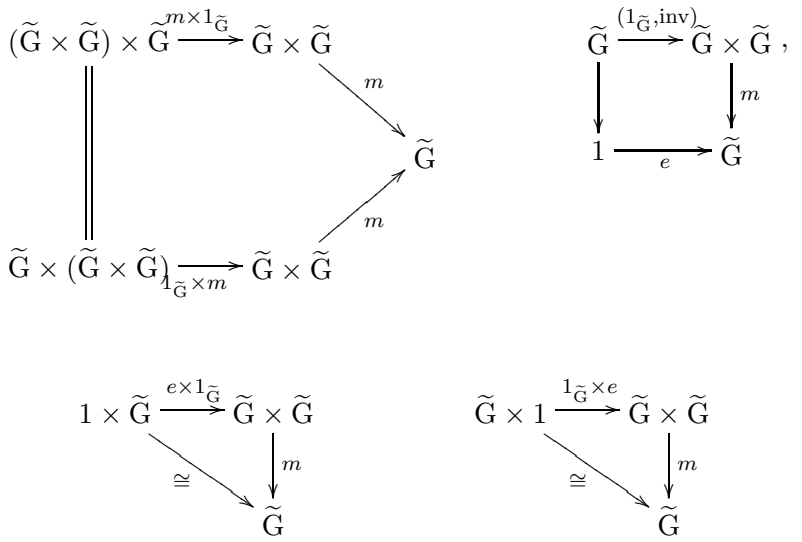
(Inv) *le diagramme*

$$\begin{array}{ccc}
\widetilde{\mathrm{G}} & \xrightarrow{(1_{\widetilde{\mathrm{G}}}, \mathrm{inv})} & \widetilde{\mathrm{G}} \times \widetilde{\mathrm{G}} \\
\downarrow & & \downarrow{\scriptstyle m} \\
1 & \xrightarrow[e]{} & \widetilde{\mathrm{G}}
\end{array}$$

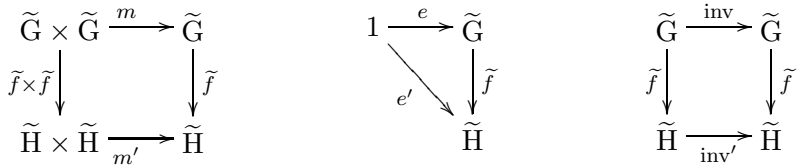
est commutatif.

Démonstration. Cette proposition est complètement triviale compte-tenu du fait qu'un groupe G (resp. un homomorphisme de groupes $f : \mathrm{G} \to \mathrm{H}$) est précisément la donnée d'un ensemble $\widetilde{\mathrm{G}}$ et d'applications $m : \widetilde{\mathrm{G}} \times \widetilde{\mathrm{G}} \to \widetilde{\mathrm{G}}$, $e : 1 \to \widetilde{\mathrm{G}}$ et $\mathrm{inv} : \widetilde{\mathrm{G}} \to \widetilde{\mathrm{G}}$ 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 $\widetilde{\mathrm{G}}$ un inverse. Ces axiomes usuels sont équivalents à la commutativité des quatre diagrammes



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



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

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

– Partant d'un foncteur G de C dans **Gr**, on définit $\widetilde{\mathrm{G}}$ comme le foncteur de C dans **Ens** obtenu en composant G par le foncteur d'oubli **Gr** $\to$ **Ens**; en clair, pour tout objet X et toute flèche f dans C, $\widetilde{\mathrm{G}}(\mathrm{X})$ est l'ensemble sous-jacent au groupe $\mathrm{G}(\mathrm{X})$ et $\widetilde{\mathrm{G}}(f)$ est l'application sous-jacente à l'homomorphisme de groupes $\widetilde{\mathrm{G}}(f)$. Pour tout objet X de C, la multiplication (resp. l'élément neutre; resp. l'inversion) du groupe $\mathrm{G}(\mathrm{X})$ définit une application $m_{\mathrm{X}} : \widetilde{\mathrm{G}}(\mathrm{X}) \times \widetilde{\mathrm{G}}(\mathrm{X}) \to \widetilde{\mathrm{G}}(\mathrm{X})$ (resp. $e_{\mathrm{X}} : 1(\mathrm{X}) \to \widetilde{\mathrm{G}}(\mathrm{X})$; resp. $\mathrm{inv}_{\mathrm{X}} : \widetilde{\mathrm{G}}(\mathrm{X}) \to \widetilde{\mathrm{G}}(\mathrm{X})$). Lorsque X varie, ces applications constituent des morphismes de foncteurs satisfaisant aux axiomes (Ass), (Uni) et (Inv).

– Partant réciproquement d'un foncteur $\widetilde{\mathrm{G}}$ de C dans **Ens** et de morphismes de foncteurs m, e et inv satisfaisant aux axiomes (Ass), (Uni) et (Inv), le quadruplet $\mathrm{G}(\mathrm{X}) = (\widetilde{\mathrm{G}}(\mathrm{X}), m_{\mathrm{X}}, e_{\mathrm{X}}, \mathrm{inv}_{\mathrm{X}})$ est un groupe pour tout objet X de C et l'application $\widetilde{\mathrm{G}}(f)$ définit un homomorphisme de groupes $\mathrm{G}(f)$ pour toute flèche f dans C. Les correspondances $\mathrm{X} \mapsto \mathrm{G}(\mathrm{X})$ et $f \mapsto \mathrm{G}(f)$ définissent un foncteur de C dans **Gr**.

□

Si G et H sont deux foncteurs de C dans **Gr** correspondant à des foncteurs $\widetilde{\mathrm{G}}$ et $\widetilde{\mathrm{H}}$ de C dans **Ens** équipés de morphismes de foncteurs $(m_{\mathrm{G}}, e_{\mathrm{G}}, \mathrm{inv}_{\mathrm{G}})$ et $(m_{\mathrm{H}}, e_{\mathrm{H}}, \mathrm{inv}_{\mathrm{H}})$ qui satisfaisont aux axiomes (Ass), (Uni) et (Inv), il revient au même de se donner

(i) un morphisme de foncteurs $\varphi : \mathrm{G} \to \mathrm{H}$;

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

$$\begin{array}{ccc} \widetilde{\mathrm{G}} \times \widetilde{\mathrm{G}} & \xrightarrow{m_{\mathrm{G}}} & \widetilde{\mathrm{G}} \\ {\scriptstyle \widetilde{\varphi}\times\widetilde{\varphi}}\downarrow & & \downarrow{\scriptstyle \widetilde{\varphi}} \\ \widetilde{\mathrm{H}} \times \widetilde{\mathrm{H}} & \xrightarrow[m_{\mathrm{H}}]{} & \widetilde{\mathrm{H}} \end{array} \qquad \begin{array}{ccc} 1 & \xrightarrow{e_{\mathrm{G}}} & \widetilde{\mathrm{G}} \\ & {\scriptstyle e_{\mathrm{H}}}\searrow & \downarrow{\scriptstyle \widetilde{\varphi}} \\ & & \widetilde{\mathrm{H}} \end{array} \qquad \begin{array}{ccc} \widetilde{\mathrm{G}} & \xrightarrow{\mathrm{inv}_{\mathrm{G}}} & \widetilde{\mathrm{G}} \\ {\scriptstyle \widetilde{\varphi}}\downarrow & & \downarrow{\scriptstyle \widetilde{\varphi}} \\ \widetilde{\mathrm{H}} & \xrightarrow[\mathrm{inv}_{\mathrm{H}}]{} & \widetilde{\mathrm{H}} \end{array}$$

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 $\widetilde{\mathrm{G}}$ obtenu en composant G par le foncteur oubli $\mathbf{Gr} \to \mathbf{Ens}$. 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 $\mathrm{h_X} : \mathrm{C} \to \mathbf{Ens}$:

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

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

On a clairement $\mathrm{h}_{u\circ v} = \mathrm{h}_v \circ \mathrm{h}_u$ pour toutes flèches composables u et v dans C. Enfin, pour tout objet X de C, $\mathrm{h}_{1_{\mathrm{X}}}$ est la transformation identique du foncteur $\mathrm{h_X}$.

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

$$\mathrm{h}_{\mathrm{X}'}(\mathrm{Y}) \to \mathrm{h_X},\ f \mapsto f \circ u.$$

Le théorème suivant est fondamental.

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

$$\left\{ \begin{array}{c} \textit{morphismes de foncteurs} \\ \varphi : \mathrm{h_X} \to \mathrm{F} \end{array} \right\} \longrightarrow \mathrm{F(X)}, \quad \varphi \mapsto \varphi_{\mathrm{X}}(1_{\mathrm{X}})$$

est une bijection.

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

$$\begin{array}{ccc} \mathrm{h_X(X)} & \xrightarrow{\varphi_{\mathrm{X}}} & \mathrm{F(X)} \\ {\scriptstyle \mathrm{h_X}(f)}\downarrow & & \downarrow{\scriptstyle \mathrm{F}(f)} \\ \mathrm{h_X(Y)} & \xrightarrow[\varphi_{\mathrm{Y}}]{} & \mathrm{F(Y)} \end{array}$$

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 $h_X(Y) = \mathrm{Hom}_C(X, Y)$ 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

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

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 $F : C \to \mathbf{Ens}$ 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*

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

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 $\varphi : h_X \to h_Y$ et l'ensemble $h_Y(X) = \mathrm{Hom}_C(Y, X)$ 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 $\varphi : h_X \to h_Y$ défini par la condition suivante : pour tout objet Z de C, φ_Z est l'application

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

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.

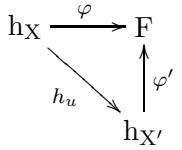
– Si u est un isomorphisme, alors $\mathrm{h}_u \circ \mathrm{h}_{u^{-1}} = \mathrm{h}_{u^{-1}\circ u} = \mathrm{h}_{1_\mathrm{Y}} = 1_{\mathrm{h}_\mathrm{Y}}$ et $\mathrm{h}_{u^{-1}} \circ \mathrm{h}_u = \mathrm{h}_{u\circ u^{-1}} = \mathrm{h}_{1_\mathrm{X}} = 1_{\mathrm{h}_\mathrm{X}}$, donc h_u est un isomorphisme de foncteurs.
– Si réciproquement h_u est un isomorphisme de foncteurs, l'isomorphisme inverse $\mathrm{h}_u^{-1} : \mathrm{h}_\mathrm{Y} \xrightarrow{\sim} \mathrm{h}_\mathrm{X}$ est de la forme h_v pour une certaine flèche $v \in \mathrm{Hom}_\mathrm{C}(\mathrm{X}, \mathrm{Y})$ et alors

$$\mathrm{h}_{u\circ v} = \mathrm{h}_v \circ \mathrm{h}_u = \mathrm{h}_{1_\mathrm{X}}, \quad \mathrm{h}_{v\circ u} = \mathrm{h}_u \circ \mathrm{h}_v = \mathrm{h}_{1_\mathrm{Y}},$$

donc $u \circ v = 1_\mathrm{X}$, $v \circ u = 1_\mathrm{Y}$ et u est un isomorphisme.

□

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



soit commutatif.

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

Ainsi, si un foncteur $\mathrm{F} : \mathrm{C} \to \mathbf{Ens}$ est représentable, tout représentant $(\mathrm{X}, \varphi_\mathrm{X})$ 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 $\mathrm{F}(\mathrm{X})$ 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 $\mathrm{F}(\mathrm{Y})$, il existe une unique flèche $f : \mathrm{X} \to \mathrm{Y}$ dans C telle que $\beta = \mathrm{F}(f)(\alpha)$. 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 $f : \mathrm{X} \xrightarrow{\sim} \mathrm{X}'$ uniquement déterminé tel que $\alpha' = \mathrm{F}(f)(\alpha)$.

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 **Ens** dans **Ens** qui associe à tout ensemble E' l'ensemble des applications $f : \mathrm{E} \to \mathrm{E}'$ telles que $f(x) = f(y)$ si $x \sim y$. Ce foncteur est repésentable par l'ensemble quotient $\mathrm{E}/\sim$ et la projection canonique p de E dans E' ; c'est la « propriété universelle du quotient ».

(ii) Prenons pour C la catégorie $\mathbf{Mod}(\mathrm{A})$ des modules (à gauche) sur un anneau A. Étant donnés un A-module M et un sous-module N, le foncteur F de $\mathbf{Mod}(\mathrm{A})$ dans la catégorie des ensembles, qui à un A-module P associe l'ensemble des applications A-linéaires $u : \mathrm{M} \to \mathrm{P}$ 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 **Top** des espaces topologiques. Le foncteur « composantes connexes » π_0 : **Top** $\to$ **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

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

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 $X = \varnothing$ (si $X \neq \varnothing$, les fonctions réelles constantes fournissent une infinité d'applications continues de X dans $\mathbb{R}$). Comme l'ensemble $\mathrm{Hom}_{\mathbf{Top}}(\varnothing, Y)$ 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 donnés 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 » $\pi_0' : \mathbf{Top} \to \mathbf{Ens}$ n'est pas représentable (même argument que pour π_0) mais le foncteur $\pi_0' : \mathbf{Hot} \to \mathbf{Ens}$ 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

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

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

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

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 topologique 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 $(E, \leqslant)$ (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* $\mathrm{X} \times \mathrm{Y}$ de deux ensembles X et Y, représentant le foncteur

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

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 apparence, ce point de vue s'avère parfois simplificateur en ce qu'il permet de construire une flèche $u : \mathrm{X} \longrightarrow \mathrm{Y}$ dans une catégorie C *a priori* compliquée en définissant seulement des applications naturelles entre les ensembles variables $\mathrm{h}_{\mathrm{Y}}(\cdot)$ et $\mathrm{h}_{\mathrm{X}}(\cdot)$. 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 algébriques 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* $\mathrm{G} : \mathbf{Alg}_k \to \mathbf{Gr}$ *tel que le foncteur en ensembles associé* $\mathbf{Alg}_k \to \mathbf{Ens}$ *soit représentable par une k-algèbre de type fini.*

(ii) Si G *et* H *sont deux groupes algébriques affines sur k, un* homomorphisme $f : \mathrm{G} \to \mathrm{H}$ *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 $\mathrm{G} : \mathbf{Alg}_k \to \mathbf{Gr}$ 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

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

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

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

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 $k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ en un nombre fini de variables par un idéal $\mathfrak{I}$:

$$\lambda : k[\mathrm{T}_1, \ldots, \mathrm{T}_n]/\mathfrak{I} \simeq \mathrm{A}.$$

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

$$\mathrm{V}_{\mathfrak{I}} : \mathbf{Alg}_k \to \mathbf{Ens},$$

associant à toute k-algèbre R l'ensemble

$$\mathrm{V}_{\mathfrak{I}}(\mathrm{R}) = \{(r_1, \ldots, r_n) \in \mathrm{R}^n \mid \mathrm{P}(r_1, \ldots, r_n) = 0 \text{ pour tout } \mathrm{P} \in \mathfrak{I}\}$$

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

$$\mathrm{V}_{\mathfrak{I}}(f) : \mathrm{V}_{\mathfrak{I}}(\mathrm{R}) \to \mathrm{V}_{\mathfrak{I}}(\mathrm{R}'), \quad (r_1, \ldots, r_n) \mapsto (f(r_1), \ldots, f(r_n)).$$

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

un groupe algébrique affine sur k, c'est un foncteur $\mathrm{G} : \mathbf{Alg}_k \to \mathbf{Gr}$ *tel que, pour toute k-algèbre* R*, l'ensemble sous-jacent au groupe* $\mathrm{G}(\mathrm{R})$ *puisse s'identitifer 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 $\mathrm{GL}_n : \mathbf{Alg}_k \to \mathbf{Gr}$, 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 $f : \mathrm{R} \to \mathrm{R}'$, l'homomorphisme de groupes induit par l'homomorphisme de monoïdes $\mathrm{M}_n(\mathrm{R}) \to \mathrm{M}_n(\mathrm{R}'),\ (x_{ij}) \mapsto (f(x_{ij}))$,

est un groupe algébrique sur k.

En effet, quelle que soit la k-algèbre R, se donner une matrice M dans $\mathrm{M}_n(\mathrm{R})$ revient à se donner n^2 éléments m_{ij} de R, c'est-à-dire un homomorphisme de la k-algèbre de polynômes $k[(\mathrm{X}_{ij})_{1\leqslant i,j\leqslant n}]$ 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 $t \in \mathrm{R}$ avec $t\det(\mathrm{M}) - 1 = 0$. La formule bien connue

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

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

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

où l'on a posé

$$\det(\mathrm{X}_{ij}) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \mathrm{X}_{1\sigma(1)} \dots \mathrm{X}_{n\sigma(n)}.$$

2. Le morphisme de foncteurs en groupes $\det : \mathrm{GL}_n \to \mathrm{GL}_1$, défini par la collection des homomorphismes de groupes $\det_{\mathrm{R}} : \mathrm{GL}_n(\mathrm{R}) \to \mathrm{GL}_1(\mathrm{R})$ 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* $\varphi : \mathrm{h}_{\mathrm{A}} \simeq \mathrm{G}$.

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 $u : \mathrm{A}' \to \mathrm{A}$ tel que le diagramme

$$\begin{array}{ccc} \mathrm{h}_{\mathrm{A}} & \xrightarrow{\mathrm{h}_u} & \mathrm{h}_{\mathrm{A}'} \\ & {\scriptstyle\varphi}\searrow \quad \swarrow{\scriptstyle\varphi'} & \\ & \mathrm{G} & \end{array}$$

soit commutatif. Cela permet de parler de l'*anneau de coordonnées* de G, noté $(\mathcal{O}(\mathrm{G}), \varphi)$ ou $(k[\mathrm{G}], \varphi)$; 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 $1 : \mathbf{Alg}_k \to \mathbf{Gr}$ 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 $\mathbb{G}_{\mathrm{a}} : \mathbf{Alg}_k \to \mathbf{Gr}$ associant à toute k-algèbre R le groupe additif sous-jacent $(\mathrm{R}, +)$ est un groupe algébrique sur k d'anneau de coordonnées la k-algèbre $k[\mathrm{X}]$. C'est le *groupe additif* sur k.

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

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

(v) Pour tout entier $n \geqslant 0$, le foncteur $\mathrm{SL}_n : \mathbf{Alg}_k \to \mathbf{Gr}$ associant à chaque k-algèbre R le groupe $\mathbf{SL}_n(\mathrm{R})$ 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 $k[(\mathrm{X}_{ij})_{1 \leqslant i,j \leqslant n}]/(\det(\mathrm{X}_{ij}) - 1)$. C'est le *groupe spécial linéaire* sur k.

(vi) Pour tout entier $n \geqslant 0$, le foncteur $\mathrm{D}_n : \mathbf{Alg}_k \to \mathbf{Gr}$ associant à chaque k-algèbre R le groupe $\mathrm{D}_n(\mathrm{R})$ 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 $k[(\mathrm{X}_i)_{1 \leqslant i \leqslant n}, \mathrm{T}]/(\mathrm{X}_1 \dots \mathrm{X}_n \mathrm{T} - 1)$.

(vii) Pour tout entier $n \geqslant 0$, le foncteur $\mathrm{B}_n : \mathbf{Alg}_k \to \mathbf{Gr}$ associant à chaque k-algèbre R le groupe $\mathrm{B}_n(\mathrm{R})$ 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 $k[(\mathrm{X}_{ij})_{1 \leqslant i \leqslant j \leqslant n}, \mathrm{T}]/(\mathrm{X}_{11} \dots \mathrm{X}_{nn} \mathrm{T} - 1)$.

(viii) Pour tout entier $n \geqslant 0$, le foncteur $\mathrm{U}_n : \mathbf{Alg}_k \to \mathbf{Gr}$ associant à chaque k-algèbre R le groupe $\mathrm{U}_n(\mathrm{R})$ 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 $k[(\mathrm{X}_{ij})_{1 \leqslant i < j \leqslant n}]$.

(ix) Pour tout entier $n \geqslant 0$, le foncteur $\mathrm{O}_n : \mathbf{Alg}_k \to \mathbf{Gr}$ associant à chaque k-algèbre R le groupe

$$\mathrm{O}_n(\mathrm{R}) = \{\mathrm{M} \in \mathrm{M}_n(\mathrm{R}) \mid {}^t\mathrm{MM} = \mathrm{I}_n\}$$

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

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

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

(x) Pour tout entier $n \geqslant 0$, le foncteur $\mathrm{Sp}_{2n} : \mathbf{Alg}_k \to \mathbf{Gr}$ associant à chaque k-algèbre R le groupe

$$\mathrm{Sp}_{2n}(\mathrm{R}) = \{\mathrm{M} \in \mathrm{M}_{2n}(\mathrm{R}) \mid {}^t\mathrm{MJ}_n\mathrm{M} = \mathrm{J}_n\},$$

où $\mathrm{J}_n = \begin{pmatrix} 0 & -\mathrm{I}_n \\ \mathrm{I}_n & 0 \end{pmatrix}$, 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

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

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

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 $\mathrm{h_A}$ 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 $\mathrm{h_A} : \mathbf{Alg}_k \to \mathbf{Ens}$ est le foncteur en ensembles associé à un foncteur en groupes, ou de dire qu'il existe des morphismes de foncteurs

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

tels que les quatre diagrammes

$$\begin{array}{ccc} (\mathrm{h_A} \times \mathrm{h_A}) \times \mathrm{h_A} & \xrightarrow{m \times 1_{\mathrm{h_A}}} & \mathrm{h_A} \times \mathrm{h_A} \\ \| & & \searrow^{m} \\ \mathrm{h_A} \times (\mathrm{h_A} \times \mathrm{h_A}) & \xrightarrow[1_{\mathrm{h_A}} \times m]{} & \mathrm{h_A} \times \mathrm{h_A} \xrightarrow{m} \mathrm{h_A} \end{array} \qquad \begin{array}{ccc} \mathrm{h_A} & \xrightarrow{(1_{\mathrm{h_A}}, \mathrm{inv})} & \mathrm{h_A} \times \mathrm{h_A} \\ \downarrow & & \downarrow{\scriptstyle m} \\ 1 & \xrightarrow[e]{} & \mathrm{h_A} \end{array},$$

$$\begin{array}{ccc} 1 \times \mathrm{h_A} & \xrightarrow{e \times 1_{\mathrm{h_A}}} & \mathrm{h_A} \times \mathrm{h_A} \\ & \searrow^{\cong} & \downarrow{\scriptstyle m} \\ & & \mathrm{h_A} \end{array} \qquad \begin{array}{ccc} \mathrm{h_A} \times 1 & \xrightarrow{1_{\mathrm{h_A}} \times e} & \mathrm{h_A} \times \mathrm{h_A} \\ & \searrow^{\cong} & \downarrow{\scriptstyle m} \\ & & \mathrm{h_A} \end{array}$$

soient commutatifs.

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

$$\mathrm{h_A} \times \mathrm{h_B} : \mathbf{Alg}_k \to \mathbf{Ens}, \quad \mathrm{R} \mapsto \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A}, \mathrm{R}) \times \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{B}, \mathrm{R})$$

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

$$\mathrm{h_A} \times \mathrm{h_B} \cong \mathrm{h_{A \otimes_k B}}.$$

En vertu du lemme de Yoneda, le morphisme de multiplication

$$m : \mathrm{h_{A \otimes_k A}} \cong \mathrm{h_A} \times \mathrm{h_A} \to \mathrm{h_A}$$

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

$$\Delta : \mathrm{A} \to \mathrm{A} \otimes_k \mathrm{A}$$

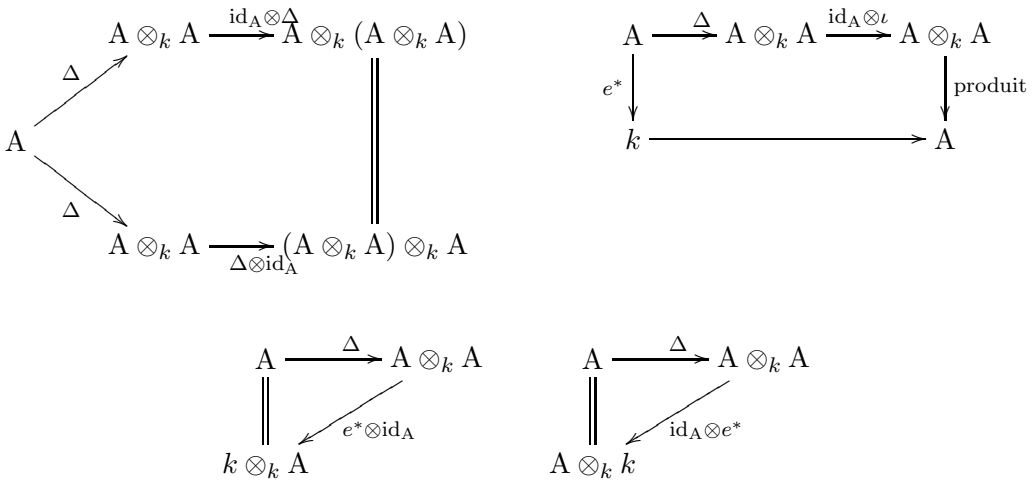
est un homomorphisme de k-algèbres uniquement déterminé.

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

$$e^* : \mathrm{A} \to k$$

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

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



soient commutatifs.

Démonstration. En vertu du lemme de Yoneda, deux homomorphismes de k-algèbres $f, g : \mathrm{R} \to \mathrm{R}'$ sont égaux si et seulement si les morphismes de foncteurs $\mathrm{h}_f, \mathrm{h}_g : \mathrm{h}_{\mathrm{R}'} \to \mathrm{h}_{\mathrm{R}}$ 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 $\mathrm{h_A}$. 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 $(\mathrm{id_A}, \mathrm{inv}) : \mathrm{h_A} \to \mathrm{h_A} \times \mathrm{h_A}$ peut également s'écrire sous la forme

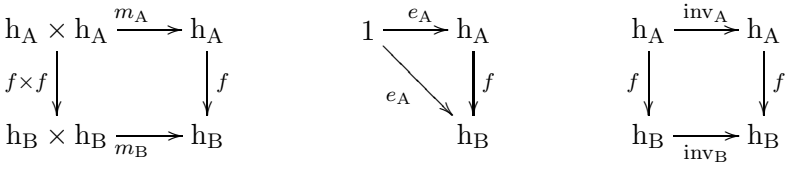
$$\mathrm{h_A} \xrightarrow{(\mathrm{id_A}, \mathrm{id_A})} \mathrm{h_A} \times \mathrm{h_A} \xrightarrow{\mathrm{id_A} \times \mathrm{inv}} \mathrm{h_A} \times \mathrm{h_A} \ .$$

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

$$(\mathrm{id_A}, \mathrm{id_A}) : \mathrm{h_A} \to \mathrm{h_A} \times \mathrm{h_A} \cong \mathrm{h}_{\mathrm{A} \otimes_k \mathrm{A}}$$

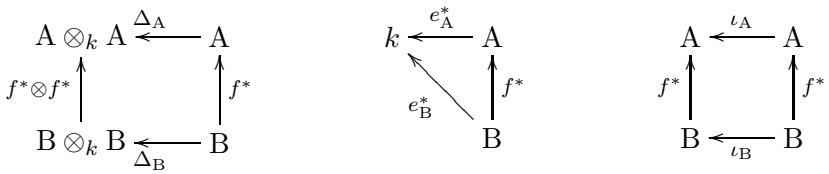
correspond à l'unique homomorphisme de k-algèbres $u : \mathrm{A} \otimes_k \mathrm{A} \to \mathrm{A}$ tel que $u(a \otimes 1) = u(1 \otimes a) = a$ pour tout $a \in \mathrm{A}$; comme $a \otimes a' = (a \otimes 1)(1 \otimes a')$, $u(a \otimes a') = aa'$ est l'homomorphisme *produit*. □

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



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 $f^* : \mathrm{B} \to \mathrm{A}$ tel que $f = \mathrm{h}_{f^*}$. De manière analogue à la proposition 2.2.1, on vérifie que la commutativité

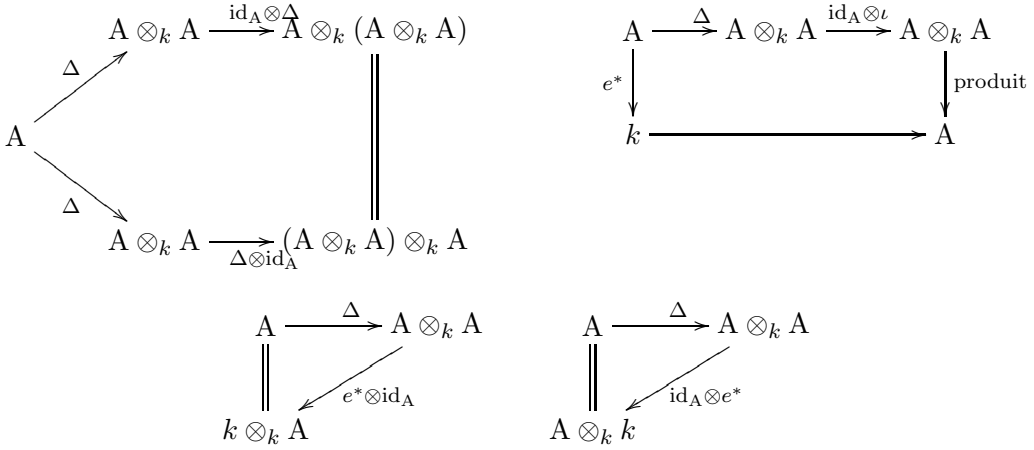
des trois diagrammes précédents est équivalente à celle des trois diagrammes suivants :



où les triplets $(\Delta_{\mathrm{A}}, e_{\mathrm{A}}^*, \iota_{\mathrm{A}})$ et $(\Delta_{\mathrm{B}}, e_{\mathrm{B}}^*, \iota_{\mathrm{B}})$ sont déduits comme ci-dessus des triplets $(m_{\mathrm{A}}, e_{\mathrm{A}}, \mathrm{inv}_{\mathrm{A}})$ et $(m_{\mathrm{B}}, e_{\mathrm{B}}, \mathrm{inv}_{\mathrm{B}})$ via le lemme de Yoneda.

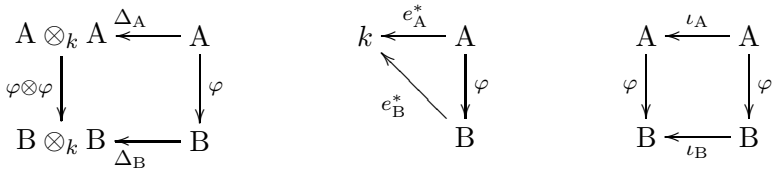
Définition 2.2.2 — *Soit k un corps.*

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



soient commutatifs.

(ii) Un morphisme *d'une k-bigèbre $(\mathrm{A}, \Delta_{\mathrm{A}}, e_{\mathrm{A}}^*, \iota_{\mathrm{A}})$ dans une k-bigèbre $(\mathrm{B}, \Delta_{\mathrm{B}}, e_{\mathrm{B}}^*, \iota_{\mathrm{B}})$ est un homomorphisme de k-algèbres $\varphi : \mathrm{A} \to \mathrm{B}$ tel que les trois diagrammes*



soient commutatifs.

On dit qu'une k-bigèbre $(\mathrm{A}, \Delta_{\mathrm{A}}, e_{\mathrm{A}}^*, \iota_{\mathrm{A}})$ 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 $(\mathrm{A}, \Delta_{\mathrm{A}}, e_{\mathrm{A}}^*, \iota_{\mathrm{A}})$;

– étant données deux k-bigèbres de type fini $(\mathrm{A}, \Delta_{\mathrm{A}}, e_{\mathrm{A}}^*, \iota_{\mathrm{A}})$ et $(\mathrm{B}, \Delta_{\mathrm{B}}, e_{\mathrm{B}}^*, \iota_{\mathrm{B}})$, la correspondance

$$\left\{ \begin{array}{c} \text{morphismes de } k\text{-bigèbres} \\ (\mathrm{A}, \Delta_{\mathrm{A}}, e_{\mathrm{A}}^*, \iota_{\mathrm{A}}) \xrightarrow{\varphi} (\mathrm{B}, \Delta_{\mathrm{B}}, e_{\mathrm{B}}^*, \iota_{\mathrm{B}}) \end{array} \right\} \to \left\{ \begin{array}{c} \text{homomorphismes de } k\text{-groupes} \\ \mathrm{h_B} \xrightarrow{\mathrm{h}_\varphi} \mathrm{h_B} \end{array} \right\}$$

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 $\mathrm{A} = k[(\mathrm{X}_{ij})_{1\leqslant i,j\leqslant n}, \mathrm{T}]/(\mathrm{T}\det(\mathrm{X}_{ij}) - 1)$: pour toute k-algèbre R,

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},\mathrm{R}) & \xrightarrow{\sim} & \mathrm{GL}_n(\mathrm{R}) \\ u & \mapsto & (u(\mathrm{X}_{ij})). \end{array}$$

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

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A} \otimes_k \mathrm{A},\mathrm{R}) & \xrightarrow{\sim} & \mathrm{GL}_n(\mathrm{R}) \times \mathrm{GL}_n(\mathrm{R}) \\ w & \mapsto & ((w(\mathrm{X}_{ij} \otimes 1)), (w(1 \otimes \mathrm{X}_{ij}))), \end{array}$$

on dispose d'un diagramme commutatif

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

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

$$((w \circ \Delta)(\mathrm{X}_{ij})) = (w(\mathrm{X}_{ij} \otimes 1))\,(w(1 \otimes \mathrm{X}_{ij}))$$

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

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

et donc finalement

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

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

$$u(\mathrm{T}) = \det(u(\mathrm{X}_{ij}))^{-1}$$

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

$$\begin{aligned} (w \circ \Delta)(\mathrm{T}) &= \det\left((w \circ \Delta)(\mathrm{X}_{ij})\right)^{-1} \\ &= \det\left((w(\mathrm{X}_{ij} \otimes 1))(w(1 \otimes \mathrm{X}_{ij}))\right)^{-1} \\ &= \det(w(\mathrm{X}_{ij} \otimes 1))^{-1} \det(w(1 \otimes \mathrm{X}_{ij}))^{-1} \\ &= w((\mathrm{T} \otimes 1)(1 \otimes \mathrm{T})) \\ &= w(\mathrm{T} \otimes \mathrm{T}) \end{aligned}$$

et donc

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

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

$$\begin{array}{ccc} 1 & \xrightarrow{\quad e \quad} & \mathrm{GL}_n(\mathrm{R}) \\ \wr\uparrow & & \uparrow\wr \\ \mathrm{Hom}_{\mathbf{Alg}_k}(k,\mathrm{R}) & \longrightarrow & \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},\mathrm{R}) \end{array}$$

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

$$(e^*(\mathrm{X}_{ij})) = \mathrm{I}_n \quad \text{et} \quad e^*(\mathrm{T}) = \det(\mathrm{I}_n)^{-1},$$

soit

$$e^*(\mathrm{X}_{ij}) = \left\{ \begin{array}{ll} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{array} \right. \quad \text{et} \quad e^*(\mathrm{T}) = 1.$$

Considérons finalement le diagramme commutatif

$$\begin{array}{ccc} \mathrm{GL}_n(\mathrm{R}) & \xrightarrow{\quad \mathrm{inv} \quad} & \mathrm{GL}_n(\mathrm{R}) \\ \wr\uparrow & & \uparrow\wr \\ \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},\mathrm{R}) & \longrightarrow & \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},\mathrm{R}) \end{array}$$

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

$$((u\circ\iota)(\mathrm{X}_{ij})) = (u(\mathrm{X}_{ij}))^{-1} = \det(u(\mathrm{X}_{ij}))^{-1}\mathrm{adj}(u(\mathrm{X}_{ij})),$$

où, pour toute matrice $\mathrm{M}\in \mathrm{M}_n(\mathrm{R})$, $\mathrm{adj}(\mathrm{M})$ est la matrice définie par

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

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

$$\begin{array}{rcl} (u\circ\iota)(\mathrm{X}_{ij}) & = & u(\mathrm{T})[\mathrm{adj}(u(\mathrm{X}_{ij}))]_{ij} \\ & = & u(\mathrm{T}[\mathrm{adj}(\mathrm{X}_{ij})]_{ij}) \end{array}$$

et donc

$$\iota(\mathrm{X}_{ij}) = \mathrm{T}[\mathrm{adj}(\mathrm{X}_{ij})]_{ij}.$$

De même,

$$(u\circ\iota)(\mathrm{T}) = u(\mathrm{T})^{-1} = \big(\det(u(\mathrm{X}_{ij}))^{-1}\big)^{-1} = \det(u(\mathrm{X}_{ij})) = u(\det(\mathrm{X}_{ij}))$$

donc

$$\iota(\mathrm{T}) = \det(\mathrm{X}_{ij}).$$

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

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

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

de la counité

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

et de la coinversion

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

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

– La comultiplication

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

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

– La counité

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

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

– La coinversion

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

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

(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* $\mathbb{G}_{\mathrm{a}}$ *et* $\mathbb{G}_{\mathrm{m}}$ *:*

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

et

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

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

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

implique

$$1 = 1^*(\mathrm{X}) = 0^*(a) = a,$$

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

$$\mathbb{G}_{\mathrm{a}} \longrightarrow 1 \xrightarrow{1} \mathbb{G}_{\mathrm{m}}$$

correspondant à l'homomorphisme de k-bigèbres

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

Il revient au même de se donner un homomorphisme $g : \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{a}}$ ou un homomorphisme de k-algèbres $g^* : k[\mathrm{T}] \to k[\mathrm{X}, \mathrm{X}^{-1}]$ compatible aux structures de bigèbres. L'homomorphisme

g^* est complètement déterminé par le polynôme de Laurent $g^*(\mathrm{T}) = \sum_{n\in\mathbb{Z}} a_n \mathrm{X}^n$. La commutativité du diagramme

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

se traduit par l'identité

$$\Delta(g^*(\mathrm{T})) = (g^*\otimes g^*)(\Delta(\mathrm{T}))$$

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

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

et il en de même du membre de droite :

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

Nous obtenons donc l'identité

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

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

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

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

$$\mathbb{G}_\mathrm{m} \longrightarrow 1 \xrightarrow{0} \mathbb{G}_\mathrm{a}$$

correspondant à l'homomorphisme de k-bigèbres

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

□

Exercices. 1) Soit Γ un groupe fini. Démontrer que le foncteur constant $\Gamma : \mathbf{Alg}_k \to \mathbf{Gr}$ défini par $\Gamma(\mathrm{R}) = \Gamma$ pour toute k-algèbre R et $\Gamma(f) = \mathrm{id}_\Gamma$ 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,

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

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 :

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

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

On considère les homomorphismes de k-algèbres

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

définis comme suit :

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

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

et

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

(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 $\underline{\Gamma}(\mathrm{R})$ 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* $i : \mathrm{H} \to \mathrm{G}$ *tel que l'homomorphisme de* k*-algèbres* $i^* : \mathcal{O}(\mathrm{G}) \to \mathcal{O}(\mathrm{H})$ *correspondant soit surjectif.*

Cette définition appelle deux commentaires.

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

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

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 $u, v \in \mathrm{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(\mathrm{H}), \mathrm{R})$ et ceci prouve que l'application i_R est injective.

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

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

induit une bijection sur le sous-ensemble de $\mathrm{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(\mathrm{G}), \mathrm{R})$ constitué des homomorphismes u tels que $u(\ker(i^*) = 0$. De manière encore plus explicite, si l'on écrit $\mathcal{O}(\mathrm{G})$ sous la forme $k[\mathrm{T}_1, \ldots, \mathrm{T}_n]/\mathfrak{I}$, alors l'idéal $\ker(i^*)$ de $\mathcal{O}(\mathrm{G})$ provient d'un idéal $\mathfrak{J}$ de $k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ contenant $\mathfrak{I}$,

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

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

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 $i : \mathrm{H} \to \mathrm{G}$ tel que, pour toute k-algèbre R, l'homomorphisme $i_\mathrm{R} : \mathrm{H}(\mathrm{R}) \to \mathrm{G}(\mathrm{R})$

soit *injectif*. On peut en effet démontrer que cette condition suffit à garantir la surjectivité de l'homomorphisme $i^* : \mathcal{O}(\mathrm{G}) \to \mathcal{O}(\mathrm{H})$.

Exemples. 1) Pour tout entier $n \geqslant 0$, 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

$$i^* : k[(\mathrm{X}_{ij})_{1\leqslant i,j\leqslant n}, \mathrm{T}]/(\mathrm{T}\det(\mathrm{X}_{ij}) - 1) \to k[(\mathrm{X}_{ij})_{1\leqslant i,j\leqslant n}]/(\det(\mathrm{X}_{ij}) - 1)$$

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

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

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

défini par $i^*(\mathrm{X}) = \mathrm{X}$ et $i^*(\mathrm{X}^{-1}) = \mathrm{X}^{n-1}$. 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 $\mathbb{G}_{\mathrm{a}}$. En effet, l'inclusion naturelle i de α_p dans $\mathbb{G}_{\mathrm{a}}$ correspond à l'homomorphisme de k-algèbres

$$i^* : k[\mathrm{T}] \to k[\mathrm{T}]/(\mathrm{T}^p)$$

défini par $i^*(\mathrm{T}) = \mathrm{T}$, 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 $\mathrm{G}_1 \times \mathrm{G}_2$ sur $\mathbf{Alg}_k$ associant

- à toute k-algèbre R, le groupe produit $\mathrm{G}_1(\mathrm{R}) \times \mathrm{G}_2(\mathrm{R})$;
- à tout homomorphisme de k-algèbres $f : \mathrm{R} \to \mathrm{R}'$, l'homomorphisme de groupes $\mathrm{G}_1(f) \times \mathrm{G}_2(f) : \mathrm{G}_1(\mathrm{R}) \times \mathrm{G}_2(\mathrm{R}) \to \mathrm{G}_1(\mathrm{R}') \times \mathrm{G}_2(\mathrm{R}')$.

Choisissons des anneaux de coordonnées $\varphi_1 : \mathrm{h}_{\mathrm{A}_1} \xrightarrow{\sim} \mathrm{G}_1$ et $\varphi_2 : \mathrm{h}_{\mathrm{A}_2} \xrightarrow{\sim} \mathrm{G}_2$ et considérons l'isomorphisme de foncteurs

$$\varphi_1 \times \varphi_2 : \mathrm{h}_{\mathrm{A}_1} \times \mathrm{h}_{\mathrm{A}_2} \xrightarrow{\sim} \mathrm{G}_1 \times \mathrm{G}_2.$$

Par définition même du produit tensoriel $\mathrm{A}_1 \otimes_k \mathrm{A}_2$, $\mathrm{h}_{\mathrm{A}_1\otimes_k\mathrm{A}_2} \simeq \mathrm{h}_{\mathrm{A}_1} \times \mathrm{h}_{\mathrm{A}_2}$ et nous obtenons donc un isomorphisme de foncteurs

$$\mathrm{h}_{\mathrm{A}_1\otimes_k\mathrm{A}_2} \longrightarrow \mathrm{G}_1 \times \mathrm{G}_2.$$

Enfin, si l'on choisit des isomorphismes $\mathrm{A}_1 \simeq k[\mathrm{T}_1, \ldots, \mathrm{T}_n]/\mathfrak{I}$ et $\mathrm{A}_2 \simeq k[\mathrm{S}_1, \ldots, \mathrm{S}_m]/\mathfrak{J}$, on obtient un isomorphisme de k-algèbres

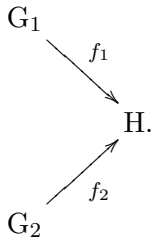
$$\begin{aligned} \mathrm{A}_1 \otimes_k \mathrm{A}_2 &\simeq k[\mathrm{T}_1, \ldots, \mathrm{T}_n]/\mathfrak{I} \otimes_k k[\mathrm{S}_1, \ldots, \mathrm{S}_m]/\mathfrak{J} \\ &\simeq k[\mathrm{T}_1, \ldots, \mathrm{T}_n, \mathrm{S}_1, \ldots, \mathrm{S}_m]/\mathfrak{K} \end{aligned}$$

où $\mathfrak{K}$ est l'idéal de $k[\mathrm{T}_1, \ldots, \mathrm{T}_n, \mathrm{S}_1, \ldots, \mathrm{S}_m]$ engendré par $\mathfrak{I}$ et $\mathfrak{J}$ (cf. appendice, 2.4, exercices 5 et 6). La k-algèbre $\mathrm{A}_1 \otimes_k \mathrm{A}_2$ 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* $\mathrm{G}_1 \times_k \mathrm{G}_2$ *est un groupe algébrique sur* k*, d'anneau de coordonnées* $\mathcal{O}(\mathrm{G}_1) \otimes_k \mathcal{O}(\mathrm{G}_2)$.

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



Pour toute k-algèbre R, l'ensemble $\mathrm{G}_1(\mathrm{R}) \times_{\mathrm{H}(\mathrm{R})} \mathrm{G}_2(\mathrm{R})$ des couples $(g_1, g_2) \in \mathrm{G}_1(\mathrm{R}) \times \mathrm{G}_2(\mathrm{R})$ tels que $f_1(g_1) = f_2(g_2)$ est un sous-groupe de $\mathrm{G}_1(\mathrm{R}) \times \mathrm{G}_2(\mathrm{R})$. Si $f : \mathrm{R} \to \mathrm{R}'$ est un homomorphisme de k-algèbres, on vérifie immédiatement que l'homomorphisme de groupes $\mathrm{G}_1(f) \times \mathrm{G}_2(f) : \mathrm{G}_1(\mathrm{R}) \times \mathrm{G}_2(\mathrm{R}) \to \mathrm{G}_1(\mathrm{R}') \times \mathrm{G}_2(\mathrm{R}')$ envoie $\mathrm{G}_1(\mathrm{R}) \times_{\mathrm{H}(\mathrm{R})} \mathrm{G}_2(\mathrm{R})$ dans $\mathrm{G}_1(\mathrm{R}') \times_{\mathrm{H}(\mathrm{R}')} \mathrm{G}_2(\mathrm{R}')$. Nous avons ainsi défini un foncteur

$$\mathrm{G}_1 \times_{\mathrm{H}} \mathrm{G}_2 : \mathbf{Alg}_k \to \mathbf{Gr}.$$

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

$$\begin{aligned} \mathrm{G}_1(\mathrm{R}) \times_{\mathrm{H}(\mathrm{R})} \mathrm{G}_2(\mathrm{R}) &= \{(g_1, g_2) \in \mathrm{G}_1(\mathrm{R}) \times \mathrm{G}_2(\mathrm{R}) \mid f_1(g_1) = f_2(g_2)\} \\ &\simeq \left\{(g_1, g_2) \in \mathrm{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(\mathrm{G}_1), \mathrm{R}) \times \mathrm{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(\mathrm{G}_2), \mathrm{R}) \mid g_1 \circ f_1^* = g_2 \circ f_2^*\right\} \\ &\simeq \mathrm{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(\mathrm{G}_1) \otimes_{\mathcal{O}(\mathrm{H})} \mathcal{O}(\mathrm{G}_2), \mathrm{R}) \end{aligned}$$

pour tout k-algèbre R. Le foncteur $\mathrm{G}_1 \times_{\mathrm{H}} \mathrm{G}_2$ est ainsi représenté par la k-algèbre $\mathcal{O}(\mathrm{G}_1) \otimes_{\mathcal{O}(\mathrm{H})} \mathcal{O}(\mathrm{G}_2)$. Cette dernière est bien de type fini, car elle est isomorphe au quotient de la k-algèbre de type fini $\mathcal{O}(\mathrm{G}_1) \otimes_k \mathcal{O}(\mathrm{G}_2)$ par l'idéal engendré par les éléments de la forme $a \otimes 1 - 1 \otimes a$, $a \in \mathcal{O}(\mathrm{H})$.

Nous venons ainsi de démontrer la proposition suivante.

Proposition 2.3.3 — *Étant donnés des groupes algébriques* $\mathrm{G}_1, \mathrm{G}_2$ *et* H *ainsi que des homomorphismes* $f_1 : \mathrm{G}_1 \to \mathrm{H}$ *et* $f_2 : \mathrm{G}_2 \to \mathrm{H}$*, le foncteur en groupes*

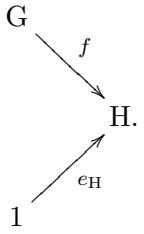
$$\mathrm{G}_1 \times_{\mathrm{H}} \mathrm{G}_2 : \mathbf{Alg}_k \to \mathbf{Gr}, \quad \mathrm{R} \mapsto \{(g_1, g_2) \in \mathrm{G}_1(\mathrm{R}) \times \mathrm{G}_2(\mathrm{R}) \mid f_1(g_1) = f_2(g_2)\}$$

est un groupe algébrique, d'anneau de coordonnées $\mathcal{O}(\mathrm{G}_1) \otimes_{\mathcal{O}(\mathrm{H})} \mathcal{O}(\mathrm{G}_2)$*. Ce groupe est le* produit fibré *des groupes* G_1 *et* G_2 *au-dessus de* H *et il c'est naturellement un sous-groupe du groupe produit* $\mathrm{G}_1 \times \mathrm{G}_2$*.*

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

Proposition 2.3.4 — *Soit* $f : \mathrm{G} \to \mathrm{H}$ *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* $f_{\mathrm{R}} : \mathrm{G}(R) \to \mathrm{H}(R)$*, est un groupe algébrique, d'anneau de coordonnées* $\mathcal{O}(\mathrm{G}) \otimes_{\mathcal{O}(\mathrm{H})} k$*. Il s'agit d'un sous-groupe de* G*.*

Démonstration. Considérons le diagramme



Pour toute k-algèbre R,

$$\begin{aligned}(\mathrm{G}\times_{\mathrm{H}}1)(\mathrm{R}) &= \{(g,1)\in\mathrm{G}(\mathrm{R})\times\{1\}\mid f(g)=e_{\mathrm{H}}(1)\}\\ &= \{(g,1)\in\mathrm{G}(\mathrm{R})\times\{1\}\mid f(g)=1_{\mathrm{H}}\}\\ &\cong \ker(f_{\mathrm{R}})\end{aligned}$$

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

Exemples. 1) Le groupe SL_n est le noyau de l'homomorphisme $\det:\mathrm{GL}_n\to\mathrm{GL}_1$.

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

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

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

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

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

$$\mathbf{Alg}_k\to\mathbf{Gr},\quad \mathrm{R}\mapsto\mathrm{im}\left(\mathrm{G}(\mathrm{R})\xrightarrow{f_{\mathrm{R}}}\mathrm{H}(\mathrm{R})\right)$$

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

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

n'est généralement pas un groupe algébrique.

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

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

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

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 $\varphi:\mathrm{h}_{\mathrm{A}}\to\mathrm{h}_{k[\mathrm{X},\mathrm{X}^{-1}]}$ tels que, pour toute k-algèbre R, l'application

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

soit une bijection sur le sous-ensemble de $\mathrm{R}^\times$ constitué des puissances n-èmes. En vertu du lemme de Yoneda, il existe un unique homomorphisme de k-algèbre $\pi:k[\mathrm{X},\mathrm{X}^{-1}]\to\mathrm{A}$ tel que $\varphi=\mathrm{h}_\pi$. Posant $\alpha=\pi(\mathrm{X})$, 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 $r : k[\mathrm{X}, \mathrm{X}^{-1}] \to \mathrm{R}$ tel que $r(\mathrm{X})$ soit une puissance n-ème dans R, il existe un unique homomorphisme $\overline{r} : \mathrm{A} \to \mathrm{R}$ tel que $\overline{r}(\alpha) = r(\mathrm{X})$, c'est-à-dire tel que le diagramme

$$\begin{array}{ccc} k[\mathrm{X}, \mathrm{X}^{-1}] & \xrightarrow{r} & \mathrm{R} \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{r}} & \\ \mathrm{A} & & \end{array}$$

soit commutatif.

Nous allons maintenant démontrer que *tout* homomorphisme $r : k[\mathrm{X}, \mathrm{X}^{-1}] \to \mathrm{R}$ 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 fausse si $n \geqslant 2$ (considérer par exemple X dans $k[\mathrm{X}, \mathrm{X}^{-1}]$). Pour ce faire, nous allons commencer par construire $\overline{r}$ 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 $r : k[\mathrm{X}, \mathrm{X}^{-1}] \to \mathrm{R}$; posons $a = r(\mathrm{X})$. La k-algèbre $\mathrm{R}_1 = \mathrm{R}[\mathrm{T}_1]/(\mathrm{T}_1^n - a)$ contient R et a y est manifestement une puissance n-ème ; il existe donc un unique homomorphisme $\overline{r}_1 : \mathrm{A} \to \mathrm{R}_1$ tel que $\overline{r}_1(\alpha) = a$. De même, la k-algèbre $\mathrm{R}_2 = k[\mathrm{T}_2]/(\mathrm{T}_2^n - a)$ contient R et a y est manifestement une puissance n-ème ; il existe donc un unique homomorphisme $\overline{r}_2 : \mathrm{A} \to \mathrm{R}_2$ tel que $\overline{r}_2(\alpha) = a$. Posant

$$\mathrm{R}_{12} = \mathrm{R}[\mathrm{T}_1, \mathrm{T}_2]/(\mathrm{T}_1 - a, \mathrm{T}_2 - a) = \mathrm{R}_1[\mathrm{T}_2]/(\mathrm{T}_2 - a) = \mathrm{R}_2[\mathrm{T}_1]/(\mathrm{T}_1 - a)$$

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 $i_1 \circ \overline{r}_1 = i_2 \circ \overline{r}_2$.

En tant que R-module, R_1 (resp. R_2) est libre de base $(1, \mathrm{T}_1, \ldots, \mathrm{T}_1^{n-1})$ (resp. $(1, \mathrm{T}_2, \ldots, \mathrm{T}_2^{n-1})$) ; de même, $\mathrm{R}_{12} = \mathrm{R}_1[\mathrm{T}_2]/(\mathrm{T}_2 - a)$ est un R_1-module libre de base $1, \mathrm{T}_2, \ldots, \mathrm{T}_2^{n-1}$. Nous en déduisons que R_{12} est un R-module libre de base les monômes $\mathrm{T}_1^{\nu_1}\mathrm{T}_2^{\nu_2}$ avec $0 \leqslant \nu_1, \nu_2 \leqslant n-1$. Quel que soit l'élément t de A, $\overline{r}_1(t)$ s'écrit de manière unique sous la forme $u_0 + u_1\mathrm{T}_1 + \ldots + u_{n-1}\mathrm{T}_1^{n-1}$ avec $u_0, \ldots, u_{n-1} \in \mathrm{R}$; de même, $\overline{r}_2(t)$ s'écrit de manière unique sous la forme $v_0 + v_1\mathrm{T}_2 + \ldots + v_{n-1}\mathrm{T}_2^{n-1}$ avec $v_0, \ldots, v_{n-1} \in \mathrm{R}$. L'identité $i_1 \circ \overline{r}_1 = i_2 \circ \overline{r}_2$ implique

$$u_0 + u_1\mathrm{T}_1 + \ldots + u_{n-1}\mathrm{T}_1^{n-1} = v_0 + v_1\mathrm{T}_2 + \ldots + v_{n-1}\mathrm{T}_2^{n-1}$$

dans R_{12}, donc

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

L'homomorphisme $\overline{r}_1 : \mathrm{A} \to \mathrm{R}_1$ 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. □

Pour toute k-algèbre R, l'homomorphisme $[n]_{\mathrm{R}} : \mathbb{G}_{\mathrm{m}}(\mathrm{R}) \to \mathbb{G}_{\mathrm{m}}(\mathrm{R})$ induit un isomorphisme entre le groupe quotient $\mathbb{G}_{\mathrm{m}}(\mathrm{R})/\mu_n(\mathrm{R})$ et le sous-groupe de $\mathbb{G}_{\mathrm{m}}(\mathrm{R}) = \mathrm{R}^\times$ 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 $n \geqslant 2$, le foncteur*

$$\mathbf{Alg}_k \to \mathbf{Ens}, \ \mathrm{R} \mapsto \mathbb{G}_{\mathrm{m}}(\mathrm{R})/\mu_n(\mathrm{R})$$

n'est pas représentable.

Exercices. 1) Soit $(\mathrm{A}, \Delta, e^*, \iota)$ une k-bigèbre de type fini et soit $\mathfrak{I}$ un idéal de A. On désigne par p la projection canonique de A sur $\mathrm{A}/\mathfrak{I}$.

(i) À quelle condition existe-t-il une structure de foncteur en groupes sur $\mathrm{h}_{\mathrm{A}/\mathfrak{I}}$ telle que le morphisme $\mathrm{h}_p : \mathrm{h}_{\mathrm{A}/\mathfrak{I}} \to \mathrm{h}_{\mathrm{A}}$ soit un homomorphisme de groupes algébriques ?

(ii) Si $\mathrm{h}_{\mathrm{A}/\mathfrak{I}}$ est un sous-groupe de h_{A}, à quelle condition est-ce un sous-groupe *distingué*, c'est-à-dire tel que $\mathrm{h}_{\mathrm{A}/\mathfrak{I}}(\mathrm{R})$ soit distingué dans $\mathrm{h}_{\mathrm{A}}(\mathrm{R})$ pour toute k-algèbre R ?

2) Considérons l'homomorphisme de groupes algébriques $i : \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}} \times \mathbb{G}_{\mathrm{m}}$ défini par

$$i_{\mathrm{R}} : \mathrm{R}^\times \to \mathrm{R}^\times \times \mathrm{R}^\times, \quad t \mapsto (t, t)$$

pour toute k-algèbre R.

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

$$\mathbf{Alg}_k \to \mathbf{Gr}, \quad \mathrm{R} \mapsto \mathbb{G}_{\mathrm{m}}(R) \times \mathbb{G}_{\mathrm{m}}(\mathrm{R})/\mathbb{G}_{\mathrm{m}}(\mathrm{R})$$

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 $\mathcal{O}(\mathrm{G}) \otimes_k k'$.*

Démonstration. Pour toute k'-algèbre R$'$,

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

donc le foncteur

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

est représenté par la k'-algèbre $\mathcal{O}(\mathrm{G}) \otimes_k k'$. En outre, comme $\mathcal{O}(\mathrm{G})$ est de type fini sur k, $\mathcal{O}(\mathrm{G}) \simeq k[\mathrm{T}_1, \ldots, \mathrm{T}_n]/\mathfrak{I}$ et donc

$$\mathcal{O}(\mathrm{G}) \otimes_k k' \simeq (k[\mathrm{T}_1, \ldots, \mathrm{T}_n]/\mathfrak{I}) \otimes_k k' \simeq k'[\mathrm{T}_1, \ldots, \mathrm{T}_n]/\mathfrak{I}$$

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

Étant donnés un groupe algébrique G sur k et une extension de corps k'/k, on note $\mathrm{G} \otimes_k k'$ 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 $a, b \in \mathrm{R}$ tels que $a^2 + b^2 \in \mathrm{R}^\times$ est un sous-groupe de $\mathrm{GL}_2(\mathrm{R})$; on en déduit que le foncteur

$$\mathrm{G} : \mathbf{Alg}_k \to \mathbf{Gr}, \quad \mathrm{R} \mapsto \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{M}_2(\mathrm{R}) \;\middle|\; a^2 + b^2 \in \mathrm{R}^\times \right\}$$

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

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

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 $a, b \in \mathrm{R}$ et l'application

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

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

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

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

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

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

et

$$(\mathbb{G}_\mathrm{m} \times \mathbb{G}_\mathrm{m})(\mathbb{R}) = \mathbb{R}^\times \times \mathbb{R}^\times$$

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

$$\mathrm{U}(n) = \left\{ \mathrm{M} \in \mathrm{M}_n(\mathbb{C}) \mid {}^t\overline{\mathrm{M}}\mathrm{M} = \mathrm{I}_n \right\},$$

où $\overline{\mathrm{M}}$ désigne la matrice déduite de M par conjugaison des coefficients. Peut-on écrire ce groupe sous la forme $\mathrm{G}(\mathrm{R})$ 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 $\mathrm{R} \otimes_{\mathbb{Q}} \mathbb{Q}[\mathrm{T}]/(\mathrm{T}^2+1) = \mathrm{R}[\mathrm{T}]/(\mathrm{T}^2+1)$ est munie d'un automorphisme R-linéaire canonique σ défini par $\sigma(\mathrm{T}) = -\mathrm{T}$. L'ensemble

$$\mathrm{G}(\mathrm{R}) = \left\{ \mathrm{M} \in \mathrm{M}_n(\mathrm{R}[\mathrm{T}]/(\mathrm{T}^2+1)) \mid {}^t\sigma(\mathrm{M})\mathrm{M} = \mathrm{I}_n \right\}$$

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

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

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

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

$$\varepsilon : \mathrm{R}[\mathrm{T}]/(\mathrm{T}^2+1) \to \mathrm{R} \times \mathrm{R}, \quad a + b\mathrm{T} \mapsto (a+b\xi, a-b\xi)$$

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

$$\mathrm{M}_2(\mathrm{R} \times \mathrm{R}) \cong \mathrm{M}_2(\mathrm{R}) \times \mathrm{M}_2(\mathrm{R}),$$

on en déduit que le groupe $\mathrm{G}(\mathrm{R})$ est isomorphe au sous-groupe de $\mathrm{GL}_2(\mathrm{R}) \times \mathrm{GL}_2(\mathrm{R})$ constitué des couples $(\mathrm{M}_1, \mathrm{M}_2)$ tels que ${}^t(\mathrm{M}_2, \mathrm{M}_1)(\mathrm{M}_1, \mathrm{M}_2) = (\mathrm{I}_n, \mathrm{I}_n)$, c'est-à-dire tels que

$${}^t\mathrm{M}_2\mathrm{M}_1 = {}^t\mathrm{M}_1\mathrm{M}_2 = \mathrm{I}_n.$$

Ainsi, la première projection $\mathrm{GL}_2(\mathrm{R}) \times \mathrm{GL}_2(\mathrm{R}) \to \mathrm{GL}_2(\mathrm{R})$ induit un isomorphisme entre $\mathrm{G}(\mathrm{R})$ et $\mathrm{GL}_2(\mathrm{R})$.

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

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

On constate aisément que les groupes $\mathrm{U}(n)$ et $\mathrm{GL}_n(\mathbb{R})$ 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 $\mathrm{G} \otimes_{\mathbb{Q}} \mathbb{Q}(i)$ 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

$$\varphi : \mathrm{G} \times \mathrm{E} \to \mathrm{E}$$

tel que les diagrammes

$$\begin{array}{ccc} \mathrm{G}\times\mathrm{G}\times\mathrm{E} & \xrightarrow{\mathrm{id}_\mathrm{G}\times\varphi} & \mathrm{G}\times\mathrm{E} \\ {\scriptstyle m\times\mathrm{id}_\mathrm{E}}\downarrow & & \downarrow{\scriptstyle\varphi} \\ \mathrm{G}\times\mathrm{E} & \xrightarrow[\varphi]{} & \mathrm{E} \end{array} \qquad \text{et} \qquad \begin{array}{ccc} 1\times\mathrm{E} & \xrightarrow{e\times\mathrm{id}_\mathrm{E}} & \mathrm{G}\times\mathrm{E} \\ & \searrow^{\sim} & \downarrow{\scriptstyle\varphi} \\ & & \mathrm{E} \end{array}$$

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 $\varphi : \mathrm{G} \times \mathrm{E} \to \mathrm{E}$ 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 $f : \mathrm{X} \to \mathrm{Y}$ dans C, l'application $\mathrm{E}(f) : \mathrm{E}(\mathrm{X}) \to \mathrm{E}(\mathrm{Y})$ soit équivariante relativement aux groupes G(X) et G(Y), i.e.

$$\mathrm{E}(f)(\varphi_\mathrm{X}(g,x)) = \varphi_\mathrm{Y}(\mathrm{G}(f)(g), \mathrm{E}(f)(x))$$

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

Exemple — Si G est un foncteur en groupes sur C, on peut considérer le foncteur en ensembles $\widetilde{\mathrm{G}}$ associé à G (i.e. $\widetilde{\mathrm{G}}(\mathrm{X})$ est l'ensemble sous-jacent au groupe G(X)) et faire agir G sur $\widetilde{\mathrm{G}}$ par translation à gauche en considérant le morphisme de foncteurs $\varphi : \mathrm{G} \times \widetilde{\mathrm{G}} \to \widetilde{\mathrm{G}}$ défini par $\varphi_\mathrm{X}(g,h) = gh$ pour tout objet X de C et tous $g, h \in \mathrm{G}(\mathrm{X})$. On peut également faire agir G sur $\widetilde{\mathrm{G}}$ 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 $f : \mathrm{X} \to \mathrm{Y}$ 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 $\underline{\mathrm{V}} : \mathbf{Alg}_k \to \mathbf{Ens}$ en posant
- pour toute k-algèbre R, $\underline{\mathrm{V}}(\mathrm{R})$ est le R-module libre $\mathrm{V} \otimes_k \mathrm{R}$;
- pour tout homomorphisme de k-algèbre $f : \mathrm{R} \to \mathrm{R}'$, $\underline{\mathrm{V}}(f)$ est l'application R-linéaire

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

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

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

$$u(\sum_\alpha v_\alpha \otimes \lambda_\alpha) = \sum_\alpha u(v_\alpha \otimes 1)\lambda_\alpha.$$

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

$$\begin{array}{ccc} \mathrm{V} \otimes_k \mathrm{R}' & \xrightarrow{f^*(\alpha)} & \mathrm{V} \otimes_k \mathrm{R}' \\ {\scriptstyle \mathrm{id}_\mathrm{V}\otimes f}\uparrow & & \uparrow{\scriptstyle \mathrm{id}_\mathrm{V}\otimes f} \\ \mathrm{V} \otimes_k \mathrm{R} & \xrightarrow[\alpha]{} & \mathrm{V} \otimes_k \mathrm{R}' \end{array}$$

soit commutatif.

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

Démonstration. L'application composée

$$\mathrm{V} \xrightarrow{\alpha} \mathrm{V} \otimes_k \mathrm{R} \xrightarrow{\mathrm{id}_\mathrm{V}\otimes f} \mathrm{V} \otimes_k \mathrm{R}'$$

est k-linéaire et donc se prolonge de manière unique en une application R′-linéaire $\alpha' : \mathrm{V} \otimes_k \mathrm{R}' \to \mathrm{V} \otimes_k \mathrm{R}'$. Par construction, les applications R-linéaires $\alpha' \circ (\mathrm{id}_\mathrm{V} \otimes f)$ et $(\mathrm{id}_\mathrm{V} \otimes f) \circ \alpha$ de $\mathrm{V} \otimes_k \mathrm{R}$ dans $\mathrm{V} \otimes_k \mathrm{R}'$ coïncident sur le sous-ensemble $\mathrm{V} \otimes 1$ de $\mathrm{V} \otimes_k \mathrm{R}$; 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 $\mathrm{V} \otimes 1$ de $\mathrm{V} \otimes_k \mathrm{R}'$ est donnée.

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

Le lemme précédent permet de définir un foncteur en groupes GL_V sur Alg_k :
- pour toute k-algèbre R, $\mathrm{GL}_\mathrm{V}(\mathrm{R})$ est le groupe des automorphismes R-linéaires du R-module $\mathrm{V} \otimes_k \mathrm{R}$;
- pour toute flèche $f : \mathrm{R} \to \mathrm{R}'$, $\mathrm{GL}_\mathrm{V}(f)$ est l'homomorphisme $\mathrm{GL}_\mathrm{V}(\mathrm{R}) \to \mathrm{GL}_\mathrm{V}(\mathrm{R}')$ 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 $(e_i)_{i\in \mathrm{I}}$ de V sur k permet de définir un isomorphisme de foncteurs en groupes entre GL_V et le foncteur

$$\mathrm{G}_\mathrm{I} : \mathbf{Alg}_k \to \mathrm{Gr}, \quad \mathrm{R} \mapsto \{\text{matrices inversibles dans } \mathrm{M}_\mathrm{I}(\mathrm{R})\}$$

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

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

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

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

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* $\underline{\mathrm{V}}$ *telle que, pour toute* k*-algèbre* R*, le groupe* G(R) *agisse par automorphismes* R*-linéaires sur* $\mathrm{V} \otimes_k \mathrm{R}$*.*

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

$$\rho_{\mathrm{R}}(g) = \varphi_{\mathrm{R}}(g, \cdot)$$

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

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

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.(\mathrm{X}, \mathrm{Y}) = (\mathrm{X}, \mathrm{Y}) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a\mathrm{X} + b\mathrm{Y}, c\mathrm{X} + d\mathrm{Y}).$$

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

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.\mathrm{X}^2 = (a\mathrm{X} + b\mathrm{Y})^2 = a^2\mathrm{X}^2 + 2ab\mathrm{XY} + b^2\mathrm{Y}^2,$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.\mathrm{Y}^2 = (c\mathrm{X} + d\mathrm{Y})^2 = c^2\mathrm{X}^2 + 2cd\mathrm{XY} + d^2\mathrm{Y}^2$$

et

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.\mathrm{XY} = (a\mathrm{X} + b\mathrm{Y})(c\mathrm{X} + d\mathrm{Y}) = ac\mathrm{X}^2 + (ad + bc)\mathrm{XY} + bd\mathrm{Y}^2.$$

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

$$(g.\mathrm{X}_1, \ldots, g.\mathrm{X}_n) = (\mathrm{X}_1, \ldots, \mathrm{X}_n)\ {}^t g$$

et il en découle une action de $\mathrm{SL}_n(\mathrm{R})$ sur $\mathrm{R}[\mathrm{X}_1, \ldots, \mathrm{X}_n]_d = k[\mathrm{X}_1, \ldots, \mathrm{X}_n]_d \otimes_k \mathrm{R}$ définie par

$$g.\mathrm{P}(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \mathrm{P}(g.\mathrm{X}_1, \ldots, g.\mathrm{X}_n).$$

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

Il est aisé d'expliciter cette représentation en utilisant la base canonique de $\mathrm{M}_n(k)$ formée des matrices élémentaires E_{ij} $(1 \leqslant i, j \leqslant n)$. Pour $n = 2$, on obtient les formules suivantes : si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_n(\mathrm{R})$ et $\delta = ad - bc$, alors

$$g.\mathrm{E}_{11} = \frac{1}{\delta}(ad\mathrm{E}_{11} - ab\mathrm{E}_{12} + cd\mathrm{E}_{21} - bc\mathrm{E}_{22}), \quad g.\mathrm{E}_{12} = \frac{1}{\delta}(-ac\mathrm{E}_{11} + a^2\mathrm{E}_{12} - c^2\mathrm{E}_{21} + ac\mathrm{E}_{22})$$

$$g.\mathrm{E}_{21} = \frac{1}{\delta}(bd\mathrm{E}_{11} - b^2\mathrm{E}_{12} + d^2\mathrm{E}_{21} - bd\mathrm{E}_{22}) \quad \text{et} \quad g.\mathrm{E}_{22} = \frac{1}{\delta}(-bc\mathrm{E}_{11} + ab\mathrm{E}_{12} - cd\mathrm{E}_{21} + ad\mathrm{E}_{22}).$$

(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*

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

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

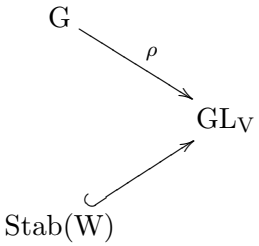
Démonstration. Considérons une base $(e_1, \ldots, e_m)$ de W et complétons-la en une base $(e_1, \ldots, e_n)$ de V. L'isomorphisme $\mathrm{GL}_\mathrm{V} \xrightarrow{\sim} \mathrm{GL}_n$ obtenu en associant à tout élément $g \in \mathrm{GL}_\mathrm{V}(\mathrm{R}) = \mathrm{GL}(\mathrm{V} \otimes_k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

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

pour toute k-algèbre R.

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

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



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

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

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

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

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

Ce dernier est surjectif, [(2)] donc $\mathrm{Stab_G(W)}$ 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 $\rho : \mathrm{G} \to \mathrm{GL_V}$ une représentation linéaire. Ayant choisi un isomorphisme de foncteurs $\mathrm{G} \simeq \mathrm{h_A}$, on dispose pour toute k-algèbre R et tout élément g de $\mathrm{G(R)} = \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A}, \mathrm{R})$ d'un digramme commutatif

$$\begin{array}{ccc} \mathrm{G(A)} \times \mathrm{V} & \xrightarrow{\rho_\mathrm{A}} & \mathrm{V} \otimes_k \mathrm{A} \\ \downarrow{\scriptstyle \mathrm{G}(g)\times \mathrm{id_V}} & & \downarrow{\scriptstyle \mathrm{id_V}\otimes g} \\ \mathrm{G(R)} \times \mathrm{V} & \xrightarrow[\rho_\mathrm{R}]{} & \mathrm{V} \otimes_k \mathrm{R} \end{array}$$

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

$$\rho_\mathrm{R}(g, v) = ((\mathrm{id_V} \otimes g) \circ \rho_\mathrm{A})(\mathrm{id_A}, v)$$

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

$$\widetilde{\rho} = \rho_\mathrm{A}(\mathrm{id_A} \otimes \cdot) : \mathrm{V} \to \mathrm{V} \otimes_k \mathrm{A}.$$

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

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

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

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

$$\mathrm{Hom}_{\mathbf{Alg}_k}(k[\mathrm{T}], \mathrm{R}) \to \mathbb{G}_\mathrm{a}(\mathrm{R}) = \mathrm{R}, \quad u \mapsto u(\mathrm{T})$$

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

$$\mathrm{V} \to \mathrm{V} \otimes_k k[\mathrm{T}], \quad e_1 \mapsto e_1 \otimes 1, \quad e_2 \mapsto e_1 \otimes \mathrm{T} + e_2 \otimes 1$$

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

$$\mathrm{V} \xrightarrow{\widetilde{\rho}} \mathrm{V} \otimes_k k[\mathrm{T}] \xrightarrow{\mathrm{id_V}\otimes t} \mathrm{V} \otimes_k \mathrm{R}$$

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 $\rho : \mathrm{G} \to \mathrm{GL_V}$;

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

$$\mathcal{O}(\mathrm{G}) \to \mathcal{O}(\mathrm{G}) \otimes_{\mathcal{O}(\mathrm{GL_V})} \mathcal{O}(\mathrm{Stab(W)})$$

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

(ii) une application k-linéaire $\widetilde{\rho}\colon \mathrm{V} \to \mathrm{V} \otimes_k \mathrm{A}$ telle que les deux diagrammes

$$\begin{array}{ccc} \mathrm{V} & \xrightarrow{\widetilde{\rho}} & \mathrm{V}\otimes_k \mathrm{A} \\ {\scriptstyle\widetilde{\rho}}\downarrow & & \downarrow{\scriptstyle\widetilde{\rho}\otimes \mathrm{id}_\mathrm{A}} \\ \mathrm{V}\otimes_k \mathrm{A} & \xrightarrow[\mathrm{id}_\mathrm{V}\otimes\Delta]{} & \mathrm{V}\otimes_k \mathrm{A}\otimes_k \mathrm{A} \end{array} \qquad \textit{et} \qquad \begin{array}{ccc} \mathrm{V} & \xrightarrow{\widetilde{\rho}} & \mathrm{V}\otimes_k \mathrm{A} \\ & \searrow & \downarrow{\scriptstyle \mathrm{id}_\mathrm{V}\otimes e^*} \\ & & \mathrm{V}\otimes_k k \end{array}$$

soient commutatifs.

À une représentation linéaire ρ correspond l'application $\widetilde{\rho} = \rho_\mathrm{A}(\mathrm{id}_\mathrm{A}, \cdot)$.

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

$$\mathrm{V} \xrightarrow{\widetilde{\rho}} \mathrm{V}\otimes_k \mathrm{A} \xrightarrow{\mathrm{id}_\mathrm{V}\otimes g} \mathrm{V}\otimes_k \mathrm{R}.$$

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

$$\mathrm{V} \xrightarrow{\widetilde{\rho}} \mathrm{V}\otimes_k \mathrm{A} \xrightarrow{\mathrm{id}_\mathrm{R}\otimes g} \mathrm{V}\otimes_k \mathrm{R}\ .$$

Considérons deux éléments g, h de $\mathrm{G}(\mathrm{R})$ et calculons successivement $\rho_\mathrm{R}(gh)$ et $\rho_\mathrm{R}(g)\circ\rho_\mathrm{R}(h)$.

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

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

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

$$\mathrm{V} \xrightarrow{\widetilde{\rho}} \mathrm{V}\otimes_k \mathrm{A} \xrightarrow{\mathrm{id}_\mathrm{V}\otimes\Delta} \mathrm{V}\otimes_k \mathrm{A}\otimes_k \mathrm{A} \xrightarrow{\mathrm{id}_\mathrm{V}\otimes g\otimes h} \mathrm{V}\otimes_k \mathrm{R}\otimes_k \mathrm{R} \xrightarrow{\mathrm{id}_\mathrm{V}\otimes\mathrm{mult}} \mathrm{V}\otimes_k \mathrm{R}.$$

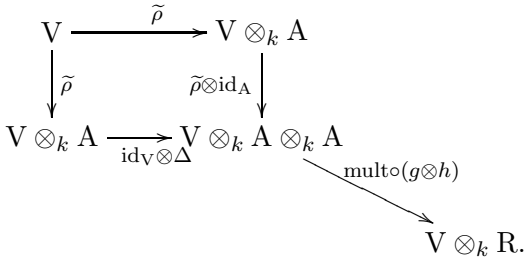
D'autre part, si v est un vecteur de V, alors $\rho_\mathrm{R}(h).v = \sum_i v_i \otimes \lambda_i$ avec $v_i \in \mathrm{V}$ et $\lambda_i \in \mathrm{R}$, puis

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

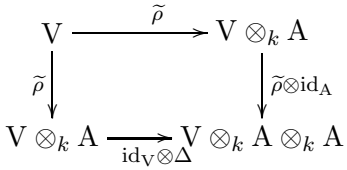
dans $\mathrm{V}\otimes_k\mathrm{R}$. Ainsi, $\rho_\mathrm{R}(g)\circ\rho_\mathrm{R}(h)$ est l'unique automorphisme R-linéaire de $\mathrm{V}\otimes_k\mathrm{R}$ prolongeant l'application k-linéaire

$$\mathrm{V} \xrightarrow{\widetilde{\rho}} \mathrm{V}\otimes_k \mathrm{A} \xrightarrow{\widetilde{\rho}\otimes\mathrm{id}_\mathrm{A}} \mathrm{V}\otimes_k \mathrm{A}\otimes_k \mathrm{A} \xrightarrow{\mathrm{id}_\mathrm{V}\otimes g\otimes h} \mathrm{V}\otimes_k \mathrm{R}\otimes_k \mathrm{R} \xrightarrow{\mathrm{id}_\mathrm{V}\otimes\mathrm{mult}} \mathrm{V}\otimes_k \mathrm{R}\ .$$

L'identité $\rho_{\mathrm{R}}(gh) = \rho_{\mathrm{R}}(g) \circ \rho_{\mathrm{R}}(h)$ est donc équivalente à la commutativité du diagramme

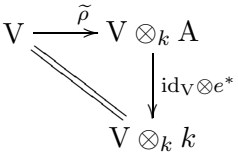


Comme ceci doit être vrai pour toute k-algèbre R et tous $g, h \in \mathrm{G}(\mathrm{R}) = \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A}, \mathrm{R})$, on en déduit immédiatement que le diagramme



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

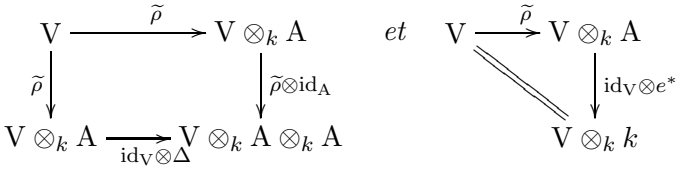
L'élément neutre e_{R} du groupe $\mathrm{G}(\mathrm{R})$ correspond à l'homomorphisme de k-algèbres de A dans R obtenu en composant $e^* : \mathrm{A} \to k$ par l'unique homomorphisme de k-algèbres $u : k \to \mathrm{R}$. Par suite, l'identité $\rho_k(e_k) = \mathrm{id}_{\mathrm{V}}$ équivaut à la commutativité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



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

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

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



soient commutatifs.

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

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

$$k[\mathrm{X},\mathrm{Y}]_2 \to k[\mathrm{X},\mathrm{Y}]_2 \otimes_k \mathrm{A}$$

définie par

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

et

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

3.2. Représentation régulière

Soit G un groupe algébrique sur k d'anneau de coordonnées A ; on fixe un isomorphisme de foncteurs $\mathrm{h_A} \simeq \mathrm{G}$, d'où l'on déduit une structure de k-bigèbre $(\mathrm{A}, \Delta, e^*, \iota)$ sur A (voir 2.2.1). La comultiplication $\Delta : \mathrm{A} \to \mathrm{A} \otimes_k \mathrm{A}$ 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 $\mathrm{G} \to \mathrm{GL_A}$, appelée *représentation régulière*.

On peut donner de cette représentation une interprétation instructive. Étant donnée une k-algèbre R, on désigne par $\mathcal{F}(\mathrm{G(R)},\mathrm{R})$ 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 $\overline{f} \in \mathcal{F}(\mathrm{G(R)},\mathrm{R})$, à savoir

$$\mathrm{G(R)} = \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},\mathrm{R}) \to \mathrm{R}, \quad s \mapsto \overline{f}(s) = s(f).$$

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

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

$$\overline{f}(st) = \sum_i \overline{g_i}(s)\overline{h_i}(t).$$

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 $\mathrm{A} \otimes_k \mathrm{R}$: à $s \in \mathrm{G(R)}$ correspond l'unique automorphisme R-linéaire $\rho(s)$ de $\mathrm{A} \otimes_k \mathrm{R}$ prolongeant l'application k-linéaire

$$\mathrm{A} \to \mathrm{A} \otimes_k \mathrm{R}, \quad f \mapsto (\mathrm{id_A} \otimes s)\Delta(f).$$

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

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

On dispose ainsi d'un diagramme commutatif

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

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

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

Cette interprétation de la représentation régulière $\rho : \mathrm{G} \to \mathrm{GL}_{\mathrm{A}}$ 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 $\mathrm{G}(\mathrm{R})$ tel que $\rho_{\mathrm{R}}(s)$ soit l'identité de $\mathrm{A}\otimes_k \mathrm{R}$, alors $\overline{f}(\cdot s) = \overline{f}$ pour tout $f \in \mathrm{A}$, donc

$$s(f) = \overline{f}(s) = \overline{f}(e_{\mathrm{R}} s) = \overline{f}(e_{\mathrm{R}}) = e_{\mathrm{R}}(f)$$

pour tout élément f de A, et par suite $s = e_{\mathrm{R}}$ 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 $\mathrm{A}/\mathfrak{I}$ pour un certain idéal $\mathfrak{I}$ de A.

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

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

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

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

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

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

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

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 $\rho : \mathrm{G} \to \mathrm{GL_V}$ induise un isomorphisme de G sur un sous-groupe de $\mathrm{GL_V}$.

(ii) Étant donné un sous-groupe H de G, il existe un espace vectoriel V de dimension finie, une représentation linéaire $\rho : \mathrm{G} \to \mathrm{GL_V}$ et un sous-espace vectoriel W de V tels que ρ induise un isomorphisme de G sur un sous-groupe de $\mathrm{GL_V}$ et $\mathrm{H} = \mathrm{Stab_G(W)}$.

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 $(a_i)_{i\in \mathrm{I}}$ de A en tant que k-espace vectoriel. Tout élément de $\mathrm{V} \otimes_k \mathrm{A}$ s'écrit d'une manière et d'une seule sous la forme $\sum_{i\in \mathrm{I}} v_i \otimes a_i$, où $(v_i)_{i\in \mathrm{I}}$ 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

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

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 $(\widetilde{\rho} \otimes \mathrm{id_A}) \circ \widetilde{\rho} = (\mathrm{id_V} \otimes \Delta) \circ \widetilde{\rho}$, où Δ désigne la comultiplication de A. On a

$$[(\widetilde{\rho} \circ \mathrm{id_A}) \circ \widetilde{\rho}](v) = \sum_{i\in \mathrm{I}} \widetilde{\rho}(v_i) \otimes a_i$$

et

$$[(\mathrm{id_V} \circ \Delta) \circ \widetilde{\rho}](v) = \sum_{i\in \mathrm{I}} v_i \otimes \Delta(a_i).$$

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

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

avec $\lambda^i_{j,\ell} \in k$; par suite,

$$\begin{aligned}[(\mathrm{id_V} \circ \Delta) \circ \widetilde{\rho}](v) &= \sum_{(i,j,\ell)\in \mathrm{I}^3} \lambda^i_{j,\ell} v_i \otimes a_j \otimes a_\ell \\ &= \sum_{\ell\in \mathrm{I}} \left(\sum_{(i,j)\in \mathrm{I}^2} \lambda^i_{j,\ell} v_i \otimes a_j \right) \otimes a_\ell.\end{aligned}$$

En comparant les deux expressions obtenues pour $[(\widetilde{\rho} \circ \mathrm{id_A}) \circ \widetilde{\rho}](v) = [(\mathrm{id_V} \circ \Delta) \circ \widetilde{\rho}](v)$, on obtient

$$\widetilde{\rho}(v_\ell) = \sum_{(i,j)\in \mathrm{I}^2} \lambda^i_{j,\ell} v_i \otimes a_j$$

pour tout $\ell \in \mathrm{I}$. On a ainsi $\widetilde{\rho}(v_\ell) \in \mathrm{W}_0 \otimes \mathrm{A}$ pour tout $\ell \in \mathrm{I}$, donc $\widetilde{\rho}(\mathrm{W}_0) \subset \mathrm{W}_0 \otimes_k \mathrm{A}$.

Finalement, $\mathrm{W} = \mathrm{W}_0 + kv$ est un sous-espace vectoriel de V de dimension finie contenant v et tel que $\widetilde{\rho}(\mathrm{W}) \subset \mathrm{W} \otimes_k \mathrm{A}$. □

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 $t_1, \ldots, t_\mathrm{N}$ en tant que k-algèbre (c'est-à-dire que tout élément de A s'écrit sous la forme d'un polynôme en les $t_1, \ldots, t_\mathrm{N}$ à coefficients dans k).

En vertu du lemme précédent, $t_1, \ldots, t_\mathrm{N}$ sont contenus dans un sous-comodule V de A de dimension finie. La représentation régulière $\mathrm{G} \to \mathrm{GL_A}$ induit une représentation linéaire

$\rho : \mathrm{G} \to \mathrm{GL_V}$ et il nous reste à vérifier que ρ induit un isomorphisme de G sur un sous-groupe de $\mathrm{GL_V}$, c'est-à-dire que l'homomorphisme $\rho^* : \mathcal{O}(\mathrm{GL_V}) \to \mathcal{O}(\mathrm{G}) = \mathrm{A}$ est surjectif.

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

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

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

Nous allons conclure en vérifiant que A_0 contient les générateurs $t_1, \ldots, t_\mathrm{N}$ 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

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

est commutatif ; on a par conséquent

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

Ces identités mettent en évidence le fait que la base (e_i) de V est contenue dans A_0, donc $\mathrm{V} \subset \mathrm{A}_0$. On a ainsi $\mathrm{A} = \mathrm{A}_0$ et l'homomorphisme ρ^* est surjectif.

(ii) Soit $\mathfrak{I}$ l'idéal de A définissant le sous-groupe H de G – c'est-à-dire le noyau de l'homomorphisme $\mathcal{O}(\mathrm{G}) \to \mathcal{O}(\mathrm{H})$. L'anneau A étant une k-algèbre de type fini, il est noethérien et l'idéal $\mathfrak{I}$ 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 $f_1, \ldots, f_n$ de l'idéal $\mathfrak{I}$. Comme on vient de l'établir, la représentation linéaire $\rho : \mathrm{G} \to \mathrm{GL_V}$ induite par la représentation régulière de G fournit un isomorphisme de G sur un sous-groupe de $\mathrm{GL_V}$.

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

$$\rho_\mathrm{R}(s, f_i) = \sum_{1 \leqslant j \leqslant n} f_j \otimes \lambda_{ij}$$

avec $\lambda_{ij} \in \mathrm{R}$, d'où

$$s(f_i) = \overline{f}_i(s) = \overline{f_i}(e_\mathrm{R} s) = \overline{\rho_\mathrm{R}(s, f_i)}(e_\mathrm{R}) = \sum_{1 \leqslant j \leqslant n} f_j(e_\mathrm{R}) \lambda_{ij} = 0$$

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

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

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

□

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, $(\mathrm{W} \otimes_k \mathrm{R}) \cap (\mathrm{W}' \otimes_k \mathrm{R}) = (\mathrm{W} \cap \mathrm{W}') \otimes_k \mathrm{R}$.

Démonstration. Posons $\mathrm{L} = \mathrm{W} \cap \mathrm{W}'$. Partant d'une base de L, nous pouvons la compléter en une base de $\mathrm{W} + \mathrm{W}'$ 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 $(e_i)_{i \in \mathrm{I}}$ de V. On dispose par construction de deux sous-ensembles J et J' de I tels que les familles $(e_i)_{i \in \mathrm{J}}$, $(e_i)_{i \in \mathrm{J}'}$ et $(e_i)_{i \in \mathrm{J} \cap \mathrm{J}'}$ soient des bases de W, W' et L respectivement.

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

(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 $d \in \{1, \ldots, n\}$ d'une représentation linéaire naturelle λ_d de GL_{V} dans la d-ème puissance extérieure $\Lambda^d(\mathrm{V})$ de V : quelle que soient la k-algèbre R et l'automorphisme R-linéaire g de $\mathrm{V} \otimes_k \mathrm{R}$, $\lambda_{d,\mathrm{R}}(g)$ est l'automorphisme R-linéaire de $\Lambda^d(\mathrm{V}) \otimes_k \mathrm{R} = \Lambda^d(\mathrm{V} \otimes_k \mathrm{R})$ qui envoie un d-vecteur de la forme $v_1 \wedge \ldots \wedge v_d$ sur le d-vecteur $g(v_1) \wedge \ldots \wedge g(v_d)$.

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

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

(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* $\mathrm{Stab}(\mathrm{W})$ *de* GL_{V} *est le stabilisateur de la droite* $\Lambda^d(\mathrm{W})$ *de* $\Lambda^d(\mathrm{V})$.

Démonstration. Fixons une base de V, disons $(e_1, \ldots, e_n)$, et considérons la base (e_φ) de $\Lambda^d(\mathrm{V})$ 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 $\mathrm{M} \in \mathrm{GL}_n(\mathrm{R})$, les conditions

(a) la matrice M est de la forme $\left(\begin{array}{c|c} \mathrm{A} & \mathrm{B} \\ \hline 0 & \mathrm{D} \end{array}\right)$ avec $\mathrm{A} \in \mathrm{GL}_d(\mathrm{R})$, $\mathrm{B} \in \mathrm{M}_{d,n-d}(\mathrm{R})$ et $\mathrm{D} \in \mathrm{GL}_{n-d}(\mathrm{R})$;

(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

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

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* $\rho : G \to GL_V$ *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 $\rho' : G \to GL_{V'}$ induisant un isomorphisme de G sur un sous-groupe de $GL_{V'}$ 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 $\Lambda^d\rho = \lambda_d \circ \rho' : G \to GL_{\Lambda^d(V')}$.

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 ($k \to k,\ x \mapsto x^p$) 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 $\overline{k}$ une clôture algébrique de k. Il est facile de voir que l'endomorphisme $f \otimes \mathrm{id}$ de $\mathrm{V} \otimes_k \overline{k}$ 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

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

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

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

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

$$\overline{k}[\mathrm{X}] \to \mathrm{End}(\mathrm{V} \otimes_k \overline{k}), \quad \mathrm{P} \mapsto \mathrm{P}(f \otimes \mathrm{id})$$

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

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

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 $\mathrm{G}(k)$ 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 $\mathrm{G}(k)$ satisfaisant aux deux conditions suivantes :*

(i) $g_s g_u = g_u g_s$;

(ii) pour toute représentation linéaire de dimension finie $\rho : \mathrm{G} \to \mathrm{GL_V}$, $\rho_k(g_s)$ (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 donnés une représentation linéaire de dimension finie $\rho : \mathrm{G} \to \mathrm{GL_V}$ et un élément g de $\mathrm{G}(k)$,

- $\rho_k(g) \in \mathrm{GL}(\mathrm{V})$ 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 $\rho_k(g)$ est il n'est pas clair que l'on obtienne des éléments du sous-groupe $\rho_k(\mathrm{G}(k))$ de $\mathrm{GL}(\mathrm{V})$;
- 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 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 $\overline{k}$ 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 $\mathrm{GL}_2(\overline{k})$. S'il existait une telle décomposition dans $\mathrm{GL}_2(k)$, la composante semi-simple serait l'homothétie $\alpha \mathrm{I}_2$ 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* $g \in \mathrm{GL}(\mathrm{V})$.

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

(i) g est unipotent ;

(ii) il existe un entier $\mathrm{N} \geqslant 0$ *tel que* $g^{p^{\mathrm{N}}} = 1$.

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

(i) g est unipotent ;

(ii) il existe un homomorphisme $u : \mathbb{G}_{\mathrm{a}} \to \mathrm{G}$ *et un élément t de* $\mathbb{G}_{\mathrm{a}}(k) = k$ *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 $g - \mathrm{id}$ est nilpotent et donc $(g - \mathrm{id})^{p^{\mathrm{N}}} = 0$ si l'entier N est suffisamment grand ; on obtient alors $g^{p^{\mathrm{N}}} - \mathrm{id} = 0$ et ainsi g est bien d'ordre une puissance de p.

Réciproquement, s'il existe un entier $\mathrm{N} \geqslant 0$ tel que $g^{p^{\mathrm{N}}} = \mathrm{id}$, le polynôme minimal de g divise $\mathrm{X}^{p^{\mathrm{N}}} - 1 = (\mathrm{X} - 1)^{p^{\mathrm{N}}}$ 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 $n = g - \mathrm{id}$. Le polynôme $\sum_{m \geqslant 1} (-1)^{m+1} \frac{n^m}{m}$ définit un endomorphisme de V, que l'on note $\mathrm{Log}(g)$; ce dernier est nilpotent puisqu'il s'agit d'une somme d'endomorphismes nilpotents qui commutent. L'homomorphisme de foncteurs $u : \mathbb{G}_{\mathrm{a}} \to \mathrm{GL}_{\mathrm{V}}$ défini par

$$u_{\mathrm{R}}(t) = \sum_{m \geqslant 0} \frac{t^m}{m!} \mathrm{Log}(g)^m$$

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

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

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

$$g = u_k(1)$$

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

Considérons réciproquement un homomorphisme de groupes algébriques $u : \mathbb{G}_{\mathrm{a}} \to \mathrm{GL_V}$ et vérifions que, pour tout $t \in k = \mathbb{G}_{\mathrm{a}}(k)$, 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 $(e_1, \ldots, e_n)$ de V trigonalisant simultanément tous ces automorphismes. Chacun d'entre eux induit un automorphisme de la droite vectorielle $\mathrm{V}_i = \mathrm{Vect}(e_1, \ldots, e_i)/\mathrm{Vect}(e_1, \ldots, e_{i-1}) = k\overline{e}_i$ et il existe donc une application $\chi_i : k \to k^\times$ telle que

$$u_k(t)\overline{e_i} = \chi_i(t)\overline{e_i}$$

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 $(e_1, \ldots, e_n)$ pour identifier $\mathrm{GL_V}$ avec GL_n et que l'on note P_i le polynôme $u^*(\mathrm{X}_{ii}) \in k[\mathrm{T}]$, alors $\chi_i(t) = \mathrm{P}_i(t)$ pour tout $t \in k$.

Le polynôme P_i ne s'annulant pas, il est constant puisque k est algébriquement clos ; comme en outre $\mathrm{P}_i(0) = 1$, nous obtenons $\mathrm{P}_i = 1$. Ainsi, $u_k(t)\overline{e}_i = \overline{e}_i$ 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. □

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* $\mathrm{G}(k)$*, les conditions suivantes sont équivalentes :*

(i) pour toute représentation linéaire de dimension finie $\rho : \mathrm{G} \to \mathrm{GL_V}$, l'automorphisme $\rho_k(g)$ est unipotent ;

(ii) il existe une représentation linéaire fidèle de dimension finie $\rho : \mathrm{G} \to \mathrm{GL_V}$ telle que l'automorphisme $\rho(g)$ soit unipotent ;

(iiia) si $\mathrm{car}(k) = p > 0$*, il existe un entier* $\mathrm{N} \geqslant 0$ *tel que* $g^{p^{\mathrm{N}}} = e$ *;*

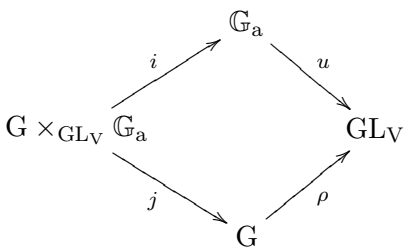
(iiib) si $\mathrm{car}(k) = 0$*, il existe un homomorphisme $u : \mathbb{G}_{\mathrm{a}} \to \mathrm{G}$ tel que g appartienne à l'image de u_k.*

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 $\rho : \mathrm{G} \hookrightarrow \mathrm{GL_V}$ 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 $\mathrm{car(k)} = p > 0$, il existe un entier $n \geqslant 0$ tel que $\rho_k(g)^{p^n} = \mathrm{id_V}$ donc $g^{p^n} = e$ puisque l'homomorphisme ρ_k est injectif.

Si $\mathrm{car(k)} = 0$, il existe un homomorphisme $u : \mathbb{G}_{\mathrm{a}} \to \mathrm{GL_V}$ ainsi qu'un élément t de $\mathbb{G}_{\mathrm{a}}(k) = k$ tels que $g = u_k(t)$. Considérons alors le diagramme commutatif



définissant le produit fibré $\mathrm{H} = \mathrm{G} \times_{\mathrm{GL_V}} \mathbb{G}_{\mathrm{a}}$ (cf. 2.3.3) ; l'homomorphisme ρ faisant de G un sous-groupe de $\mathrm{GL_V}$, l'homomorphisme i fait de H un sous-groupe de $\mathbb{G}_{\mathrm{a}}$. En outre, l'élément (g, t) de $\mathrm{H}(k)$ 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 $\mathrm{car}(k) = 0$ et du lemme ci-dessous que i est un isomorphisme. Désignant alors par v l'homomorphisme $j \circ i^{-1}$ de $\mathbb{G}_{\mathrm{a}}$ 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. □

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

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

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

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

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

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

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

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

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

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

(i) il existe une représentation linéaire fidèle de dimension finie $\rho : \mathrm{G} \to \mathrm{GL_V}$ telle que l'automorphisme $\rho_k(g)$ soit unipotent ;

(iia) si $\mathrm{car}(k) = p > 0$, il existe un entier $\mathrm{N} \geqslant 0$ tel que $g^{p^{\mathrm{N}}} = e$;

(iib) si $\mathrm{car}(k) = 0$, il existe un homomorphisme $u : \mathbb{G}_{\mathrm{a}} \to \mathrm{G}$ et un élément t de $\mathbb{G}_{\mathrm{a}}(k) = k$ 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 $f : \mathrm{G} \to \mathrm{H}$ un homomorphisme de groupes algébriques sur un corps k. Si $g \in \mathrm{G}(k)$ 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 $\chi : \mathrm{G} \to \mathbb{G}_{\mathrm{m}}$.*

L'ensemble $\mathrm{X}(\mathrm{G})$ 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

$$(\chi + \psi)_{\mathrm{R}}(g) = \chi_{\mathrm{R}}(g)\psi_{\mathrm{R}}(g)$$

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

Exemples — 1. Le groupe additif $\mathbb{G}_{\mathrm{a}}$ n'a pas de caractère non trivial en vertu de la proposition 2.2.3.

2. Le déterminant $\det : \mathrm{GL}_n \to \mathbb{G}_{\mathrm{m}}$ 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* $\mathrm{A}^\times$ *constitué des éléments* a *tels que* $\Delta(a) = a \otimes a$.

Démonstration. Un caractère de G est par définition un homomorphisme $\chi : \mathrm{G} \to \mathbb{G}_{\mathrm{m}}$ et donc correspond à un homomorphisme de k-bigèbres $\chi^* : k[\mathrm{X}, \mathrm{X}^{-1}] \to \mathrm{A}$. Ce dernier est entièrement déterminé par l'élément $a = \chi^*(\mathrm{X})$ dans $\mathrm{A}^\times$, 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 $a \in \mathrm{A}$ tel que $\Delta(a) = a \otimes a$,

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

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

Corollaire 4.3.3 — *Pour tout nombre entier* $d \geqslant 1$*, le groupe des caractère du groupe* $\mathbb{G}_{\mathrm{m}}^d$ *est un groupe abélien libre de rang* d *dont une base est formée des éléments* $\mathrm{X}_1, \ldots, \mathrm{X}_d$ *de* $k[\mathrm{X}_1^{\pm 1}, \ldots, \mathrm{X}_n^{\pm 1}]$.

Démonstration — Les éléments inversibles de $k[\mathrm{X}_1^{\pm 1}, \ldots, \mathrm{X}_d^{\pm 1}]$ sont les éléments de la forme $a = \lambda \mathrm{X}_1^{\nu_1} \ldots \mathrm{X}_d^{\nu_d}$ avec $\lambda \in k^\times$ et $\nu_1, \ldots, \nu_d \in \mathbb{Z}$. 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 $\mathbb{G}_{\mathrm{m}}^d$ tel que $\chi_i^*(\mathrm{X}) = \mathrm{X}_i$, alors l'application $(\mathbb{Z}^d \to \mathrm{X}(\mathrm{G}), \underline{\nu} \mapsto \nu_1\chi_1 + \ldots + \nu_d\chi_d)$ est un homomorphisme de groupes surjectif. L'injectivité est évidente : étant donné $\underline{\nu} \in \mathbb{Z}^d$ distinct de 0, il existe $i \in \{1, \ldots, d\}$ tel que $\nu_i \neq 0$ et, quitte à renuméroter les X_i, il est loisible de supposer que l'on a $\nu_1 \neq 0$; quel que soit alors l'élément t d'une clôture algébrique $\overline{k}$ de k qui ne soit pas une racine ν_1-ème de l'unité, le caractère $\nu_1\chi_1 + \ldots + \nu_d\chi_d$ prend la valeur $t^{\nu_1} \neq 1$ au point $(t, 1, \ldots, 1)$ de $\mathbb{G}_{\mathrm{m}}^d(\overline{k}) = \overline{k}^{\times d}$ et il est donc non trivial. □

Proposition 4.3.4 — *Si* $n \geqslant 2$*, 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 $k[(\mathrm{X}_{ij}), \det(\mathrm{X}_{ij})^{-1}]$ de GL_n sont les éléments a de la forme $\lambda \det(\mathrm{X}_{ij})^m$ 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 $n \geqslant 2$ et si K est un corps, le groupe $\mathrm{SL}_n(\mathrm{K})$ est engendré par les commutateurs, sauf si $n = 2$ et $\mathrm{K} = \mathbb{F}_2$ (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 $\overline{k}$ une clôture algébrique de k, il découle de ce que l'on vient de dire que l'homomorphisme $\chi_{\overline{k}} : \mathrm{SL}_n(\overline{k}) \to \mathbb{G}_{\mathrm{m}}(\overline{k}) = \overline{k}^\times$ 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 $\mathrm{SL}_n(\overline{k})$; d'après le *Nullstellensatz* de Hilbert, $a - 1$ est alors un élément nilpotent de A. On vérifie facilement que l'anneau $\mathrm{A} = [(\mathrm{X}_{ij})]/(\det(\mathrm{X}_{ij}) - 1)$ est *réduit* :

- l'homomorphisme

$$\mathrm{A}[\mathrm{T}, \mathrm{T}^{-1}] \to k[(\mathrm{X}_{ij}), \mathrm{T}]/(\mathrm{T}\det(\mathrm{X}_i j) - 1)$$

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. □

(4.3.2) Soit G un groupe algébrique sur un corps k et soit $\rho : G \to GL_V$ 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 $\chi_{v,R} : G(R) \to \mathbb{G}_m(R) = R^\times$ ainsi définies donnent naissance à un caractère $\chi_v : G \to \mathbb{G}_m$.

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

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

(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 $(e_1, \ldots, e_n)$ de V telle que $e_1 = v$, alors $V \otimes_k A$ est un A-module libre de base $(e_1 \otimes 1, \ldots, e_n \otimes 1)$ et les coordonnées de $\rho^*(v)$ dans cette dernière sont bien définis. En outre,

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

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 $\rho : G \to GL_V$, 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 $\rho : G \to GL_V$, il existe une base de V telle que, pour toute k-algèbre R, l'image de l'homomorphisme $\rho_R : G(R) \to GL_V(R) \simeq GL_n(R)$ 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 $\rho : G \to GL_V$ une représentation linéaire fidèle de dimension finie. Puisque V est engendré par les vecteurs propres de ρ, il existe une base $(e_1, \ldots, e_n)$ de V formée de vecteurs propres de ρ. Utilisant cette base pour identitifier GL_V et GL_n, l'homomorphisme $G \to GL_n$ déduit de ρ induit un isomorphisme entre G et un sous-groupe du groupe des matrices diagonales, lui-même isomorphe au groupe

$\mathbb{G}_{\mathrm{m}}^n$. Par suite, la bigèbre A de G est isomorphe à un quotient de la bigèbre $k[\mathrm{X}_1^{\pm 1}, \ldots, \mathrm{X}_n^{\pm 1}]$ de $\mathbb{G}_{\mathrm{m}}^n$ et, comme cette dernière est engendrée par les $2n$ caractères $\mathrm{X}_i^{\pm 1}$, A est engendrée par des caractères (les images des $\mathrm{X}_i^{\pm 1}$).

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 $(a_i)_{i\in \mathrm{I}}$ de A sur k constituée de caractères.

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

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

En vertu de l'identité $(\rho^* \otimes \mathrm{id}_{\mathrm{A}}) \circ \rho^* = (\mathrm{id}_{\mathrm{V}} \otimes \Delta) \circ \rho^*$,

$$\begin{aligned} \sum_{i\in \mathrm{I}} \rho^*(v_i) \otimes a_i &= [(\rho^* \otimes \mathrm{id}_{\mathrm{A}}) \circ \rho^*](v) \\ &= [(\mathrm{id}_{\mathrm{V}} \otimes \Delta) \circ \rho^*](v) \\ &= \sum_{i\in \mathrm{I}} v_i \otimes \Delta(a_i) \\ &= \sum_{i\in \mathrm{I}} v_i \otimes a_i \otimes a_i \end{aligned}$$

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. □

Corollaire 4.3.7 — *1. Pour tout entier $d \geqslant 1$, le groupe $\mathbb{G}_{\mathrm{m}}^d$ est diagonalisable.*
2. Pour tout entier $n \geqslant 1$ 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 $\mathbb{G}_{\mathrm{m}}^d$ est diagonalisable car sa bigèbre $k[\mathrm{X}_1^{\pm 1}, \ldots, \mathrm{X}_n^{\pm 1}]$ est engendrée par les $2n$ caractères $\mathrm{X}_i^{\pm 1}$.

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

$$\overline{k} \otimes_k k[\mathrm{X}]/(\mathrm{X}^n - 1) = \overline{k}[\mathrm{X}]/((\mathrm{X}^{n'} - 1)^{p^\alpha}) \cong \oplus_{\xi \in \mu_{n'}(\overline{k})} \overline{k}[\mathrm{X}]/\left((\mathrm{X} - \xi)^{p^\alpha}\right) \simeq \oplus_{\xi \in \mu_{n'}(\overline{k})} \overline{k}[\mathrm{X}]/(\mathrm{X}^{p^\alpha})$$

n'est clairement pas engendrée pas 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 $\mathrm{A} \to \mathrm{B}$ 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 $\mathrm{G} \times \mathrm{H}$ est le groupe algébrique de bigèbre $\mathrm{A} \otimes_k \mathrm{B}$, la comultiplication étant définie par $\Delta(a \otimes b) = \Delta_{\mathrm{G}}(a) \otimes \Delta_{\mathrm{H}}(b)$. Par suite, si $(a_i)_{i\in \mathrm{I}}$ et $(b_j)_{j\in \mathrm{J}}$ sont des familles de caractères de G et H respectivement engendrant les k-algèbres A et B, alors la k-algèbre $\mathrm{A} \otimes \mathrm{B}$ est engendrée par les caractères $a_i \otimes b_j$ et donc $\mathrm{G} \times \mathrm{H}$ est diagonalisable. □

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*

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

avec $d \geqslant 0$ *et* $n_1, \ldots, n_r$ *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* $(n_1, \ldots, n_r)$ *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 $k[\mathrm{X}_1^{pm1}, \ldots, \mathrm{X}_\mathrm{N}^{\pm 1}]$ de $\mathbb{G}_\mathrm{m}^\mathrm{N}$ pour un entier $\mathrm{N} \geqslant 1$ convenable. Il en découle que la k-algèbre A est engendrée par les caractères $a_1^{\pm 1}, \ldots, a_\mathrm{N}^{\pm 1}$; en particulier, tout caractère de A s'écrit sous la forme d'une combinaison linéaire finie des caractères $a_1^{\nu_1} \ldots a_\mathrm{N}^{\nu_\mathrm{N}}$, $\nu \in \mathbb{Z}^\mathrm{N}$. Vu l'indépendance linéaire des caractère (lemme ci-dessous), on en déduit que tout caractère de G est de la forme $a_1^{\nu_1} \ldots a_\mathrm{N}^{\nu_\mathrm{N}}$ pour un certain $\nu \in \mathbb{Z}^\mathrm{N}$ 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 $\chi \in \mathrm{X(G)}$,

$$\mathrm{A} = \bigoplus_{\chi \in \mathrm{X(G)}} k a_\chi$$

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 $\chi, \psi \in \mathrm{X(G)}$.

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

$$\begin{aligned} k[\mathrm{X}_1^\pm, \ldots, \mathrm{X}_d^\pm, \mathrm{X}_{d+1}, \ldots, \mathrm{X}_{d+r}]/(\mathrm{X}_{d+1}^{n_1} - 1, \ldots, \mathrm{X}_{d+r}^{n_r} - 1) \\ = k[\mathrm{X}_1^{\pm 1}, \ldots, \mathrm{X}_d^{\pm 1}] \otimes_k k[\mathrm{X}]/(\mathrm{X}^{n_1} - 1) \otimes_k \ldots \otimes_k k[\mathrm{X}]/(\mathrm{X}^{n_r} - 1) \end{aligned}$$

et donc $\mathrm{G} \simeq \mathbb{G}_\mathrm{m}^d \times \mu_{n_1} \times \ldots \times \mu_{n_r}$. □

Lemme 4.3.9 (Indépendance linéaire des caractères) — *Soit* G *un groupe algébrique sur un corps* k *de bigèbre* A*. Toute famille* $(a_i)_{i \in \mathrm{I}}$ *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 $(a_i)_{i \in \mathrm{J}}$ soit libre et maximale. Si $\mathrm{I} \neq \mathrm{J}$, choisissons $i_0 \in \mathrm{I} - \mathrm{J}$ et considérons une relation de dépendance linéaire

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

Appliquant Δ, il vient

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

La famille $(a_i \otimes a_j)_{(i,j)\in \mathrm{J}^2}$ étant libre dans $\mathrm{A} \otimes_k \mathrm{A}$, $\lambda_i\lambda_j = 0$ pour tous i, j distincts dans J et il existe donc un unique $i \in \mathrm{J}$ 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, $\mathrm{J} = \mathrm{I}$ et le lemme est démontré. □

(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* $u : \mathrm{D} \to \mathrm{GL_V}$ *tel que* g *appartienne à l'image de* $\mathrm{D}(k)$*.*

Démonstration. Si g est diagonalisable, il existe une base $(e_1, \ldots, e_n)$ de V formée de vecteurs propres de g. Utilisant cette base pour identifier $\mathrm{GL_V}$ et GL_n, g appartient donc à $\mathrm{T}(k)$, où T est le sous-groupe de $\mathrm{GL_V}$ correspondant au sous-groupe des matrices diagonales dans GL_n. Comme $\mathrm{T} \simeq \mathbb{G}_{\mathrm{m}}^n$, 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 $u : \mathrm{D} \to \mathrm{GL_V}$. Il existe par hypothèse une base $(e_1, \ldots, e_n)$ de V constituée de vecteurs propres de u. Utilisant cette base pour identifier $\mathrm{GL_V}$ 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 $\mathrm{D}(k)$ a une matrice diagonale dans la base $(e_1, \ldots, e_n)$ et donc est diagonalisable. □

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

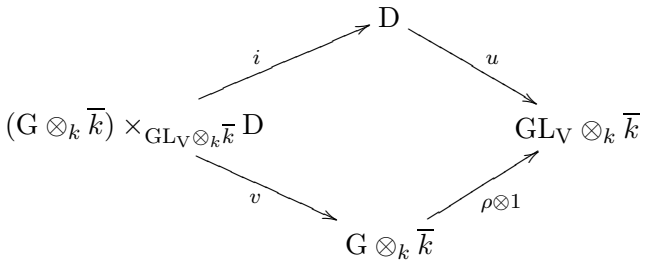
(i) quelle que soit la représentation linéaire de dimension finie $\rho : \mathrm{G} \to \mathrm{GLV}$*, l'automorphisme* $\rho_k(g)$ *est semi-simple ;*

(ii) il existe une représentation linéaire fidèle de dimension finie $\rho : \mathrm{G} \to \mathrm{GL_V}$ *telle que l'automorphisme* $\rho_k(g)$ *soit semi-simple ;*

(iii) il existe un $\overline{k}$*-groupe algébrique diagonalisable* D *et un homomorphisme* $u : \mathrm{D} \to \mathrm{G} \otimes_k \overline{k}$ *tel que* g *appartienne à l'image de* $\mathrm{D}(\overline{k})$ *dans* $\mathrm{G}(\overline{k})$*.*

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

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



définissant le produit fibré $\mathrm{D}' = (\mathrm{G} \otimes_k \overline{k}) \times_{\mathrm{GL_V}\otimes_k\overline{k}} \mathrm{D}$. Comme ρ fait de G un sous-groupe de $\mathrm{GL_V}$, 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 $\mathrm{D}'(\overline{k})$ tel que $\rho_{\overline{k}}(v_{\overline{k}}(h)) = \rho_{\overline{k}}(g)$ dans $\mathrm{GL}(\mathrm{V} \otimes_k \overline{k})$, donc tel que $v_{\overline{k}}(h) = g$ puisque l'homomorphisme $\rho_{\overline{k}}$ est injectif. L'assertion (iii) est ainsi établie.

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

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

(i) quelle que soit la représentation linéaire de dimension finie $\rho : \mathrm{G} \to \mathrm{GLV}$*, l'automorphisme* $\rho_k(g)$ *est semi-simple ;*

(ii) il existe une représentation linéaire fidèle de dimension finie $\rho : \mathrm{G} \to \mathrm{GL_V}$ *telle que l'automorphisme* $\rho_k(g)$ *soit semi-simple ;*

(iii) il existe un $\overline{k}$*-groupe algébrique diagonalisable* D *et un homomorphisme* $u : \mathrm{D} \to \mathrm{G} \otimes_k \overline{k}$ *tel que* g *appartienne à l'image de* $\mathrm{D}(\overline{k})$ *dans* $\mathrm{G}(\overline{k})$*.*

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 $\overline{k}$ une clôture algébrique de k ; comme k est pafait, l'extension $\overline{k}/k$ est galoisienne.

Étant donné un élément g de $\mathrm{G}(k)$, la décomposition de Jordan $g = g'_s g'_u$ dans $\mathrm{G}(\overline{k})$ est valable sur une extension galoisienne finie k' de k : en effet, les éléments g'_s et g'_u de $\mathrm{G}(\overline{k})$ correspondent à des k-homomorphismes de la bigèbre A de G dans $\overline{k}$ 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 $\Gamma = \mathrm{Gal}(k'|k)$ opère naturellement par automorphismes du groupe $\mathrm{G}(k')$ et

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

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

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

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

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

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

et donc

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

puisque Γ opère par automorphismes du corps k'.

- Si h est un élément de $\mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A}, k')$ 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 $\mathrm{G}(\overline{k})$ sont respectivement semi-simples et unipotents. Par unicité de la décomposition de Jordan dans $\mathrm{G}(\overline{k})$, 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 $\mathrm{G}(k)$ avec g_s (resp. g_u) semi-simple (resp. unipotent) dans $\mathrm{G}(\overline{k})$. Quelle que soit la représentation linéaire de dimension finie $\rho : \mathrm{G} \to \mathrm{GL_V}$, les automorphismes $\rho_k(g_s)$ et $\rho_k(g_u)$ sont respectivement semi-simples et unipotents sur $\overline{k}$; ils le sont donc également sur k. Nous avons ainsi établi l'existence d'une décomposition de Jordan dans $\mathrm{G}(k)$ et l'unicité vient de l'unicité de cette décomposition dans $\mathrm{G}(\overline{k})$.

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

Deuxième étape : le cas $\mathrm{G} = \mathrm{GL_V}$.

Il n'y a pratiquement rien à faire. Étant donné $g \in \mathrm{GL_V}(k) = \mathrm{GL(V)}$, 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 $\rho : \mathrm{GL_V} \to \mathrm{GL_W}$ 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 GL(V) avec g'_s et g'_u d'images respectives semi-simples et unipotentes dans toute représentation linéaire de $\mathrm{GL_V}$, 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 $\mathrm{G} = \mathrm{GL_V}$, et on a en outre prouvé que la décomposition obtenue n'est autre que la décomposition de Jordan multiplicative élémentaire rappelée en introduction.

Troisième étape : cas général

Le corps k est toujours supposé algébriquement clos. Soit G un groupe algébrique sur k et soit $\rho : \mathrm{G} \to \mathrm{GL_V}$ une représentation linéaire fidèle de G (théorème de Chevalley, cf. 3.3) ; on utilise ρ pour identifier G à un sous-groupe de $\mathrm{GL_V}$. En appliquant de nouveau le théorème de Chevalley, il existe une représentation linéaire fidèle de dimension finie $\mu : \mathrm{GL_V} \to \mathrm{GL_W}$ et un sous-espace vectoriel W_0 de W tels que G soit le sous-groupe de $\mathrm{GL_V}$ stabilisant W_0. Soit alors $g \in \mathrm{G}(k)$ et soit $g = g_s g_u = g_u g_s$ la décomposition de Jordan de g dans 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 $\mathrm{G}(k)$; comme en outre l'homomorphisme μ_k est injectif, nous en concluons à l'appartenance de g_s et g_u au sous-groupe $\mathrm{G}(k)$ de GL(V).

Les éléments g_s et g_u de $\mathrm{G}(k)$ 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 $\mathrm{G}(k)$ tandis que l'unicité découle immédiatement de l'unicité dans GL(V). Le théorème 4.1.3 est ainsi démontré.

5. Groupes algébriques et variétés algébriques

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 $\mathrm{GL}_n(\mathrm{R})$. Suivant l'approche fonctorielle que nous avons adoptée, la connaissance du sous-groupe G(R) de $\mathrm{GL}_n(\mathrm{R})$ 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 $\mathrm{G}(k)$ de $\mathrm{GL}_n(k)$, et cette question conduit à s'intéresser aux sous-groupes de $\mathrm{GL}_n(k)$ définis par des équations polynomiales en les coefficients 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

(5.1.1) Soit $\mathrm{A} = k[(\mathrm{X}_{ij}), \mathrm{T}]/(\mathrm{T}\det(\mathrm{X}_{ij}) - 1)$ la bigèbre du groupe algébrique GL_n. À chaque élément f de A correspond une fonction $\underline{f}$ sur le groupe $\mathrm{GL}_n(k)$ à valeurs dans k, définie par

$$\underline{f}(s) = f((s_{ij}), \det(s)^{-1}).$$

Comme

$$\underline{\mathrm{X}_{ij}}(s) = s_{ij} \quad \text{et} \quad \underline{\mathrm{T}}(s) = \det(s)^{-1},$$

les fonctions obtenues de la sorte sont précisément les fonctions polynomiales en les coefficients de s et $\det(s)^{-1}$.

Lemme 5.1.1 — *(i) L'anneau* A *est intègre.*
(ii) Si le corps k est infini, l'application

$$\mathrm{A} \to \mathrm{Hom}_{\mathbf{Ens}}(\mathrm{GL}_n(k), k), \quad f \mapsto \underline{f}$$

est injective.

Démonstration. (i) Considérons l'homomorphisme

$$\iota : k[(\mathrm{X}_{ij}), \mathrm{T}] \to k(\mathrm{X}_{ij})$$

défini en envoyant chaque indéterminée X_{ij} sur elle-même et T sur la fraction rationnelle $\det(\mathrm{X}_{ij})^{-1}$. Il est clair que ι s'annule identiquement sur l'idéal principal I de $k[(\mathrm{X}_{ij}), \mathrm{T}]$ engendré par $\mathrm{T}\det(\mathrm{X}_{ij})$. Soit $\mathrm{F} \in k[(\mathrm{X}_{ij}), \mathrm{T}]$ un polynôme, que l'on écrit sous la forme

$$\mathrm{F} = \sum_{\ell=0}^{n} a_\ell \mathrm{T}^\ell$$

avec $a_\ell \in k[(\mathrm{X}_{ij})]$ et $a_n \neq 0$. Vu les identités

$$\begin{aligned} \det(\mathrm{X}_{ij})^n \mathrm{F} &= \sum_{\ell=0}^{n} a_\ell \det(\mathrm{X}_{ij})^{n-\ell} (\mathrm{T}\det(\mathrm{X}_{ij}))^\ell \\ &\equiv \sum_{\ell=0}^{n} a_\ell \det(\mathrm{X}_{ij})^{n-\ell} \pmod{\mathrm{I}} \end{aligned}$$

et

$$\iota(\mathrm{F}) = \frac{\sum_{\ell=0}^{n} a_\ell \det(\mathrm{X}_{ij})^{n-\ell}}{\det(\mathrm{X}_{ij})^n},$$

$\iota(\mathrm{F}) = 0$ si et seulement si F appartient à I. L'homomomorphisme ι induit ainsi un isomorphisme entre A et un sous-anneau du corps $k(\mathrm{X}_{ij})$, ce qui prouve l'intégrité de A.

(ii) Soit $\mathrm{F} \in k[(\mathrm{X}_{ij}), \mathrm{T}]$ un polynôme tel que $\mathrm{F}((s_{ij}), \det(s)^{-1}) = 0$ pour tout élément s de $\mathrm{GL}_n(k)$. Vu ce qui précède, il existe un entier naturel $n \geqslant 0$ et un polynôme $\mathrm{F} \in k[(\mathrm{X}_{ij})]$ tels que

$$\det(\mathrm{X}_{ij})^n \mathrm{F} \equiv \mathrm{G} \pmod{\mathrm{I}} ;$$

on a alors $\mathrm{G}(s) = \mathrm{G}((s_{ij})) = 0$ pour tout élément $s \in \mathrm{GL}_n$. Quels que soient $s, t \in \mathrm{GL}_n(k)$ et $\lambda \in k$, la matrice $s + \lambda t$ appartient à $\mathrm{GL}_n(k)$ pour tout λ distinct des racines du polynôme non nul

$$\det(s + \lambda t) = \lambda^n \det(t) + \ldots + \det(s),$$

donc pour une infinité de λ dans k puisque k est infini. Il en découle que le polynôme en $\mathrm{G}(s + \mathrm{X}t) \in k[\mathrm{X}]$ admet une infinité de racines dans k, donc est identiquement nul ; comme toute matrice $x \in \mathrm{M}_n(k)$ s'écrit sous la forme $s + \lambda t$ avec $s, t \in \mathrm{GL}_n(k)$ et $\lambda \in k$ convenablement choisis, nous en concluons que le polynôme G s'annule identiquement sur k^{n^2}. Le corps k étant infini, ceci implique $\mathrm{G} = 0$ (raisonner par récurrence sur le nombre des variables du polynôme G) et donc $\mathrm{F} \in \mathrm{I}$. □

Étant donné un sous-groupe $\mathrm{G} \hookrightarrow \mathrm{GL}_n$, la bigèbre de G est un quotient de A et il existe donc un idéal $\mathfrak{I}$ de A tel que

$$\mathrm{G}(k) = \{s \in \mathrm{GL}_n(k) \mid \underline{f}(s) = 0, \quad \forall f \in \mathfrak{I}\}.$$

Cette observation met en évidence une condition nécessaire pour qu'un sous-groupe Γ de $\mathrm{GL}_n(k)$ provienne d'un sous-groupe du groupe algébrique GL_n : Γ doit être un sous-ensemble de $\mathrm{GL}_n(k)$ défini par des équations polynomiales en les coefficients et l'inverse du déterminant des matrices $s \in \mathrm{GL}_n(k)$. Il s'avère que cette condition est suffisante.

Proposition 5.1.2 — *Soit Γ un sous-groupe de $\mathrm{GL}_n(k)$ et soit $\mathfrak{I}$ l'idéal de A constitué des éléments f de A tels que la fonction $\underline{f}$ s'annule identiquement sur Γ.*

(i) L'anneau quotient $\mathrm{A}/\mathfrak{I}$ est la bigèbre d'un sous-groupe algébrique G_Γ de GL_n.

(ii) On a

$$\mathrm{G}_\Gamma(k) = \{s \in \mathrm{GL}_n(k) \mid \underline{f}(s) = 0, \quad \forall f \in \mathfrak{I}\} \ ;$$

en particulier, $\Gamma \subset \mathrm{G}_\Gamma(k)$.

(iii) Si Γ est défini par des équations polynomiales, alors $\mathrm{G}_\Gamma(k) = \Gamma$.

Démonstration. (i) Nous allons vérifier qu'il existe une unique structure de bigèbre sur $\mathrm{B} = \mathrm{A}/\mathfrak{I}$ telle que la projection canonique $p : \mathrm{A} \to \mathrm{B}$ soit un homomorphisme de bigèbres.

Désignons par Δ la comultiplication de A. Étant donnés un élément $f \in \mathrm{A}$ et une écriture de $\Delta(f)$ sous la forme $\Delta(f) = \sum_i g_i \otimes h_i$,

$$\underline{f}(st) = \sum_i \underline{g_i}(s)\underline{h_i}(t)$$

(cf. 3.2). L'existence d'une application k-linéaire $\overline{\Delta} : \mathrm{B} \to \mathrm{B} \otimes_k \mathrm{B}$ s'insérant dans un diagramme commutatif

$$\begin{array}{ccc} \mathrm{A} & \xrightarrow{\Delta} & \mathrm{A} \otimes_k \mathrm{A} \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p\otimes p} \\ \mathrm{B} & \xrightarrow[\overline{\Delta}]{} & \mathrm{B} \otimes_k \mathrm{B} \end{array}$$

équivaut à l'inclusion $\Delta(\mathfrak{I}) \subseteq \mathfrak{I} \otimes_k \mathrm{A} + \mathrm{A} \otimes_k \mathfrak{I}$.

Soit $(a_\lambda)_\Lambda$ une base du k-espace vectoriel A contenant une base du sous-espace vectoriel $\mathfrak{I}$, disons $(a_\lambda)_{\Lambda_0}$ avec $\Lambda_0 \subset \Lambda$. La famille $(a_\lambda \otimes a_{\lambda'})_{\Lambda^2}$ constitue une base de $\mathrm{A} \otimes_k \mathrm{A}$. Soit $f \in \mathfrak{I}$ et écrivons $\Delta(f)$ sous la forme

$$\Delta(f) = \sum_{(\lambda_1, \lambda_2) \in \Lambda^2} c_{\lambda_1, \lambda_2} a_{\lambda_1} \otimes a_{\lambda_2}$$

avec $c_{\lambda_1,\lambda_2} \in k$. Quel que soit $s \in \Gamma$, la fonction translatée

$$\underline{f}(s\cdot) = \sum_{(\lambda_1,\lambda_2)\in\Lambda^2} c_{\lambda_1,\lambda_2}\underline{a_{\lambda_1}}(s)a_{\lambda_2}$$

s'annule identiquement sur Γ ; on a donc

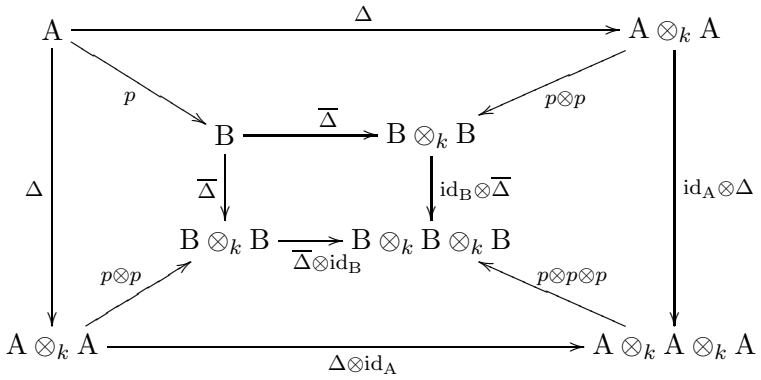
$$\sum_{(\lambda_1,\lambda_2)\in\Lambda^2} c_{\lambda_1,\lambda_2}\underline{a_{\lambda_1}}(s)a_{\lambda_2} \in \mathfrak{I},$$

puis $c_{\lambda_1,\lambda_2}\underline{a_{\lambda_1}}(s) = 0$ pour tout couple (λ_1, λ_2) dans $\Lambda \times (\Lambda - \Lambda_0)$. Comme s est un élément arbitraire de Γ,

$$\sum_{\lambda_1\in\Lambda,\lambda_2\notin\Lambda_0} c_{\lambda_1,\lambda_2}a_{\lambda_1} \in \mathfrak{I}$$

et donc $c_{\lambda_1,\lambda_2} = 0$ si $\lambda_1 \notin \Lambda_0$. Au final, nous obtenons $c_{\lambda_1,\lambda_2} = 0$ pour tout couple $(\lambda_1, \lambda_2) \in (\Lambda - \Lambda_0)^2$ et $\Delta(f)$ appartient donc bien à $\mathfrak{I} \otimes_k \mathrm{A} + \mathrm{A} \otimes_k \mathfrak{I}$.

La coassociativité de $\overline{\Delta}$ se déduit aisément de la coassociativité de Δ. Le diagramme suivant



est en effet commutatif par construction de $\overline{\Delta}$ et donc

$$\begin{aligned}[(\overline{\Delta}\otimes \mathrm{id_B})\circ\overline{\Delta}]\circ p &= (p\otimes p\otimes p)\circ[(\Delta\otimes \mathrm{id_A})\circ\Delta] \\ &= (p\otimes p\otimes p)\circ[(\mathrm{id_A}\otimes\Delta)\circ\Delta] \\ &= [(\mathrm{id_B}\otimes\overline{\Delta})\circ\overline{\Delta}]\circ p.\end{aligned}$$

L'identité $(\mathrm{id_B}\otimes\overline{\Delta})\circ\overline{\Delta} = (\overline{\Delta}\circ\mathrm{id_B})\circ\overline{\Delta}$ s'en déduit puisque p est une surjection.

En procédant de façon analogue, on prouve que la counité e^* et la coinversion ι de A induise respectivement des applications k-linéaires $\overline{e}^* : \mathrm{B} \to k$ et $\overline{\iota} : \mathrm{B} \to \mathrm{B}$ vérifiant $\overline{e}^* \circ p = e^*$ et $p \circ \iota = \overline{\iota} \circ p$, et telles que $(\mathrm{B}, \overline{\Delta}, \overline{e}^*, \overline{\iota})$ soit une bigèbre. On désigne par G_Γ le sous-groupe de GL_n correspondant à ce quotient de A.

(ii) Par construction, $\mathrm{G}_\Gamma(k)$ est le sous-ensemble de $\mathrm{GL}_n(k)$ défini par les équations $\underline{f}(s) = 0$, $f \in \mathfrak{I}$. L'inclusion

$$\Gamma \subset \mathrm{G}_\Gamma(k)$$

est évidente puisque $\mathfrak{I}$ est par définition l'idéal des $f \in \mathrm{A}$ s'annulant identiquement sur Γ.

(iii) Supposons qu'il existe un idéal $\mathfrak{J}$ de A tel que

$$\Gamma = \{s \in \mathrm{GL}_n(k) \mid \underline{(f)}(s) = 0, \quad \forall f \in \mathfrak{J}\}.$$

L'inclusion $\mathfrak{J} \subset \mathfrak{I}$ est évidente et implique $\mathrm{G}_\Gamma(k) \subset \Gamma$; comme on a toujours $\Gamma \subset \mathrm{G}_\Gamma(k)$, nous obtenons bien

$$\Gamma = \mathrm{G}_\Gamma(k).$$

□

L'assertion (ii) de la proposition précédente a une conséquence qui mérite d'être explicitée.

Corollaire 5.1.3 — *Soit* Γ *un sous-groupe de* $\mathrm{GL}_n(k)$. *Désignant par* $\mathfrak{I}$ *l'idéal des* $f \in \mathrm{A}$ *qui s'annulent identiquement sur* Γ, *le sous-ensemble*

$$\overline{\Gamma} = \{s \in \mathrm{GL}_n(k) \mid \underline{f}(s) = 0, \quad \forall f \in \mathfrak{I}\}$$

de $\mathrm{GL}_n(k)$ *est un sous-groupe contenant* Γ.

On verra un peu plus loin que, lorsque $\mathfrak{I}$ parcourt l'ensembles des idéaux de A, les parties de $\mathrm{GL}_n(k)$ de la forme

$$\{s \in \mathrm{GL}_n(k) \mid \underline{f}(s) = 0, \quad \forall f \in \mathfrak{I}\}$$

satisfont aux axiomes caractérisant les parties fermées d'une topologie sur $\mathrm{GL}_n(k)$, la *topologie de Zariski*. De ce point de vue, le corollaire précédent affirme que l'adhérence d'un sous-groupe de $\mathrm{GL}_n(k)$ est encore un sous-groupe.

(5.1.2) Il reste à comparer les deux constructions dont nous disposons :

- partant d'un sous-groupe G du groupe algébrique GL_n, on considère le sous-groupe $\mathrm{G}(k)$ de $\mathrm{GL}_n(k)$;
- partant d'un sous-groupe Γ de $\mathrm{GL}_n(k)$, on considère le sous-groupe G_Γ de GL_n.

On sait déjà que, pour tout sous-groupe Γ de $\mathrm{GL}_n(k)$, $\mathrm{G}_\Gamma(k)$ est l'adhérence de Γ dans $\mathrm{GL}_n(k)$ équipé de la topologie de Zariski.

Proposition 5.1.4 — *Soit* G *un sous-groupe de* GL_n.

(i) Le groupe algébrique $\mathrm{G}_{\mathrm{G}(k)}$ *est un sous-groupe de* G.

(ii) Supposons que le corps k *soit* algébriquement clos. *Pour que* $\mathrm{G}_{\mathrm{G}(k)}$ *coïncide avec* G, *il faut et il suffit que la bigèbre de* G *soit un anneau* réduit *(c'est-à-dire sans élément nilpotent non nul).*

Démonstration. (i) Soit $\mathfrak{J}$ l'idéal de A définissant le sous-groupe G. Comme

$$\mathrm{G}(k) = \{s \in \mathrm{GL}_n(k) \mid \underline{f}(s) = 0, \quad \forall f \in \mathfrak{J}\},$$

$\mathfrak{J}$ est contenu dans l'idéal $\mathfrak{I}$ des $f \in \mathrm{A}$ s'annulant identiquement sur $\mathrm{G}(k)$; la bigèbre $\mathrm{A}/\mathfrak{I}$ du groupe algébrique $\mathrm{G}_{\mathrm{G}(k)}$ est donc un quotient de la bigèbre $\mathrm{A}/\mathfrak{J}$ de G, ce qui signifie précisément que $\mathrm{G}_{\mathrm{G}(k)}$ est un sous-groupe de G.

(ii) Sans hypothèse sur k, $\mathrm{GL}_n(k)$ s'identifie naturellement à l'ensemble $\mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A}, k)$ des homomorphismes de k-algèbres de A dans k. Un tel homomorphisme est complètement déterminé par son noyau, lequel est un idéal maximal de A ; on obtient de la sorte une identification entre $\mathrm{GL}_n(k)$ et l'ensemble des idéaux maximaux $\mathfrak{m}$ de A tels que $\mathrm{A}/\mathfrak{m} = k$. Comme en outre l'évaluation $\underline{f}(s)$ d'un élément f de A au point s de $\mathrm{GL}_n(k)$ n'est autre que l'évaluation $s(f)$ de l'homomorphisme $s : \mathrm{A} \to k$ en f, la condition $\underline{f}(s) = 0$ signifie précisément que f appartient à l'idéal maximal $\ker(s)$ de A correspondant à s.

Lorsque le corps k est algébriquement clos, il découle du Nullstellensatz (Appendice, 3) que *tout* idéal maximal $\mathfrak{m}$ de A est tel que $\mathrm{A}/\mathfrak{m} = k$. Désignant toujours par $\mathfrak{J}$ l'idéal de A définissant G, l'ensemble des éléments f de A qui s'annulent identiquement sur $\mathrm{G}(k)$ est par conséquent l'intersection de tous les idéaux maximaux de A contenant $\mathfrak{J}$, soit encore l'idéal

$$\sqrt{\mathfrak{J}} = \{f \in \mathrm{A} \ ; \ \exists n \geqslant 0, \quad f^n \in \mathfrak{J}\}$$

par une nouvelle application du Nullstellensatz. Le sous-groupe $\mathrm{G}_{\mathrm{G}(k)}$ de G correspondant par construction au quotient $\mathrm{A}/\sqrt{\mathfrak{J}}$ de $\mathrm{A}/\mathfrak{J}$, on obtient $\mathrm{G} = \mathrm{G}_{\mathrm{G}(k)}$ si et seulement si $\sqrt{\mathfrak{J}} = \mathfrak{J}$, donc si et seulement si l'anneau $\mathrm{A}/\mathfrak{J}$ est *réduit*. □

Exemples 5.1.5 — Il est facile d'illustrer la nécessité des différentes hypothèses introduites en vue de comparer un sous-groupe de GL_n au sous-groupe $\mathrm{G}(k)$ de $\mathrm{GL}_n(k)$.

a) Considérons le groupe algébrique μ_n sur $\mathbb{Q}$, que l'on voit comme un sous-groupe de GL_n en identifiant $\mu_n(\mathrm{R}) = \{t \in \mathrm{R} \mid t^n = 1\}$ au groupe G des homothéties $\mathrm{diag}(t, \ldots, t)$ de déterminant 1. Le sous-groupe $\Gamma = \mathrm{G}(\mathbb{Q})$ de $\mathrm{GL}_n(\mathbb{Q})$ est réduit à l'identité et G_Γ est le groupe trivial **1**. Le groupe μ_n est ainsi totalement annihilé si $n \geqslant 2$. Par contre, si l'on remplace $\mathbb{Q}$ par sa clôture algébrique $\overline{\mathbb{Q}}$ dans $\mathbb{C}$, alors $\Gamma = \mathrm{G}(\overline{\mathbb{Q}})$ est le sous-groupe de $\mathrm{GL}_n(\overline{\mathbb{Q}})$ défini par les équations

$$\mathrm{X}_{ij} = 0 \quad \text{si} \quad i \neq j, \quad \mathrm{X}_{11}^n = 1, \quad \mathrm{X}_{ii} - \mathrm{X}_{11} = 0 \ \ (1 \leqslant i \leqslant n) \quad \text{et} \quad \det(\mathrm{X}_{ij}) = 1$$

et donc $\mathrm{G}_\Gamma \simeq \mu_n$.

b) Soit k un corps algébriquement clos de caractéristique $p > 0$. On considère le k-groupe algébrique α_p, défini par $\alpha_p(\mathrm{R}) = \{t \in \mathrm{R} \mid t^p = 0\}$ pour toute k-algèbre R. On voit α_p comme un sous-groupe de GL_2 en identifiant $\alpha_p(\mathrm{R})$ et le sous-groupe de $\mathrm{GL}_2(\mathrm{R})$ constitué des matrices $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ avec $t^p = 0$. Le sous-groupe $\Gamma = \alpha_p(k)$ de $\mathrm{GL}_2(k)$ est réduit à la matrice identité et G_Γ est de nouveau le groupe trivial. La bigèbre de α_p est l'anneau non réduit $k[\mathrm{T}]/(\mathrm{T}^p)$.

En vertu de la proposition précédente, un sous-groupe G du groupe algébrique GL_n est entièrement déterminé par le sous-groupe $\mathrm{G}(k)$ de $\mathrm{GL}_n(k)$ lorsque le corps k est algébriquement clos et la bigèbre de G est un anneau réduit.

Définition 5.1.6 — *Soit $\overline{k}$ une clôture algébrique du corps k. Un groupe algébrique* G *sur k de bigèbre* A *est dit* lisse *si l'anneau $\mathrm{A} \otimes_k \overline{k}$ est réduit.*

Signalons sans démonstration le théorème important suivant, dû à P. Cartier.

Théorème 5.1.7 — *Tout groupe algébrique sur un corps de caractéristique* nulle *est lisse.*

Démonstration. Voir [Milne], p. 22 ou [Waterhouse], p. 86. □

(5.1.3) Considérons deux sous-groupes Γ et Γ' de $\mathrm{GL}_n(k)$ et $\mathrm{GL}_m(k)$ respectivement. Étant donné un homomorphisme de groupes « abstraits » $\varphi : \Gamma \to \Gamma'$, il est naturel de se demander s'il existe un homomorphisme de groupes algébriques $\Phi : \mathrm{G}_\Gamma \to \mathrm{G}_{\Gamma'}$ tel que $\varphi = \Phi_k$.

Notons A (resp. A′) la bigèbre de GL_n (resp. de GL_m) et soit $\mathfrak{I}$ (resp. $\mathfrak{I}'$) l'idéal de A (resp. A′) définissant G_Γ (resp. $\mathrm{G}_{\Gamma'}$). Un homomorphisme de groupes algébriques $\Phi : \mathrm{G}_\Gamma \to \mathrm{G}_{\Gamma'}$ correspond à un homomorphisme de bigèbres $\Phi^* : \mathrm{A}'/\mathfrak{I}' \to \mathrm{A}/\mathfrak{I}$ et, pour tout élément f de A′,

$$\underline{\Phi^*(f)} = \underline{f} \circ \Phi_k$$

(identité entre fonctions sur $\mathrm{G}_\Gamma(k)$). On obtient ainsi une condition nécessaire à l'existence de Φ : l'application

$$\mathrm{Hom}_{\mathbf{Ens}}(\Gamma', k) \to \mathrm{Hom}_{\mathbf{Ens}}(\Gamma, k)$$

doit envoyer l'image de $\mathrm{A}'/\mathfrak{I}'$ dans l'image de $\mathrm{A}/\mathfrak{I}$. De manière imagée : composée avec φ, toute fonction polynomiale sur Γ' est une fonction polynomiale sur Γ (ici, « polynomiale » veut dire « polynomiale en les coefficients matriciels et l'inverse du déterminant »).

Il est aisé de voir que cette condition est également suffisante. En effet, si $\varphi : \Gamma \to \Gamma'$ est un homomorphisme de groupes tel que, pour tout $f \in \mathrm{A}'$, la fonction $\underline{f} \circ \varphi$ sur Γ provienne d'un élément de A, ce dernier est uniquement déterminé modulo l'idéal $\mathfrak{I}$ des élément de A s'annulant identiquement sur Γ et il existe donc un unique homomorphisme de k-algèbres $\Psi : \mathrm{A}' \to \mathrm{A}/\mathfrak{I}$ tel que

$$\underline{f} \circ \varphi = \underline{\Psi(f)}$$

pour tout $f \in \mathrm{A}'$. Il s'agit automatiquement d'un homomorphisme de bigèbres. Notant en effet Δ (resp. Δ') la comultiplication de A (resp. de A′),

$$\begin{aligned}\underline{(\Delta\circ\Psi)(f)}(s,t) &= \underline{\Psi(f)}(st)\\ &= \underline{f}(\varphi(st))\\ &= \underline{f}(\varphi(s)\varphi(t))\\ &= \underline{((\Psi\otimes\Psi)\circ\Delta')(f)}(s,t)\end{aligned}$$

pour tous $s,t\in\Gamma$ et donc

$$\Delta\circ\Psi = (\Psi\otimes\Psi)\circ\Delta'$$

en tant qu'homomorphismes de $\mathrm{A}'\otimes_k\mathrm{A}'$ dans $\mathrm{A}/\mathfrak{I}\otimes_k\mathrm{A}/\mathfrak{I}$ en vertu du lemme ci-dessous. Cette identité établit que l'homomorphisme Ψ est compatible aux comultiplications ; un raisonnement analogue permet de vérifier que Ψ est également compatible aux conuités et aux coinversions, de sorte qu'il s'agit finalement d'un homomorphisme de bigèbres. Finalement, l'homomorphisme de bigèbres $\mathrm{A}'/\mathfrak{I}'\to\mathrm{A}/\mathfrak{I}$ induit par Ψ définit un homomorphisme de groupes algébriques $\Phi:\mathrm{G}_\Gamma\to\mathrm{G}_{\Gamma'}$ tel que $\Phi_k=\varphi$.

Lemme 5.1.8 — *Avec les notations en vigueur, le noyau de l'application*

$$\mathrm{A}\otimes_k\mathrm{A}\to\mathrm{Hom}_{\mathbf{Ens}}(\Gamma\times\Gamma,k),\quad \sum a_i\otimes b_i\mapsto\sum\underline{a_ib_i}$$

est l'idéal $\mathfrak{I}\otimes_k\mathrm{A}+\mathrm{A}\otimes_k\mathfrak{I}$.

Démonstration. Soit $(a_\lambda)_{\lambda\in\Lambda}$ une base du k-espace vectoriel A contenant une base $(a_\lambda)_{\lambda\in\Lambda_0}$ du sous-espace vectoriel $\mathfrak{I}$. Un élément f de $\mathrm{A}\otimes_k\mathrm{A}$ s'écrit de manière unique sous la forme $f=\sum_{(\lambda,\lambda')\in\Lambda^2}c_{\lambda,\lambda'}a_\lambda\otimes a_{\lambda'}$ avec $c_{\lambda,\lambda'}\in k$. Si f s'annule identiquement sur $\Gamma\times\Gamma$, l'élément

$$\sum_{\lambda'\in\Lambda}\left(\sum_{\lambda\in\Lambda}c_{\lambda,\lambda'}\underline{a_\lambda}(s)\right)a_{\lambda'}=\sum_{(\lambda,\lambda')\in\Lambda}c_{\lambda,\lambda'}\underline{a_\lambda}(s)a_{\lambda'}$$

de A s'annule identiquement sur Γ pour tout $s\in\Gamma$. Vu la définition de $\mathfrak{I}$, on en déduit que $\sum_\lambda c_{\lambda,\lambda'}a_\lambda$ s'annule identiquement sur Γ pour tout $\lambda'\in\Lambda-\Lambda_0$, puis $c_{\lambda,\lambda'}=0$ pour tout couple (λ,λ') appartenant à $(\Lambda-\Lambda_0)^2$. □

Nous pouvons résumer et préciser la discussion qui précède.

Proposition 5.1.9 — *Étant donnés des sous-groupes fermés* Γ *et* Γ' *de* $\mathrm{GL}_n(k)$*, la correspondance* $\Phi\mapsto\Phi_k$ *établit une bijection entre l'ensemble des homomorphismes de groupes algébriques* $\mathrm{G}_\Gamma\to\mathrm{G}'_\Gamma$ *et l'ensemble des homomorphismes de groupes* $\Gamma\to\Gamma'$ *transformant toute fonction polynomiale sur* Γ *en une fonction polynomiale sur* Γ'*.*

En particulier : si le corps k *est algébriquement clos, tout homomorphisme d'un groupe algébrique lisse* G *dans un groupe algébrique* H *est complètement déterminé par l'homomorphisme qu'il induit de* $\mathrm{G}(k)$ *dans* $\mathrm{H}(k)$*.*

Démonstration. Pour ce qui est de la première assertion, le seul point restant à vérifier est le fait qu'un homomorphisme $\Phi:\mathrm{G}_\Gamma\to\mathrm{G}_\Gamma$ est complètement déterminé par l'homomorphisme Φ_k. C'est immédiat : si Φ et Φ' sont deux homomorphismes tels que $\Phi_k=\Phi'_k$, alors $\underline{\Phi(f)}=\underline{\Phi'}(f)$ pour tout élément f de la bigèbre de $\mathrm{G}_{\Gamma'}$, puis $\Phi(f)=\Phi'(f)$ par construction de G_Γ et donc finalement $\Phi=\Phi'$.

La seconde assertion se déduit aisément de la première : il suffit d'invoquer le théorème de Chevalley pour plonger H dans GL_n puis d'utiliser la proposition 5.1.4 pour écrire les groupes lisses G et GL_n sous la forme G_Γ et $\mathrm{G}_{\Gamma'}$ avec $\Gamma=\mathrm{G}(k)$ et $\Gamma'=\mathrm{GL}_n(k)$. □

Remarque — L'exponentielle définit un homomorphisme de groupes de $\mathbb{C}$ dans $\mathbb{C}^\times$ qui ne provient pas d'un homomorphisme de groupes algébriques $\mathbb{G}_{\mathrm{a}} \to \mathbb{G}_{\mathrm{m}}$ car la fonction polynomiale $\underline{\mathrm{X}}$ sur $\mathbb{C}^\times$ est transformée en la fonction $t \mapsto e^t$ sur $\mathbb{C}$, laquelle n'est pas polynomiale. On sait d'ailleurs qu'il n'existe pas d'homomorphisme non trivial du groupe $\mathbb{G}_{\mathrm{a}}$ dans le groupe $\mathbb{G}_{\mathrm{m}}$ (Proposition 2.2.3).

(5.1.4) On peut illustrer les constructions précédentes en associant un k-groupe algébrique $\underline{\Gamma}$ à tout groupe fini Γ de telle sorte que $\underline{\Gamma}(k) = \Gamma$.

Quel que soit le corps k, on sait en effet plonger tout groupe fini Γ dans le groupe $\mathrm{GL}_n(k)$ avec $n = |\Gamma|$: il suffit d'identifier Γ à un sous-groupe du groupe symétrique $\mathfrak{S}_n$, puis de plonger $\mathfrak{S}_n$ dans $\mathrm{GL}_n(k)$ de manière usuelle : à une permutation σ correspond la matrice $m(\sigma)$ définie par $m(\sigma)e_i = e_{\sigma(i)}$ pour tout vecteur e_i de la base canonique de k^n.

Par ailleurs, tout sous-ensemble *fini* de $\mathrm{GL}_n(k)$ est défini par des équations polynomiales : il suffit de le vérifier pour un ensemble réduit à un point — car les parties de $\mathrm{GL}_n(k)$ définies par des équations polynomiales sont les fermés d'une topologie sur $\mathrm{GL}_n(k)$ (cf. 5.2.1) — auquel cas le résultat est trivial puisque $\{s\}$ est le lieu des zéros des n^2 polynômes $\mathrm{X}_{ij} - s_{ij}$. Vu la proposition 5.1.2, on déduit de cette discussion que l'on peut attacher à tout groupe fini Γ (plongé dans $\mathrm{GL}_n(k)$) un groupe algébrique G_Γ sur k tel que $\mathrm{G}_\Gamma(k) = \Gamma$.

Contrairement aux apparences, la construction précédente est intrinsèque : il suffit d'indexer les coefficients des matrices par les éléments de Γ, de sorte que la bigèbre du groupe G_Γ soit un quotient de l'anneau $k[(\mathrm{X}_{\gamma\gamma'})_{(\gamma,\gamma')\in\Gamma^2}, \mathrm{T}]/(\det(\mathrm{X}_{\gamma\gamma'})\mathrm{T}-1)$. Ceci dit, il s'avère que l'on peut donner une description plus agréable du groupe algébrique G_Γ (cf. Exercice 2, page 19). La k-algèbre des fonctions sur Γ à valeurs dans k est munie d'une structure de k-bigèbre comme suit : identifiant $k^\Gamma \otimes_k k^\Gamma$ et $k^{\Gamma\times\Gamma}$ via l'isomorphisme naturel

$$k^\Gamma \otimes_k k^\Gamma \to k^{\Gamma\times\Gamma}, \quad \sum a_i \otimes b_i \mapsto \sum a_i b_i,$$

on définit Δ, e^* et ι par les identités suivantes :

$$\Delta(f)(\gamma,\gamma') = f(\gamma\gamma'), \quad e^*(f)(\gamma) = \delta_{\gamma,e} \quad \text{et} \quad \iota^*(f)(\gamma) = f(\gamma^{-1}).$$

Proposition 5.1.10 — *L'application canonique*

$$\Gamma \to \underline{\Gamma}(k) = \mathrm{Hom}_{\mathbf{Alg}_k}(k^\Gamma, k), \quad \gamma \mapsto (f \mapsto f(\gamma))$$

est un isomorphisme de groupes.

Démonstration. L'injectivité est évidente.

Les fonctions caractéristiques $(\mathbf{1}_\gamma)_{\gamma\in\Gamma}$ constituent une base du k-espace vectoriel k^Γ et vérifient

$$\mathbf{1}_\gamma \mathbf{1}_{\gamma'} = \delta_{\gamma,\gamma'}\mathbf{1}_\gamma, \quad \sum_\gamma \mathbf{1}_\gamma = 1.$$

Par suite, pour tout homomorphisme de k-algèbres $u : k^\Gamma \to k$,

$$u(\mathbf{1}_\gamma)u(\mathbf{1}_{\gamma'}) = \delta_{\gamma,\gamma'}u(\mathbf{1}_\gamma) \quad \text{et} \quad \sum_\gamma u(\mathbf{1}_\gamma) = 1$$

et il existe donc un unique $\gamma \in \Gamma$ tel que $u(\mathbf{1}_\gamma) \neq 0$; on a alors $u(\mathbf{1}_\gamma) = 1$ et donc finalement $u(f) = f(\gamma)$ pour toute fonction $f \in k^\Gamma$.

Enfin, cette application est bien un homomorphisme de groupes puisque

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

pour tous $\gamma, \gamma' \in k^\Gamma$, $f \in k^\Gamma$. □

5.2. La variété d'un groupe algébrique

On vient de voir qu'il est intéressant de considérer les sous-ensembles de $\mathrm{GL}_n(k)$ définis par des équations polynomiales, c'est-à-dire de la forme

$$\{s \in \mathrm{GL}_n(k) \mid \underline{f}(s) = 0, \quad \forall f \in \mathfrak{I}\}$$

où $\mathfrak{I}$ est un idéal de la bigèbre A du groupe algébrique GL_n.

L'ensemble $\mathrm{GL}_n(k)$ s'identifie naturellement à l'ensemble $\mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A}, k)$ des homomorphismes de k-algèbres de A dans k. Étant donné $s \in \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A}, k)$, l'application $\mathrm{A}/\ker(\mathrm{s}) \hookrightarrow k$ induite par s est un isomorphisme puisque $s(\lambda) = \lambda$ pour tout $\lambda \in k$ par k-linéarité de s. Il découle de cette observation que

(i) le noyau de s est un idéal maximal de A ;

(ii) l'homomorphisme s est entièrement déterminé par son noyau $\ker(s)$, car s est le composé de la projection canonique $\mathrm{A} \to \mathrm{A}/\ker(s)$ par l'inverse de l'isomorphisme canonique $k \xrightarrow{\sim} \mathrm{A}/\ker(s)$.

Notons que les conditions $\underline{f}(s) = 0$ et $f \in \ker(s)$ sont tautologiquement équivalentes pour tous $f \in \mathrm{A}$, $s \in \mathrm{GL}_n(k)$.

Notant $\mathrm{Max}(\mathrm{A})$ l'ensemble des idéaux maximaux de A, nous obtenons ainsi une application *injective*

$$\mathrm{GL}_n(k) = \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A}, k) \to \mathrm{Max}(\mathrm{A}), \quad s \mapsto \ker(s) = \{f \in \mathrm{A} \mid \underline{f}(s) = 0\}.$$

Lorsque le corps k est algébriquement clos, cette application est surjective en vertu du Nullstellensatz ; en général, il convient de remplacer $\mathrm{GL}_n(k)$ par $\mathrm{Max}(\mathrm{A})$.

(5.2.1) Soit k un corps et soit A une k-algèbre de type fini. On désigne par $\mathrm{Max}(\mathrm{A})$ l'ensemble des idéaux maximaux de A. Étant donné un idéal $\mathfrak{I}$ de A, on désigne par $\mathrm{V}(\mathfrak{I})$ l'ensemble des idéaux maximaux $\mathfrak{m}$ de A contenant $\mathfrak{I}$ et on y pense comme le sous-ensemble de $\mathrm{Max}(\mathrm{A})$ défini par les équations $f = 0$, $f \in \mathfrak{I}$; ceci fait parfaitement sens si l'on définit $f(\mathfrak{m})$ comme l'image de f dans le corps quotient $\mathrm{A}/\mathfrak{m}$.

Proposition 5.2.1 — *Il existe une unique topologie sur* $\mathrm{Max}(\mathrm{A})$ *pour laquelle les parties fermées sont les sous-ensembles* $\mathrm{V}(\mathfrak{I})$ *de* $\mathrm{Max}(\mathrm{A})$ *associés aux idéaux* $\mathfrak{I}$ *de* A.

Démonstration. On a $\mathrm{V}(1) = \varnothing$ et $\mathrm{V}(0) = \mathrm{Max}(\mathrm{A})$. Si $\mathfrak{I}$ et $\mathfrak{J}$ sont deux idéaux de A, les conditions ($\mathfrak{I}\mathfrak{J} \subset \mathfrak{m}$) et ($\mathfrak{I} \subset \mathfrak{m}$ ou $\mathfrak{J} \subset \mathfrak{m}$) sont équivalentes (si $\mathfrak{I} \subsetneq \mathfrak{m}$ et $\mathfrak{J} \subsetneq \mathfrak{m}$, il existe $f \in \mathfrak{I}$ et $g \in \mathfrak{J}$ n'appartenant pas à $\mathfrak{m}$ et donc $fg \notin \mathfrak{m}$) ; par suite, $\mathrm{V}(\mathfrak{I}) \cup \mathrm{V}(\mathfrak{J}) = \mathrm{V}(\mathfrak{I}\mathfrak{J})$. Enfin, si $(\mathfrak{I}_\lambda)_{\lambda\in\Lambda}$ est une famille d'idéaux de A,

$$\bigcap_{\lambda\in\Lambda} \mathrm{V}(\mathfrak{I}_\lambda) = \mathrm{V}\left(\sum_{\lambda\in\Lambda} \mathfrak{I}_\lambda\right).$$

Nous venons de vérifier que les parties de $\mathrm{Max}(\mathrm{A})$ de la forme $\mathrm{V}(\mathfrak{I})$ satisfont aux conditions caractérisant les fermés d'un espace topologique. □

La topologie que l'on vient de définir est appelée *topologie de Zariski*.

Proposition 5.2.2 — *La correspondance* $\mathfrak{I} \mapsto \mathrm{V}(\mathfrak{I})$ *induit une bijection décroissante entre l'ensemble des idéaux de* A *égaux à leur racine et l'ensemble des parties fermées de* $\mathrm{Max}(\mathrm{A})$.

Les idéaux premiers *correspondent aux fermés non vides* Y *satisfaisant à la condition suivante : pour toute décomposition* $\mathrm{Y} = \mathrm{Y}_1 \cup \mathrm{Y}_2$ *de* Y *en la réunion de deux fermés non vides,* $\mathrm{Y} = \mathrm{Y}_1$ *ou* $\mathrm{Y} = \mathrm{Y}_2$.

Démonstration. La première assertion découle directement du fait que, pour tout idéal $\mathfrak{I}$ de A,

$$\bigcap_{\mathfrak{m}\in \mathrm{V}(\mathfrak{I})} \mathfrak{m} = \sqrt{\mathfrak{I}}$$

en vertu du Nullstellensatz (Appendice, 3).

Soit $\mathfrak{I}$ un idéal égal à sa racine et soit $\mathrm{Y} = \mathrm{V}(\mathfrak{I})$. Pour que $\mathfrak{I}$ soit premier, il faut et il suffit que $\mathfrak{I}$ soit un idéal propre de A satisfaisant à la condition suivante : $a \in \mathfrak{I}$ ou $b \in \mathfrak{I}$ pour tous $a, b \in \mathrm{A}$ tels que $ab \in \mathfrak{I}$. La non vacuité de $\mathrm{V}(\mathfrak{I})$ équivaut à la condition $\mathfrak{I} \subsetneq \mathrm{A}$ en vertu du théorème de Krull, tandis que la condition $\mathrm{V}(\mathfrak{I}) = \mathrm{V}(\mathfrak{I}_1) \cup \mathrm{V}(\mathfrak{I}_2) = \mathrm{V}(\mathfrak{I}_1\mathfrak{I}_2)$ se traduit par $\mathfrak{I} = \sqrt{\mathfrak{I}_1\mathfrak{I}_2}$. La première assertion permet de supposer $\mathfrak{I}_1$ et $\mathfrak{I}_2$ égaux à leur racine. Si $\mathrm{V}(\mathfrak{I}) \neq \mathrm{V}(\mathfrak{I}_1), \mathrm{V}(\mathfrak{I}_2)$, alors $\mathfrak{I} \subsetneq \mathfrak{I}_1,\ \mathfrak{I}_2$ et il existe donc $a \in \mathfrak{I}_1 - \mathfrak{I},\ b \in \mathfrak{I}_2 - \mathfrak{I}$; comme ab appartient à $\mathfrak{I}_1\mathfrak{I}_2 \subset \sqrt{\mathfrak{I}_1\mathfrak{I}_2} = \mathfrak{I}$, l'idéal $\mathfrak{I}$ n'est pas premier.

Si l'on suppose réciproquement que $\mathfrak{I}$ n'est pas premier et que l'on considère $a, b \in \mathrm{A} - \mathfrak{I}$ tels que $ab \in \mathfrak{I}$, alors $\mathrm{V}(\mathfrak{I}) = \mathrm{V}(\mathfrak{I} + \mathrm{A}a) \cup \mathrm{V}(\mathfrak{I} + \mathrm{A}b)$ et $\mathrm{V}(\mathfrak{I} + \mathrm{A}a), \mathrm{V}(\mathfrak{I} + \mathrm{A}b) \neq \mathrm{V}(\mathfrak{I})$. □

Les fermés de Max(A) associés aux idéaux *premiers* de A sont dits *irréductibles*. Il s'agit de manière équivalente des parties fermées non vides Y de Max(A) qui ne peuvent pas s'écrire comme réunion de deux fermés propres et non vides. Vu la proposition précédente, les fermés irréductibles maximaux (au sens de l'inclusion) sont précisément les parties de la forme $\mathrm{V}(\mathfrak{p})$, où $\mathfrak{p}$ est un idéal premier *minimal* de A ; il s'agit par définition des *composantes irréductibles* de Max(A).

Proposition 5.2.3 — *L'ensemble* $(\mathrm{Y}_i)_{i\in \mathrm{I}}$ *des composantes irréductibles de* Max(A) *est fini et*

$$\mathrm{Max}(\mathrm{A}) = \bigcup_{i\in \mathrm{I}} \mathrm{Y}_i.$$

Démonstration. Supposons que l'espace topologique $\mathrm{X} = \mathrm{Max}(\mathrm{A})$ ait une infinité de composantes irréductibles. Comme X n'est pas irréductible, il existe deux parties fermées propres Y_1 et Y_1' telles que $\mathrm{X} = \mathrm{Y}_1 \cup \mathrm{Y}_1'$; vu notre hypothèse, l'un au moins de ces fermés possède une infinité de composantes irréductibles. En itérant ce processus, on obtient une suite strictement décroissante $(\mathrm{Y}_n)_n$ de parties fermées de X. En vertu de la proposition précédente, chaque fermé Y_n s'écrit sous la forme $\mathrm{Y}_n = \mathrm{V}(\mathfrak{I}_n)$ pour un unique idéal $\mathfrak{I}_n$ de A égal à sa racine. La suite $(\mathfrak{I}_n)$ ainsi obtenue est strictement croissante ; comme A est une k-algèbre de type fini, c'est un anneau noethérien et nous aboutissons à une contradiction.

Il est d'autre part clair que Max(A) est la réunion de ses composantes irréductibles car tout idéal maximal contient un idéal premier minimal. □

Exemples 5.2.4 — 1. Si $\mathrm{A} = k[\mathrm{T}]$, les points de Max(A) sont en bijection avec les polynômes irréductibles unitaires dans $k[\mathrm{T}]$: à un tel polynôme $f \in k[\mathrm{T}]$ correspond l'idéal maximal (f). On identifie naturellement k à un sous-ensemble de Max(A) via l'application

$$k \to \mathrm{Max}(\mathrm{A}), \quad t \mapsto (\mathrm{T} - t).$$

La topologie induite sur k par celle de Max(A) se décrit aisément : les fermés sont les parties de la forme

$$\{t \in k \mid f(t) = 0, \ \ \forall f \in \mathfrak{I}\},$$

où $\mathfrak{I}$ est un idéal de $k[\mathrm{T}]$. Comme l'anneau $k[\mathrm{T}]$ est principal, il s'agit de manière équivalente des ensembles de racines d'un polynôme $f \in k[\mathrm{T}]$; outre les fermés triviaux k (correspondant à $f = 0$) et $\varnothing$ (pour $f = 1$), on obtient précisément tous les sous-ensembles *finis* de k. On constate sur cet exemple que la topologie de Zariski est par nature assez grossière. Notons

en outre que les fermés irréductibles de Max(A) sont les points et l'espace tout entier car les idéaux premiers de A sont les idéaux maximaux et l'idéal nul.

2. Considérons maintenant $\mathrm{A} = k[\mathrm{T}_1, \mathrm{T}_2]$ et supposons pour simplifier que le corps k soit algébriquement clos. Comme Max(A) s'identifie à k^2 en vertu du Nullstellensatz, cet ensemble Max(A) est le produit cartésien des ensembles $\mathrm{Max}(k[\mathrm{T}_1])$ et $\mathrm{Max}(k[\mathrm{T}_2])$. Toutefois, la topologie de Zariski sur k^2 n'est *pas* le produit des topologies de Zariski sur k : en effet, les parties fermés de cette dernière sont, outre k^2 et $\varnothing$, les réunions finies de parties de la forme $\{t_1\} \times k$, $k \times \{t_2\}$ ou $\{(t_1, t_2)\}$ avec $t_1, t_2 \in k$ tandis que, pour tout polynôme $f(\mathrm{T}_1, \mathrm{T}_2) \in k[\mathrm{T}_1, \mathrm{T}_2]$, l'ensemble $\{(t_1, t_2) \in k^2 \mid f(t_1, t_2) = 0\}$ est un fermé Zariski de k^2.

Il est aisé d'exhiber une base d'ouverts pour la topologie de Zariski sur Max(A).

Proposition 5.2.5 — *Les parties de* Max(A) *de la forme*

$$\mathrm{D}(f) = \{\mathfrak{m} \in \mathrm{Max(A)} \mid f \notin \mathfrak{m}\} = \mathrm{Max(A)} - \mathrm{V}(f)$$

sont des ouverts, dits principaux*, et constituent une base de la topologie de* Max(A).

Démonstration. Il est clair que les parties de Max(A) de la forme $\mathrm{D}(f)$ sont ouvertes. Tout ouvert U de Max(A) est de la forme $\mathrm{Max(A)} - \mathrm{V}(\mathfrak{I})$ pour un certain idéal $\mathfrak{I}$. On a alors

$$\begin{aligned} \mathrm{U} &= \{\mathfrak{m} \in \mathrm{Max(A)} \mid \mathfrak{I} \notin \mathfrak{m}\} \\ &= \{\mathfrak{m} \in \mathrm{Max(A)} \mid \exists f \in \mathfrak{I}, \quad f \notin \mathfrak{m}\} \\ &= \bigcup_{f \in \mathfrak{I}} \mathrm{D}(f) \end{aligned}$$

et U est donc bien une réunion d'ouverts principaux. □

Une conséquence immédiate de la proposition précédente est la *quasi compacité* de l'espace topologique Max(A).

Proposition 5.2.6 — *L'espace topologique* Max(A) *est* quasi compact *: tout recouvrement ouvert possède un sous-recouvrement fini.*

Démonstration. Vu la proposition précédente, il suffit de démontrer que tout recouvrement $(\mathrm{D}(f_i))_{i \in \mathrm{I}}$ de Max(A) par des ouverts principaux possède un sous-recouvrement fini. L'hypothèse $\mathrm{Max(A)} = \bigcup_{i \in \mathrm{I}} \mathrm{D}(f_i)$ signifie précisément qu'il existe, pour chaque idéal maximal $\mathfrak{m}$ de A, un indice $i \in \mathrm{I}$ tel que $f_i \notin \mathfrak{m}$; il revient au même de dire que l'idéal $\sum_{i \in \mathrm{I}} \mathrm{A} f_i$ engendré par les f_i n'est contenu dans *aucun* idéal maximal de A. Comme tout idéal propre de A est contenu dans un idéal maximal (théorème de Krull), ceci se traduit encore par la condition $\sum_{i \in \mathrm{I}} \mathrm{A} f_i = \mathrm{A}$ et on en déduit qu'il existe un sous-ensemble fini J de I tel que

$$1 = \sum_{i \in \mathrm{J}} a_i f_i$$

avec $a_i \in \mathrm{A}$. En vertu de ce qui précède, la condition $\sum_{i \in \mathrm{J}} \mathrm{A} f_i = \mathrm{A}$ que l'on vient d'obtenir est équivalente au fait que Max(A) soit recouvert par les ouverts principaux $\mathrm{D}(f_i)$, $i \in \mathrm{J}$, et nous avons ainsi extrait un sous-recouvrement fini de notre recouvrement initial. □

Remarque 5.2.7 — Comme le montre l'exemple 5.2.4, les ouverts de Max(A) sont en général trop gros pour que deux points distincts soient contenus dans deux ouverts disjoints et l'espace topologique Max(A) n'est donc généralement pas séparé. On dispose d'une condition de séparation plus faible : étant donnés deux points distincts $\mathfrak{m}, \mathfrak{m}' \in \mathrm{Max(A)}$, il existe un ouvert contenant l'un et non l'autre (il suffit de considérer un élément f de $\mathfrak{m}'$ n'appartenant pas à $\mathfrak{m}$: $\mathfrak{m} \in \mathrm{D}(f)$ et $\mathfrak{m}' \notin \mathrm{D}(f)$).

On peut démontrer que l'espace topologique Max(A) est séparé si et seulement si tous les idéaux premiers de A sont maximaux.

(5.2.2) Considérons deux k-algèbres de type fini A, B ainsi qu'un k-homomorphisme $\varphi : \mathrm{A} \to \mathrm{B}$. Pour tout idéal maximal $\mathfrak{m}$ de B, $\varphi^{-1}(\mathfrak{m})$ est un idéal maximal de A (cf. Appendice, 3, assertion (iii) du *Nullstellensatz*) et l'on dispose donc ainsi d'une application naturelle

$$^a\varphi : \mathrm{Max(B)} \to \mathrm{Max(A)}, \quad \mathfrak{m} \mapsto \varphi^{-1}(\mathfrak{m}).$$

Il est facile de voir qu'il s'agit d'une application *continue* : pour tout idéal $\mathfrak{I}$ de A,

$$\begin{aligned} (^a\varphi)^{-1}(\mathrm{V}(\mathfrak{I}) &= \{\mathfrak{m} \in \mathrm{Max(B)} \mid \mathfrak{I} \subset^a \varphi(\mathfrak{m})\} \\ &= \{\mathfrak{m} \in \mathrm{Max(B)} \mid \mathfrak{I} \subset \varphi^{-1}(\mathfrak{m})\} \\ &= \{\mathfrak{m} \in \mathrm{Max(B)} \mid \varphi(\mathfrak{I}) \subset \mathfrak{m}\} \\ &= \mathrm{V}(\varphi(\mathfrak{I})). \end{aligned}$$

(5.2.3) Si G est un groupe algébrique sur k de bigèbre A, on pose $|\mathrm{G}| = \mathrm{Max(A)}$; cet espace topologique est bien défini à un homéomorphisme près (deux bigèbres de G sont canoniquement isomorphes). Tout homomorphisme $f : \mathrm{G} \to \mathrm{H}$ entre deux groupes algébriques sur k induit naturellement une application continue $|f| : |\mathrm{G}| \to |\mathrm{H}|$.

Le groupe $\mathrm{G}(k)$ s'identifie natutellement au sous-ensemble de $|\mathrm{G}| = \mathrm{Max(A)}$ constitué des idéaux maximaux $\mathfrak{m}$ de A tels que $\mathrm{A}/\mathfrak{m} = k$.

Le groupe $\mathrm{G}(k)$ opère naturellement par homéomorphismes sur l'espace topologique $|\mathrm{G}|$: pour tout $s \in \mathrm{G}(k)$, l'application

$$\lambda_s : \mathrm{A} \to \mathrm{A}, \quad f \mapsto [\mathrm{mult} \circ (s \otimes \mathrm{id_A}) \circ \Delta](f)$$

est un automorphisme de k-algèbres induisant un homéomorphisme de $|\mathrm{G}|$. L'application induite sur le sous-ensemble $\mathrm{G}(k)$ de $|\mathrm{G}|$ n'est autre que la translation à gauche par s en vertu de l'identité

$$\underline{f}(st) = \underline{\lambda_s(f)}(t)$$

pour tous $t \in \mathrm{G}(k)$, $f \in \mathrm{A}$.

5.3. Connexité

Intéressons-nous maintenant à la connexité de l'espace topologique Max(A).

(5.3.1) Dans ce paragraphe, A désigne toujours une algèbre de type fini sur un corps k.

Proposition 5.3.1 — *L'espace topologique* Max(A) *n'a qu'un nombre fini de composantes connexes.*

Démonstration. La démonstration de la proposition 5.2.3 se transcrit mot pour mot en remplaçant « composante irréductible » par « composante connexe ». □

Corollaire 5.3.2 — *Les composantes connexes de l'espace topologique* Max(A) *sont ses parties ouvertes et fermées minimales.*

Rappelons qu'un élément e de A est dit *idempotent* si $e^2 = e$. Il est clair que 1 et 0 sont idempotents, et on dit que A n'a pas d'idempotent non trivial si ce sont les seuls.

Proposition 5.3.3 — *La correspondance* $e \mapsto \mathrm{D}(e)$ *réalise une bijection entre l'ensemble des éléments idempotents de* A *et l'ensemble des parties ouvertes et fermées de* Max(A).

Démonstration. Soit e un élément idempotent de A. Vu l'identité $e(e-1) = 0$, chaque idéal maximal $\mathfrak{m}$ de A contient e ou $1 - e$; en outre, comme $1 = e + (1 - e)$, $\mathfrak{m}$ ne peut contenir simultanément e et $e - 1$. On a donc

$$\mathrm{D}(e) = \mathrm{V}(e-1) \quad \text{et} \quad \mathrm{Max(A)} = \mathrm{D}(e) \sqcup \mathrm{V}(e) = \mathrm{D}(e) \sqcup \mathrm{D}(1-e) = \mathrm{V}(1-e) \sqcup \mathrm{V}(e),$$

ce qui montre que $\mathrm{D}(e)$ est une partie ouverte et fermée de Max(A).

Supposons que e et e' soient deux éléments idempotents de A tels que $\mathrm{D}(e) = \mathrm{D}(e')$. On a également $\mathrm{V}(e) = \mathrm{V}(e')$, ce qui signifie que les idéaux $\mathrm{A}e$ et $\mathrm{A}e'$ ont la même racine ; il existe donc un entier naturel $n \geqslant 0$ tel que $e^n \in \mathrm{A}e'$ et $e'^n \in \mathrm{A}e$, soit encore $e^n = ae'$ et $e'^n = be$ avec $a, b \in \mathrm{A}$. Comme $e^2 = e$ et $e'^2 = e'$, il vient $e = ae'$ et $e' = be$, puis

$$e = ae'^2 = (ae')(be) = abee' \quad \text{et} \quad e' = be^2 = (be)(ae') = abee'$$

et donc $e = e'$.

Considérons enfin une partie ouverte et fermée Ω de $\mathrm{Max}(\mathrm{A})$. Il existe par hypothèse deux idéaux $\mathfrak{I}$ et $\mathfrak{J}$ de A tels que $\Omega = \mathrm{V}(\mathfrak{I}) = \mathrm{Max}(\mathrm{A}) - \mathrm{V}(\mathfrak{J})$. Les conditions $\mathrm{V}(\mathfrak{I}\mathfrak{J}) = \mathrm{V}(\mathfrak{I}) \cup \mathrm{V}(\mathfrak{J}) = \mathrm{Max}(\mathrm{A})$ et $\mathrm{V}(\mathfrak{I} + \mathfrak{J}) = \mathrm{V}(\mathfrak{I}) \cap \mathrm{V}(\mathfrak{J}) = \varnothing$ sont respectivement équivalentes aux conditions

$$\mathfrak{I}\mathfrak{J} \subset \mathrm{Nil}(\mathrm{A}) \quad \text{et} \quad \mathfrak{I} + \mathfrak{J} = \mathrm{A}.$$

On en déduit que l'on peut écrire 1 sous la forme $1 = a + b$ avec $a \in \mathfrak{I}$, $b \in \mathfrak{J}$ et $ab \in \mathrm{Nil}(\mathrm{A})$. Choisissons en entier naturel $n \geqslant 0$ tel que $(ab)^n = 0$ et élevons l'identité $a + b = 1$ à la puissance $2n$ pour obtenir $a^n u + b^n v = 1$. Posant alors $e = b^n v$, on obtient $e(1-e) = a^n u b^n v = 0$ et donc e est idempotent. On a par ailleurs $\mathrm{A}e \subset \mathrm{A}b \subset \mathfrak{J}$ et $\mathrm{A}(1-e) \subset \mathrm{A}a \subset \mathfrak{I}$, d'où $\mathrm{V}(\mathfrak{J}) \subset \mathrm{V}(e)$ et $\mathrm{V}(\mathfrak{I}) \subset \mathrm{V}(1-e)$ puis

$$\mathrm{Max}(\mathrm{A}) = \mathrm{V}(\mathfrak{I}) \sqcup \mathrm{V}(\mathfrak{J}) = \mathrm{V}(e) \sqcup \mathrm{V}(1-e)$$

et donc, finalement, $\mathrm{D}(e) = \mathrm{V}(1-e) = \mathrm{V}(\mathfrak{I}) = \Omega$. □

Corollaire 5.3.4 — *Pour que l'espace topologique* $\mathrm{Max}(\mathrm{A})$ *soit connexe, il faut et il suffit que l'anneau* A *ne possède pas d'élément idempotent non trivial.*

Un élément idempotent e de A est dit *primitif* si $\mathrm{D}(e)$ est une composante connexe de $\mathrm{Max}(\mathrm{A})$. Noter que, si $\mathrm{A} \neq 0$, alors 0 n'est pas un idempotent primitif puisque $\mathrm{D}(0) = \varnothing$.

Lemme 5.3.5 — *Soit* $(e_i)_{i\in\mathrm{I}}$ *l'ensemble des idempotent primitifs de* A. *L'application*

$$\mathrm{A} \prod_{i\in\mathrm{I}} \mathrm{A}e_i, \quad a \mapsto (ae_i)_{i\in\mathrm{I}}$$

est un isomorphisme d'anneaux.

Démonstration. Les ouverts $\mathrm{D}(e_i)_{i\in\mathrm{I}}$ forment par hypothèse une partition de $\mathrm{Max}(\mathrm{A})$.

- La condition $\mathrm{Max}(\mathrm{A}) = \bigcup_{i\in\mathrm{I}} \mathrm{D}(e_i)$ équivaut à $\sum_{i\in\mathrm{I}} \mathrm{A}e_i = \mathrm{A}$.
- Si $i \neq j$, la condition $\mathrm{D}(e_i) \cap \mathrm{D}(e_j) = \varnothing$ équivaut à $e_i e_j \in \mathrm{Nil}(\mathrm{A})$, soit encore $e_i e_j = 0$ puisque $(e_i e_j)^2 = e_i e_j$.

Le premier point permet d'écrire 1 sous la forme $1 = \sum_{i\in\mathrm{I}} a_i e_i$ avec $a_i \in \mathrm{A}$ et le second fournit les identités $e_i = a_i e_i^2 = a_i$ pour tout $i \in \mathrm{I}$. On obtient ainsi $1 = \sum_{i\in\mathrm{I}} e_i^2 = \sum_{i\in\mathrm{I}} e_i$, et il est immédiat d'en déduire que l'application

$$\mathrm{A} \to \prod_{i\in\mathrm{I}} \mathrm{A}e_i, \quad a \mapsto (ae_i)_{i\in\mathrm{I}}$$

est bijective. □

Exemple 5.3.6 — L'équation $e(e-1) = 0$ n'a que les deux solutions évidentes $e = 0$ et $e = 1$ si l'anneau A est *intègre*, de sorte que $\mathrm{Max}(\mathrm{A})$ est alors connexe. Cette observation permet souvent de démontrer la connexité de $\mathrm{Max}(\mathrm{A})$: il suffit de prouver que A est un anneau intègre. Cette condition n'est toutefois pas nécessaire : par exemple, si p est un nombre premier, l'anneau $\mathrm{A} = \mathbb{F}_p[\mathrm{T}]/(\mathrm{T}^p - 1)$ n'est pas intègre mais $\mathrm{Max}(\mathrm{A})$ est connexe car cet ensemble est réduit à l'unique idéal maximal de A.

Remarque 5.3.7 — Soit A une k-algèbre de type fini et soit $\overline{k}/k$ une clôture algébrique de k. En général, $\mathrm{Max}(\mathrm{A})$ peut être connexe sans que $\mathrm{Max}(\mathrm{A} \otimes_k \overline{k})$ ne le soit. Il n'est pas difficile de

donner un exemple : si $k = \mathbb{Q}$ et $\mathrm{A} = \mathbb{Q}[\mathrm{X}]/(\mathrm{X}^2+1)$, alors $\mathrm{Max}(\mathrm{A})$ est connexe car l'anneau A est intègre mais $\mathrm{Max}(\mathrm{A} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}})$ n'est pas connexe car l'anneau

$$\mathrm{A} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \cong \overline{\mathbb{Q}}[\mathrm{X}]/(\mathrm{X}^2+1) \cong \overline{\mathbb{Q}} \times \overline{\mathbb{Q}}$$

contient un idempotent non trivial, par exemple l'élément $(1,0)$ de $\overline{\mathbb{Q}} \times \overline{\mathbb{Q}}$ (correspondant à l'élément $\frac{-1}{2}\mathrm{X} \otimes i + \frac{1}{2}1 \otimes 1$ de $\mathrm{A} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$).

Toutefois, si $\mathrm{Max}(\mathrm{A})$ est connexe, l'existence d'un homomorphisme de k-algèbres $s : \mathrm{A} \to k$ suffit à garantir la connexité de $\mathrm{A} \otimes_k \overline{k}$. En effet, l'application naturelle $p : \mathrm{Max}(\mathrm{A} \otimes_k \overline{k}) \to \mathrm{Max}(\mathrm{A})$ envoie chaque composante connexe de $\mathrm{Max}(\mathrm{A} \otimes_k \overline{k})$ *surjectivement* sur $\mathrm{Max}(\mathrm{A})$ (cf. Appendice, 3) et sa fibre au-dessus d'un idéal maximal $\mathfrak{m}$ de A est en bijection avec l'ensemble des k-plongements du corps $\mathrm{A}/\mathfrak{m}$ dans $\overline{k}$ (idem). Comme $\mathrm{A}/\ker(s) = k$, il y a un *unique* point dans $\mathrm{Max}(\mathrm{A} \otimes_k \overline{k})$ au-dessus de s et l'espace topologique $\mathrm{Max}(\mathrm{A} \otimes_k \overline{k})$ est donc connexe.

(5.3.2) Considérons maintenant un groupe algébrique G sur k et désignons par A sa bigèbre. La counité $e^* : \mathrm{A} \to k$ permet d'isoler canoniquement un idempotent primitif dans A.

Proposition 5.3.8 — *(i) Il existe un unique idempotent primitif $e_0 \in \mathrm{A}$ tel que $e^*(e_0) = 1$. (ii) Le quotient de* A *par l'idéal $\mathfrak{I}_0 = \{a \in \mathrm{A} \mid ae_0 = 0\}$ est la bigèbre d'un sous-groupe* G^0 *de* G *tel que $|\mathrm{G}^0|$ soit la composante connexe $\mathrm{D}(e_0)$ de $|\mathrm{G}|$. Ce sous-groupe est la* composante neutre *de* G.

Démonstration. (i) Notons $(e_i)_{i\in\mathrm{I}}$ l'ensemble des idempotents primitifs de A. Leurs images par l'homomorphisme $e^* : \mathrm{A} \to k$ sont des idempotents de k tels que $e^*(e_i)e^*(e_j) = 0$ pour tous $i \neq j$ et $1 = \sum_{i\in\mathrm{I}} e^*(e_i)$. Utilisant le fait que k est un anneau intègre, il existe un unique indice $i \in \mathrm{I}$ tel que $e^*(e_i) = 1$ et $e^*(e_j) = 0$ pour tout $j \in \mathrm{I} - \{i\}$.

(ii) Notons p la projection canonique de A sur $\mathrm{A}/\mathfrak{I}_O$ et soit Δ la comultiplication de A. La décomposition $\mathrm{A} \cong \prod_{i\in\mathrm{I}} \mathrm{A}e_i$ induit une décomposition de $\mathrm{A} \otimes_k \mathrm{A}$ sous la forme

$$\mathrm{A} \otimes_k \mathrm{A} \cong \prod_{(i,j)\in\mathrm{I}^2} \mathrm{A}e_i \otimes e_j.$$

Étant donné $f \in \mathfrak{I}_0$, $\Delta(f)$ s'écrit sous la forme $\Delta(f) = a_{0,0}e_0 \otimes e_0 + \sum_{(i,j)\neq(0,0)} a_{ij}e_i \otimes e_j$; l'identité $[\mathrm{mult} \circ (\mathrm{id}_\mathrm{A} \otimes e^*) \circ \Delta] = \mathrm{id}_\mathrm{A}$ implique alors

$$f = a_{00}e_0 + \sum_{(i,j)\neq(0,0)} a_{ij}e_i e^*(e_j) = a_{0,0}e_0 + \sum_{i\in\mathrm{I}-\{0\}} a_{i0}e_i$$

et donc

$$a_{00} = fe_0 = 0.$$

Ce calcul établit l'inclusion $\Delta(\mathfrak{I}_0) \subset \mathfrak{I}_0 \otimes_k \mathrm{A} + \mathrm{A} \otimes_k \mathfrak{I}_0$, de laquelle on déduit que Δ induit une application k-linéaire $\overline{\Delta} : \mathrm{A}/\mathfrak{I}_0 \to (\mathrm{A}/\mathfrak{I}_0) \otimes (\mathrm{A}/\mathfrak{I}_0)$ telle que $\overline{\Delta} \circ p = (p \otimes p) \circ \Delta$. La fin de la démonstration est la même que pour la proposition 5.1.2.

L'idéal $\mathfrak{I}_0$ définissant le sous-groupe G_0 est par construction tel que $|\mathrm{G}^0| = \mathrm{V}(\mathfrak{I}_0) = \mathrm{D}(e_0)$. □

Définition 5.3.9 — *Un groupe algébrique* G *sur un corps k est dit* connexe *si l'espace topologique $|\mathrm{G}|$ est connexe ; il revient au même de dire que* G *coïncide avec sa composante neutre* G^0.

Nous terminons ce paragraphe en comparant la connexité d'un sous-groupe de $\mathrm{GL}_n(k)$ et celle du groupe algébrique qui lui est associé (cf. 5.1.1).

Proposition 5.3.10 — *Soit Γ un sous-groupe de $\mathrm{GL}_n(k)$. Pour que le groupe algébrique G_Γ soit connexe, il faut et il suffit que Γ soit une partie connexe de $\mathrm{GL}_n(k)$. En particulier : Γ est connexe si et seulement si son adhérence $\overline{\Gamma}$ est connexe.*

Démonstration. La bigèbre B du groupe G_Γ est par définition le quotient de la bigèbre A de GL_n par l'idéal $\mathfrak{I}$ des $f \in \mathrm{A}$ s'annulant identiquement sur Γ. Si G_Γ n'est pas connexe, l'anneau B contient un idempotent non trivial e. Choisissant un élément $\tilde{e}$ de A relevant e, l'identité $e(e-1)=0$ se traduit par $\tilde{e}(\tilde{e}-1) \in \mathfrak{I}$ et donc $\underline{\tilde{e}}(s)=0$ ou $\overline{\tilde{e}(s)}=1$ pour tout $s \in \Gamma$. En outre, aucune des fonctions $\underline{\tilde{e}}$ et $\underline{\tilde{e}}-1$ n'est identiquement nulle sur Γ car sinon $\tilde{e} \in \mathfrak{I}$ ou $\tilde{e}-1 \in \mathfrak{I}$ (par définition de $\mathfrak{I}$) et donc $e=0$ ou $e-1=0$. On obtient par conséquent une décomposition

$$\Gamma = \Gamma \cap \{\underline{e}=0\} \sqcup \Gamma \cap \{\underline{e}=1\}$$

de Γ en la réunion de deux parties fermées disjointes, ce qui montre que Γ n'est pas connexe.

Supposons réciproquement que Γ ne soit pas connexe et considérons deux fermés propres $\mathrm{Y}_1,\ \mathrm{Y}_2$ de Γ tels que $\Gamma = \mathrm{Y}_1 \sqcup \mathrm{Y}_2$. On a $\mathrm{Y}_1 = \mathrm{V}(\mathfrak{I}_1) \cap \mathrm{GL}_n(k)$ et $\mathrm{Y}_2 = \mathrm{V}(\mathfrak{I}_2) \cap \mathrm{GL}_n(k)$ avec deux idéaux $\mathfrak{I}_1$ et $\mathfrak{I}_2$ de A égaux à leur racine. Les inclusions $\mathfrak{I} \subset \mathfrak{I}_1$ et $\mathfrak{I} \subset \mathfrak{I}_2$ sont strictes, de sorte qu'il existe des éléments f_1 et f_2 de A ne s'annulant pas identiquement sur Γ tels que $\underline{f_1 f_2}_{|\Gamma} = 0$. Par définition de l'idéal $\mathfrak{I}$, cette dernière condition équivaut à $f_1 f_2 \in \mathfrak{I}$ et l'anneau $\mathrm{A}/\mathfrak{I}$ n'est donc pas intègre ; comme cet anneau est par construction réduit, il en découle que l'espace topologique $\mathrm{Max}(\mathrm{A})$ admet au moins deux composantes irréductibles distinctes. Dans ces conditions, la conclusion découle du lemme suivant. □

Lemme 5.3.11 — *Soit* G *un groupe algébrique sur un corps k. Si* G *est connexe, l'espace topologique* $|\mathrm{G}|$ *est irréductible.*

Démonstration. Supposons que l'espace topologique $|\mathrm{G}|$ soit réductible. Les composantes irréductibles de $|\mathrm{G}|$ étant fermées, elles ne peuvent être mutuellement disjointes si $|\mathrm{G}|$ est connexe et il existe alors deux composantes irréductibles distinctes Y et Y′ telles que $\mathrm{Y} \cap \mathrm{Y}' \neq \varnothing$.

La fin de la démonstration consiste à justifier qu'une telle situation est impossible : les points de $\mathrm{Y} \cap \mathrm{Y}'$ sont trop « singuliers » pour ne pas violer l'« homogénéité » de $|\mathrm{G}|$.

Il est facile de donner un sens précis à cette idée sous les hypothèses additionnelles suivantes :
- $\mathrm{Y} \cap \mathrm{Y}'$ contient un point de $\mathrm{G}(k)$;
- il existe un point de $\mathrm{G}(k)$ n'appartenant qu'à une seule composante irréductible de $|\mathrm{G}|$.

En effet, l'action de $\mathrm{G}(k)$ par translation à gauche sur l'espace topologique $|\mathrm{G}|$ permute ses composantes irréductibles ; si s est un élément de $\mathrm{G}(k)$ appartenant à $\mathrm{Y} \cap \mathrm{Y}'$, alors tout élément $t=(ts^{-1})s$ de $\mathrm{G}(k)$ appartient aux deux composantes irréductibles distinctes $(ts^{-1})\mathrm{Y}$ et $(ts^{-1})\mathrm{Y}'$ de $|\mathrm{G}|$.

Le cas général se traite en remplaçant k par une clôture algébrique $\overline{k}$ et en considérant l'application naturelle $p : |\mathrm{G} \otimes_k \overline{k}| \to |\mathrm{G}|$, continue et surjective (cf. Appendice, 3) :
- si l'espace topologique $|\mathrm{G}|$ n'est pas irréductible, il en est de même de $|\mathrm{G} \otimes_k \overline{k}|$: étant donnés deux fermés propres Y et Y′ recouvrant $|\mathrm{G}|$, alors $p^{-1}(\mathrm{Y})$ et $p^{-1}(\mathrm{Y}')$ sont deux fermés propres recouvrant $|\mathrm{G} \otimes_k \overline{k}|$;
- le corps $\overline{k}$ étant algébriquement clos, $|\mathrm{G} \otimes_k \overline{k}|$ coïncide avec $\mathrm{G}(\overline{k})$ et les deux conditions introduites précédemment sont donc remplies.

Vu ce qui précède, il en découle de ces deux observations que le groupe $\mathrm{G} \otimes_k \overline{k}$ n'est pas connexe ; cette conclusion vaut *a fortiori* pour le groupe G en vertu de la remarque 5.3.7. □

5.4. Exemples

(5.4.1) (i) Le groupe $\mathbb{G}_\mathrm{a}$ est connexe car sa bigèbre $k[\mathrm{T}]$ est un anneau intègre.

(ii) Pour tout $n \geqslant 0$, le groupe GL_n est connexe car sa bigèbre est un anneau intègre (Lemme 5.1.1).

(iii) Pour toute k-algèbre R, l'application

$$\mathrm{GL}_n(\mathrm{R}) \to \mathrm{SL}_n(\mathrm{R}) \times \mathbb{G}_\mathrm{m}(\mathrm{R}), \quad g \mapsto (\det(g)^{-1}g, \det(g))$$

est une bijection fonctorielle. On a ainsi défini un isomorphisme de foncteurs en ensembles

$$\mathrm{h}_{\mathrm{B}\otimes_k k[\mathrm{X},\mathrm{X}^{-1}]} \xrightarrow{\sim} \mathrm{h}_\mathrm{A} \ ,$$

où A et B sont les bigèbres respectives de GL_n et de SL_n. Via le lemme de Yoneda, on en déduit que les k-algèbres A et $\mathrm{B}[\mathrm{X}, \mathrm{X}^{-1}]$ sont isomorphes. Comme A est un anneau intègre, il en est de même pour l'anneau B et nous avons ainsi établi la connexité du groupe SL_n.

(iii) Soit $n \geqslant 2$ un entier naturel écrit sous la forme $n = p^\alpha m$, où p est la caractéristique du corps k et m est premier à p ; si k est de caractéristique nulle, alors $m = n$. Pour que le groupe algébrique μ_n soit connexe, il faut et il suffit que l'on ait $m \geqslant 2$. La bigèbre de ce groupe est en effet l'anneau $k[\mathrm{X}]/(\mathrm{X}^n - 1)$ dont les idéaux maximaux correspondent biunivoquement aux facteurs irréductibles de $\mathrm{X}^n - 1$ dans $k[\mathrm{X}]$; l'espace topologique discret Max(A est donc connexe si et seulement si $\mathrm{X}^n - 1 = (\mathrm{X} - 1)^n$.

(5.4.2) *Connexité de* GL_n — Nous allons donner une autre démonstration de la connexité du groupe algébrique GL_n reposant sur la *décomposition de Bruhat.*

Considérons les sous-groupes algébriques suivants de GL_n : T est le sous-groupe des matrices diagonales, B le sous-groupe des matrices triangulaires supérieures et U le sous-groupe des matrices triangulaires supérieures à diagonale identité. On désigne en outre par W le sous-groupe de $\mathrm{SL}_n(k)$ image de l'homomorphisme

$$\mathfrak{S}_n \to \mathrm{GL}_n(k), \quad \sigma \mapsto m(\sigma),$$

où $m(\sigma)$ est la matrice de permutation définie par $m(\sigma)e_i = e_{\sigma(i)}$ pour tout vecteur e_i de la base canonique de k^n.

Exemple — Si $n = 2$, W est constitué des matrices

$$m(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad m(1,2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Si $n = 3$, W est constitué des matrices

$$m(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ m(1,2) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ m(1,3) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \ m(2,3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

et

$$m(1,2,3) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad m(1,3,2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Proposition 5.4.1 — *Tout élément g de $\mathrm{GL}_n(k)$ s'écrit sous la forme*

$$g = um(\sigma)b$$

avec $u \in \mathrm{U}(k)$, $b \in \mathrm{B}(k)$ et $\sigma \in \mathfrak{S}_n$. La permutation σ est uniquement déterminée par cette condition et peut être décrite comme suit : pour tout $i \in \{1, \ldots, n\}$, $\sigma(i)$ est le plus grand $j \in \{1, \ldots, n\}$ tel que le déterminant mineur

$$\begin{vmatrix} g_{\sigma(1)1} & g_{\sigma(1)2} & \cdots & g_{\sigma(1)i} \\ g_{\sigma(2)1} & g_{\sigma(2)2} & \cdots & g_{\sigma(2)i} \\ \vdots & \vdots & \vdots & \vdots \\ g_{j1} & g_{j2} & \cdots & g_{ji} \end{vmatrix}$$

soit non nul.

Démonstration. Pour tous $i, j \in \{1, \dots, n\}$ avec $i < j$ et tout $\lambda \in k$, notons $u_{ij}(\lambda)$ l'élément de $\mathrm{U}(k)$ défini par

$$u_{ij}(\lambda)e_\ell = e_\ell + \delta_{j\ell}\lambda e_j.$$

Quelle que soit la matrice $g \in \mathrm{SL}_n(k)$, $u_{ij}(\lambda)g$ (resp. $gu_{ij}(\lambda)$) se déduit de g en remplaçant la ligne i par la combinaison linéaire (ligne i) $+ \lambda$(ligne j) (resp. la colonne j par la combinaison linéaire (colonne j) $+ \lambda$(colonne i)).

Soit $\sigma(1)$ le plus grand élément de $\{1, \dots, n\}$ tel que $g_{\sigma(1)1} \neq 0$. Utilisant ce coefficient comme pivot, il existe $u_1 \in \mathrm{U}(k)$ et $b_1 \in \mathrm{B}(k)$ tels la matrice $g_1 = u_1 g b_1$ vérifie les conditions suivantes :

$$(g_1)_{\alpha 1} = \delta_{\sigma(1)\alpha} \quad \text{et} \quad (g_1)_{\sigma(1)\beta} = \delta_{1\beta}$$

pour tous $\alpha, \beta \in \{1, \dots, n\}$.

On définit alors $\sigma(2)$ comme le plus grand élément de $\{1, \dots, n\}$ tel que $(g_1)_{\sigma(2)2} \neq 0$; noter que $\sigma(2)$ est distinct de $\sigma(1)$ puisque $(g_1)_{\sigma(1)2} = 0$. On obtient de nouveau par pivot des matrices $u_2 \in \mathrm{U}(k)$ et $b_2 \in \mathrm{B}(k)$ telles que les deux premières colonnes de la matrice $g_2 = u_2 g_1 b_2$ coïncident avec celles d'une matrice de permutation envoyant 1 sur $\sigma(1)$ et 2 sur $\sigma(2)$. Itérant ce processus, on définit de proche en proche une permutation σ de $\{1, \dots, n\}$ et on aboutit finalement à des matrices $u^{-1} = u_n \dots u_2 u_1 \in \mathrm{U}(k)$ et $b^{-1} = b_1 b_2 \dots b_n \in \mathrm{B}(k)$ telles que $g = um(\sigma)b$. Il est clair que la permutation σ obtenue par ce procédé est celle décrite dans l'énoncé.

Finalement, si σ et τ sont deux permutations telles que $um(\sigma) = m(\tau)b$ avec $u \in \mathrm{U}(k)$ et $b \in \mathrm{B}(k)$, alors $b = m(\tau^{-1})um(\sigma)$; cette matrice se déduisant de u en permutant les colonnes selon σ et les lignes selon τ, $b_{ij} = u_{\tau(i)\sigma(j)}$ pour tous $i, j \in \{1, \dots, n\}$. En particulier, $u_{\tau(i)\sigma(i)} \neq 0$ pour tout i, donc $\tau(i) \leqslant \sigma(i)$ et finalement $\tau = \sigma$. □

Pour toute permutation $\sigma \in \mathfrak{S}_n$, on désigne par $\Omega(\sigma)$ le sous-ensemble de $\mathrm{GL}_n(k)$ formé des éléments g s'écrivant sous la forme $g = um(\sigma)b$ avec $u \in \mathrm{U}(k)$ et $b \in \mathrm{B}(k)$.

Corollaire 5.4.2 — *L'ensemble $\Omega(\sigma)$ est une partie localement fermée non vide et connexe de $\mathrm{GL}_n(k)$ pour toute permutation $\sigma \in \mathfrak{S}_n$. Si σ_0 désigne la permutation $(1, n)(2, n-1)\dots$, alors $\Omega(\sigma_0)$ est une partie ouverte de $\mathrm{GL}_n(k)$.*

Démonstration. Vu la proposition précédente, $\Omega(\sigma)$ est le sous-ensemble de $\mathrm{GL}_n(k)$ défini par les conditions suivantes :

$$\begin{vmatrix} \mathrm{X}_{\sigma(1)1} & \mathrm{X}_{\sigma(1)2} & \dots & \mathrm{X}_{\sigma(1)m} \\ \mathrm{X}_{\sigma(2)1} & \mathrm{X}_{\sigma(2)2} & \dots & \mathrm{X}_{\sigma(2)m} \\ \vdots & \vdots & & \vdots \\ \mathrm{X}_{j1} & \mathrm{X}_{j2} & \dots & \mathrm{X}_{jm} \end{vmatrix} = 0 \quad (m \in \{1, \dots, n\}, \quad j > \sigma(m))$$

et

$$\begin{vmatrix} \mathrm{X}_{\sigma(1)1} & \mathrm{X}_{\sigma(1)2} & \dots & \mathrm{X}_{\sigma(1)m} \\ \mathrm{X}_{\sigma(2)1} & \mathrm{X}_{\sigma(2)2} & \dots & \mathrm{X}_{\sigma(2)m} \\ \vdots & \vdots & & \vdots \\ \mathrm{X}_{j1} & \mathrm{X}_{\sigma(m)2} & \dots & \mathrm{X}_{\sigma(m)m} \end{vmatrix} \neq 0 \quad (m \in \{1, \dots, m\}).$$

Ainsi $\Omega(\sigma)$ est-elle une partie localement fermée de $\mathrm{GL}_n(k)$, non vide puisque contenant $m(\sigma)$.

La connexité de $\Omega(\sigma)$ se déduit immédiatement du fait qu'il s'agit de l'image de l'espace connexe $\mathrm{U}(k) \times \mathrm{B}(k)$ par l'application continue

$$\mathrm{U}(k) \times \mathrm{B}(k) \to \mathrm{GL}_n(k), \quad (u, b) \mapsto um(\sigma)b.$$

La permutation σ_0, correspondant à la matrice

$$m(\sigma_0) = \begin{pmatrix} 0 & 0 & \dots & 1 \\ \vdots & \vdots & & 0 \\ 0 & 1 & \dots & 0 \\ 1 & 0 & \dots & 0 \end{pmatrix},$$

est telle que $\sigma_0(1) = n$, $\sigma_0(2) = n-1, \dots, \sigma_0(n) = 1$. Le sous-ensemble $\Omega(\sigma_0)$ est par suite défini par les n conditions suivantes :

$$\begin{vmatrix} \mathrm{X}_{\sigma(1)1} & \mathrm{X}_{\sigma(1)2} & \dots & \mathrm{X}_{\sigma(1)m} \\ \mathrm{X}_{\sigma(2)1} & \mathrm{X}_{\sigma(2)2} & \dots & \mathrm{X}_{\sigma(2)m} \\ \vdots & \vdots & & \vdots \\ \mathrm{X}_{\sigma(m)1} & \mathrm{X}_{\sigma(m)2} & \dots & \mathrm{X}_{\sigma(m)m} \end{vmatrix} \neq 0 \quad (1 \leqslant m \leqslant n)$$

et il s'agit donc d'une partie ouverte de $\mathrm{GL}_n(k)$. □

Corollaire 5.4.3 — *Le groupe algébrique* GL_n *est connexe.*

Démonstration. Étant donnée une matrice $g \in \mathrm{GL}_n(k)$, une permutation de ses colonnes permet d'obtenir une matrice appartenant à $\Omega(\sigma_0)$; par suite,

$$\mathrm{GL}_n(k) = \bigcup_{\tau \in \mathfrak{S}_n} \Omega(\sigma_0) m(\tau).$$

Si le corps k est algébriquement clos, on construit aisément une matrice appartenant simultanément aux ouverts $\Omega(\sigma_0)m(\tau)$ et $\Omega(\sigma_0)$. La connexité de $\mathrm{GL}_n(k)$ s'en déduit alors immédiatement puisque toute réunion de parties connexes deux à deux non disjointes est connexe. En général, cet argument fournit la connexité de $\mathrm{GL}_n(\overline{k})$, où $\overline{k}$ est une clôture algébrique de k, et la connexité du groupe algébrique GL_n s'en déduit par application de la proposition 5.3.10. □

Exercices **1.** Justifier avec soin l'assertion suivante : si le corps k est *infini*, l'ouvert $\Omega(\sigma_0) \cap \Omega(\sigma_0)m(\tau)$ de $\mathrm{GL}_n(k)$ est non vide. (*Indication* : on pourra rechercher une matrice appartenant à cet ouvert sous la forme $\lambda m(\sigma_0) + \mu m(\sigma_0\tau)$ avec $\lambda, \mu \in k$).

2. On peut aisément adapter les arguments qui précèdent pour démontrer que le groupe SL_n est connexe.

(i) Quelle que soit la permutation $\sigma \in \mathfrak{S}_n$, démontrer que $\Omega(\tau) \cap \mathrm{SL}_n$ est une partie localement fermée connexe et non vide de $\mathrm{GL}_n(k)$. (*Indication* : examiner séparément le cas d'une permutation paire et celui d'une permutation impaire ; dans le second cas, on pourra faire intervenir la matrice $\chi = \mathrm{diag}(-1, 1, \dots, 1)$ appartenant à $\mathrm{B}(k)$.)

(ii) Montrer que $\Omega(\sigma_0) \cap \Omega(\sigma_0)m(\tau)$ rencontre $\mathrm{SL}_n(k)$ pour toute permutation τ. En conclure que $\mathrm{SL}_n(k)$ est connexe.

3. Soit k un corps de caractéristique distincte de 2 et soit V un k-espace vectoriel de dimension finie n. On considère une forme quadratique non dégénérée q sur V et on note b la forme bilinéaire symétrique correspondante. On désigne enfin par $\mathrm{O}(\mathrm{V}, q)$ le sous-groupe de $\mathrm{GL}(\mathrm{V})$ constitué des automorphismes g tels que $q(g(x), g(y)) = q(x, y)$ pour tous $x, y \in \mathrm{V}$ et on pose $\mathrm{SO}(\mathrm{V}, q) = \mathrm{O}(\mathrm{V}, q) \cap \mathrm{SL}(\mathrm{V})$.

Si $x \in \mathrm{V}$ est un vecteur tel que $q(x) \neq 0$ (on dit que x est *non isotrope*), l'application

$$r_x : \mathrm{V} \to \mathrm{V}, \quad y \mapsto y - 2\frac{b(y,x)}{q(x)}x$$

est un élément de $\mathrm{O}(\mathrm{V}, q)$, appelé *réflexion.*

(i) On munit GL(V) de la topologie de Zariski (via le choix d'une base de V). Vérifier que $\mathrm{O}(\mathrm{V}, q)$ et $\mathrm{SO}(\mathrm{V}, q)$ sont des sous-espaces fermés.

(ii) En considérant l'homomorphisme $\det : \mathrm{O}(\mathrm{V}, q) \to k^\times$, démontrer que le groupe $\mathrm{O}(\mathrm{V}, q)$ n'est pas connexe.

(iii) Démontrer que le groupe $\mathrm{O}(\mathrm{V}, q)$ est engendré par les réflexions (cf. D. Perrin, *Cours d'algèbre*, Ellipses, Chap. VIII, théorème 5.7) et vérifier qu'un élément de $\mathrm{O}(\mathrm{V}, q)$ appartient à $\mathrm{SO}(\mathrm{V}, q)$ si et seulement s'il est le produit d'un nombre pair de réflexions.

(iv) Le choix d'une base permet d'identifier V et k^n. Étant donné en entier naturel $m \geqslant 0$, démontrer que l'application

$$\mathrm{V}^m \to \mathrm{O}(\mathrm{V}, q), \quad (x_1, \ldots, x_n) \mapsto r_{x_1} \circ \ldots \circ r_{x_m}$$

est polynomiale en les coordonnées sur $\mathrm{V}^m \simeq k^{nm}$. En déduire que le groupe $\mathrm{SO}(\mathrm{V}, q)$ est connexe.

6. Groupes résolubles et groupes unipotents

6.1. Groupes algébriques résolubles

(6.1.1) On rappelle qu'un groupe Γ est dit *résoluble* s'il existe une suite de composition

$$\{e\} = \Gamma_0 \lhd \Gamma_1 \lhd \ldots \lhd \Gamma_{n-1} \lhd \Gamma_n = \Gamma$$

à quotients abéliens. Cette condition peut se reformuler de manière légèrement différente en introduisant le *groupe dérivé* de Γ, c'est-à-dire le sous-groupe $\mathrm{D}(\Gamma)$ engendré par les commutateurs $[x, y] = xyx^{-1}y^{-1}$ $(x, y \in \Gamma)$; ce sous-groupe est distingué, le quotient $\Gamma/\mathrm{D}(\Gamma)$ est abélien et $\mathrm{D}(\Gamma)$ peut en fait être caractérisé comme le plus petit sous-groupe distingué de Γ à quotient abélien. Soit $(\mathrm{D}^n(\Gamma))_{n\geqslant 0}$ la suite de sous-groupes de Γ définie par

$$\mathrm{D}^0(\Gamma) = \Gamma \quad \text{et} \quad \mathrm{D}^{n+1}(\Gamma) = \mathrm{D}(\mathrm{D}^n(\Gamma)).$$

Il est immédiat de vérifier que le groupe Γ est résoluble si et seulement s'il existe un entier $n \geqslant 0$ tel que $\mathrm{D}^n(\Gamma) = \{e\}$.

(6.1.2) Passons maintenant aux groupes algébriques ; pour simplifier, nous nous limiterons aux groupes de matrices $\Gamma \subseteq \mathrm{GL}_n$.

Lemme 6.1.1 — *Soit Γ un sous-groupe de $\mathrm{GL}_n(k)$ et soit $\overline{\Gamma}$ son adhérence ; on a $\mathrm{D}(\overline{\Gamma}) \subset \overline{\mathrm{D}(\Gamma)}$.*

Démonstration. Considérons l'application continue

$$\iota_n : \overline{\Gamma}^{2n} \to \overline{\Gamma}, \quad (x_1, y_1, \ldots, x_n, y_n) \mapsto [x_1, y_1] \ldots [x_n, y_n].$$

L'image réciproque du sous-groupe fermé $\overline{\mathrm{D}(\Gamma)}$ de $\overline{\Gamma}$ contient le sous-ensemble Γ^{2n} ; ce dernier étant dense dans $\overline{\Gamma}^{2n}$, $\iota_n(\overline{\Gamma}) \subset \overline{\mathrm{D}(\Gamma)}$ et donc

$$\mathrm{D}(\overline{\Gamma}) = \bigcup_{n\geqslant 0} \mathrm{im}(\iota_n) \subset \overline{\mathrm{D}(\Gamma)}.$$

□

Proposition 6.1.2 — *Soit Γ un sous-groupe de $\mathrm{GL}_n(k)$ et soit $\overline{\Gamma}$ son adhérence.*

(i) Pour que le groupe Γ soit résoluble, il faut et il suffit que $\overline{\Gamma}$ le soit.

(ii) Si Γ est connexe, $\mathrm{D}(\Gamma)$ est connexe.

Démonstration. (i) En vertu du lemme précédent,

$$\mathrm{D}^n(\Gamma) \leqslant \mathrm{D}^n(\overline{\Gamma}) \leqslant \overline{\mathrm{D}^n(\Gamma)}$$

pour tout entier $n \geqslant 0$. Les conditions $\mathrm{D}^n(\Gamma) = \{e\}$ et $\mathrm{D}^n(\overline{\Gamma}) = \{e\}$ sont donc équivalentes.

(ii) Considérons de nouveau l'application continue

$$\iota_n : \overline{\Gamma}^{2n} \to \overline{\Gamma}, \quad (x_1, y_1, \ldots, x_n, y_n) \mapsto [x_1, y_1] \ldots [x_n, y_n].$$

Si Γ est connexe, il en est de même de Γ^{2n} et l'image de ι_n est donc une partie connexe de Γ. On en déduit que

$$\mathrm{D}(\Gamma) = \bigcup_{n \geqslant 0} \mathrm{im}(\iota_n),$$

réunion d'une suite croissante de parties connexes de Γ, est connexe. □

(6.1.3) Le sous-groupe $\Gamma = \mathrm{B}_n(k)$ de $\mathrm{GL}_n(k)$ formé des matrices triangulaires supérieures est résoluble. Désignons en effet par $(e_1, \ldots, e_n)$ la base canonique de k^n et posons $\mathrm{V}_0 = \{0\}$, $\mathrm{V}_i = \mathrm{Vect}(e_1, \ldots, e_i)$ $(1 \leqslant i \leqslant n)$. Le sous-groupe $\mathrm{B}_n(k)$ de $\mathrm{GL}_n(k)$ est constitué des automorphismes g tels que $g(\mathrm{V}_i) = \mathrm{V}_i$ pour tout i. Étant donné $\ell \geqslant 0$, définissons Γ_ℓ comme le sous-groupe de $\mathrm{B}_n(k)$ constitué des automorphismes $g \in B_n(k)$ opérant trivialement sur les quotients $\mathrm{V}_{i+\ell}/\mathrm{V}_i$ pour tout $i \geqslant 0$ (où $\mathrm{V}_m = \mathrm{V}_n$ pour tout $m \geqslant n$) ; chacun de ces sous-groupes est distingué dans $\mathrm{B}_n(k)$. Si $\ell \geqslant 1$, les éléments de Γ_ℓ sont les matrices triangulaires supérieures à diagonale identité dont les $\ell - 1$ premières surdiagonales sont nulles.

On a $\Gamma_n = \{e\}$, $\Gamma_0 = \mathrm{B}_n(k)$ et

$$\Gamma_0/\Gamma_1 \xrightarrow{\sim} \textstyle\prod_{i=0}^{n-1} \mathrm{GL}(\mathrm{V}_{i+1}/\mathrm{V}_i) \simeq \prod_{i=0}^{n-1} k^\times \ .$$

Lorsque $\ell \geqslant 1$, $\Gamma_\ell/\Gamma_{\ell+1}$ est isomorphe au produit de $n - \ell$ copies du groupe additif k. Ainsi, les sous-groupes Γ_ℓ de Γ définissent une suite de composition à quotients abéliens et le groupe Γ est par conséquent résoluble.

Théorème 6.1.3 — *Supposons que le corps k soit algébriquement clos. Tout sous-groupe connexe et résoluble Γ de $\mathrm{GL}_n(k)$ est conjugué à un sous-groupe de $\mathrm{B}_n(k)$.*

Démonstration. Il suffit de démontrer que les éléments de Γ possèdent un vecteur propre commun dans k^n. Comme le groupe $\overline{\Gamma}$ est également connexe et résoluble en vertu des propositions 5.3.10 et 6.1.2, nous pouvons supposer que Γ est fermé. Dans ces conditions, la conclusion découle directement du lemme suivant puisque $\mathrm{D}^m(\Gamma) = \{e\}$ pour m assez grand. □

Lemme 6.1.4 — *Soit Γ un sous-groupe fermé et connexe de $\mathrm{GL}_n(k)$. Si le groupe $\mathrm{D}(\Gamma)$ stabilise une droite dans k^n, il en est de même du groupe Γ.*

Démonstration. Soit v un vecteur non nul dans V tel que le groupe $\mathrm{D}(\Gamma)$ stabilise la droite kv et soit $\chi_v : \mathrm{D}(\Gamma) \to k^\times$ l'homomorphisme de groupes (caractère) défini par l'identité

$$nv = \chi_v(n)v \qquad (n \in \mathrm{D}(\Gamma)).$$

Quels que soient $n \in \mathrm{D}(\Gamma)$ et $g \in \Gamma$, $g^{-1}ng$ appartient à $\mathrm{D}(\Gamma)$ et donc

$$n(gv) = g(g^{-1}ng)v = g(\chi_v(g^{-1}ng)v) = \chi_v(g^{-1}ng)(gv).$$

Cette identité montre que gv est également un vecteur propre pour le groupe $\mathrm{D}(\Gamma)$, associé au caractère

$$\chi_{gv} = \chi_v(g^{-1} \cdot g).$$

Le sous-groupe Γ_0 de Γ constitué des éléments g tels que $\chi_{\rho(g)v} = \chi_v$ est fermé : en effet, Γ_0 est l'intersection des sous-ensembles

$$\{g \in \Gamma \mid \chi_v(g^{-1}ng) = \chi_v(n)\},$$

$n \in \mathrm{D}(\Gamma)$, lesquels sont fermés car l'application

$$\Gamma \to k, \quad g \mapsto \chi_v(g^{-1}ng)$$

est polynomiale en les coefficients et l'inverse du déterminant de g. Par ailleurs, Γ_0 est d'indice fini dans Γ : en effet, puisque des vecteurs propres correspondant à des caractères différents sont linéairement indépendants, la finitude de $\dim(\mathrm{V})$ implique celle de l'ensemble $\{\chi_{gv},\ g \in \Gamma\}$ et donc celle de l'indice $(\Gamma : \Gamma_0)$.

Tout sous-groupe fermé d'indice fini est évidemment ouvert ; comme Γ est supposé connexe, $\Gamma_0 = \Gamma$ et donc $\chi_{gv} = \chi_v$ pour tout $g \in \Gamma$. Par suite,

$$n(gv) = \chi_v(n)(gv)$$

et donc chaque élément n de $\mathrm{D}(\Gamma)$ opère comme une homothétie sur le sous-espace vectoriel $\mathrm{V} = \mathrm{Vect}(gv,\ g \in \Gamma)$. Comme $\mathrm{D}(\Gamma)$ est engendré par les commutateurs, $\chi_v(n)^{\dim \mathrm{V}} = \det(n_{|\mathrm{V}}) = 1$ pour tout $n \in \mathrm{D}(\Gamma)$; en outre, $\mathrm{D}(\Gamma)$ étant connexe, son image par χ_v est une partie connexe de $k^\times$ et donc $\chi_v(n) = 1$ pour tout $n \in \mathrm{D}(\Gamma)$. Le groupe $\mathrm{D}(\Gamma)$ opère ainsi *trivialement* sur V, ce qui implique que le groupe Γ opère via le quotient $\Gamma/\mathrm{D}(\Gamma)$; ce dernier étant un groupe abélien, il possède un vecteur propre dans V puisque le corps k est supposé algébriquement clos et nous obtenons ainsi un vecteur propre pour Γ. □

Remarque — Les hypothèses introduites dans le théorème précédent sont toutes nécessaires.

(i) Un sous-groupe d'un groupe résoluble est résoluble. Comme le groupe $\mathrm{B}_n(k)$ est résoluble, il est nécessaire de supposer que Γ soit résoluble.

(ii) *Contre-exemple lorsque k n'est pas algébriquement clos* : le sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ constitué des matrices de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ avec $a, b \in \mathbb{R}$ est abélien, mais il n'est pas trigonalisable car la matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ n'a pas de valeur propre réelle.

(iii) *Contre-exemple lorsque Γ n'est pas connexe* : considérons le sous-groupe

$$\Gamma = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \quad \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix} \ ; \quad a, b \in k^\times \right\}$$

de $\mathrm{GL}_2(k)$ constitué des matrices *monomiales*. Notant Γ_0 le sous-groupe des matrices diagonales, on dispose d'une suite exacte courte

$$e \longrightarrow \Gamma_0 \longrightarrow \Gamma \longrightarrow \mathfrak{S}_2 \longrightarrow e$$

montrant que Γ est un groupe résoluble. C'est également un groupe non connexe puisque Γ_0 est un sous-groupe fermé propre d'indice fini. Le groupe Γ n'est pas trigonalisable car il n'existe pas vecteur propre commun à toutes les matrices le constituant.

6.2. Groupes algébriques unipotents

Définition 6.2.1 — *Un sous-groupe Γ de $\mathrm{GL}_n(k)$ est dit* unipotent *si tous ses éléments sont unipotents.*

Un exemple standard de groupe unipotent est le sous-groupe $\mathrm{U}_n(k)$ de $\mathrm{GL}_n(k)$ constitué des matrices triangulaires supérieures à diagonale unité.

Théorème 6.2.2 — *Tout sous-groupe unipotent de $\mathrm{GL}_n(k)$ est conjugué à un sous-groupe de $\mathrm{U}_n(k)$.*

Démonstration. Il suffit de démontrer qu'il existe un vecteur non nul $v \in k^n$ fixé par chaque élément de Γ : en effet, l'image de Γ dans $\mathrm{GL}(k^n/kv)$ est un sous-groupe unipotent et on

construit ainsi itérativement une base de k^n dans laquelle les éléments de Γ ont une matrice triangulaire supérieure à diagonale identité. On cherche donc à démontrer que le sous-espace vectoriel

$$\mathrm{V} = \{v \in k^n \mid (g - \mathrm{id})v = 0, \quad g \in \Gamma\}$$

est non nul ; il suffit de le vérifier après extension des scalaires à une clôture algébrique de k, ce qui permet de supposer que le corps k est algébriquement clos. Enfin, si W est un sous-espace vectoriel non nul de k^n stabilisé par Γ, l'image de Γ dans $\mathrm{GL}(\mathrm{W})$ est un sous-groupe unipotent et il est loisible de remplacer k^n par W ; nous pouvons donc supposer que l'action de Γ sur k^n est *irréductible*, c'est-à-dire qu'il n'existe pas de sous-espace vectoriel propre et non nul stabilisé par Γ.

Comme chaque élément g de Γ est unipotent, $\mathrm{Tr}(g) = n$ et donc

$$\mathrm{Tr}((\mathrm{id} - g)g') = \mathrm{Tr}(g') - \mathrm{Tr}(gg') = 0$$

pour tous $g, g' \in \Gamma$. L'action de Γ étant irréductible et le corps k étant algébriquement clos, il découle du théorème de Burnside (lemme 6.2.3) que l'espace vectoriel $\mathrm{End}(k^n)$ est engendré par l'image de Γ. Par suite,

$$\mathrm{Tr}((\mathrm{id} - g)u) = 0$$

pour tous $g \in \Gamma$ et $u \in \mathrm{End}(k^n)$, ce qui implique immédiatement $g = \mathrm{id}_{\mathrm{V}}$. Ainsi, les hypothèses que l'on a faites impliquent $\Gamma = \{e\}$ et l'existence d'un vecteur non nul fixé par Γ est maintenant triviale. □

Lemme 6.2.3 (Théorème de Burnside) — *Soit k un corps algébriquement et soit Γ un groupe opérant sur un k-espace vectoriel de dimension finie. Si l'action de Γ est irréductible — c'est-à-dire, s'il n'existe pas de sous-espace vectoriel propre et non nul Γ-invariant — alors l'espace vectoriel* $\mathrm{End}(\mathrm{V})$ *est engendré par Γ.*

Démonstration. Il découle de l'hypothèse d'irréductibilité que la k-algèbre

$$\mathrm{R} = \{u \in \mathrm{End}(\mathrm{V}) \mid u \circ g = g \circ u, \quad \forall g \in \Gamma\}$$

des endomorphismes commutant aux éléments de Γ est une algèbre à division (un corps gauche) : en effet, tout élément non nul u de R est inversible car son noyau, sous-espace vectoriel propre et Γ-invariant, est nul. Par ailleurs, tout élément de R est algébrique sur k en vertu du théorème de Cayley-Hamilton. Le corps k étant algébriquement clos, ces deux observations impliquent $\mathrm{R} = k$: les seuls endomorphismes de V commutant aux éléments de Γ sont les homomothéties.

Il reste à appliquer le théorème du bicommutant (lemme 6.2.4) : le sous-espace vectoriel de $\mathrm{End}(\mathrm{V})$ engendré par Γ est coïncide avec son bicommutant, c'est-à-dire avec le commutant de R dans $\mathrm{End}(\mathrm{V})$; comme $\mathrm{R} = k$, il s'agit de l'espace vectoriel $\mathrm{End}(\mathrm{V})$ tout entier. □

Lemme 6.2.4 (Théorème du bicommutant) — *Soit* V *un espace vectoriel de dimension finie sur un corps k et soit Γ un groupe d'automorphisme de* V. *On désigne par* R *la sous-k-algèbre de* $\mathrm{End}(\mathrm{V})$ *engendrée par Γ et on pose*

$$\mathrm{R}' = \{u \in \mathrm{End}(\mathrm{V}) \mid ug = gu, \quad \forall g \in \mathrm{R}\} \quad (\textit{ commutant}),$$

$$\mathrm{R}'' = \{u \in \mathrm{End}(\mathrm{V}) \mid uv = vu, \quad \forall v \in \mathrm{R}'\} \quad (\textit{ bicommutant}).$$

Si l'action de Γ sur V *est irréductible, alors* $\mathrm{R}'' = \mathrm{R}$.

Démonstration. Posons $n = \dim(\mathrm{V})$ et considérons l'action naturelle de Γ sur V^n.

Tout sous-espace Γ-invariant $\mathrm{W} \subset \mathrm{V}^n$ admet un supplémentaire Γ-invariant. Désignons en effet par $\mathrm{V}_i \simeq \mathrm{V}$ la composante d'indice i dans V^n $(1 \leqslant i \leqslant n)$ et soit J le plus grand sous-ensemble de $\{1, \ldots, n\}$ tel que $\mathrm{W} \cap \sum_{i \in \mathrm{J}} \mathrm{V}_i = \{0\}$. Posons $\mathrm{W}' = \sum_{i \in \mathrm{J}} \mathrm{V}_i$ et considérons i dans $\{1, \ldots, n\} - \mathrm{J}$. Comme $(\mathrm{W} + \mathrm{W}') \cap \mathrm{V}_i$ est un sous-espace Γ-invariant de V_i, $\mathrm{W} \cap \mathrm{V}_i = \{0\}$ ou $\mathrm{W} \cap \mathrm{V}_i = \mathrm{V}_i$ en vertu de l'hypothèse d'irréductibilité ; le premier cas de figure étant exclu par

maximalité de J, nous obtenons finalement $W + W' = V^n$ et W' est ainsi un supplémentaire Γ-invariant de W.

Identifions maintenant $\mathrm{End}(V^n)$ et $M_n(\mathrm{End}(V))$. Un élément g de R agissant diagonalement sur V^n définit un endomorphisme de V^n correspondant à la matrice diagonale par blocs $\mathrm{diag}(g, \ldots, g) \in M_n(\mathrm{End}(V))$; par suite, les endomorphismes de V^n commutant aux éléments de Γ correspondent aux éléments de $M_n(R')$. Enfin, il et clair que toute matrice diagonale par blocs dans $M_n(\mathrm{End}(V))$ de la forme $\mathrm{diag}(v, \ldots, v)$ avec $v \in R''$ définit un endomorphisme de V^n appartenant au bicommutant de Γ dans $\mathrm{End}(V^n)$.

On considère une base $(e_1, \ldots, e_n)$ de V^n et on désigne par W le sous-espace vectoriel Γ-invariant de V^n engendré par le vecteur $\mathbf{e} = (e_1, \ldots, e_n)$; $W = R\mathbf{e}$. Dire que W admet un supplémentaire Γ-invariant revient à dire qu'il existe un projecteur $\pi \in \mathrm{End}(V^n)$ d'image W qui commute aux éléments de Γ. D'après ce que l'on vient de dire, $\pi \circ v = v \circ \pi$ pour tout élément v de R'' opérant diagonalement sur V^n ; par suite, $v(\mathbf{e}) = \pi(v(\mathbf{e}))$ appartient à W et il existe donc $g \in R$ tel que $g(\mathbf{e}) = v(\mathbf{e})$; on a ainsi $v(e_i) = g(e_i)$ pour tout i, d'où finalement $v = g$. □

Exercices — **1.** Soit Γ un sous-groupe unipotent $\mathrm{GL}_n(k)$. Si $\Gamma \neq \{e\}$, démontrer qu'il existe un homomorphisme non trivial $G_\Gamma \to \mathbb{G}_a$, où G_Γ est le groupe algébrique associé à Γ (cf. 5.1).

2. Soit k un corps de caractéristique $p > 0$ et soit W le k-groupe algébrique tel que, pour toute k-algèbre R, W(R) soit l'ensemble R^2 muni de la loi de groupe définie par

$$(x, y)(x', y') = (x + x', y + y' + \Phi(x, x')),$$

où Φ est le polynôme à coefficients entiers défini par la relation

$$(U + V)^p = U^p + V^p + p\Phi(U, V).$$

(i) Démontrer que W est isomorphe à un sous-groupe de GL_{p+1}. Expliciter un tel plongement pour $p = 2$ et $p = 3$.

(ii) Démontrer que, pour toute représentation linéaire de dimension finie $\rho : W \to \mathrm{GL}(V)$ et tout $g \in W(k)$, l'automorphisme $\rho_k(g)$ est unipotent.

(iii) Démontrer que l'application

$$W(k) \to W(k), \quad g \mapsto g^p$$

est un homomorphisme de groupes de noyau non trivial. En déduire que W n'est pas isomorphe au groupe $\mathbb{G}_a \times \mathbb{G}_a$.

3. Soit Γ un sous-groupe fermé de $\mathrm{GL}_n(k)$, connexe et résoluble, et soit Γ_u le sous-ensemble formé des éléments unipotents.

(i) Démontrer que Γ_u est un sous-groupe fermé de Γ. (*Indication* : considérer une clôture algébrique $\overline{k}$ de k et travailler dans $\mathrm{GL}_n(\overline{k})$)

(ii) Si l'on suppose que tous les éléments de Γ sont semi-simples, démontrer que Γ est commutatif.

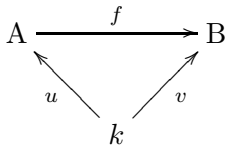
Appendice : notions d'algèbre commutative et de géométrie algébrique

On renvoie pour toutes les questions d'algèbre commutative au livre *Intoduction 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 $k \xrightarrow{u} \mathrm{A}$. Un *homomorphisme* de k-algèbres $f : (\mathrm{A}, u) \to (\mathrm{B}, v)$ est un homomorphisme d'anneaux $f : \mathrm{A} \to \mathrm{B}$ tel que $f \circ u = v$, c'est-à-dire tel que le diagramme



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 $k - \mathbf{alg}$. En général, si (A, u) est une k-algèbre, on omet de mentionner l'homomorphisme u et on parle simplement de la k-algèbre B.

Voici un exemple fondamental de k-algèbre : étant donné un ensemble I et une famille d'indéterminées $(\mathrm{X}_i)_{i\in\mathrm{I}}$, l'anneau de polynômes $k[(\mathrm{X}_i)_{i\in_I}]$ muni de l'homomorphisme canonique $k \to k[(\mathrm{X}_i)_{i\in_I}]$ (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

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

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

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

(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 $\mathfrak{N}(\mathrm{A})$. On dit que l'anneau A est *réduit* s'il ne contient pas d'élément nilpotent non nul, c'est-à-dire si $\mathfrak{N}(\mathrm{A}) = \{0\}$.

Un *diviseur de zéro* dans A est un élément a de A tel qu'il existe $b \in \mathrm{A} - \{0\}$ 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 $\mathfrak{m}$ de A est *maximal* si l'anneau quotient $A/\mathfrak{m}$ est un corps. On vérifie facilement que ceci équivaut à dire que $\mathfrak{m}$ 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 Spec(A). Le *spectre maximal* de A est l'ensemble de ses idéaux maximaux ; on le note 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) $\mathrm{Spec}(A) = \varnothing$, (ii) $\mathrm{Spm}(A) = \varnothing$ et (iii) $A = \{0\}$.

(1.4) *Modules* — Si A est un anneau, on note 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 $c : I \to A$ 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 $u : I \to M$, il existe une unique application A-linéaire $\tilde{u} : A^{(I)} \to M$ telle que $u = \tilde{u}(e_i)$. En d'autres termes : le couple constitué du A-module $A^{(I)}$ et de l'application $(I \to A^{(I)},\ i \mapsto e_i)$ représente le foncteur

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

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-bilinéaire $b : M \times N \to M \otimes_k N$ qui vérifie la propriété universelle suivante : pour tout k-module P et toute application k-bilinéaire $\Phi : M \times N \to P$, il existe une unique application k-linéaire $\varphi : M \otimes_k N \to P$ telle que $\Phi = \varphi \circ b$. En d'autres termes : le couple $(M \otimes_k N, b)$ représente le foncteur

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

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 $b : M \times N \to M \otimes_k N = k^{(M \times N)}/R$ 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 $f : k \to k'$ 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 $u : \mathrm{M} \to \mathrm{P}$, il existe une unique application k'-linéaire $\tilde{u} : k' \otimes_k \to \mathrm{P}$ telle que $u(m) = \tilde{u}(1 \otimes m)$ pour tout $m \in \mathrm{M}$.

D'autre part, si M, N sont deux k-modules et $u : \mathrm{M} \to \mathrm{N}$ est une application k-linéaire, on vérifie qu'il existe une unique application k-linéaire $u_{k'} = k' \otimes_k u : k' \otimes_k \mathrm{M} \to k' \otimes_k \mathrm{N}$ telle que $u_{k'}(\mu \otimes m) = \mu \otimes u(m)$ pour tous $\mu \in k'$, $m \in \mathrm{M}$. On définit ainsi un foncteur

$$k' \otimes_k \cdot : \mathrm{Mod}(k) \to \mathrm{Mod}(k'),$$

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 $\mathrm{A} \otimes_k \mathrm{B}$ telle que $(a \otimes b)(a' \otimes b') = (aa') \otimes (bb')$ pour tous $a, a' \in \mathrm{A}$, $b, b' \in \mathrm{B}$. 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 $w : k \to \mathrm{A} \otimes_k \mathrm{B}$, $\lambda \mapsto w(\lambda) = u(\lambda) \otimes 1 = 1 \otimes v(\lambda)$.

Désignons respectivement par i_A et i_B les applications $(\mathrm{A} \to \mathrm{A} \otimes_k \mathrm{B}, a \mapsto a \otimes 1)$ et $(\mathrm{B} \to \mathrm{A} \otimes_k \mathrm{B}, b \mapsto 1 \otimes b)$; ce sont manifestement des homomorphismes de k-algèbres. On vérifie facilement que, pour toute k-algèbre R et tous homomorphismes de k-algèbres $f_\mathrm{A} : \mathrm{A} \to \mathrm{R}$, $f_\mathrm{B} : \mathrm{B} \to \mathrm{R}$, il existe un unique homomorphisme de k-algèbres $f : \mathrm{A} \otimes_k \mathrm{B} \to \mathrm{R}$ tel que $f_\mathrm{A} = f \circ i_\mathrm{A}$ et $f_\mathrm{B} = f \circ i_\mathrm{B}$. En d'autres termes : le triplet $(\mathrm{A} \otimes_k \mathrm{B}, i_\mathrm{A}, i_\mathrm{B})$ représente le foncteur

$$\mathbf{Alg}_k \to \mathbf{Ens},\ \mathrm{R} \mapsto \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A}, \mathrm{R}) \times \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{B}, \mathrm{R}).$$

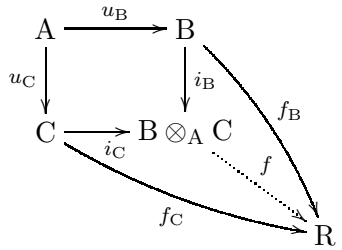
Plus généralement, étant données trois k-algèbres A, B et C ainsi que des homomorphismes de k-algèbres

$$\begin{array}{ccc} \mathrm{A} & \xrightarrow{u_\mathrm{B}} & \mathrm{B}\,, \\ {\scriptstyle u_\mathrm{C}}\downarrow & & \\ \mathrm{C} & & \end{array}$$

la k-algèbre $\mathrm{B} \otimes_\mathrm{A} \mathrm{C}$ représente le foncteur

$$\mathbf{Alg}_k \to \mathbf{Ens},\ \mathrm{R} \mapsto \left\{(f_\mathrm{B}, f_\mathrm{C}) \in \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{B}, \mathrm{R}) \times \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{C}, \mathrm{R}) \mid f_\mathrm{B} \circ u_\mathrm{B} = f_\mathrm{C} \circ u_\mathrm{C}\right\}.$$

Autrement dit : pour toute k-algèbre R, se donner un homomorphisme f de $\mathrm{B} \otimes_\mathrm{A} \mathrm{C}$ dans R équivaut à se donner des homomorphismes $f_\mathrm{B} : \mathrm{B} \to \mathrm{R}$ et $f_\mathrm{C} : \mathrm{C} \to \mathrm{R}$ tels que le diagramme en traits pleins



soit commutatif.

(2.4) ***Exercices***. Les exercices suivants présentent des propriétés importantes du produit tensoriel que l'on établiera 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 donnés un anneau A, un idéal $\mathfrak{I}$ de A et un A-module M, démontrer que le $\mathrm{A}/\mathfrak{I}$-module $\mathrm{A}/\mathfrak{I} \otimes_\mathrm{A} \mathrm{M}$ est canoniquement isomorphe au $\mathrm{A}/\mathfrak{I}$-module $\mathrm{M}/\mathfrak{I}\mathrm{M}$.

3. Soit $\mathrm{A} \to \mathrm{B}$ un homomorphisme d'anneaux et soit I un ensemble. Démontrer que les B-modules $\mathrm{B} \otimes_\mathrm{A} \mathrm{A}^{(\mathrm{I})}$ et $\mathrm{B}^{(\mathrm{I})}$ sont canoniquement isomorphes et expliciter cet isomorphisme.

4. Soit $k \to k'$ un homomorphisme d'anneaux. Étant donnés un ensemble I et des indéterminées $(\mathrm{X}_i)_{i\in\mathrm{I}}$, démontrer que les k'-algèbres $k' \otimes_k k[(\mathrm{X}_i)_{i\in\mathrm{I}}]$ et $k'[(\mathrm{X}_i)_{i\in\mathrm{I}}]$ sont canoniquement isomorphes.

5. Soit k un anneau. Étant donnés deux ensembles I et J ainsi que des indéterminées $(\mathrm{X}_i)_{i\in\mathrm{I}}$ et $(\mathrm{Y}_j)_{j\in\mathrm{J}}$, démontrer que la k-algèbre $k[(\mathrm{X}_i)_{i\in\mathrm{I}}] \otimes_k k[(\mathrm{Y}_j)_{j\in\mathrm{J}}]$ est canoniquement isomorphe à la k-algèbre $k[(\mathrm{Z}_\ell)_{\ell\in\mathrm{I}\cup\mathrm{J}}]$, où $\mathrm{Z}_\ell = \mathrm{X}_\ell \otimes 1$ si $\ell \in \mathrm{I}$ et $\mathrm{Z}_\ell = 1 \otimes \mathrm{Y}_\ell$ si $\ell \in \mathrm{J}$.

6. Soient k un anneau et A, B deux k-algèbres. Étant donnés des idéaux $\mathfrak{I}$ et $\mathfrak{J}$ de A et B respectivement, démontrer que la k-algèbre$\mathrm{A}/\mathfrak{I} \otimes_k \mathfrak{B}/\mathfrak{J}$ est canoniquement isomorphe au quotient de la k-algèbre $\mathrm{A} \otimes_k \mathrm{B}$ par l'idéal engendré par $\mathfrak{I} \otimes_k \mathrm{B} + \mathrm{A} \otimes_k \mathfrak{J}$.

3. Algèbres de type fini sur un corps

Dans tout ce paragraphe, k désigne un corps. Une k-algèbre A est dite *de type fini* si elle est engendrée, en tant que k-algèbre, par un nombre fini d'éléments ; il revient au même de dire que que A est isomorphe au quotient d'un anneau de polynômes $k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$.

(3.1) La géométrie algébrique naît d'une formulation géométrique des propriétés algébriques d'une k-algèbre de type fini, formulation dont le théorème suivant fournit le fondement.

Théorème (Nullstellensatz de Hilbert) — *Soit* A *une k-algèbre de type fini.*

(i) Pour tout idéal maximal $\mathfrak{m}$ de A*, le corps $\mathrm{A}/\mathfrak{m}$ est une extension finie de k. En particulier : si le corps k est algébriquement clos, l'application canonique*

$$\mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A}, k) \to \mathrm{Max}(\mathrm{A}), \quad s \mapsto \ker(s)$$

est une bijection.

(ii) Tout idéal premier de A *est l'intersection des idéaux maximaux le contenant.*

(iii) Considérons une k-algèbre B *et un homomorphisme $f : \mathrm{B} \to \mathrm{A}$. Pour tout idéal maximal $\mathfrak{m}$ de* A*, $f^{-1}(\mathfrak{m})$ est un idéal maximal de* B*.*

Faisons quelques remarques importantes.

1. Supposons que le corps k soit algébriquement clos. Appliquée à la k-algèbre de type fini $k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$, l'assertion (i) dit que l'application canonique
$$k^n \to \mathrm{Max}(k[\mathrm{T}_1, \ldots, \mathrm{T}_n]), \quad (t_1, \ldots, t_n) \mapsto (\mathrm{T}_1 - t_1, \ldots, \mathrm{T}_n - t_n)$$
est une bijection. En effet, un homomorphisme u de $k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ dans k s'identifie canoniquement au n-uplet $(t_1, \ldots, t_n) \in k^n$ des images des indéterminées $\mathrm{T}_1, \ldots, \mathrm{T}_n$ et son noyau est l'idéal $(\mathrm{T}_1 - t_1, \ldots, \mathrm{T}_n - t_n)$.
2. Soit $\mathfrak{I}$ un idéal maximal de $k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ et soit $\mathrm{A} = k[\mathrm{T}_1, \ldots, \mathrm{T}_n]/\mathfrak{I}$. L'ensemble $\mathrm{Max}(\mathrm{A})$ des idéaux maximaux de A s'identifie canoniquement à l'ensemble des idéaux maximaux de $k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ contenant l'idéal $\mathfrak{I}$; si k est algébriquement clos, il découle de la remarque précédente que $\mathrm{Max}(\mathrm{A})$ s'identifie à l'ensemble des zéros des éléments de $\mathfrak{I}$ dans k^n :
$$\mathrm{Max}(\mathrm{A}) \cong \{(t_1, \ldots, t_n) \in k^n \mid f(t_1, \ldots, t_n) = 0, \quad \forall f \in \mathfrak{I}\}.$$
3. Si le corps k est algébriquement clos, un polynôme $f \in k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ est inversible si et seulement si $f(t_1, \ldots, t_n) \neq 0$ pour tous $t_1, \ldots, t_n \in k$. Cette condition est trivialement nécessaire ; qu'elle soit suffisante découle de (i) puisqu'un polynôme f ne s'annulant en aucun point de k^n n'appartient à aucun idéal maximal de $k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ et donc est inversible.
4. L'assertion (ii) se généralise aisément sous la forme suivante : pour tout idéal $\mathfrak{I}$ de A, l'intersection des idéaux maximaux de A contenant $\mathfrak{I}$ est l'idéal
$$\sqrt{\mathfrak{I}} = \{f \in \mathrm{A} \mid \exists n \geqslant 0, \quad f^n \in \mathfrak{I}\}$$

(la *racine* de $\mathfrak{I}$). En effet, dans tout anneau commutatif la racine d'un idéal est l'intersection des idéaux premiers le contenant ; dans une k-algèbre de type fini, c'est donc également l'intersection des idéaux maximaux le contenant.

5. L'assertion (iii) se déduit aisément de (i). En effet, f induisant un homomorphisme injectif $\mathrm{B}/f^{-1}(\mathfrak{m}) \hookrightarrow \mathrm{A}/\mathfrak{m}$, il découle de (i) que tout élément x de $\mathrm{B}/\mathfrak{m}$ est *algébrique* sur k ; on a donc une relation $x^n+a_{n-1}x^{n-1}+\ldots+a_0 = 0$ dans $\mathrm{B}/f^{-1}(\mathfrak{m})$ avec $a_i \in k$. Comme $\mathrm{B}/f^{-1}(\mathfrak{m})$ est isomorphe à un sous-anneau d'un corps, c'est un anneau intègre ; si x est non nul, on en déduit facilement que l'on peut supposer $a_0 \neq 0$ (considérer une relation de degré minimal). Dans ces conditions, l'identité $xa_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1) = 1$ montre que x est inversible dans $\mathrm{B}/f^{-1}(\mathfrak{m})$; ce dernier anneau est donc un corps et $f^{-1}(\mathfrak{m})$ est un idéal maximal de B.

(3.2) Considérons une clôture algébrique $\overline{k}$ de k et soit k^{s} la clôture séparable de k dans $\overline{k}$, c'est-à-dire la réunion des extensions finies séparables de k dans $\overline{k}$. L'extension k^{s}/k est galoisienne tandis que l'extension $\overline{k}/k^{\mathrm{s}}$ est purement inséparable : si le corps k n'est pas parfait et de caractéristique $p > 0$, chaque élément α de $\overline{k}$ vérifie $\alpha^{p^n} \in k^{\mathrm{s}}$ pour un certain entier $n \geqslant 0$. Enfin, tout k-automorphisme du corps $\overline{k}$ stabilise le sous-corps k^{s} et l'application de restriction

$$\mathrm{Aut}(\overline{k}|k) \to \mathrm{Aut}(k^{\mathrm{s}}|k) = \mathrm{Gal}(k^{\mathrm{s}}|k), \quad \sigma \mapsto \sigma_{|k^{\mathrm{s}}}$$

est un isomorphisme.

Proposition — *Pour toute k-algèbre de type fini* A*, l'application*

$$\iota : \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A}, \overline{k}) \to \mathrm{Max}(\mathrm{A}), \quad s \mapsto \ker(s)$$

identifie les idéaux maximaux de A *aux orbites de l'action naturelle de* $\mathrm{Gal}(k^{\mathrm{s}}|k)$ *sur* $\mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A}, \overline{k})$.

Démonstration. L'argument invoqué à la remarque 5 ci-dessus montre que le noyau d'un homomorphisme de k-algèbres $\mathrm{A} \to \overline{k}$ est un idéal maximal de A. L'application ι est manifestement constante sur les orbites de $\mathrm{Gal}(k^{\mathrm{s}}|k)$ et elle est surjective en vertu de l'assertion (i) du Nullstellensatz. Enfin, si deux homomorphismes $s, s' : \mathrm{A} \to \overline{k}$ ont le même noyau $\mathfrak{m}$, tous deux induisent un k-plongement du corps $\mathrm{A}/\mathfrak{m}$ dans $\overline{k}$; les extensions $s : \mathrm{A}/\mathfrak{m} \hookrightarrow \overline{k}$ et $s' : \mathrm{A}/\mathfrak{m} \hookrightarrow \overline{k}$ étant deux clôtures algébriques de ce corps, on déduit de l'unicité à isomorphisme près des clôtures algébriques l'existence d'un automorphisme σ de $\overline{k}$ tel que $s' = \sigma \circ s$; comme s et s' sont en outre k-linéaires, σ induit l'identité sur k et σ appartient donc à $\mathrm{Aut}(\overline{k}|k) \cong \mathrm{Gal}(k^{\mathrm{s}}|k)$. □

Proposition — *L'application naturelle*

$$p : \mathrm{Max}(\mathrm{A} \otimes_k \overline{k}) \to \mathrm{Max}(\mathrm{A}), \quad \mathfrak{m} \mapsto \mathfrak{m} \cap \mathrm{A}$$

applique chaque composante connexe de $\mathrm{Max}(\mathrm{A} \otimes_k \overline{k})$ *sur une composante connexe de* $\mathrm{Max}(\mathrm{A})$.

Démonstration. Les composantes connexes de $\mathrm{Max}(\mathrm{A})$ sont de la forme $\mathrm{D}(e) = \mathrm{V}(e-1)$, où e est un idempotent primitif de A. Comme $\mathrm{V}(e-1) \cong \mathrm{Max}(\mathrm{A}/(e-1)\mathrm{A})$, nous pouvons, quitte à remplacer A par $\mathrm{A}/(e-1)$, supposer que $\mathrm{Max}(\mathrm{A})$ est connexe.

Observons tout d'abord que les idempotents de $\mathrm{A} \otimes_k \overline{k}$ appartiennent tous au sous-anneau $\mathrm{A} \otimes_k k^{\mathrm{s}}$. En effet, si le corps k est imparfait de caractéristique $p > 0$, alors il existe pour chaque élément a de $\mathrm{A} \otimes_k \overline{k}$ un entier $n \geqslant 0$ tel que $a^{p^n} \in \mathrm{A} \otimes_k k^{\mathrm{s}}$; appliquant ceci à un idempotent e de $\mathrm{A} \otimes_k \overline{k}$, on en déduit que e appartient à $\mathrm{A} \otimes_k k^{\mathrm{s}}$ puisque $e = e^2$.

L'action naturelle du groupe $\mathrm{Gal}(k^{\mathrm{s}}|k)$ sur $\mathrm{A} \otimes_k k^{\mathrm{s}}$ permute les éléments idempotents en préservant le caractère primitif puisque $\mathrm{Gal}(k^{\mathrm{s}}|k)$ permute les composantes connexes de $\mathrm{Max}(\mathrm{A} \otimes_k \overline{k})$. Étant donnée une composante connexe C de $\mathrm{Max}(\mathrm{A} \otimes_k \overline{k})$, la réunion $\widetilde{\mathrm{C}}$ des conjugués de C est une partie ouverte et fermée de $\mathrm{Max}(\mathrm{A} \otimes_k \overline{k})$ invariante sous $\mathrm{Gal}(k^{\mathrm{s}}|k)$.

Cette partie est donc de la forme $\widetilde{\mathrm{C}} = \mathrm{D}(e)$, où e est un idempotent de $\mathrm{A} \otimes_k k^{\mathrm{s}}$ invariant sous $\mathrm{Gal}(k^{\mathrm{s}}|k)$; ceci implique $e \in \mathrm{A}$ et donc $e = 1$ puisque $\mathrm{Max}(\mathrm{A})$ est connexe. On a ainsi $\widetilde{\mathrm{C}} = \mathrm{D}(1) = \mathrm{Max}(\mathrm{A} \otimes_k \overline{k})$ et l'action du groupe $\mathrm{Gal}(k^{\mathrm{s}}|k)$ sur $\mathrm{Max}(\mathrm{A} \otimes_k \overline{k})$ permute donc transitivement les composantes connexes.

Nous pouvons maintenant conclure : étant donné un point x de $\mathrm{Max}(\mathrm{A})$, il existe un point x' de $\mathrm{Max}(\mathrm{A} \otimes_k \overline{k})$ au-dessus de x car l'application p est surjective (cf. proposition précédente). Quelle que soit la composante connexe C de $\mathrm{Max}(\mathrm{A} \otimes_k \overline{k})$, il existe un élément σ de $\mathrm{Gal}(k^{\mathrm{s}}|k)$ tel que x' appartienne à $\sigma(\mathrm{C})$; on a alors $\sigma^{-1}(x') \in \mathrm{C}$ — ce qui prouve que C rencontre la fibre de p au-dessus de x — et ainsi $p(\mathrm{C}) = \mathrm{Max}(\mathrm{A})$. □

Table des matières