REPRÉSENTATIONS DES GROUPES ALGÉBRIQUES ET ÉQUATIONS FONCTIONNELLES

(COURS DE TROISIÈME CYCLE, DEUXIÈME NIVEAU, 2008/2009)

J. Sauloy [1]

11 décembre 2009

[1]Institut mathématique de Toulouse et U.F.R. M.I.G., Université Paul Sabatier, 118, route de Narbonne, 31062 Toulouse CEDEX 4

Résumé

Le but du cours est de donner le minimum de connaissances sur les représentations des groupes algébriques linéaires complexes qui permette de définir le groupe de Galois d'une équation différentielle ou aux q-différences analytique. On prouvera la partie facile du "théorème de Tanaka" et on admettra l'autre partie, que l'on appliquera à des exemples intéressants en théorie de Galois.
Contenu du cours :

- *Catégories et foncteurs*
- *Géométrie algébrique affine*
- *Groupes algébriques linéaires*
- *Comment reconstruire un groupe algébrique à partir de la catégorie de ses représentations.*
- *Complété proalgébrique d'un groupe.*
- *La correspondance de Riemann-Hilbert et le groupe de Galois.*

Bibliographie :

1. *Ahlfors L. : Complex Analysis*
2. *Borel A. : Linear Algebraic Groups.*
3. *Deligne P. and Milne J. S. : Tannakian categories in L.N.M. 900*
4. *Douady R. et Douady A. : Algèbre et théories galoisiennes.*
5. *Springer T. A. : Linear Algebraic Groups*

Le résumé ci-dessus reproduit la présentation du cours telle qu'elle figurait sur le site "Enseignement" du département de mathématiques. Je ne prétends pas que ce (vaste) programme soit réalisable. Le véritable plan du cours et la véritable bibliographie apparaissent plus loin ! ! !
Outre le cours polycopié, les documents suivants ont été distribués aux étudiants :

- Le premier chapitre de mon cours de DEA de 2004-2005 ; ce chapitre porte sur le prolongement analytique et la correspondance de Riemann-Hilbert.
- Des feuilles d'exercices de géométrie algébrique de M1.
- Le chapitre de géométrie algébrique d'un cours de L3 sous la direction de Jean-Pierre Ramis et André Warusfel, édité chez De Boeck.
- L'appendice de ma thèse portant sur le calcul élémentaire de l'enveloppe proalgébrique de $\mathbf{Z}$.

Table des matières

Conventions. La notation $A := B$ signifiera que le terme A est défini par la formule B. Les expressions nouvelles sont écrites en *italiques* au moment de la définition. Noter qu'une définition peut apparaitre au cours d'un théorème, d'un exemple, d'un exercice, etc.

Exemple 0.0.1 L'espace vectoriel $E^* := \mathrm{Hom}_K(E,K)$ est appelé *dual* de E.

Première partie

Les bases

Chapitre 1

En guise d'introduction : groupe(s) attaché(s) à une équation différentielle.

Ce chapitre a un rôle introductif, presque culturel : il sert essentiellement à motiver le cours. On y montre de quelle manière des groupes interviennent naturellement dans l'étude des équations différentielles, et en quel sens on peut parler de thorie de Galois. La présentation n'est pas très détaillée.

L'étudiant que le M1 n'a pas suffisamment familiarisé avec le problème du prolongement analytique et du passage du local au global compensera cette lacune avec le chapitre 8 de [2], qu'il complètera (agréablement) de [38] pour savoir où l'appliquer. Pour la correspondance de Riemann-Hilbert, il consultera avec profit [3] (chap. 1), [4] (chap. 7), [19] (chap. 1) et (mais oui !) [5]. Mon cours [31] (première partie) peut aider. Enfin, pour la théorie de Galois différentielle, la seule référence actuellement accessible est [26]. Noter enfin que [12] expose le point de vue "moderne" (dû à Grothendieck) sur les théories galoisiennes.

1.1 Équations différentielles linéaires analytiques

Soit une équation différentielle linéaire analytique scalaire d'ordre n (ouf !) dans le domaine (*i.e.* ouvert connexe non vide) X de $\mathbf{C}$:

$$a_0(z) f^{(n)}(z) + \cdots + a_n(z) f(z) = 0, \tag{1.1.0.1}$$

où $a_0, \ldots, a_n \in O(X)$ (anneau des fonctions holomorphes sur X) et où $a_0 \neq 0$ (*i.e.* ce n'est pas la fonction nulle). Le plus souvent, $X = \mathbf{C}$ (le plan complexe) ou $X = \mathbf{S}$ (la sphère de Riemann, c'est-à-dire la droite projective complexe $\mathbf{P}^1(\mathbf{C})$), et les a_i sont des fractions rationnelles, ou des polynômes, ce qui revient au même puisque l'on peut chasser les dénominateurs. En vue d'appliquer le théorème de Cauchy à l'équation (1.1.0.1), on introduit son *lieu singulier* :

$$\Sigma := \{z \in X \mid a_0(z) = 0\}.$$

C'est un fermé discret de X et $X' := X \setminus \Sigma$ est encore un domaine. (Pourquoi ?)

1.1.1 Le faisceau des solutions de (1.1.0.1) sur X'

Pour tout ouvert U de $X' = X \setminus \Sigma$, on notera :

$$\mathcal{F}(U) := \{ f \in \mathcal{O}(U) \mid a_0 f^{(n)} + \cdots + a_n f = 0 \}$$

le **C**-espace vectoriel des solutions de (1.1.0.1) sur U. (Par convention, ou par raisonnement capillotracté mais correct, $\mathcal{F}(\emptyset)$ est l'espace vectoriel trivial.) On obtient ainsi un *faisceau de* **C***-espaces vectoriels sur* X', le faisceau des solutions de (1.1.0.1) ; cette terminologie résume les propriétés suivantes.

À chaque inclusion d'ouverts $V \subset U \subset X'$ est associé un *morphisme de restriction* :

$$\rho_V^U : \mathcal{F}(U) \to \mathcal{F}(V),\ f \mapsto f_{|V}.$$

C'est une application linéaire, et l'ensemble des ρ_V^U vérifie les propriétés de compatibilité suivantes : on a $\rho_U^U = \mathrm{Id}_{\mathcal{F}(U)}$ et $\rho_W^V \circ \rho_V^U = \rho_W^U$. On résume cela en disant que $\mathcal{F}$ est un *préfaisceau*.

Soit $U = \bigcup_{i \in I} U_i$ un recouvrement ouvert de l'ouvert $U \subset X'$. Soit $f \in \mathcal{F}(U)$. Il découle de la première propriété que la famille des restrictions $f_i := \rho_{U_i}^U(f) \in \mathcal{F}(U_i)$ satisfait la relation suivante :

$$\forall i, j \in I\ ,\ \rho_{U_i \cap U_j}^{U_i}(f_i) = \rho_{U_i \cap U_j}^{U_j}(f_j).$$

On peut le formuler ainsi : les "données locales" $f_i \in \mathcal{F}(U_i)$, obtenues par restrictions à partir de la "donnée globale" $f \in \mathcal{F}(U)$ sont "compatibles" sur leurs lieux de définition communs $U_i \cap U_j$. Réciproquement, si l'on se donne *a priori* des données locales compatibles, on peut les "recoller" en une unique donnée globale :

$$\forall (f_i)_{i \in I} \in \prod_{i \in I} \mathcal{F}(U_i) \text{ t.q. } \forall i, j \in I\ ,\ \rho_{U_i \cap U_j}^{U_i}(f_i) = \rho_{U_i \cap U_j}^{U_j}(f_j)\ ,\ \exists ! f \in \mathcal{F}(U)\ :\ \forall i \in I\ ,\ f_i := \rho_{U_i}^U(f).$$

C'est cette dernière propriété (existence et unicité du recollement de données locales compatibles) que l'on résume en disant que $\mathcal{F}$ est un faisceau. On peut aussi l'écrire sous forme de suite exacte :

$$0 \longrightarrow \mathcal{F}(U) \longrightarrow \prod_{i \in I} \mathcal{F}(U_i) \longrightarrow \prod_{i,j \in I} \mathcal{F}(U_i \cap U_j).$$

(Le lecteur définira lui-même les flèches de cette suite.)

1.1.2 Le faisceau $\mathcal{F}$ est un système local

Nous allons résumer sans preuve (pour ces dernières, voir[1] [2]) les propriétés caractéristiques du faisceau $\mathcal{F}$. Ces propriétés sont liées, pour l'essentiel, au théorème de Cauchy sur les équations différentielles linéaires analytiques complexes, et au principe du prolongement analytique. Le lecteur est invité à formuler la contrepartie réelle de chacun des énoncés ci-dessous et de voir lesquels sont propres au champ complexe.

[1] Dans [2], les faisceaux sont présentés à partir des "espaces étalés". Le lien entre les deux points de vue est explicité dans l'ouvrage [13].

Exercice 1.1.1 (Lemme du wronskien) Pour tout ouvert connexe $U \subset X'$, on a $\dim_{\mathbf{C}} \mathcal{F}(U) \leq n$.

Exercice 1.1.2 (Théorème de Cauchy) Soient $z_0 \in X'$ et $b_0, \ldots, b_{n-1} \in \mathbf{C}$. Montrer qu'il existe une unique série entière $f(z) := \sum_{k \in \mathbf{N}} c_k (z - z_0)^k$ solution de (1.1.0.1) et dont les n premiers coefficients soient $c_0 := b_0, \ldots, c_{n-1} := b_{n-1}$.

Et maintenant, la liste des propriétés caractéristiques de notre faiceau, qui en font un "système local".

Exercice 1.1.3 ($\mathcal{F}$ est un système local)

1. Soit $z_0 \in X'$. Il existe alors $r > 0$ tel que $U := \overset{\circ}{\mathrm{D}}(z_0, r) \subset X'$ (il s'agit du disque ouvert de centre z_0 et de rayon r) et que $\mathcal{F}(U)$ est de dimension n. (C'est une conséquence immédiate du lemme du wronskien et du théorème de Cauchy.)
2. Soient deux ouverts $V \subset U \subset X'$ tels que U est connexe et V non vide. Alors le morphisme de restriction $\rho_V^U : \mathcal{F}(U) \to \mathcal{F}(V)$ est injectif. (Cela découle du principe de prolongement analytique.)
3. Soit $U \subset X'$ un ouvert non vide simplement connexe. Alors $\dim_{\mathbf{C}} \mathcal{F}(U) = n$. (Raisonnement purement topologique à partir de ce qui précède.)

Supposons maintenant que $U_1, U_2 \subset X'$ sont deux ouverts non vides simplement connexes et soit $V \subset U_1 \cap U_2$ un ouvert connexe non vide. D'après ce qui précède, on a deux *isomorphismes* $\rho_V^{U_i} : \mathcal{F}(U_i) \to \mathcal{F}(V)$: ils sont injectifs, la dimension est n à la source et $\leq n$ au but. On a donc des isomorphismes :

$$\mathcal{F}(U_1) \longrightarrow \mathcal{F}(V) \longleftarrow \mathcal{F}(U_2), \text{ d'où, par composition : } \mathcal{F}(U_1) \longrightarrow \mathcal{F}(U_2).$$

Si $V = U_1 \cap U_2$ (*i.e.* si cette intersection est connexe), on en déduit que *toute solution de* (1.1.0.1) *sur* U_1 *admet un unique prolongement à* U_2 *défini par compatibilité sur* $U_1 \cap U_2$.

Mais, si $U_1 \cap U_2$ n'est pas connexe, on peut définir un tel isomorphisme $\mathcal{F}(U_1) \simeq \mathcal{F}(U_2)$ pour chaque composante connexe V de $U_1 \cap U_2$! (Ces composantes sont bien ouvertes.) Rien ne dit *a priori* que ces "prolongements analytiques" sont les mêmes.

Remarque 1.1.4 Nous n'avons pas défini ce qu'est un "système local". C'est essentiellement un faisceau sur lequel on peut faire des raisonnements du type précédent : voir [8] pour une étude en forme.

1.2 Exemples basiques

1.2.1 Les "caractères"

On prend $X := \mathbf{C}$. Pour un certain $\alpha \in \mathbf{C}$, on considère :

$$z f'(z) - \alpha f(z) = 0. \text{ Ainsi, } \Sigma = \{0\} \text{ et } X' = \mathbf{C}^*. \tag{1.2.0.1}$$

Soient $z_0 \in \mathbf{C}^*$ et $U := \overset{\circ}{\mathrm{D}}(z_0, |z_0|)$. La série de Newton :

$$\left(1 + \frac{z - z_0}{z_0}\right)^{\alpha} = \sum_{n \geq 0} \binom{\alpha}{n} \left(\frac{z - z_0}{z_0}\right)^n$$

définit une solution f_{z_0} de (1.2.0.1) non triviale sur U, et l'on peut prouver que $\mathcal{F}(U) = \mathrm{Vect}(f_{z_0})$. (Méthode : pour toute telle solution f, le wronskien $f f'_{z_0} - f' f_{z_0}$ est trivial.) En revanche, on prouve également que, pour qu'il y ait des solutions non triviales globales, *i.e.* $\mathcal{F}(\mathbf{C}^*) \neq \{0\}$, il faut, et il suffit, que $\alpha \in \mathbf{Z}$. (Méthode pour l'implication non triviale : si f est une telle solution, appliquer la formule des résidus à f'/f.)

Considérons maintenant les disques ouverts $U_\ell := \overset{\circ}{\mathrm{D}}(\mathrm{i}^\ell, 1)$, $\ell = 0,1,2,3$ (et $U_4 = U_0$) et notons $f_\ell := f_{\mathrm{i}^\ell} \in \mathcal{F}(U_\ell)$ les "fonctions-bases" correspondantes. Il est clair que, pour chaque ℓ, l'intersection $U_\ell \cap U_{\ell+1}$ est un ouvert connexe non vide (le dessiner), et l'on en déduit un isomorphisme $\mathcal{F}(U_\ell) \simeq \mathcal{F}(U_{\ell+1})$. Celui-ci est parfaitement caractérisé par l'image de f_ℓ, qui est un multiple (non trivial) de $f_{\ell+1}$. Il y a donc une unique constante $\alpha_\ell \in \mathbf{C}^*$ telle que les restrictions de f_ℓ et de $\alpha_\ell f_{\ell+1}$ à $U_\ell \cap U_{\ell+1}$ coïncident.

En composant ces isomorphismes, on obtient l'automorphisme de $\mathcal{F}(U_0)$ qui envoie f_0 sur $a f_0$, où $a := \alpha_0\alpha_1\alpha_2\alpha_3 \in \mathbf{C}^*$. Plus généralement, en prolongeant une solution $f \in \mathcal{F}(U_0)$ par la méthode ci-dessus (restriction-dérestriction de disque en disque voisin), on obtient la solution $af \in \mathcal{F}(U_0)$.

Pour savoir s'il s'est passé quelque chose, *i.e.* si $a \neq 1$, il importe de calculer les α_ℓ. On peut le faire de la manière suivante. On constate d'abord que, pour chaque ℓ et pour tout $z \in U_\ell$, on a $z/\mathrm{i}^\ell \in U_0$ et $f_\ell(z) = f_0(z/\mathrm{i}^\ell)$ (c'est immédiat d'après la formule). On prouve ensuite :

$$\forall z \in U_0\ ,\ f_0(z) = \rho^\alpha e^{\mathrm{i}\alpha\theta},\ \text{où } \rho := |z| \in]0,2[\text{ et } \theta := \mathrm{Arg} z \in]-\pi/2, \pi/2[\,.$$

(On note Arg la *détermination principale de l'argument*.) La même formule permet d'étendre f_0 en une fonction analytique g_0 sur $V_0 := \mathbf{C} \setminus \mathbf{R}_- \supset U_0$ et donc, plus généralement, d'étendre chaque f_ℓ en une fonction analytique g_ℓ sur $V_\ell := \mathbf{C} \setminus \mathrm{i}^\ell \mathbf{R}_- \supset U_\ell$. On a bien entendu $g_\ell \in \mathcal{F}(V_\ell)$ (car la fonction analytique $g'_\ell - \alpha g_\ell$ est nulle sur U_ℓ donc identiquement nulle sur V_ℓ). Le morphisme de restriction $\mathcal{F}(V_\ell) \to \mathcal{F}(U_\ell)$ est un isomorphisme, et notre petit jeu de restriction-dérestriction de disque en disque voisin peut aussi bien se jouer de plan fendu en plan fendu voisin.

Puisque les restrictions de f_ℓ et de $\alpha_\ell f_{\ell+1}$ à $U_\ell \cap U_{\ell+1}$ coïncident, il en est de même des restrictions de g_ℓ et de $\alpha_\ell g_{\ell+1}$ à $V_\ell \cap V_{\ell+1}$ (encore le principe de prolongement analytique). Mais $\mathrm{i}^{\ell+1} \in V_\ell \cap V_{\ell+1}$, et $g_{\ell+1}(\mathrm{i}^{\ell+1}) = 1$, d'où les formule magiques :

$$\alpha_\ell = g_\ell(\mathrm{i}^{\ell+1}) = g_1(\mathrm{i}) = e^{\mathrm{i}\pi\alpha/2},\ \text{d'où l'on déduit : } a = e^{2\mathrm{i}\pi\alpha}.$$

On peut retrouver le critère d'existence de solutions globales énoncé plus haut. Si $h \in \mathcal{F}(\mathbf{C}^*)$, notons h_ℓ sa restriction à U_ℓ. Alors l'image de h_ℓ par l'isomorphisme $\mathcal{F}(U_\ell) \to \mathcal{F}(U_{\ell+1})$ ne peut être que $h_{\ell+1}$ (elles coïncident sur l'intersection de leurs domaines) ; le prolongement analytique de h_0 est donc h_0 (car restriction d'une solution globale) et ah_0 (vrai pour toute solution locale). Cela entraine $ah_0 = h_0$, donc $ah = h$. L'existence de solutions globales non triviales implique donc $a = 1$, c'est-à-dire $\alpha \in \mathbf{Z}$.

1.2.2 Le logarithme

Le logarithme complexe peut être défini soit comme inverse à droite de l'exponentielle : $\exp(\log z) = z$, soit comme primitive : $\log'(z) = \dfrac{1}{z}$. Il n'est pas difficile de montrer que ces deux problèmes admettent des *solutions locales* au voisinage de tout point de $\mathbf{C}^*$ (le premier par le théorème d'inversion locale ; le second par intégration terme à terme de séries entières). Il n'est pas non plus très difficile de montrer qu'il ne peut exister de solution globale sur $\mathbf{C}^*$ (même simplement continue dans le premier cas). On va utiliser le point de vue des équations différentielles pour comprendre l'*obstruction topologique* à l'existence du logarithme.

Pour ce faire, on supposera connue la fonction *logarithme népérien*, notée ln : il s'agit de la *détermination principale du logarithme*, qui est définie sur $\mathbf{C} \setminus \mathbf{R}_-$, y est inverse à droite de l'exponentielle : $\exp(\ln z) = z$, et y est holomorphe, de dérivée $\ln'(z) = \dfrac{1}{z}\cdot$. De plus, on a la formule explicite :

$$\forall \rho \in \mathbf{R}_+^* \ , \ \forall \theta \in \ ]-\pi, \pi[\ , \ \ln\left(\rho e^{i\theta}\right) = \ln \rho + i\theta$$

et le développement en série entière, valable sur $\overset{\circ}{\mathrm{D}}(1,1)$:

$$\ln(1+z) = \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} z^n.$$

Pour obtenir une équation différentielle *linéaire*, on remplace la relation $\log'(z) = \dfrac{1}{z}$, qui équivaut à $z\log' = 1$, par sa dérivée : $(z\log')' = 0$. Il est bien clair que cette dernière n'implique pas la précédente et que l'on introduit ainsi des solutions "parasites", comme par exemple les constantes, qui vérifient $z\log' = 0$. Mais le fait de s'être ramené à un problème linéaire comporte des avantages qui compensent largement cet inconvénient. On considèrera donc l'équation différentielle linéaire analytique scalaire d'ordre 2 (ouf) :

$$z f''(z) + f'(z) = 0. \text{ Ainsi, } \Sigma = \{0\} \text{ et } X' = \mathbf{C}^*. \tag{1.2.0.2}$$

On notera encore $\mathcal{F}$ le faisceau sur X' des solutions de (1.2.0.2) : donc un faisceau de $\mathbf{C}$-espaces vectoriels. Soient $z_0 \in \mathbf{C}^*$ et $U := \overset{\circ}{\mathrm{D}}(z_0, |z_0|)$. La série entière :

$$\ln\left(1 + \frac{z - z_0}{z_0}\right) = \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} \left(\frac{z - z_0}{z_0}\right)^n$$

définit une solution f_{z_0} de (1.2.0.2) non triviale sur U, et l'on peut vérifier que c'est bien la solution $\ln(z/z_0)$ définie à partir du logarithme népérien. (Si $z \in U$, on a bien $z/z_0 \in \overset{\circ}{\mathrm{D}}(1,1)$.) On peut alors démontrer que $\mathcal{F}(U) = \mathrm{Vect}(1, f_{z_0})$, où l'on a abusivement noté 1 la fonction constante 1 sur U. Plus précisément, la famille $(1, f_{z_0})$ est une base de $\mathcal{F}(U)$. On peut alors noter $V_{z_0} := \mathbf{C} \setminus z_0\mathbf{R}_-$ (un plan fendu) et vérifier que l'unique fonction de $\mathcal{F}(V_{z_0})$ qui se restreint en f_{z_0} sur U_{z_0} est définie par $g_{z_0}(z) := \ln(z/z_0)$; et le $\mathbf{C}$-espace vectoriel $\mathcal{F}(V_{z_0})$ admet pour base la famille $(1, g_{z_0})$.

Pour recommencer le jeu du prolongement par restriction-dérestriction, on reprend les mêmes disques ouverts U_ℓ et les mêmes plans fendus V_ℓ que précédemment. Le $\mathbf{C}$-espace vectoriel $\mathcal{F}(V_\ell)$

admet pour base la famille $(1, g_\ell)$, où l'on note $g_\ell := g_{i^\ell}$. Pour déterminer complètement l'isomorphisme de $\mathcal{F}(V_\ell)$ sur $\mathcal{F}(V_{\ell+1})$, il suffit d'expliciter son effet sur une base, c'est-à-dire de trouver une matrice $A_\ell \in \mathrm{GL}_2(\mathbf{C})$ telle que :

$$(1, g_\ell) = (1, g_{\ell+1})A_\ell,$$

cette égalité abusive signifiant en fait que les deux membres coïncident sur l'ouvert intersection. La première colonne de A_ℓ est évidemment $\begin{pmatrix}1\\0\end{pmatrix}$. La deuxième admet pour coefficients des scalaires $a, b \in \mathbf{C}$ tels que :

$$g_\ell = a + b g_{\ell+1},$$

l'égalité ayant le même sens qu'auparavant. De la définition de ln par module et argument et de l'égalité $g_\ell(z) = \ln(z/\mathrm{i}^\ell)$, le lecteur déduira sans peine la relation suivante :

$$a = g_\ell\left(\mathrm{i}^{\ell+1}\right) = \ln(\mathrm{i}) = \frac{\mathrm{i}\pi}{2}\cdot$$

D'autre part, en dérivant, on voit que :

$$g'_\ell = b g'_{\ell+1} \Longrightarrow b = 1,$$

puisque $g'_\ell = g'_{\ell+1} = \dfrac{1}{z}$. La matrice de prolongement de $\mathcal{F}(V_\ell)$ à $\mathcal{F}(V_{\ell+1})$ est donc :

$$A_\ell = \begin{pmatrix}1 & \mathrm{i}\pi/2\\ 0 & 1\end{pmatrix}.$$

La matrice de l'automorphisme de prolongement de $\mathcal{F}(V_0)$ dans la base $(1, \ln)$ est donc :

$$A = A_3A_2A_1A_0 = \begin{pmatrix}1 & 2\mathrm{i}\pi\\ 0 & 1\end{pmatrix}.$$

Exercice 1.2.1 En déduire que les seuls éléments de $\mathcal{F}(V_0)$ qui proviennent d'une solution globale sont les constantes. (Ce sont les points fixes de l'automorphisme de prolongement.)

1.3 Retour au formalisme général

1.3.1 Le principe de monodromie

On repart du système local $\mathcal{F}$ de 1.1.2. On veut pouvoir parler de solutions au voisinage d'un point $z_0 \in X'$ sans avoir à préciser ce point. pour cela, on introduit la notion de *germe de solution* en z_0 : c'est, par définition, une classe d'équivalence de couple (f, U), où U est un voisinage ouvert de z_0 dans X' et où $f \in \mathcal{F}(U)$, la relation d'équivalence étant définie comme suit :

$$(f, U) \sim (g, V) \Longleftrightarrow \exists W \subset U \cap V \ :\ z_0 \in W \text{ et } f_{|W} = g_{|W}.$$

Ces germes forment, de manière naturelle, un $\mathbf{C}$-espace vectoriel $\mathcal{F}_{z_0}$ et l'on a, pour tout voisinage ouvert U de z_0 une application linéaire de $\mathcal{F}(U)$ dans $\mathcal{F}_{z_0}$, qui, à $f \in \mathcal{F}(U)$, associe son germe, *i.e.* la classe de (f, U) dans $\mathcal{F}_{z_0}$.

Les propriétés énumérées en 1.1.2 se traduisent alors ainsi :

1. Si U est un voisinage ouvert *connexe* de z_0 dans X', l'application linéaire de $\mathcal{F}(U)$ dans $\mathcal{F}_{z_0}$ est injective.
2. Si U est un voisinage ouvert non vide *simplement connexe* de z_0 dans X', cette application linéaire est bijective.

Le jeu du prolongement peut alors se traduire ainsi. On se donne deux points $z_0, z_1 \in X'$ et un chemin γ reliant ces deux points dans X'. Pour simplifier, on notera encore γ l'image ce ce chemin (donc un compact connexe de X'). On peut alors recouvrir γ par des disques ouverts non vides $D_1, \ldots, D_m$ inclus dans X', centrés en des points de γ, et tels que :

1. D_1 est centré en z_0 et D_m est centré en z_1.
2. Pour $\ell = 1, \ldots, m-1$, le disque D_ℓ rencontre $D_{\ell+1}$.

On obtient ainsi des isomorphismes de restriction-dérestriction $\mathcal{F}(D_\ell) \to \mathcal{F}(D_{\ell+1})$, puis, en composant, un isomorphisme $\mathcal{F}(D_1) \to \mathcal{F}(D_m)$, soit encore, en vertu des propriétés de système local énumérées plus haut, un isomorphisme de $\mathcal{F}_{z_0}$ sur $\mathcal{F}_{z_1}$. Outre les affirmations rapides qui précèdent, le lecteur prouvera sans trop de peine que *l'isomorphisme ainsi obtenu ne dépend pas du choix des disques D_ℓ*. Il ne dépend donc que du chemin γ, et nous le noterons (provisoirement) :

$$\Phi_\gamma : \mathcal{F}_{z_0} \to \mathcal{F}_{z_1}.$$

On parle de *prolongement analytique le long du chemin γ.*

En réalité, l'isomorphisme Φ_γ dépend d'encore bien moins que cela. Si l'on déforme continûment γ en un chemin γ' sans bouger ses extrémités, on obtient le même prolongement analytique :

Théorème 1.3.1 (Principe de monodromie) *Si les chemins γ et γ' d'origine z_0 et d'extrémité z_1 sont homotopes, alors $\Phi_\gamma = \Phi_{\gamma'}$.*

Il s'agit ici (et partout dans la suite) d'homotopie dans X'. Ce théorème est démontré dans [2, 8.1.5]. Notant $[\gamma]$ la classe d'homotopie du chemin γ, on est donc fondé à poser :

$$\Phi_{[\gamma]} := \Phi_\gamma.$$

En particulier, si $z_1 = z_0$, autrement dit, si γ est un lacet de base z_0, alors on obtient une application $[\gamma] \mapsto \Phi_{[\gamma]}$ de l'ensemble $\pi_1(X', z_0)$ des classes d'homotopie de lacets de base z_0 dans le groupe linéaire $\mathrm{GL}(\mathcal{F}_{z_0})$.

Exercice 1.3.2 Montrer que le lacet constant en z_0 a pour image l'automorphisme identité et en déduire que le prolongement analytique le long d'un lacet *homotopiquement trivial* (*i.e.* homotope au lacet constant) est trivial (*i.e.* c'est l'automorphisme identité).

Exemple 1.3.3 Dans le cas de $X' := \mathbf{C}^*$ et $z_0 := 1$, les deux exemples de 1.2 concernaient le "lacet fondamental" $\gamma : t \mapsto e^{2i\pi t}$. Dans chaque cas, l'automorphisme de prolongement analytique $\Phi_{[\gamma]}$ était non trivial, manifestant le fait que le lacet γ n'est pas homotopiquement trivial.

Remarque 1.3.4 Le principe de monodromie est ainsi appelé parce qu'il dit que divers chemins ("drom") donnent lieu à un seul ("mono") prolongement. Pourtant, l'effet du prolongement le long d'un chemin non homotopiquement trivial a fini par être appelé monodromie, alors qu'il se traduit par exemple par la *multiplicité* des déterminations de z^α ou du logarithme. Il y a donc eu dérive du sens étymologique ...

1.3.2 La représentation de monodromie

Si l'on compose les chemins γ_1 d'origine z_0 et d'extrémité z_1 et γ_2 d'origine z_1 et d'extrémité z_2, on obtient un chemin d'origine z_0 et d'extrémité z_2. Notons $\gamma_1.\gamma_2$ ce chemin composé[2]. Il est alors évident que :

$$\Phi_{\gamma_1.\gamma_2} = \Phi_{\gamma_2} \circ \Phi_{\gamma_1}.$$

Par ailleurs, la relation d'homotopie est compatible avec la composition des chemins, et, si l'on pose $[\gamma_1].[\gamma_2] := [\gamma_1.\gamma_2]$, on définit le composé de deux classes d'homotopie et l'on a :

$$\Phi_{[\gamma_1].[\gamma_2]} = \Phi_{[\gamma_2]} \circ \Phi_{[\gamma_1]}.$$

Dans le cas de lacets basés en un point $z_2 = z_1 = z_0$, on sait que l'opération ci-dessus fait de $\pi_1(X', z_0)$ un groupe, appelé *groupe fondamental* ou *groupe de Poincaré*. La discussion ci-dessus est résumée par le

Théorème 1.3.5 *L'application* $[\gamma] \mapsto \Phi_{[\gamma]}$ *est un* antihomomorphisme de groupes *de* $\pi_1(X', z_0)$ *dans* $GL(\mathcal{F}_{z_0})$.

Dit autrement, c'est un morphisme du groupe $\pi_1(X', z_0)^\circ$ (groupe *opposé* au groupe fondamental) dans $\mathrm{GL}(\mathcal{F}_{z_0})$. Un morphisme d'un groupe G dans un groupe linéaire est appelé *représentation (linéaire)* de G (chapitre 3), et nous venons de définir la *représentation de monodromie* en z_0 attachée à l'équation (1.1.0.1). On appelle *groupe de monodromie* de cette équation en z_0 l'image de cette représentation.

Exemple 1.3.6 Dans le cas des équations (1.2.0.1) et (1.2.0.2), $X' = \mathbf{C}^*$, et le groupe fondamental $\pi_1(X', 1)$ est isomorphe à $\mathbf{Z}$, la classe du lacet fondamental $t \mapsto e^{2i\pi t}$ étant l'un des deux générateurs. L'image dans $\mathbf{Z}$ de la classe du lacet $[\gamma]$ s'obtient en calculant l'unique entier $k \in \mathbf{Z}$ tel que γ est homotope à k fois le lacet fondamental : k est donc l'*indice* de γ tel qu'on le définit en analyse complexe ou en topologie algébrique.
Un morphisme ou un antihomomorphisme de $\mathbf{Z}$ dans $\mathrm{GL}(\mathcal{F}_1)$ est de la forme $k \mapsto \Phi_0^k$, où $\Phi_0 \in \mathrm{GL}(\mathcal{F}_1)$ est l'automorphisme de prolongement analytique le long du lacet fondamental, qui détermine donc complètement la représentation de monodromie.

Exemple 1.3.7 Dans le cas de l'équation (1.2.0.1), $\mathcal{F}_1$ est une droite vectorielle et le groupe linéaire $\mathrm{GL}(\mathcal{F}_1)$ s'identifie canoniquement (*i.e.* sans choix de base) à $\mathbf{C}^*$. On a vu que $\Phi_0 \in \mathrm{GL}(\mathcal{F}_1)$ s'identifie à $e^{2i\pi\alpha} \in \mathbf{C}^*$, et donc que la représentation de monodromie envoie le générateur $1 \in \mathbf{Z}$ sur $e^{2i\pi\alpha} \in \mathbf{C}^*$. C'est donc, modulo cette identification, l'application $k \mapsto e^{2i\pi k\alpha}$.
En particulier, le groupe de monodromie est $\{e^{2i\pi k\alpha} \mid k \in \mathbf{Z}\} \subset \mathbf{C}^*$. Il est trivial (resp. fini) si, et seulement si, $\alpha \in \mathbf{Z}$ (resp. $\alpha \in \mathbf{Q}$).

Exemple 1.3.8 Dans le cas de l'équation (1.2.0.2), $\dim_{\mathbf{C}} \mathcal{F}_1 = 2$ et le groupe linéaire $\mathrm{GL}(\mathcal{F}_1)$ s'identifie à $\mathrm{GL}_2(\mathbf{C})$, mais il faut pour cela choisir une base. Nous prendrons bien entendu la base $(1, \ln)$ (*i.e.* formée par les germes au point 1 de ces deux fonctions).
Dans ce cas, on a vu que $\Phi_0 \in \mathrm{GL}(\mathcal{F}_1)$ s'identifie à la matrice $A = \begin{pmatrix} 1 & 2i\pi \\ 0 & 1 \end{pmatrix}$. Ainsi, la représentation de monodromie (modulo ces identifications) est l'application $k \mapsto A^k$.

[2] Cette notation, traditionnelle, entraine de petites complications algébriques auxquelles il faut bien se faire ...

En particulier, le groupe de monodromie est le sous-groupe de $\mathrm{GL}(\mathcal{F}_1)$ qui correspond, dans la base donnée, au sous-groupe $\{A^k \mid k \in \mathbf{Z}\} \subset \mathbf{C}^*$ de $\mathrm{GL}_2(\mathbf{C})$. Ce groupe est infini.

Remarque 1.3.9 Décrire "la représentation de monodromie" attachée à une équation différentielle présuppose le choix d'un point de base $z_0 \in X'$; et, si l'on tient à une description matricielle, le choix d'une base de $\mathcal{F}_{z_0}$. Cependant, toutes les réalisations possibles du groupe de monodromie dans $\mathrm{GL}_n(\mathbf{C})$ sont conjuguées entre elles. En ce qui concerne l'effet du choix d'une base de $\mathcal{F}_{z_0}$, c'est évident (algèbre linéaire élémentaire). En ce qui concerne le choix d'un point base, cela découle du fait que X' est connexe par arcs.

Exercice 1.3.10 Expliciter l'effet du choix d'un point base.

1.4 La théorie de Galois différentielle

Le lecteur pourra compléter les maigres renseignements historiques qui suivent par la lecture de [3] et [4].

C'est Riemann qui, dans [29] et [30], a montré l'importance de la monodromie dans l'étude des équations différentielles dans le champ complexe ; c'est ensuite Hilbert qui en a donné la formalisation en termes de groupes et d'action linéaires (voir, dans [17], ce qui concerne le 21$^{\mathrm{e}}$ problème). La *correspondance de Riemann-Hilbert* est un thème essentiel en mathématiques.

Ce thème est dans l'esprit de la théorie de Galois : comprendre les équations même sans savoir les résoudre, à partir d'un groupe opérant sur leurs solutions ; comprendre les solutions elles-mêmes à partir du groupe attaché à l'équation.

Les "solutions" que l'on peut espérer comprendre grâce à la correspondance de Riemann-Hilbert sont les *fonctions spéciales* (voir par exemple [38]). Le type d'application que l'on peut espérer se laisse deviner à partir de deux exemples simples : si le groupe de monodromie est trivial, toutes les solutions se prolongent à X' ; dans le cas d'équations à coefficients polynomiaux, le groupe de monodromie est fini si, et seulement si, toutes les solutions sont des fonctions algébriques.

Exercice 1.4.1 Vérifier ces deux derniers énoncés sur nos exemples.

Naturellement, le cas où $X' = \mathbf{C}^*$ et le cas où $n = 1$ sont particulièrement simples parce qu'alors le groupe de monodromie est abélien. Le premier cas non trivial est celui où $X' = \mathbf{C} \setminus \Sigma$ avec $\mathrm{card}\ \Sigma = 2$, et où $n = 2$: c'est celui des *équations hypergéométriques*, sur lequel Riemann a démontré la puissance de sa méthode.

1.4.1 La théorie de Picard-Vessiot

Le calcul du groupe de monodromie d'une équation différentielle est, par nature, transcendant : il faut calculer une base de solutions, puis prolonger analytiquement ces dernières le long des lacets. La théorie de Picard-Vessiot vise à définir et calculer un groupe attaché à une équation différentielle par des voies purement algébriques et, autant que possible, à partir de l'équation elle-même. Comme on va le voir, elle s'inspire de la théorie de Galois, et le domaine auquel elle a

donné naissance est d'ailleurs appelé *théorie de Galois différentielle*.

L'idée de base est la suivante. Le prolongement analytique le long d'un chemin préserve les relations algébriques. En fait, chaque $\Phi_{[\gamma]}$ est un morphisme d'espaces vectoriels, mais également un morphisme pour la multiplication (à condition de l'étendre, au delà des germes de solutions, à toutes les fonctions analytiques susceptibles de prolongement). D'autre part, la raison pour laquelle une solution est transformée en une solution est que $\Phi_{[\gamma]}$ est compatible avec la dérivation :

$$\Phi_{[\gamma]}(f') = \big(\Phi_{[\gamma]}(f)\big)'.$$

On dit aussi que $\Phi_{[\gamma]}$ *commute à la dérivation*. On va donc chercher à caractériser les éléments du groupe de monodromie comme éléments de $\mathrm{GL}(\mathcal{F}_{z_0})$ qui préservent les relations algébriques et les relations différentielles. (La contrepartie en théorie de Galois classique est de rechercher les éléments du groupe de permutation des racines qui préservent les relations algébriques.)

Comme pour la forme "moderne" (c'est-à-dire datant du début du XX$^{\mathrm{e}}$ siècle) de la théorie de Galois, on commence par traduire cela en termes d'automorphismes pour une structure donnée. Ici, on introduit le corps K engendré par les fonctions qui servent de coefficients (par exemple les fonctions rationnelles) ainsi que les solutions de l'équation et toutes leurs dérivées. (La contrepartie en th éorie de Galois classique est le corps engendré par les éléments qui servent de coefficients, par exemple les nombres rationnels, et par les solutions de l'équation.)

Enfin, on définit le *groupe de Galois de l'équation différentielle* comme le groupe des automorphismes du corps K qui commutent à la dérivation et qui induisent l'identité sur le sous-corps K_0 des coefficients.

Exemple 1.4.2 On reprend l'exemple des caractères. Soit $\mathcal{M}(U_0)$ le corps des fonctions méromorphes sur U_0. Soit f_0 une base de $\mathcal{F}(U_0)$, par exemple z^α. On prend pour K le sous-corps de $\mathcal{M}(U_0)$ engendré par le corps des coefficients $K_0 = \mathbf{C}(z)$ (corps des fractions rationnelles) et par f_0 : comme $f_0' = \dfrac{\alpha}{z} f_0$, les dérivées viennent avec ! On cherche les automorphismes ϕ du corps K qui sont triviaux sur $\mathbf{C}(z)$ et tels que $\phi(f') = \big(\phi(f)\big)'$ pour tout f.
Soit $f := \phi(f_0)$, qui n'est donc pas nul. On a :

$$\frac{f'}{f} = \frac{\phi(f_0)'}{\phi(f_0)} = \frac{\phi(f_0')}{\phi(f_0)} = \phi\left(\frac{f_0'}{f_0}\right) = \phi\left(\frac{\alpha}{z}\right) = \frac{\alpha}{z};$$

cette dernière égalité vient de l'hypothèse que ϕ est trivial sur $K_0 = \mathbf{C}(z)$. Ainsi, f est une solution de (1.2.0.1), donc de la forme $f = \lambda f_0$ pour un certain $\lambda \in \mathbf{C}^*$.
Il est clair que ϕ est totalement déterminé par λ et que l'application $\phi \mapsto \lambda$ est un morphisme injectif du groupe de Galois de (1.2.0.1) dans $\mathbf{C}^*$. Mais ce morphisme est-il surjectif, autrement dit, tout $\lambda \in \mathbf{C}^*$ définit-il un automorphisme ϕ convenable ?
Dans le cas où $\alpha \in \mathbf{Q}$, soit $\alpha = p/q$ (fraction irréductible), on a $f_0^q = z^p \in K_0$, donc $f_0^q = \phi(f_0^q) = f^q$, donc $\lambda^q = 1$ et $\lambda \in \mu_q$, groupe des racines q^{es} de l'unité. Réciproquement, tout tel λ convient, et le groupe de Galois est donc $\mu_q \subset \mathbf{C}^*$ dans ce cas.
Dans le cas où $\alpha \notin \mathbf{Q}$, on vérifie facilement que z^α est transcendant sur $\mathbf{Q}$ et tout λ convient. Le groupe de Galois est donc $\mathbf{C}^*$ dans ce cas.

Dans tous les cas, les automorphismes de monodromie sont bien là : ce sont des “automorphismes galoisiens”.

Exemple 1.4.3 On reprend l'exemple du logarithme. Avec les mêmes notations que ci-dessus, K est ici le sous-corps de $\mathcal{M}(U_0)$ engendré par $K_0 = \mathbf{C}(z)$ et par $\ln$; comme $\ln' = 1/z$, les dérivées viennent avec. Pour tout automorphisme galoisien ϕ, notant $f := \phi(\ln)$, on a :

$$f' = \big(\phi(\ln)\big)' = \phi(\ln') = \phi(1/z) = 1/z,$$

d'où $\phi(\ln) = \ln + a$ pour une certaine constante $a \in \mathbf{C}$. Il est facile de vérifier que $\ln$ est transcendant sur K_0 et que tout a convient, et d'en déduire que le groupe de Galois est ici isomorphe à $\mathbf{C}$.
Pour y retrouver les automorphismes de monodromie, il faut se rappeler que ces derniers laissent invariant $1 \in K_0$ et qu'ils envoient $\ln$ sur $\ln + 2i\pi k$. En fait, en identifiant le groupe de Galois $\mathbf{C}$ au groupe des matrices $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ (ce sont bien des groupes isomorphes), on retrouve bien les automorphismes de monodromie comme cas particuliers d'automorphismes galoisiens.

La leçon à tirer de nos calculs est que la théorie de Galois donne un groupe qui contient le groupe de monodromie, mais qui peut être plus gros. En fait, on se retrouve dans une situation de la forme :

$$M \subset G \subset \mathrm{GL}_n(\mathbf{C}),$$

et l'on se demande quelle relation (autre que l'inclusion) relie le groupe de monodromie M au groupe de Galois G. Résumons les cas observés :

1. Équation (1.2.0.1) avec $\alpha = p/q$; Notant $\langle g \rangle$ le groupe engendré par g :

$$\begin{array}{ccccc} M & \subset & G & \subset & \mathrm{GL}_1(\mathbf{C}) \\ \| & & \| & & \| \\ \langle e^{2i\pi\alpha} \rangle = \mu_q & \subset & \mu_q & \subset & \mathbf{C}^* \end{array}$$

2. Équation (1.2.0.1) avec $\alpha \notin \mathbf{Q}$:

$$\begin{array}{ccccc} M & \subset & G & \subset & \mathrm{GL}_1(\mathbf{C}) \\ \| & & \| & & \| \\ \langle e^{2i\pi\alpha} \rangle & \subset & \mathbf{C}^* & \subset & \mathbf{C}^* \end{array}$$

   L'inclusion $M \subset G$ est ici stricte.

3. Équation (1.2.0.2) :

$$\begin{array}{ccccc} M & \subset & G & \subset & \mathrm{GL}_2(\mathbf{C}) \\ \| & & \| & & \| \\ \langle A \rangle & \subset & \{A^a \mid a \in \mathbf{C}\} & \subset & \mathrm{GL}_2(\mathbf{C}) \end{array}$$

   La matrice A étant unipotente, la puissance A^a est bien définie. L'inclusion $M \subset G$ est encore stricte.

On constate que, dans chaque cas, le sous-ensemble G de $\mathrm{GL}_n(\mathbf{C})$ peut être caractérisé par des équations algébriques : $X^q = 1$ dans le premier cas, aucune équation dans le deuxième cas, $X_{1,1} - 1 = X_{2,2} - 1 = X_{1,2} = 0$ dans le troisième cas. On dit que G est un *sous-ensemble algébrique* de $\mathrm{GL}_n(\mathbf{C})$.

On constate aussi dans chaque cas (mais c'est un peu moins évident) que G est le plus petit sous-ensemble algébrique de $\mathrm{GL}_n(\mathbf{C})$ contenant M.

Exercice 1.4.4 Le vérifier dans chaque cas.

Comme on le verra (mais c'est facile à démontrer), l'assertion "G est le plus petit sous-ensemble algébrique de $\mathrm{GL}_n(\mathbf{C})$ contenant M" est équivalente à la suivante : "toute fonction rationnelle sur $\mathrm{Mat}_n(\mathbf{C})$ définie sur $\mathrm{GL}_n(\mathbf{C})$ et nulle sur M est nulle sur G". Cela s'apparente à une propriété de densité, et l'on dit en effet que M est *Zariski-dense* dans G.

En fait, c'est un théorème dû à Schlesinger que, pour une équation différentielle dont les singularités sont "raisonnables", le groupe de Galois est toujours le plus petit sous-ensemble algébrique du groupe linéaire contenant le groupe de monodromie ; autrement dit, le groupe de monodromie est Zariski-dense dans le groupe de Galois. Nous ne définirons pas "raisonnable", mais le lecteur intéressé peut regarder dans [2] ou dans d'autres ouvrages ce qui concerne les "singulartiés régulières" ou les "équations fuchsiennes".

Exercice 1.4.5 Vérifier que c'est faux pour l'équation $f' = f$. (Le groupe de monodromie est trivial, le groupe de Galois est égal à $\mathrm{GL}_1(\mathbf{C}) = \mathbf{C}^*$.) La raison en est que cette équation admet une singularité "déraisonnable" à l'infini !

Ce qui est vrai sans restriction, c'est que le groupe de Galois d'une équation différentielle linéaire se réalise toujours comme sous-ensemble algébrique (et sous-groupe) du groupe linéaire, d'où l'intérêt d'étudier de tels groupes : ce sont les *groupes algébriques linéaires*.

1.4.2 La dualité tannakienne

En théorie de Galois clasique, le groupe de Galois ne porte qu'une information partielle. Ce qui est vraiment important, c'est l'action de ce groupe sur les racines ou sur un corps. De la même manière, dans la théorie de Riemann-Hilbert, le groupe de monodromie ne porte qu'une information partielle, ce qui est vraiment important, c'est la représentation de monodromie. De la même manière, en théorie de Galois différentielle, c'est l'action du groupe de Galois qui nous intéresse ; on verra que c'est encore une représentation linéaire, et même "rationnelle" (cette propriété met en jeu la structure de groupe algébrique).

En fait, on a prouvé (*cf.* par exemple [10]) que l'on pouvait calculer le groupe de Galois à partir de la classe de toutes ses représentations ; ce point de vue a d'ailleurs été appliqué à la théorie de Galois classique, et a permis de lui donner une allure géométrique en l'unifiant avec la théorie des revêtements en topologie algébrique (*cf.* par exemple [12]). Cette méthode a une chance de fonctionner parce qu'il arrive que l'on sache d'avance qu'une certaine "catégorie" d'objets (le mot sera défini plus loin) s'identifie à la catégorie des représentations rationnelles d'un certain groupe algébrique, que l'on peut alors définir explicitement. Une telle catégorie est dite "tannakienne". Nous ne les étudierons cependant pas en toute généralité. Dans notre cas, c'est la catégorie des représentations de M qui s'identifie la catégorie des représentations rationnelles de G, et nous verrons comment en déduire G.

Signalons enfin que le but n'est pas seulement de disposer d'une alternative à la théorie de Picard-Vessiot. D'abord, la méthode tannakienne apporte plus d'informations sur le groupe de Galois (par exemple, son comportement quand on change le corps de base) ; ensuite, elle s'applique dans des domaines où la théorie de Picard-Vessiot a échoué (théorie de Galois transcendante des équations aux q-différences). En contrepartie (mais peut-être est-ce un avantage ?), elle exige d'investir dans des techniques variées.

Chapitre 2

Catégories, foncteurs, équivalences, limites, produit tensoriel

Ce chapitre a pour but d'introduire le langage des catégories et des foncteurs, indispensable pour toutes les théories qui utilisent la géométrie algébrique (et bien d'autres). Il y a surtout du vocabulaire et des énoncés élémentaires, entrecoupés d'exemples destinés à faciliter la digestion. L'essentiel de la théorie se trouve dans le classique [22]. Pour usage ultérieur, et comme exemple de propriété universelle, nous rappelons rapidement ce qui aurait dû être vu en M1 (où, sinon ?) sur le produit tensoriel ; un exposé complet figure dans [21].

2.1 Catégories et foncteurs

2.1.1 Catégories

La théorie des catégories permet par exemple de parler de la catégorie des ensembles. Comme le lecteur sait, ou devrait savoir, qu'il n'y a pas d'ensemble de tous les ensembles, il est clair que l'on ne peut pas formuler cette théorie dans le cadre habituel de la théorie des ensembles. Pour ne pas noyer ce qui nous importe dans du formalisme (il y en aura déjà bien assez), nous éluderons ce genre de difficulté et utiliserons le mot "classe" dans les cas douteux.

Définition 2.1.1 (Catégories) Une *catégorie* $\mathcal{C}$ est la donnée :
- d'une "classe" d'*objets*, notée $\mathrm{Ob}(\mathcal{C})$;
- d'une "classe" de *morphismes (ou flèches)* notée $\mathrm{Mor}_{\mathcal{C}}$;
- pour chaque $f \in \mathrm{Mor}_{\mathcal{C}}$, d'une *source* (ou *source*) $s(f) \in \mathrm{Ob}(\mathcal{C})$ et d'un *but* (ou *target*) $t(f) \in \mathrm{Ob}(\mathcal{C})$: on dit que f va de X dans Y et l'on écrit $f : X \to Y$;
- pour chaque objet $X \in \mathrm{Ob}(\mathcal{C})$, d'un *morphisme identité* $\mathrm{Id}_X \in \mathrm{Mor}_{\mathcal{C}}$ de source et but X ;
- pour chaque couple de flèches $f, g \in \mathrm{Mor}_{\mathcal{C}}$ telles que $t(f) = s(g)$, d'une *composée* notée $g \circ f \in \mathrm{Mor}_{\mathcal{C}}$, telle que $s(g \circ f) = s(f)$ et $t(g \circ f) = t(g)$.

Ces données sont assujetties aux axiomes suivants :
- Pour tous $X, Y \in \mathrm{Ob}(\mathcal{C})$, les flèches $f \in \mathrm{Mor}_{\mathcal{C}}$ telles que $s(f) = X$ et $t(f) = Y$ forment un ensemble noté $\mathrm{Mor}_{\mathcal{C}}(X,Y)$, ou $\mathrm{Mor}(X,Y)$, ou $\mathrm{Hom}_{\mathcal{C}}(X,Y)$, ou encore $\mathrm{Hom}(X,Y)$; ces ensembles sont donc deux à deux disjoints, $\mathrm{Id}_X \in \mathrm{Mor}_{\mathcal{C}}(X,X)$ et $(f,g) \mapsto g \circ f$ est une application (dite *de composition*) de $\mathrm{Mor}_{\mathcal{C}}(X,Y) \times \mathrm{Mor}_{\mathcal{C}}(Y,Z)$ dans $\mathrm{Mor}_{\mathcal{C}}(X,Z)$.

– chaque $\mathrm{Id}_X \in \mathrm{Mor}_{\mathcal{C}}(X,X)$ est "neutre à gauche et à droite", *i.e.* les égalités ci-dessous sont vérifiées chaque fois qu'elles ont un sens :

$$f \circ \mathrm{Id}_X = f \text{ et } \mathrm{Id}_X \circ g = g.$$

– La "loi de composition partielle" est associative, *i.e.* l'égalité ci-dessous est vérifiée chaque fois qu'elle a un sens :

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Terminologie.

1. Un *endomorphisme* de X est un morphisme de X dans X. Ils forment l'ensemble $\mathrm{End}(X)$.
2. Un *isomorphisme* de X sur Y est une flèche de X dans Y inversible à droite et à gauche ; autrement dit, $f \in \mathrm{Mor}_{\mathcal{C}}(X,Y)$ est telle qu'il existe $f', f'' \in \mathrm{Mor}_{\mathcal{C}}(Y,X)$ tels que $f' \circ f = \mathrm{Id}_X$ et $f \circ f'' = \mathrm{Id}_Y$. Ils forment l'ensemble $\mathrm{Iso}(X)$.
3. Un *automorphisme* de X est un isomorphisme de X sur X. Ils forment l'ensemble $\mathrm{Aut}(X)$.
4. La catégorie $\mathcal{C}'$ est une *sous-catégorie* de la catégorie $\mathcal{C}$ si $\mathrm{Ob}(\mathcal{C}') \subset \mathrm{Ob}(\mathcal{C})$ et si $\mathrm{Mor}_{\mathcal{C}'}(X,Y) \subset \mathrm{Mor}_{\mathcal{C}}(X,Y)$ pour tous $X,Y \in \mathrm{Ob}(\mathcal{C}')$.
5. La sous-catégorie $\mathcal{C}'$ de $\mathcal{C}$ est dite *pleine* si $\mathrm{Mor}_{\mathcal{C}'}(X,Y) = \mathrm{Mor}_{\mathcal{C}}(X,Y)$ pour tous $X,Y \in \mathrm{Ob}(\mathcal{C}')$; elle est dite *essentielle* si tout objet de $\mathcal{C}$ est isomorphe à un objet de $\mathcal{C}'$.

Exercice 2.1.2 1. Muni de la composition, $\mathrm{End}(X)$ est un monoïde de neutre Id_X.

2. L'inverse à gauche et l'inverse à droite d'un isomorphisme $f \in \mathrm{Mor}_{\mathcal{C}}(X,Y)$ sont égaux. On note f^{-1} ce morphisme, appelé *inverse* de f. C'est un isomorphisme et son inverse est f.
3. Muni de la composition, $\mathrm{Aut}(X)$ est un groupe de neutre Id_X ; le symétrique d'un automorphisme est son inverse.

Exemples 2.1.3 (à vérifier soigneusement) 1. La catégorie $\mathcal{E}ns$ des ensembles et des applications : c'est une manière abrégée de dire que $\mathrm{Ob}(\mathcal{E}ns)$ est la classe de tous les ensembles, que $\mathrm{Mor}_{\mathcal{E}ns}(X,Y)$ est l'ensemble des applications de l'ensemble X vers l'ensemble Y, que Id_X désigne l'application identité de X et que la composition des morphismes dans $\mathcal{E}ns$ est la composition des applications.

2. La catégorie $\mathcal{G}r$ des groupes et des morphismes de groupes.
3. La catégorie $\mathcal{T}op$ des espaces topologiques et des applications continues.
4. La catégorie $\mathcal{T}op_*$ des *espaces topologiques pointés*. Ses objets sont les couples (X,x_0) formés d'un espace topologique X et d'un point $x_0 \in X$; les morphismes de (X,x_0) dans (Y,y_0) sont les applications continues $f : X \to Y$ telles que $f(x_0) = y_0$.
5. Pour un anneau A donné (non nécessairement commutatif), la catégorie $\mathcal{M}od_A$ des A-modules à gauche et des applications A-linéaires. Lorsque A est un corps commutatif K, on écrira plutôt $\mathcal{E}v_K$.
6. Pour un corps commutatif K, la catégorie $\mathcal{E}vf_K$ des K-espaces vectoriels de dimension finie et des applications K-linéaires : donc une sous-catégorie pleine de $\mathcal{E}v_K$.
7. La catégorie $\mathcal{A}nn$ des anneaux commutatifs (sous-entendu : "et des morphismes d'anneaux").

Exercice 2.1.4 On se donne une catégorie $\mathcal{C}$. Vérifier que l'on obtient bien une catégorie $\mathcal{C}_{end}$ (resp. $\mathcal{C}_{aut}$), en prenant pour objets les couples (X, f), où $X \in \mathrm{Ob}(\mathcal{C})$ et $f \in \mathrm{End}(X)$ (resp. $f \in \mathrm{Aut}(X)$) ; et pour morphismes $(X, f) \to (Y, g)$ les $u \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$ tels que $g \circ u = u \circ f$, ce que l'on traduit en disant que le diagramme ci-dessous est commutatif :

$$\begin{array}{ccc} X & \xrightarrow{u} & Y \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ X & \xrightarrow{u} & Y \end{array}$$

2.1.2 Foncteurs

Un foncteur covariant est un "morphisme de catégories", un foncteur contravariant est un "antimorphisme de catégories". Plus précisément :

Définition 2.1.5 (Foncteurs) Soient $\mathcal{C}$ et $\mathcal{C}'$ deux catégories.
(i) On appelle *foncteur covariant* de $\mathcal{C}$ dans $\mathcal{C}'$ la donnée d'une fonction F de $\mathrm{Ob}(\mathcal{C})$ dans $\mathrm{Ob}(\mathcal{C}')$, ce que nous noterons $X \rightsquigarrow F(X)$ ou $X \rightsquigarrow FX$; et, pour tous objets X, Y de $\mathcal{C}$, d'une application également notée F de $\mathrm{Mor}_{\mathcal{C}}(X, Y)$ dans $\mathrm{Mor}_{\mathcal{C}'}(FX, FY)$; le tout, de telle sorte que $F(\mathrm{Id}_X) = \mathrm{Id}_{FX}$ et que, lorsque ces compositions sont définies, on ait $F(g \circ f) = F(g) \circ F(f)$.
(ii) On appelle *foncteur contravariant* de $\mathcal{C}$ dans $\mathcal{C}'$ la donnée d'une fonction F de $\mathrm{Ob}(\mathcal{C})$ dans $\mathrm{Ob}(\mathcal{C}')$ et, pour tous objets X, Y de $\mathcal{C}$, d'une application également notée F de $\mathrm{Mor}_{\mathcal{C}}(X, Y)$ dans $\mathrm{Mor}_{\mathcal{C}'}(FY, FX)$, de telle sorte que $F(\mathrm{Id}_X) = \mathrm{Id}_{FX}$ et que, lorsque ces compositions sont définies, on ait $F(g \circ f) = F(f) \circ F(g)$.

Lorsque l'on parlera de foncteur sans autre précision, il s'agira d'un foncteur covariant. On décrit souvent un foncteur par son seul effet sur les objets, le contexte permettant de deviner sans ambigüité quel est l'effet sur les morphismes. La notation $X \rightsquigarrow FX$, plutôt que $X \mapsto FX$, a pour but de nous rappeler que $\mathrm{Ob}(\mathcal{C})$ et $\mathrm{Ob}(\mathcal{C}')$ ne sont pas des ensembles et que la fonction F sur les objets n'est donc pas une application.

Exemples 2.1.6 (à vérifier soigneusement)

1. Dans toute catégorie, il y a un foncteur (covariant) identité dont l'effet sur les objets est $X \rightsquigarrow X$ et l'effet sur les morphismes est $f \mapsto f$.
2. On définit des *foncteurs (covariants) oublis* partant respectivement de $\mathcal{G}r$, de $\mathcal{T}op$, de $\mathcal{T}op_*$, de $\mathcal{M}od_A$, de $\mathcal{E}vf_K$ et de $\mathcal{A}nn$, et arrivant dans $\mathcal{E}ns$, par "oubli de structure" : à un objet, ils associent l'ensemble sous-jacent ; et, à un morphisme, l'application sous-jacente.
3. On définit de même des foncteurs d'oubli partiel de structure : de $\mathcal{T}op_*$ dans $\mathcal{T}op$, de $\mathcal{M}od_A$ dans $\mathcal{G}r$, de $\mathcal{A}nn$ dans $\mathcal{G}r$, etc.
4. Soit A un anneau commutatif. Le foncteur de dualité de $\mathcal{M}od_A$ dans elle-même associe à tout A-module M son dual $M^* := \mathrm{Hom}_A(M, A)$ (avec sa structure naturelle de A-module à gauche, dûe à la commutativité de A), et, à tout morphisme $f : M \to N$, son transposé ${}^t f : N^* \to M^*$ défini par ${}^t f(u) := u \circ f$. C'est un foncteur contravariant. De même, il y a un foncteur de dualité de $\mathcal{E}vf_K$ dans elle-même.
5. Plus généralement, en associant aux A-modules M, N le A-module $\mathrm{Hom}_A(M, N)$, on définit un *bifoncteur* de $\mathcal{M}od_A$ dans elle-même ; il est contravariant en M et covariant en N.
6. Le foncteur $A \rightsquigarrow \mathrm{Sp}(A)$ est contravariant de $\mathcal{A}nn$ dans $\mathcal{T}op$.

Exercice 2.1.7 Définir la catégorie $\mathcal{C}at$ des catégories et des foncteurs.

Proposition 2.1.8 *Si F est un foncteur (covariant ou contravariant) et f un isomorphisme, alors Ff est un isomorphisme et $(Ff)^{-1} = F\left(f^{-1}\right)$.*

Preuve. - Soit $f : X \to Y$ un isomorphisme et soit g l'inverse de f. Alors, dans le cas covariant :

$$F(g)\circ F(f) = F(g\circ f) = F(\mathrm{Id}_X) = \mathrm{Id}_{FX} \text{ et } F(f)\circ F(g) = F(f\circ g) = F(\mathrm{Id}_Y) = \mathrm{Id}_{FY},$$

et $F(f)$ admet $F(g)$ pour inverse. Dans le cas contravariant :

$$F(g)\circ F(f) = F(f\circ g) = F(\mathrm{Id}_Y) = \mathrm{Id}_{FY} \text{ et } F(f)\circ F(g) = F(g\circ f) = F(\mathrm{Id}_X) = \mathrm{Id}_{FX},$$

et $F(f)$ admet encore $F(g)$ pour inverse. □

Exemple 2.1.9 (à vérifier soigneusement) On définit un foncteur covariant de $\mathcal{T}op_*$ dans $\mathcal{G}r$ en associant à tout espace pointé (X,x_0) le groupe fondamental $\pi_1(X,x_0)$. Son effet sur les morphismes est le suivant : si $f : (X,x_0) \to (Y,y_0)$ est une application continue telle que $f(x_0) = y_0$, alors l'application $\gamma \mapsto f\circ\gamma$ transforme les lacets dans X basés en x_0 en lacets dans Y basés en y_0, elle est compatible avec les homotopies, et passe au quotient en un morphisme de groupes de $\pi_1(X,x_0)$ dans $\pi_1(Y,y_0)$. Par ailleurs, si $X \subset \mathbf{R}^n$ est un ensemble étoilé en x_0, le groupe $\pi_1(X,x_0)$ est trivial ; et, si $Y = \mathbf{C}^*$, son groupe fondamental basé en n'importe quel point est isomorphe à $\mathbf{Z}$. Il découle alors de la proposition que $\mathbf{C}^*$ n'est homéomorphe à aucune partie étoilée d'un $\mathbf{R}^n$.

Et maintenant, un objet vraiment étrange : le morphisme entre foncteurs.

Définition 2.1.10 (Transformation naturelle) Une *transformation naturelle* $\phi : F \to G$ entre deux foncteurs tous deux covariants ou tous deux contravariants de $\mathcal{C}$ dans $\mathcal{C}'$ est la donnée, pour tout objet X de $\mathcal{C}$, d'un morphisme $\phi_X : FX \to GX$ (c'est donc une flèche dans $\mathcal{C}'$), de telle sorte que, pour tous objets X,Y de $\mathcal{C}$, on ait $\phi_Y \circ F(f) = G(f)\circ\phi_X$. En termes de diagrammes commutatifs :

$$\begin{array}{ccc} FX & \xrightarrow{F(f)} & FY \\ {\scriptstyle\phi_X}\downarrow & & \downarrow{\scriptstyle\phi_Y} \\ GX & \xrightarrow{G(f)} & GY \end{array}$$

Exemple 2.1.11 (à vérifier soigneusement) Fixons un anneau commutatif A. Pour tout A-module M, notons F_M le foncteur covariant $N \rightsquigarrow \mathrm{Hom}_A(M,N)$ de $\mathcal{M}od_A$ dans elle-même. Alors tout morphisme $u : M \to M'$ fournit une transformation naturelle ϕ de $F_{M'}$ dans F_M : pour tout module N, on définit $\phi_N : F_{M'}(N) \to F_M(N)$ en posant $\phi_N(f) := f\circ u$.

Un *isomorphisme* $\phi : F \to G$ entre deux foncteurs tous deux covariants ou tous deux contravariants de $\mathcal{C}$ dans $\mathcal{C}'$ est une transformation naturelle telle que chaque morphisme $\phi_X : FX \to GX$ est un isomorphisme dans $\mathcal{C}'$. L'*inverse* de cet isomorphisme est alors la transformation naturelle $\psi : G \to F$ obtenue en posant $\psi_X := \phi_X^{-1}$; on la note ϕ^{-1}. Le lecteur vérifiera que c'est bien une transformation naturelle. De même, on peut composer deux transformations naturelles $\phi : F \to G$ et $\psi : G \to H$, etc.

Exercice 2.1.12 Les catégories $\mathcal{C}$ et $\mathcal{C}'$ étant fixées, définir la catégorie des foncteurs $\mathcal{C} \to \mathcal{C}'$.

2.1.3 Équivalences de catégories

Définition 2.1.13 (Équivalence de catégories) On dit que le foncteur covariant $F : \mathcal{C} \to \mathcal{C}'$ est *essentiellement surjectif* si tout objet de $\mathcal{C}'$ est isomorphe à un FX, $X \in \mathrm{Ob}(\mathcal{C})$. On dit que F est *fidèle*, resp. *plein*, resp. *pleinement fidèle* si, pour tous objets X, Y de $\mathcal{C}$, l'application $f \mapsto F(f)$ de $\mathrm{Mor}_{\mathcal{C}}(X,Y)$ dans $\mathrm{Mor}_{\mathcal{C}'}(FX,FY)$ est injective, resp. surjective, resp. bijective. On dit que F est une *équivalence de catégories* s'il est essentiellement surjectif et pleinement fidèle.

Les définitions similaires pour un foncteur contravariant conduiraient à la notion d'*antiéquivalence*.

Exemple 2.1.14 Si $\mathcal{C}$ est une sous-catégorie de $\mathcal{C}'$, il y a un foncteur évident d'inclusion de $\mathcal{C}$ dans $\mathcal{C}'$. Ce foncteur est fidèle ; il est essentiellement surjectif (resp. pleinement fidèle) si, et seulement si, la sous-catégorie est essentielle (resp. pleine).

Proposition 2.1.15 *Pour que le foncteur covariant $F : \mathcal{C} \to \mathcal{C}'$ soit une équivalence de catégories, il faut, et il suffit, qu'il existe un foncteur covariant $G : \mathcal{C}' \to \mathcal{C}$ tel que $G \circ F$ soit isomorphe au foncteur identité de $\mathcal{C}$ et que $F \circ G$ soit isomorphe au foncteur identité de $\mathcal{C}'$.*

La preuve est donnée dans [22]. Un tel foncteur G est appelé *quasi-inverse* de F. Il n'y a pas unicité, mais tous les quasi-inverses de F sont isomorphes entre eux.

Remarque 2.1.16 La notion d'équivalence de catégories est plus faible que celle d'isomorphisme dans la catégorie des catégories : dans ce dernier cas, on exigerait que les foncteurs $G \circ F$ et $F \circ G$ soient égaux aux foncteurs identités. C'est pourtant bien l'équivalence qui dit si deux catégories sont "essentiellement les mêmes". En effet, ce n'est pas l'égalité des objets qui compte mais leur isomorphie. Par exemple, peut-on dire que le groupe $\mathbf{Z}$ est dans l'image du foncteur "groupe fondamental" ? Par exemple, $\mathbf{Z}$ est-il *égal* à $\pi_1(\mathbf{C}^*, 1)$? Les éléments de ce dernier groupe sont des classes d'homotopie de lacets. L'une d'elle est-elle égale au nombre entier 1 ? Quelle que soit la définition choisie de $\mathbf{Z}$, c'est absurde. Ce qui est vrai, et important, c'est que $\mathbf{Z}$ est isomorphe à $\pi_1(\mathbf{C}^*, 1)$ et qu'il appartient donc à "l'image essentielle" du foncteur "groupe fondamental".

Exemple 2.1.17 Lorsque l'on étudie la réduction des endomorphismes sur un corps commutatif K, on utilise le fait qu'il "revient au même" de munir le K-espace vectoriel de dimension finie E d'un endomorphisme f ou bien de faire de E un module sur l'anneau des polynômes $K[X]$. Nous allons formaliser cette équivalence, mais sans nous restreindre aux espaces de dimension finie.
Considérons donc la catégorie $\mathcal{C}$ des couples (E, f) formés d'un K-espace vectoriel E et d'un endomorphisme f de E. Les morphismes de (E, f) dans (E', f') sont les applications linéaires $u : E \to E'$ telles que $f' \circ u = u \circ f$ (c'est le procédé de l'exercice 2.1.4). Considérons d'autre part la catégorie $\mathcal{C}' := \mathcal{M}od_{K[X]}$. Pour tout (E, f) de $\mathcal{C}$, on peut définir un $K[X]$-module M dont le groupe sous-jacent est E et dont la loi externe est définie par :

$$\forall P \in K[X]\ ,\ \forall x \in M\ ,\ P.x := P(f)(x).$$

(C'est bien un $K[X]$-module.) Si u est un morphisme de (E, f) dans (E', f'), alors c'est un morphisme des $K[X]$-modules associés. On a ainsi défini un foncteur de $\mathcal{C}$ dans $\mathcal{C}'$.
Pour tout $K[X]$-module, notant E le K-espace vectoriel sous-jacent, on voit que $f : x \mapsto X.x$ est un endomorphisme de E et donc (E, f) un objet de $\mathcal{C}$. Le lecteur définira l'effet sur les morphismes du foncteur correspondant, et vérifiera que c'est un quasi-inverse du précédent.

Exercice 2.1.18 Interpréter de manière analogue la catégorie des (E, f) où f est un automorphisme de E, puis (dans l'autre sens) la catégorie des $K[X,Y]$-modules.

2.2 Problèmes universels

2.2.1 Limites inductives (direct limits)

C'est une sorte de généralisation de la réunion. La version la plus générale est décrite dans [22], nous n'étudions ici que les systèmes inductifs indexés par des ensembles ordonnés filtrants. Noter que [21] contient un exposé concis dans le cas de la catégorie $\mathcal{M}od_A$.

Exemple 2.2.1 Pour définir l'anneau $K[X_1,\ldots,X_n,\ldots]$ des polynômes à une infinité (dénombrable) d'indéterminées sur le corps commutatif K, l'idée naturelle est de prendre la réunion des $K[X_1,\ldots,X_n]$ pour $n \in \mathbf{N}$. Mais, dans les constructions usuelles, ces ensembles ne sont pas inclus les uns dans les autres : par exemple l'élément a de K n'est pas le polynôme constant a de $K[X_1]$, il sont seulement identifiés via le morphisme canonique de K dans $K[X_1]$. En fait, dans la "réunion" des $K[X_1,\ldots,X_n]$ tous les morphismes canoniques de $K[X_1,\ldots,X_n]$ dans $K[X_1,\ldots,X_p]$ pour $n \leq p$ interviennent comme contraintes d'identification.

Définition 2.2.2 (Système inductif) Soit I un ensemble ordonné *filtrant (à droite)*, autrement dit :

$$\forall i,j \in I\ ,\ \exists k \in I\ :\ (i \leq k \text{ et } j \leq k).$$

Un *système inductif* indexé par I dans la catégorie $\mathcal{C}$ est la donnée d'une famille $(X_i)_{i\in I}$ d'objets de $\mathcal{C}$ et d'une famille $(\phi^i_j)_{\substack{i,j\in I\\ i\leq j}}$ de morphismes de $\mathcal{C}$ tels que $\phi^i_j \in \mathrm{Mor}_{\mathcal{C}}(X_i,X_j)$ et que :

$$\big(\forall i \in I\ ,\ \phi^i_i = \mathrm{Id}_{X_i}\big) \text{ et } \big(\forall i,j,k \in I\ ,\ i \leq j \leq k\ ,\ \phi^j_k \circ \phi^i_j = \phi^i_k\big).$$

Exercice 2.2.3 Faire de I une catégorie dont les objets sont les éléments de I et les morphismes sont les couples (i,j) tels que $i \leq j$ et vérifier qu'un système inductif est alors la même chose qu'un foncteur covariant.

Définition 2.2.4 (Limite inductive) Une *limite inductive* du système inductif $\big((X_i)_{i\in I}, (\phi^i_j)_{\substack{i,j\in I\\ i\leq j}}\big)$, est la donnée d'un objet X de $\mathcal{C}$ et d'une famille $(\phi^i)_{i\in I}$ de morphismes $\phi^i : X_i \to X$, le tout assujetti à deux conditions :
(i) La famille des ϕ^i est "compatible" avec le système inductif, au sens où l'on a :

$$\forall i,j \in I\ ,\ i \leq j\ ,\ \phi^j \circ \phi^i_j = \phi^i.$$

(On peut penser que l'on a remplacé k par ∞ dans les relations de la définition précédente.)
(ii) Le couple $\big(X,(\phi^i)_{i\in I}\big)$ est *initial* parmi tous les couples vérifiant (i). Cela signifie que, pour tout $\big(Y,(\psi^i)_{i\in I}\big)$ de même nature et vérifiant (i), il existe un unique morphisme $f : X \to Y$ rendant commutatifs tous les diagrammes concernés :

$$\forall \big(Y,(\psi^i)_{i\in I}\big) \text{ t.q. } \Big(\forall i,j \in I\ ,\ i \leq j\ ,\ \psi^j \circ \phi^i_j = \psi^i\Big)\ ,\ \exists !\, f : X \to Y\ :\ (\forall i \in I\ ,\ \psi^i = f \circ \phi^i).$$

Cette définition est en un sens analogue à celle de la borne supérieure comme le plus petit des majorants. Ainsi, la réunion d'une famille de parties d'un ensemble en est la borne supérieure (pour l'inclusion), mais aussi la limite inductive en un sens que le lecteur pourra chercher à préciser.

Exercice 2.2.5 Préciser l'affirmation suivante : les $K[X_1,\dots,X_n]$ forment un système inductif indexé par $\mathbf{N}$ dans $\mathcal{A}nn$ et $K[X_1,\dots,X_n,\dots]$ en est une limite inductive.

Remarque 2.2.6 Conformément à un abus de langage courant, aucun morphisme n'a été mentionné dans l'énoncé précédent, ce qui sous-entend que l'on peut les deviner sans ambigüité. Le lecteur soigneux commencera donc par les citer explicitement.

Contrairement aux limites habituelles, la limite inductive n'est pas tout à fait unique, mais presque ...

Lemme 2.2.7 *Soit $\left(X,(\phi^i)_{i\in I}\right)$ une limite inductive du système inductif $\left((X_i)_{i\in I},(\phi^i_j)_{\substack{i,j\in I\\ i\leq j}}\right)$. Soit $h:X\to X$ tel que : $\forall i\in I$, $h\circ\phi^i=\phi^i$. Alors $h=Id_X$.*

Preuve. - Appliquer l'assertion d'unicité du (ii) de la définition au cas de $\left(Y,(\psi^i)_{i\in I}\right):=\left(X,(\phi^i)_{i\in I}\right)$: le f de la définition est alors à la fois h et Id_X □

Proposition 2.2.8 *Soient $\left(X,(\phi^i)_{i\in I}\right)$ et $\left(Y,(\psi^i)_{i\in I}\right)$ deux limites inductives du système inductif $\left((X_i)_{i\in I},(\phi^i_j)_{\substack{i,j\in I\\ i\leq j}}\right)$. Il existe alors un unique isomorphisme $f:X\to Y$ rendant commutatifs tous les diagrammes concernés :*

$$\exists!\, f\in Iso_C(X,Y)\ :\ (\forall i\in I\ ,\ \psi^i=f\circ\phi^i).$$

Preuve. - Il s'agit de voir que l'unique morphisme f vérifiant ces égalités (selon le (ii) de la définition) est bien un isomorphisme. Les deux couples jouant un rôle symétrique, il existe g : $Y\to X$ tel que l'on ait les commutations $g\circ\psi^i=\phi^i$. Posant $h:=g\circ f$, on voit que $h\circ\phi^i=\phi^i$. On applique alors le lemme, pour conclure que $g\circ f=\mathrm{Id}_X$. On démontre de même que $f\circ g=\mathrm{Id}_Y$. □

Noter que rien ne garantit l'existence des limites inductives. Sous nos hypothèses (I filtrant), elles existent dans la plupart des catégories d'usage courant - mais pas, par exemple, dans $\mathcal{E}v\!f_K$ (à cause de la dimension).

Exemple 2.2.9 Soit $\left((M_i)_{i\in I},(\phi^i_j)_{\substack{i,j\in I\\ i\leq j}}\right)$ un système inductif de A-modules. On construit sa limite inductive comme suit : le module M est le quotient de la somme directe $N:=\bigoplus_{i\in I}M_i$ par le sous-module R engendré par les $x-\phi^i_j(x)$, où $i\leq j$ et $x\in M_i$. On a ici identifié les éléments $x\in M_i$ et $\phi^i_j(x)\in M_j$ avec leurs images dans N. Les morphismes $\phi^i:M_i\to M$ sont obtenus en composant les inclusions $M_i\to N$ avec la projection $N\to N/R$. La preuve que l'on a bien une limite inductive est facile et laissée au lecteur.

Exercice 2.2.10 Si l'on suppose de plus que les M_i sont tous des sous-modules d'un même module M' et si les ϕ^i_j sont des inclusions $M_i\subset M_j$, vérifier que l'union des M_i en est une limite inductive.

2.2.2 Limites projectives (inverse limits)

Comme à la section 2.2.1, la version la plus générale est décrite dans [22], nous n'étudions ici que les systèmes projectifs indexés par des ensembles ordonnés filtrants (et [21] contient un exposé concis). Comme les raisonnements sont très proches de ceux qui précèdent, on sera beaucoup plus bref. En fait, tout ce qui concerne les limites projectives se déduit de l'analogue inductif en inversant le sens des flèches dans $\mathcal{C}$.

Exemple 2.2.11 Une série formelle $f := \sum_{n\geq 0} a_n X^n \in K[[X]]$ est un "polynôme à une infinité de termes". On peut considérer f comme une sorte de limite de ses troncatures $f_n := \sum_{k=0}^{n} a_k X^k$. Chaque f_n peut être considéré comme un polynôme défini modulo X^{n+1}, *i.e.* comme un élément de l'anneau quotient $K[X]/ < X^{n+1} >$. Ces éléments f_n "convergent" vers une série formelle parce qu'ils sont plus précis (moins tronqués) les uns que les autres, c'est-à-dire parce que, pour $n \leq p$, la surjection canonique $K[X]/ < X^{p+1} > \to K[X]/ < X^{n+1} >$ envoie f_p sur f_n. Ainsi, on peut identifier f à la famille des $f_n \in K[X]/ < X^{n+1} >$ assujettie aux conditions de compatibilité ci-dessus. On dit que $K[[X]]$ est la "limite projective" des $K[X]/ < X^{n+1} >$.
Remarquons que l'anneau $\mathbf{Z}_p$ des nombres p-adiques s'obtient par une construction en tous points similaires : c'est la "limite projective" des $\mathbf{Z}/p^{n+1}\mathbf{Z}$.

Définition 2.2.12 (Système projectif) Soit I un ensemble ordonné filtrant (à droite). Un *système projectif* indexé par I dans la catégorie $\mathcal{C}$ est la donnée d'une famille $(X_i)_{i\in I}$ d'objets de $\mathcal{C}$ et d'une famille $(\phi_i^j)_{\substack{i,j\in I \\ i\leq j}}$ de morphismes de $\mathcal{C}$ tels que $\phi_i^j \in \mathrm{Mor}_{\mathcal{C}}(X_j, X_i)$ et que :

$$\big(\forall i \in I\ ,\ \phi_i^i = \mathrm{Id}_{X_i}\big) \text{ et } \big(\forall i,j,k \in I\ ,\ i \leq j \leq k\ ,\ \phi_i^j \circ \phi_j^k = \phi_i^k\big).$$

Exercice 2.2.13 Montrer qu'un système projectif est la même chose qu'un foncteur contravariant.

Définition 2.2.14 (Limite projective) Une *limite projective* du système projectif $\big((X_i)_{i\in I}, (\phi_i^j)_{\substack{i,j\in I \\ i\leq j}}\big)$, est la donnée d'un objet X de $\mathcal{C}$ et d'une famille $(\phi_i)_{i\in I}$ de morphismes $\phi_i : X \to X_i$, le tout assujetti à deux conditions :
(i) La famille des ϕ_i est "compatible" avec le système projectif, au sens où l'on a :

$$\forall i,j \in I\ ,\ i \leq j\ ,\ \phi_i^j \circ \phi_j = \phi_i.$$

(On peut penser que l'on a remplacé k par ∞ dans les relations de la définition précédente.)
(ii) Le couple $\big(X, (\phi_i)_{i\in I}\big)$ est *final* parmi tous les couples vérifiant (i). Cela signifie que, pour tout $\big(Y, (\psi_i)_{i\in I}\big)$ de même nature et vérifiant (i), il existe un unique morphisme $f : Y \to X$ rendant commutatifs tous les diagrammes concernés :

$$\forall \big(Y, (\psi_i)_{i\in I}\big) \text{ t.q. } \Big(\forall i,j \in I\ ,\ i \leq j\ ,\ \phi_i^j \circ \psi_j = \psi_i\Big)\ ,\ \exists !\, f : Y \to X\ :\ (\forall i \in I\ ,\ \psi_i = \phi_i \circ f).$$

Exercice 2.2.15 Préciser l'affirmation suivante : les $K[X]/ < X^{n+1} >$ forment un système projectif indexé par $\mathbf{N}$ dans $\mathcal{A}nn$ et $K[[X]]$ en est une limite projective.

La limite projective n'est pas tout à fait unique, mais presque !

Lemme 2.2.16 *Soit $\left(X,(\phi_i)_{i\in I}\right)$ une limite projective du système projectif $\left((X_i)_{i\in I},(\phi_i^j)_{\substack{i,j\in I\\ i\leq j}}\right)$. Soit $h:X\to X$ tel que : $\forall i\in I\ ,\ \phi_i\circ h=\phi_i$. Alors $h=Id_X$.*

Proposition 2.2.17 *Soient $\left(X,(\phi_i)_{i\in I}\right)$ et $\left(Y,(\psi_i)_{i\in I}\right)$ deux limites projectives du système projectif $\left((X_i)_{i\in I},(\phi_i^j)_{\substack{i,j\in I\\ i\leq j}}\right)$. Il existe alors un unique isomorphisme $f:Y\to X$ rendant commutatifs tous les diagrammes concernés :*

$$\exists!\, f\in Iso_{\mathcal{C}}(X,Y)\ :\ (\forall i\in I\ ,\ \psi_i=\phi_i\circ f).$$

Noter que rien ne garantit l'existence des limites projectives. Sous nos hypothèses (I filtrant), elles existent dans la plupart des catégories d'usage courant - mais pas, par exemple, dans $\mathcal{E}vf_K$ (toujours à cause de la dimension).

Exemple 2.2.18 Soit $\left((M_i)_{i\in I},(\phi_i^j)_{\substack{i,j\in I\\ i\leq j}}\right)$ un système projectif de A-modules. On pose $N:=\prod M_i$ et : $M:=\{(x_i)_{i\in I}\in N\mid \forall i,j\in I \text{ t.q. } i\leq j\ ,\ \phi_i^j(x_j)=x_i\}$. Alors M est une limite projective des M_i.

Exercice 2.2.19 Préciser toutes les flèches et prouver l'assertion.

Caractères sur un groupe abélien. Pour tout groupe abélien G, notons $\hat{G}:=\mathrm{Hom}_{\mathcal{G}r}(G,\mathbf{C}^*)$ le groupe des *caractères* de G (multiplication évidente). Dans le cas où G est un groupe abélien fini, la structure de $\hat{G}$ est complètement décrite dans [34]. Si G est abélien de type fini, il est de la forme $H\times\mathbf{Z}^r$ et $\hat{G}=\hat{H}\times(\mathbf{C}^*)^r$. Dans le cas général, notons $I:=\mathcal{P}_f(G)$ l'ensemble des parties finies de G, que l'on ordonne par inclusion (il est filtrant). Pour tout $i\in I$, notons G_i le sous-groupe de G engendré par la partie i : c'est donc un groupe abélien de type fini. Puisque $i\leq j\Rightarrow G_i\subset G_j$, les G_i forment un système inductif de sous-groupes de G et leur limite inductive est G (exercice 2.2.10 avec $A=\mathbf{Z}$). Par ailleurs, si $i\leq j$ et donc $G_i\subset G_j$, on a "dualement" un morphisme de restriction de $\hat{G_j}$ dans $\hat{G_i}$ défini par $\chi\mapsto\chi_{|G_i}$. Les $\hat{G_i}$ forment ainsi un système projectif de groupes. De même, les inclusions $G_i\subset G$ donnent lieu à des morphismes de restriction de $\hat{G}$ dans $\hat{G_i}$ définis par $\chi\mapsto\chi_{|G_i}$. Il est aisé de voir que la famille de ces morphismes est compatible avec le système projectifet que le groupe $\hat{G}$ est la limite projective des $\hat{G_i}$.

2.2.3 Le produit tensoriel : rappels et compléments

C'est une construction classique de l'algèbre linéaire, mais c'est également une solution de "problème universel", tout comme les limites inductives et projectives. On fixe un corps commutatif K et deux K-espaces vectoriels V,W. On écrira simplement $\mathcal{E}v$ pour $\mathcal{E}v_K$. Pour tout K-espace vectoriel E, on note :

$$\mathrm{Bil}(V,W;E):=\{\phi:V\times W\to E\mid \phi \text{ est bilinéaire}\}.$$

C'est, de façon naturelle, un K-espace vectoriel. Pour tout $f\in\mathrm{Mor}_{\mathcal{E}v}(E,F)$, l'application de $\mathrm{Bil}(V,W;E)$ dans $\mathrm{Bil}(V,W;F)$ définie par $\phi\mapsto f\circ\phi$ est linéaire. On a obtient ainsi un foncteur covariant $\mathrm{Bil}(V,W;-)$ de la catégorie $\mathcal{E}v$ dans elle-même.

Par ailleurs, on sait définir le *produit tensoriel* de V et W, noté $V\otimes_K W$, ou simplement $V\otimes W$. C'est un K-espace vectoriel muni d'une application bilinéaire $\mu\in\mathrm{Bil}(V,W;V\otimes W)$, notée $(v,w)\mapsto v\otimes w$, et satisfaisant à la propriété suivante : si $(v_i)_{i\in I}$ et $(w_j)_{j\in J}$ sont respectivement des bases de V et W, alors $(v_i\otimes w_j)_{(i,j)\in I\times J}$ est une base de $V\otimes W$. Un corollaire de cette propriété est que

l'ensemble des $v \otimes w$, $v \in V$, $w \in W$, est une partie génératrice de $V \otimes W$. Un autre corollaire est que $\mathcal{E}vf_K$ est stable par produit tensoriel et que $\dim_K(V \otimes_K W) = (\dim_K V)(\dim_K W)$. Enfin, de la propriété des bases, on peut déduire la suivante, qui est plus intrinsèque : toute forme bilinéaire sur $V \times W$ se factorise de manière unique par $V \otimes W$. De manière plus précise :

Proposition 2.2.20 (Propriété universelle du produit tensoriel) *Pour tout espace vectoriel E et pour toute application bilinéaire $\phi \in Bil(V,W;E)$, il existe une unique application linéaire $f : V \otimes W \to E$ telle que $\phi = f \circ \mu$. Autrement dit : $\phi(v,w) = f(v \otimes w)$.*

Pour la preuve, voir [21]. On peut reformuler cette propriété en termes de foncteurs. L'espace $V \otimes W$ et la forme μ étant donnés, pour tout E, on a une application linéaire $f \mapsto f \circ \mu$ de $\mathrm{Mor}_{\mathcal{E}v}(V \otimes W, E)$ dans $\mathrm{Bil}(V,W;E)$. Il est facile de voir que cela définit une transformation naturelle entre les foncteurs covariants $\mathrm{Mor}_{\mathcal{E}v}(V \otimes W, -)$ et $\mathrm{Bil}(V,W;-)$. La propriété universelle dit que cette transformation naturelle est un isomorphisme.

Construction. Le produit tensoriel s'obtient par la construction suivante : c'est le quotient de l'espace[1] des "combinaisons linéaires formelles" $\sum \lambda_i(v_i,w_i)$ d'éléments de $V \times W$ par le sous-espace vectoriel engendré par tous les éléments $(v,w+w') - (v,w) - (v,w')$, $(v+v',w) - (v,w) - (v',w)$, $(v,\lambda w) - \lambda(v,w)$, $(\lambda v,w) - \lambda(v,w)$, où $v,v' \in V$, $w,w' \in W$, $\lambda \in K$. On note alors $V \otimes W$ l'espace vectoriel quotient et $v \otimes w$ l'image de (v,w) dans ce quotient. Il est facile de voir que l'application $(v,w) \mapsto v \otimes w$ est bilinéaire, et pas très difficile non plus de prouver la propriété universelle. (La propriété portant sur les bases est moins évidente.) Notons d'ailleurs que la même construction peut être faite dans $\mathcal{M}od_A$, avec les mêmes propriétés.

Exercice 2.2.21 (i) Montrer à l'aide de la propriété universelle que, si $f \in \mathrm{Mor}_{\mathcal{E}v}(V,V')$ et $g \in \mathrm{Mor}_{\mathcal{E}v}(W,W')$, il existe une unique application linéaire $f \otimes g$ de $V \otimes W$ dans $V' \otimes W'$ telle que $v \otimes w \mapsto v' \otimes w'$. En déduire que le produit tensoriel est un bifoncteur covariant en chaque argument.
(ii) Démontrer la formule :
(2.2.21.1)
$\forall u : U \to V$, $\forall v : V \to W$, $\forall u' : U' \to V'$, $\forall v' : V' \to W'$, $(v \otimes v') \circ (u \otimes u') = (v \circ u) \otimes (v' \circ u')$.

(Vérifier que les deux membres ont même effet sur $x \otimes x' \in U \otimes U'$.)

Produit tensoriel d'algèbres (voir [21]). Soient A,B deux algèbres sur le corps commutatif K. On fait du K-espace vectoriel $A \otimes_K B$ une K-algèbre en posant :

$$(a \otimes b)(a' \otimes b') := (aa') \otimes (bb').$$

Le neutre est évidemment $1 \otimes 1$. On a alors les propriétés :

1. Soient $I \subset A$ et $J \subset B$ des idéaux. Alors le morphisme d'algèbres $A \otimes B \to (A/I) \otimes (B/J)$ est surjectif de noyau $I \otimes B + A \otimes J$.
2. Les algèbres $A \otimes_K K[X]$ et $K[X] \otimes_K A$ sont canoniquement isomorphes à $A[X]$. En particulier :

$$K[X_1,\ldots,X_n] \otimes_K K[Y_1,\ldots,Y_p] = K[X_1,\ldots,X_n,Y_1,\ldots,Y_p].$$

[1] Rappelons que l'espace des "combinaisons linéaires formelles" d'éléments d'un ensemble X est simplement l'espace vectoriel $K^{(X)}$ des applications à support fini de X dans K, dans lequel on note $\sum \lambda_i x_i$ l'application telle que $x_i \mapsto \lambda_i$ et nulle ailleurs. Après identification de $x \in X$ à l'application $x \mapsto 1$ et nulle ailleurs, on voit que X est une base de $K^{(X)}$.

Chapitre 3

Représentations linéaires de groupes, enveloppe proalgébrique

Notre but étant de relier la correspondance de Riemann-Hilbert à la théorie de Galois différentielle (pour laquelle le corps de base est K), nous exposerons la théorie sur un corps de base K de caractéristique nulle et algébriquement clos.

Pour la théorie générale des représentations linéaires, les grands classiques sont [33] et [20] ; mais l'essentiel de nos besoins est couvert par [21]. Notre but, qui est d'en tirer une première approche de la dualité tannakienne, n'est abordé par voie élémentaire nulle part. (L'approche de [36] porte sur un autre aspect de la théorie.) D'autres références seront donc fournies à la fin de ce cours.

3.1 Représentations linéaires

Définition 3.1.1 (Représentation linéaire d'un groupe) Une *représentation K-linéaire de dimension finie* d'un groupe G est une action de G sur un K-espace vectoriel de dimension finie V, notée $(g,x) \mapsto g.x$, telle que, pour tout $g \in G$, l'application $x \mapsto g.x$ soit linéaire. Pour faire court, nous dirons "représentation" pour "représentation K-linéaire de dimension finie".

Notant $\rho(g)$ l'application $x \mapsto g.x$, on a donc $\rho(g) \in \mathrm{GL}(V)$. En fait, $\rho : G \to \mathrm{GL}(V)$ est un morphisme de groupes en vertu du calcul suivant (dans lequel $g, g' \in G$) :

$$\Big(\forall x \in V\ ,\ \rho(gg')(x) = (gg').x = g.(g'.x) = \rho(g)\big(\rho(g')(x)\big)\Big) \Longrightarrow \rho(gg') = \rho(g) \circ \rho(g') = \rho(g)\rho(g').$$

Réciproquement, pour tout morphisme de groupes $\rho : G \to \mathrm{GL}(V)$, en posant $g.x := \rho(g)(x)$, on définit une représentation linéaire. Une définition alternative du mot "représentation" est donc "morphisme de groupes de G dans un groupe linéaire". On dit d'ailleurs aussi bien "représentation linéaire de G dans $\mathrm{GL}(V)$" que "représentation linéaire de G dans V". Lorsque le groupe G est fixé, nous noterons fréquemment (V,ρ) la représentation $\rho : G \to \mathrm{GL}(V)$.

Remarque 3.1.2 Lorsque le groupe G est muni d'une structure supplémentaire, on peut décider de se restreindre à des espaces vectoriels munis d'une structure analogue et à des représentations compatibles avec ces structures. Par exemple, si G est un groupe topologique et V un espace

vectoriel topologique, une représentation de G dans V est dite continue si l'application $(g,x) \mapsto g.x$ de $G \times V$ dans V est continue : cette condition est d'ailleurs strictement plus forte que celle qui requiert la continuité de $\rho : G \to \mathrm{GL}(V)$. Un autre exemple est celui des "représentations rationnelles des groupes algébriques" (chapitre 6).

Bien entendu (what else ?)[1], nous voulons faire une catégorie !

Définition 3.1.3 (Morphisme de représentations) Soient (V,ρ), (V',ρ') deux représentations de G. Un *morphisme* de (V,ρ) dans (V',ρ') est une application linéaire $u : V \to V$ telle que :

$$\forall g \in G\ ,\ \forall x \in V;\ ,\ u(g.x) = g.u(x).$$

De manière équivalente :

$$\forall g \in G\ ,\ u \circ \rho(g) = \rho'(g) \circ u.$$

On obtient ainsi une *catégorie des représentations de G*, notée $\mathcal{R}ep_K(G)$.

Exercice 3.1.4 (i) Préciser ce que sont la composition et les identités dans cette catégorie.
(ii) Vérifier l'existence d'un foncteur d'oubli $(V,\rho) \rightsquigarrow V$ de $\mathcal{R}ep_K(G)$ dans $\mathcal{E}vf_K$.

3.1.1 Représentations de G et $K[G]$-modules

L'étude des représentations peut être en partie ramenée à l'étude des modules sur un anneau non commutatif, en vertu de la définition et du théorème qui suivent.

Définition 3.1.5 (Algèbre d'un groupe) Notons $K[G]$ l'espace vectoriel $C^{(G)}$ des combinaisons K-linéaires formelles d'éléments de G, muni de la multiplication :

$$\left(\sum_{g\in G} \lambda_g g\right)\left(\sum_{g\in G} \mu_g g\right) := \sum_{g\in G} \nu_g g,\ \text{ où }\ \forall g \in G\ ,\ \nu_g := \sum_{\substack{g',g''\in G \\ g'g''=g}} \lambda_{g'}\mu_{g''}.$$

(C'est donc la seule multiplication K-bilinéaire qui étende la loi de groupe de G). On appelle *algèbre du groupe G* (sur K) la K-algèbre associative unitaire ainsi obtenue.

Remarque 3.1.6 Modulo l'identification de la combinaison linéaire formelle $\sum_{g\in G} \lambda_g g$ avec l'application à support fini $\lambda : G \to K$, la multiplication ci-dessus s'identifie au produit de convolution :

$$\nu = \lambda \star \mu\ \text{ où }\ \forall g \in G\ ,\ (\lambda\star\mu)(g) := \sum_{\substack{g',g''\in G \\ g'g''=g}} \lambda(g')\mu(g'').$$

(Il faut naturellement vérifier que $\lambda\star\mu$ est à support fini.)

À toute représentation (V,ρ), on peut associer un $K[G]$-module dont le groupe sous-jacent est V et dans lequel la multiplication externe est définie par la formule :

$$\forall \left(\sum_{g\in G} \lambda_g g\right) \in K[G]\ ,\ \forall x \in V\ ,\ \left(\sum_{g\in G} \lambda_g g\right).x := \sum_{g\in G} \lambda_g (g.x).$$

On notera encore abusivement V le $K[G]$-module ainsi défini. (On l'appelle parfois également "G-module".)

[1] Traduction dans l'esprit : "comment pourrait-il en être autrement ?"

Exercice 3.1.7 (i) Vérifier que $K[G]$ est bien une K-algèbre associative unitaire. Est-elle commutative ? Quels sont ses inversibles ?
(ii) Vérifier que la construction ci-dessus définit bien un $K[G]$-module.
(iii) Vérifier que tout morphisme $u : V \to V'$ de la représentation (V,ρ) dans la représentation (V',ρ') est une application $K[G]$-linéaire.
(iv) Vérifier qu'en associant à la représentation (V,ρ) le $K[G]$-module V et au morphisme de représentations u le morphisme de $K[G]$-modules u, on définit un foncteur de $\mathcal{R}ep_K(G)$ dans $\mathcal{M}od_{K[G]}$.

Théorème 3.1.8 *Ce foncteur est pleinement fidèle ; autrement dit, c'est une équivalence de la catégorie $\mathcal{R}ep_K(G)$ avec une sous-catégorie pleine de la catégorie $\mathcal{M}od_{K[G]}$.*

Preuve. - Notons d'abord que tout $K[G]$-module peut être vu comme un K-espace vectoriel. La sous-catégorie pleine en question est celle des $K[G]$-modules qui, vus comme K-espaces vectoriels, sont de dimension finie. Ils forment l'image essentielle de notre foncteur (cela va découler de l'argument qui suit) : notons provisoirement $\mathcal{D}$ cette catégorie.
Par ailleurs, il y a une notion évidente de "représentation pas nécessairement de dimension finie", ces dernières forment une catégorie $\mathcal{D}'$ et la construction ci-dessus définit en fait un foncteur de $\mathcal{D}'$ dans $\mathcal{M}od_{K[G]}$. Réciproquement, à tout $K[G]$-module V, on associe d'abord le K-espace vectoriel V (comme ci-dessus), puis une représentation de G dans V définie par $(g,x) \mapsto g.x$ (le membre de droite désigne ici le produit externe de $g \in K[G]$ par $x \in V$). De même, toute application $K[G]$-linéaire donne lieu à un morphisme de représentations.
On a donc obtenu un foncteur de $\mathcal{M}od_{K[G]}$ dans $\mathcal{D}'$, et le lecteur vérifiera que c'est un quasi-inverse du précédent (voir après la proposition 2.1.15 de la page 22).
Enfin, il est clair que ces foncteurs se restreignent en des foncteurs quasi-inverses l'un de l'autre entre $\mathcal{R}ep_K(G)$ et $\mathcal{D}$. □

Remarque 3.1.9 Parmi tout les $K[G]$-modules, il est possible de caractériser ceux qui sont de dimension finie sur K de manière purement "ring theoretic" : ce sont les modules de longueur finie.

3.1.2 Représentations de Z

Un objet d'intérêt *topologique* particulier est la catégorie des représentations de $\mathbf{Z}$. En effet, le cas le plus simple de groupe fondamental non trivial est celui du "trou" $\pi_1(\mathbf{C}^*, z_0)$. Ce qui suit fait partie de l'étude de la topologie du trou.

Une représentation de $\mathbf{Z}$ dans V est un morphisme de groupes $\rho : \mathbf{Z} \to \mathrm{GL}(V)$, et il est entièrement déterminé par l'image $\phi := \rho(1) \in \mathrm{GL}(V)$. Il revient donc au même de se donner la représentation (V,ρ) ou le couple (V,ϕ). La condition pour que l'application linéaire $u : V \to V'$ soit un morphisme de représentations de (V,ρ) dans (V',ρ') entraîne immédiatement $\phi' \circ u = u \circ \phi$, où l'on a posé $\phi := \rho(1)$ et $\phi' := \rho'(1)$; mais il est facile de vérifier que la réciproque est vraie, *i.e.* :

$$\big(\rho'(1) \circ u = u \circ \rho(1)\big) \Longrightarrow \big(\forall n \in \mathbf{Z}\ ,\ \rho'(n) \circ u = u \circ \rho(n)\big).$$

(Plus généralement, pour un groupe G quelconque, il est suffisant de tester la condition de morphisme entre représentations de G sur des générateurs de G.) On voit donc que la catégorie $\mathcal{R}ep_K(\mathbf{Z})$ est équivalente à la catégorie suivante :

- Les objets sont les couples (V,ϕ), où V est un K-espace vectoriel de dimension finie et où $\phi \in \mathrm{GL}(V)$;
- les morphismes de (V,ϕ) dans (V',ϕ') sont les applications linéaires $u : V \to V'$ telles que $\phi' \circ u = u \circ \phi$; autrement dit, le diagramme suivant est commutatif :

$$\begin{array}{ccc} V & \xrightarrow{u} & V' \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi'} \\ V & \xrightarrow{u} & V' \end{array}$$

(C'est la catégorie $\mathcal{C}_{aut}$ de l'exercice 2.1.4 page 20.)

Selon le théorème 3.1.8, on obtiendra un autre modèle de $\mathcal{R}ep_K(\mathbf{Z})$ si l'on décrit l'algèbre du groupe $\mathbf{Z}$. Pour cela, il est préférable de partir d'une forme multiplicative de ce groupe : $\mathbf{Z} \simeq \{X^n \mid n \in \mathbf{Z}\}$. Il est alors immédiat que l'algèbre de groupe de $\mathbf{Z}$ est isomorphe à l'anneau $K[X,X^{-1}]$. On retrouve le résultat de l'exercice 2.1.18, page 23. L'anneau $K[X,X^{-1}]$ étant principal, on sait complètement décrire ses modules de type fini (et d'autant plus simplement que K est algébriquement clos). La classification des représentations de $\mathbf{Z}$ (au sens de la section 3.2, c'est-à-dire à isomorphisme près) en découle . En fait, cette classification se ramène essentiellement à la théorie de la réduction des matrices. En effet :

1. Tout couple (V,ϕ) est isomorphe à un couple (K^n,A), où $n \in \mathbf{N}$ et où $A \in \mathrm{GL}_n(K)$ est considéré comme un automorphisme de K^n. (Cette assertion vient simplement de la possibilité de choisir une base de V.)
2. Pour que le couple (K^n,A) soit isomorphe au couple (K^p,B), il faut, et il suffit, que $n = p$ et que les matrices $A,B \in \mathrm{GL}_n(K)$ soient conjuguées (*i.e.* semblables). En effet, la condition sur les dimensions est évidente, et l'isomorphisme u prend ici la forme de $U \in \mathrm{GL}_n(K)$ tel que $BU = UA$.

3.2 Quelques questions de classification (effleurées)

Dans le cas $G = \mathbf{Z}$, on sait construire toutes les représentations à partir d'objets élémentaires et décider à quelle condition deux représentations sont isomorphes : c'est la théorie de la réduction. Comme corollaire, on sait décrire "l'espace des modules de représentations de $\mathbf{Z}$". Le mot historique "module" signifie ici plus ou moins "classe d'isomorphie décrite à l'aide d'un jeu complet d'invariants". Ici, ces invariants sont par exemple les invariants de similitudes (une suite finie de polynômes) ; ou bien le spectre et la liste des dimensions des blocs de Jordan.

Exercice 3.2.1 Lorsque G est trivial, le seul invariant est la dimension et l'espace des modules est $\mathbf{N}$.

On va voir que le problème est complètement résolu lorsque G est abélien fini ; le cas d'un groupe fini non abélien est le cœur de la théorie classique, il remplit le livre [33]. Le cas le plus important pour nous est celui d'un groupe non abélien de *présentation finie*, *i.e.* défini par un

nombre fini de générateurs et de relations : c'est en effet le cas des groupes fondamentaux que l'on rencontre dans la vie courante, par exemple les groupes fondamentaux des surfaces compactes connexes. Il n'y a pas de solution complète générale dans ce cas.

Exemples 3.2.2 (i) Le groupe fondamental de $\mathbf{C} \setminus \{0,1\}$ est le groupe libre sur deux générateurs g_1, g_2.
(ii) Le groupe fondamental du tore $S^1 \times S^1$ est $\mathbf{Z}^2$, quotient du groupe libre sur deux générateurs g_1, g_2 par la relation $g_1 g_2 = g_2 g_1$; autrement dit, le groupe défini par les générateurs g_1, g_2 et la relation $g_1 g_2 g_1^{-1} g_2^{-1}$.

Exercice 3.2.3 (i) Soit G le groupe défini par les générateurs $g_1, \ldots, g_\ell$ et les relations $R_1, \ldots, R_m$. On rappelle que cela signifie que G est le quotient du groupe libre L de générateurs $G_1, \ldots, G_\ell$ par le plus petit sous-groupe distingué contenant $R_1, \ldots, R_m \in L$. Décrire la catégorie des représentations de G dans l'esprit de l'exercice 2.1.4 page 20.
(ii) Appliquer aux deux exemples qui précèdent.

3.2.1 Vocabulaire de la classification

Définition 3.2.4 (Sous-représentations, représentations irréductibles) (i) Une *sous-représentation* de (V, ρ) est une représentation (V', ρ'), où $V' \subset V$ et où cette inclusion est un morphisme de représentations ; de manière équivalente, c'est un sous-espace V' de V stable sous l'action de G et muni de la *représentation induite* ρ' définie par :

$$\forall g \in G\,,\ \rho'(g) := \rho(g)_{|V'} \in \mathrm{GL}(V').$$

Les sous-représentations *banales* de (V, ρ) sont la sous-représentation triviale et (V, ρ) elle-même.
(ii) Une représentation est dite *irréductible* si elle est non triviale et si de plus elle n'admet pas de sous-représentation non banale ; de manière équivalente, si $V \neq \{0\}$ et si les seuls sous-espaces G-stables de V sont $\{0\}$ et V.

Remarque 3.2.5 Il est de coutume de considérer comme "irréductibles", "simples, "premiers" ... des objets élémentaires mais non triviaux : par exemple un nombre premier n'est pas égal à 1. Lorsque l'on vise un théorème de décomposition unique en facteurs élémentaires, cette condition de non trivialité est indispensable (pour l'unicité).

Exercice 3.2.6 Par quelle propriété de $K[G]$-module se traduit l'irréductibilité ?

Si (V', ρ') est une sous-représentation de (V, ρ), en choisissant une base de V qui étend une base de V', on obtient une description matricielle comme morphisme de G dans le sous-groupe de $\mathrm{GL}_n(K)$, $n := \dim V$, formé des matrices triangulaires par blocs $\begin{pmatrix} A_{1,1} & A_{1,2} \\ 0 & A_{2,2} \end{pmatrix}$, où $A_{1,1} \in \mathrm{GL}_{n'}(K)$, $n' := \dim V'$, $A_{2,2} \in \mathrm{GL}_{n''}(K)$, $n'' := n - n'$, et $A_{1,2} \in \mathrm{Mat}_{n',n''}(K)$.

Définition 3.2.7 (Sommes directes de représentations, représentations indécomposables) (i) La *somme directe* des représentations (V, ρ) et (V', ρ') de G est la représentation $(V \oplus V', \rho \oplus \rho')$, où l'on pose

$$\forall g \in G\,,\ (\rho \oplus \rho')(g) := \rho(g) \oplus \rho'(g) \in \mathrm{GL}(V \oplus V').$$

(ii) Une représentation est dite *indécomposable* si elle n'est pas triviale et si elle n'est pas somme directe de deux sous-représentations non triviales (*i.e.* de dimensions >0) ; de manière équivalente, c'est une représentation (V,ρ) telle que V n'admette aucun sous-espace non trivial G-stable admettant un supplémentaire non trivial G-stable.

Si (V,ρ) est la somme directe de (V',ρ') et de de (V'',ρ''), en choisissant une base de V qui soit la juxtaposition de bases de V' et de V'', on obtient une description matricielle comme morphisme de G dans le sous-groupe de $\mathrm{GL}_n(K)$, $n := \dim V$, formé des matrices diagonales par blocs $\begin{pmatrix} A_{1,1} & 0 \\ 0 & A_{2,2} \end{pmatrix}$, où $A_{1,1} \in \mathrm{GL}_{n'}(K)$, $n' := \dim V'$ et $A_{2,2} \in \mathrm{GL}_{n''}(K)$, $n'' := \dim V''$.

Exercice 3.2.8 Montrer que la représentation $\left(K^2, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)$ de $\mathbf{Z}$ est indécomposable mais pas irréductible.

3.2.2 Représentations complètement réductibles

Théorème 3.2.9 *Si une représentation est somme directe de représentations irréductibles (on dit alors qu'elle est* complètement réductible*), les composantes et leurs multiplicités (voir la suite pour ce terme) sont uniquement déterminées à l'ordre près.*

Preuve. - Une représentation irréductible est un $K[G]$-module simple, c'est-à-dire non trivial et n'admettant aucun autre sous-module que 0 et lui-même. Une représentation complètement réductible est donc un module semi-simple, c'est-à-dire somme directe de modules simples. Ici, il s'agit d'une somme directe finie (à cause des dimensions), et l'on peut écrire $M = P_1^{k_1} \oplus \cdots \oplus P_r^{k_r}$, avec $r \in \mathbf{N}^*$, $k_1, \ldots, k_r \in \mathbf{N}^*$ et les P_i simples et deux à deux non isomorphes. Le théorème est donc la conséquence de la proposition qui suit. □

Proposition 3.2.10 *Soient A un anneau non nécessairement commutatif, $r,s \in \mathbf{N}^*$, $k_1,\ldots,k_r,\ell_1,\ldots,\ell_s \in \mathbf{N}^*$ et $P_1,\ldots,P_r,Q_1,\ldots,Q_s$ des modules simples tels que :*

$$P_1^{k_1} \oplus \cdots \oplus P_r^{k_r} \simeq Q_1^{\ell_1} \oplus \cdots \oplus Q_s^{\ell_s}.$$

On suppose les P_i (resp. les Q_j) deux à deux non isomorphes. Alors $r = s$, et, quitte à renuméroter, $k_i = \ell_i$ et $P_i \simeq Q_i$.

Preuve. - Nous esquissons une preuve ; pour une démonstration différente et plus détaillée, voir [21].

En vertu du lemme de Schur ci-dessous, $\mathrm{Hom}\left(P_i^{k_i}, Q_j^{\ell_j}\right) = 0$, sauf si $P_i \simeq Q_j$. On a donc $r = s$ et, après réindexation, on peut supposer que $P_i^{k_i} \simeq Q_i^{\ell_i}$. On en déduit d'abord que $P_i \simeq Q_i \simeq P$, puis que $P^k \simeq P^\ell$. On a donc une matrice $k \times \ell$ inversible, à coefficients dans $\mathrm{End}(P)$, qui est un corps (toujours en vertu du lemme de Schur), donc $k = \ell$. □

Lemme 3.2.11 (Lemme de Schur) *Soient P,Q deux modules simples et $f \in \mathrm{Hom}(P,Q)$. Alors f est nul ou bijectif.*

Preuve. - Le noyau de f est un sous-module du module simple P, il est donc nul ou égal à P. De même, l'image de f est nulle ou égale à Q. □

3.2.3 Représentations des groupes abéliens finis

Théorème 3.2.12 (Théorème de Maschke) *Toute représentation d'un groupe fini est complètement réductible.*

Preuve. - Il suffit de démontrer que, si (V,ρ) est une représentation de G, tout sous-espace G-stable V' de V admet un supplémentaire G-stable V'' ; ensuite, on raisonnera par récurrence sur $\dim V$.

Pour le voir, on choisit une projection arbitraire p de V sur V', et l'on pose :

$$\pi := \frac{1}{\mathrm{card} G} \sum_{g\in G} \rho(g)\circ p\circ \rho(g)^{-1}.$$

On vérifie d'abord que l'image de π est dans V' (ce qui utilise la G-stabilité) et que π se restreint en l'identité sur V' (idem) ; autrement dit, π est une projection de V sur V'. D'autre part, un petit calcul standard montre que :

$$\forall g\in G\ ,\ \rho(g)\circ\pi\circ\rho(g)^{-1} = \pi,$$

d'où l'on tire facilement que le supplémentaire $V'' := \mathrm{Ker}\,\pi$ de V' est G-stable. □

Remarque 3.2.13 Cette démonstration, et donc le théorème, restent valables pour un corps quelconque sous la seule hypothèse que card G n'est pas multiple de la caractéristique. Cette hypothèse ne peut être relâchée, comme le montre l'exemple suivant.

Exercice 3.2.14 Soient $K := \mathbf{F}_2$ (*i.e.* le corps à 2 éléments), $G := \mathbf{Z}/2\mathbf{Z}$ (*i.e.* le groupe à 2 éléments), $V := K^2$ et $\rho : G \to \mathrm{GL}_2(K)$ définie par :

$$\forall a\in \mathbf{Z}/2\mathbf{Z}\ ,\ \rho(a) := \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

Vérifier que l'on a bien une représentation et qu'elle n'est pas complètement réductible.

Théorème 3.2.15 *Toute représentation irréductible d'un groupe abélien est de rang* 1. *(On appelle* rang *d'une représentation* (V,ρ) *la dimension de l'espace* V*.)*

Preuve. - C'est du niveau L2 ! L'ensemble $\rho(G)\subset \mathrm{GL}(V)$ est formé de matrices trigonalisables qui commutent deux à deux, donc cotrigonalisables. Cet ensemble admet donc une droite propre commune, qui est donc G-stable. Si la dimension de V est >1, la représentation n'est pas irréductible. □

Corollaire 3.2.16 *Toute représentation d'un groupe fini abélien est somme directe de représentations de rang* 1.

Exercice 3.2.17 Donner des contre-exemples en relâchant successivement l'une ou l'autre des hypothèses de finitude et d'abélianité.

Corollaire 3.2.18 (Agrégation externe 2003, Mathématiques générales) *Toute sous-groupe fini abélien de $GL_n(\mathbf{C})$ est diagonalisable*, i.e. *conjugué à un groupe de matrices diagonales.*

3.3 Première approche de la dualité

De manière générale, une représentation (V,ρ) de rang 1 d'un groupe G est caractérisée, à isomorphisme près, par le morphisme $\rho : G \to \mathrm{GL}(V) = K^*$, cette dernière égalité reflétant un isomorphisme canonique (non dépendant d'un choix de base). Connaitre les représentations de rang 1 de G revient donc à connaitre les *caractères* de G, c'est-à-dire les éléments de son *dual* :

$$\hat{G} := \mathrm{Hom}_{\mathcal{G}r}(G, K^*).$$

On définit de plus une loi de groupe sur $\hat{G}$ en posant $(\chi.\chi')(g) := \chi(g)\chi'(g)$. (La lettre χ est traditionnelle dans ce contexte.)

Lorsque G est un groupe abélien fini, on a vu (corollaire 3.2.16) que la connaissance des caractères détermine la connaissance de toutes les représentations de G. En fait, la connaissance du groupe des caractères détermine la connaissance du groupe G :

Théorème 3.3.1 (Bidualité des groupes abéliens finis) *Pour tout groupe G, l'application :*

$$g \mapsto \big(\phi_g : \chi \mapsto \chi(g)\big)$$

est un morphisme de groupes de G dans son bidual $\hat{\hat{G}}$. Dans le cas d'un groupe abélien fini, c'est un isomorphisme.

La preuve est donnée dans [34]. On peut donc reconstituer un groupe abélien fini à partir de ses représentations de rang 1, à condition de savoir les multiplier. Ce théorème admet une extension facile au cas des groupes abéliens de type fini [34], et une extension, nettement moins triviale, au cas des groupes abéliens localement compacts[2] (dualité de Pontryaguine).

3.3.1 Peut-on reconstituer G à partir de $\mathcal{R}ep_K(G)$?

Pour passer au cas nettement plus difficile d'un groupe non abélien, on peut tout d'abord se convaincre que les représentations de rang 1 n'ont aucune chance de permettre de reconstituer le groupe.

Exercice 3.3.2 Déterminer $\hat{G}$ dans le cas du groupe symétrique sur n éléments.

C'est Tannaka qui a le premier formulé et prouvé (en 1938) un théorème de reconstitution d'un groupe à partir de ses représentations de rang arbitraire ; le cadre était celui des groupes de Lie compacts. Nous allons tenter de reconstituer le groupe "abstrait" (*i.e.* sans structure supplémentaire) G à partir de la catégorie $\mathcal{R}ep_K(G)$.

[2] Dans ce cas, le dual $\hat{G}$ est défini comme le groupe des morphismes continus de G dans le cercle unité, muni d'une topologie convenable.

Sens direct. Comme on l'a vu dans le théorème 3.3.1, il s'agit d'un mécanisme de bidualité, il faut donc faire agir G sur la catégorie $\mathcal{R}ep_K(G)$. Soit donc $g \in G$. Pour tout objet $X := (V, \rho)$ de $\mathcal{R}ep_K(G)$, c'est sur V que g agit naturellement, via l'automorphisme $\rho(g)$. On est donc conduit à introduire le *foncteur oubli :*

$$\omega : X := (V, \rho) \rightsquigarrow V,$$

de $\mathcal{R}ep_K(G)$ dans $\mathcal{E}vf_K$ (effet évident sur les morphismes).

Proposition 3.3.3 *(i) L'élément g de G étant fixé, en posant :*

$$\phi_g : X := (V, \rho) \rightsquigarrow \big(\rho(g) : \omega(X) \to \omega(X)\big),$$

on définit une transformation naturelle du foncteur covariant ω dans lui-même.
(ii) L'application $g \mapsto \phi_g$ est un morphisme de groupes de G dans le groupe $Aut(\omega)$ des automorphismes du foncteur oubli ω.

Preuve. - (i) La fonctorialité se prouve ainsi. Pour tout morphisme de représentations $u : X := (V, \rho) \to X' := (V', \rho')$, on veut montrer que le diagramme :

$$\begin{array}{ccc} \omega(X) & \xrightarrow{\omega(u)} & \omega(X') \\ {\scriptstyle \phi_g(X)}\downarrow & & \downarrow{\scriptstyle \phi_g(X)} \\ \omega(X) & \xrightarrow{\omega(u)} & \omega(X') \end{array}$$

est commutatif. Mais ce diagramme s'identifie à :

$$\begin{array}{ccc} V & \xrightarrow{u} & V' \\ {\scriptstyle \rho(g)}\downarrow & & \downarrow{\scriptstyle \rho'(g)} \\ V & \xrightarrow{u} & V' \end{array}$$

qui est commutatif par définition d'un morphisme de représentations.
(ii) Il reste à vérifier que ϕ_1 est l'automorphisme identité et que $\phi_{gg'} = \phi_g \phi_{g'}$, ce qui est facile et laissé au lecteur. □

Sens réciproque. Peut-on dire que le groupe des automorphismes du foncteur oubli est le bidual recherché, et peut-être même G ? On va d'abord voir à quoi ressemble un automorphisme de ω dans le cas où G est un groupe abélien fini.

Soit donc $\phi \in \mathrm{Aut}(\omega)$. Tout d'abord, les morphismes de projections de $X \oplus X'$ sur X, X' donnent lieu à des morphismes de $\omega(X \oplus X')$ sur $\omega(X), \omega(X')$, puis à un isomorphisme de $\omega(X \oplus X')$ sur $\omega(X) \oplus \omega(X')$. En appliquant la propriété de fonctorialité de ϕ à ces morphismes et à cet isomorphisme, on voit que $\phi(X \oplus X')$ est déterminé par $\phi(X)$ et $\phi(X')$. Ainsi, ϕ est déterminé par son effet sur les représentations de rang 1.

Pour une telle représentation $X := (V, \chi)$, où X est une droite, on a $\chi \in \hat{G}$ et $\phi(X)$ est un automorphisme de la droite V, donc une homothétie de rapport $\mu \in K^*$. De plus, un isomorphisme de

$X := (V,\chi)$ avec $X' := (V,\chi')$ signifie que $\chi,\chi' \in \mathrm{GL}_1(K)$ sont conjugués, *i.e.* égaux ; et, dans ce cas, $\phi(X)$ et $\phi(X')$ sont également conjugués, donc égaux. Autrement dit, μ est une fonction de χ seul. Nous noterons encore $\phi : \hat{G} \to K^*$ cette fonction. Pour résumer : étant donnée l'application $\phi : \hat{G} \to K^*$, la transformation naturelle ϕ associe à toute représentation $X := (V,\chi)$ de rang 1 l'automorphisme de $\omega(X) = V$ homothétie de rapport $\mu := \phi(\chi)$.

De plus, quelle que soit l'application ϕ de départ, on peut étendre la transformation naturelle ϕ à toute représentation en décomposant celle-ci en somme directe de représentations de rang 1. Précisément, si $X = \bigoplus(V_i,\chi_i)$, alors $\phi(X)$ agit sur chaque composante de V_i de $\omega(X) = \bigoplus V_i$ comme homothétie de rapport $\phi(\chi_i)$: c'est la seule possibilité, et elle définit bien une transformation naturelle.

Proposition 3.3.4 *Le groupe $Aut(\omega)$ est isomorphe au groupe $(K^*)^{\hat{G}}$ de toutes les applications $\hat{G} \to K^*$.*

Preuve. - On a déjà montré que ces deux ensembles sont égaux. La composée des homothéties de rapports μ,μ' est l'homothétie de rapport $\mu\mu'$. La composée des transformations naturelles définies par les applications $\phi,\phi' : \hat{G} \to K^*$ est donc la transformation naturelle définie par l'application $\phi\phi' : \hat{G} \to K^*$. □

Ce groupe est beaucoup plus gros que $G = \hat{\hat{G}}$. On a perdu la condition que ϕ devait respecter la structure multiplicative de $\hat{G}$:

$$\phi(\chi\chi') = \phi(\chi)\phi(\chi').$$

Il aurait fallu faire intervenir une représentation de caractère $\chi\chi'$ et lui associer un automorphisme de droite qui soit une homothétie de rapport $\mu\mu' = \phi(\chi)\phi(\chi')$; autrement dit : il aurait fallu pouvoir "multiplier" des représentations X et des espaces sous-jacents V, et imposer à la transformation naturelle ϕ d'être compatible avec ces structures multiplicatives.

3.3.2 Produit tensoriel de représentations

On peut en effet munir $\mathcal{R}ep_K(G)$ d'une structure multiplicative à l'aide du produit tensoriel. Soient $X := (V,\rho)$ et $X' := (V',\rho')$ deux représentations de G. Pour tout $g \in G$, l'application linéaire définie par $x \otimes x' \mapsto \rho(g)(x) \otimes \rho'(g)(x')$ de $V \otimes V'$ dans lui-même est bien définie et c'est un automorphisme $\rho(g) \otimes \rho'(g) \in \mathrm{GL}(V \otimes V')$. De la formule (2.2.21.1) (exercice 2.2.21, page 27), on déduit que $\rho \otimes \rho' : g \mapsto \rho(g) \otimes \rho'(g)$ est un morphisme de G dans $\mathrm{GL}(V \otimes V')$, d'où une représentation $X \otimes X' := (V \otimes V', \rho \otimes \rho')$ appelée *produit tensoriel* des représentations X et X'. Le rang de la représentation $X \otimes X'$ est donc le produit des rangs de X et de X'.

Soient $X := (V,\rho)$, $X' := (V',\rho')$ $Y := (W,\sigma)$ et $Y' := (W',\sigma')$ quatre représentations de G. À l'aide de la formule (2.2.21.1), on voit que, si $u : X \to Y$ et $u' : X' \to Y'$ sont des morphismes de représentations, alors l'application linéaire $u \otimes u'$ de $V \otimes V'$ dans $W \otimes W'$ est encore un morphisme de représentations de $X \otimes X'$ dans $Y \otimes Y'$.

Enfin, le foncteur oubli ω est *compatible au produit tensoriel* (on dit aussi $\otimes$-*compatible*) :

$$\omega(X \otimes X') = \omega(X) \otimes \omega(X') \text{ et } \omega(u \otimes u') = \omega(u) \otimes \omega(u').$$

Exemple 3.3.5 Soient $X := (V,\chi)$ et $X' := (V',\chi')$ deux représentations de rang 1 de G. Alors $X \otimes X'$ est la représentation $(V \otimes V', \chi\chi')$. En effet, V et V' sont des droites, donc $V \otimes V'$ aussi. Pour tout $g \in G$, les automorphismes $\chi(g), \chi'(g)$ sont des homothéties de rapports μ, μ' donc $\chi(g) \otimes \chi'(g)$ est l'automorphisme de $V \otimes V'$ défini par $x \otimes x' \mapsto \mu x \otimes \mu' x' = \mu\mu' x \otimes x'$, *i.e.* l'homothétie de rapport $\mu\mu' = \chi\chi'(g)$.

Remarque 3.3.6 Dans le cas de représentations de rang 1, il n'y a aucun mal à se restreindre à des objets de la forme (K,χ), en particulier parce que $K \otimes K$ s'identifie naturellement à K.
Pour les dimensions supérieures, si l'on veut se ramener à des descriptions matricielles $X := (K^n, \rho)$ avec $\rho : G \to \mathrm{GL}_n(K)$, on sera conduit à utiliser l'isomorphisme : $K^n \otimes K^p \simeq K^{np}$. Mais cet isomorphisme n'est pas unique. En fait, la base "naturelle" de $K^n \otimes K^p$ est formée des $e_i \otimes f_j$ où les e_i (resp. les f_j) forment la base canonique de K^n (resp. de K^p). Toute bijection de $\{1,\dots,n\} \times \{1,\dots,p\}$ sur $\{1,\dots,np\}$ fournit un ordre total sur cette base naturelle, donc un isomorphisme $K^n \otimes K^p \simeq K^{np}$.
L'une des complications de la théorie (si l'on tient à des descriptions matricielles, ce qui n'est pas obligatoire) est donc de choisir, pour tous $n, p \in \mathbf{N}$ une bijection de $\{1,\dots,n\} \times \{1,\dots,p\}$ sur $\{1,\dots,np\}$ de manière à obtenir des formule cohérentes, comme dans l'exercice suivant.

Exercice 3.3.7 (i) Vérifier l'existence d'un isomorphisme naturel de $V \otimes (V' \otimes V'')$ sur $(V \otimes V') \otimes V''$.
(ii) Montrer que le choix, pour tous $n, p \in \mathbf{N}$, d'une bijection de $\{1,\dots,n\} \times \{1,\dots,p\}$ sur $\{1,\dots,np\}$, donne lieu, pour tous $n, p, q \in \mathbf{N}$, à des isomorphismes de $K^n \otimes (K^p \otimes K^q)$ et de $(K^n \otimes K^p) \otimes K^q$ sur K^{npq}.
(iii) Y a-t-il automatiquement compatibilité entre les isomorphismes trouvés aux questions précédentes ?

3.3.3 Enveloppe proalgébrique d'un groupe

Puisque nous avons muni $\mathcal{R}ep_K(G)$ d'une structure multiplicative (tensorielle), on peut maintenant sélectionner, à l'intérieur de $\mathrm{Aut}(\omega)$, les éléments qui préservent cette structure.

Ce formalisme garde un sens dans un cadre plus général, où l'on n'a pas nécessairement égalité de $\omega(X \otimes X')$ avec $\omega(X) \otimes \omega(X')$ mais seulement un isomorphisme $t_{X,X'}$ de $\omega(X) \otimes \omega(X')$ sur $\omega(X) \otimes \omega(X')$[3]. Aussi, décorerons-nous les flèches horizontales ci-dessous (ici, des égalités !) de l'étiquette $t_{X,X'}$.

Définition 3.3.8 (Automorphismes $\otimes$-compatibles de ω) Une transformation naturelle ϕ de ω dans lui-même est dite *compatible au produit tensoriel*, ou $\otimes$-*compatible* si, quelles que soient les représentations X et X', le diagramme suivant est commutatif :

$$\begin{array}{ccc} \omega(X \otimes X') & \xrightarrow{t_{X,X'}} & \omega(X) \otimes \omega(X') \\ {\scriptstyle \phi(X\otimes X')}\downarrow & & \downarrow{\scriptstyle \phi(X)\otimes\phi(X')} \\ \omega(X \otimes X') & \xrightarrow{t_{X,X'}} & \omega(X) \otimes \omega(X') \end{array}$$

L'ensemble des automorphismes $\otimes$-compatibles de ω est noté $\mathrm{Aut}^{\otimes}(\omega)$.

[3] Dans les catégories munies de telles structures, on impose cependant à la classe de ces isomorphismes de vérifier des conditions de compatibilité : voir par exemple la définition 1.8 p. 113 de [9].

De la relation (2.2.21.1) (exercice 2.2.21, page 27), et des relations (à la preuve similaire) :

$$(u \otimes u')^{-1} = u^{-1} \otimes u'^{-1} \text{ et } \mathrm{Id}_{V \otimes V'} = \mathrm{Id}_V \otimes \mathrm{Id}_{V'},$$

on déduit que $\mathrm{Aut}^{\otimes}(\omega)$ est un sous-groupe de $\mathrm{Aut}(\omega)$. De plus, par le même genre de calcul, on vérifie que l'application $g \mapsto \phi_g$ est un morphisme de groupes de G dans $\mathrm{Aut}^{\otimes}(\omega)$.

Exercice 3.3.9 Écrire les diagrammes commutatifs qui justifient ces assertions et justifier soigneusement leurs commutativités. À titre d'exemple, voici l'un des diagrammes :

$$\begin{array}{ccc}
\omega(X \otimes X') & \xrightarrow{t_{X,X'}} & \omega(X) \otimes \omega(X') \\
{\scriptstyle \psi(X \otimes X')}\downarrow & & \downarrow{\scriptstyle \psi(X) \otimes \psi(X')} \\
\omega(X \otimes X') & \xrightarrow{t_{X,X'}} & \omega(X) \otimes \omega(X') \\
{\scriptstyle \phi(X \otimes X')}\downarrow & & \downarrow{\scriptstyle \phi(X) \otimes \phi(X')} \\
\omega(X \otimes X') & \xrightarrow{t_{X,X'}} & \omega(X) \otimes \omega(X')
\end{array}$$

Définition 3.3.10 (Enveloppe proalgébrique d'un groupe) Le groupe $G^{alg} := \mathrm{Aut}^{\otimes}(\omega)$, muni du morphisme $g \mapsto \phi_g$ de G dans G^{alg}, est appelé *enveloppe proalgébrique de G*.

Le morphisme $g \mapsto \phi_g$ fait partie de la structure. (Comparer au cas d'une clôture algébrique $\overline{K}$ d'un corps K : le plongement $K \to \overline{K}$ fait partie de la structure.) Nous verrons au chapitre 7 que l'enveloppe proalgébrique est caractérisée par une propriété universelle.

Proposition 3.3.11 *Pour un groupe abélien fini G, l'enveloppe proalgébrique s'identifie au bidual $\hat{\hat{G}}$ muni de l'isomorphisme de bidualité.*

Preuve. - Cela découle des sections précédentes. □

L'isomorphie de G et G^{alg} est malheureusement loin d'être le cas général. Le groupe G^{alg} peut être beaucoup plus gros : on n'a pas réussi à récupérer le groupe G à partir de ses représentations. Ce n'est cependant pas une totale défaite, le groupe G^{alg} est intéressant quand même !

Exemple 3.3.12 On verra que $\mathbf{Z}^{alg} \simeq \mathrm{Hom}_{Gr}(K^*, K^*) \times K$, avec morphisme structural $n \mapsto \big((z \mapsto z^n), n\big)$.

Chapitre 4

Rappels et compléments de géométrie algébrique affine

L'essentiel de nos besoins est couvert par le cours de M1 de géométrie algébrique, et nous le rappellerons sans preuve. Au delà, les preuves sont fournies sans trop de détails : elles pourront être complétées par la lecture des chapitres introductifs de [6] et de [36].

Le cadre est celui de la géométrie algébrique affine sur un corps K algébriquement clos de caractéristique nulle.

4.1 Ensembles algébriques affines

4.1.1 La topologie de Zariski

Soit E un espace affine de dimension finie (sur K). Tout choix d'un repère (*i.e.* d'une origine et d'une base) permet d'identifier E à K^n, donc d'interpréter les polynômes de $K[X_1,\dots,X_n]$ comme des fonctions polynomiales de E dans K ; autrement dit, on a un morphisme de K-algèbres :

$$K[X_1,\dots,X_n] \to K^E, \quad P \mapsto \big((x_1,\dots,x_n) \mapsto P(x_1,\dots,x_n)\big).$$

Le corps K étant infini, ce morphisme est injectif. De plus, l'image de ce morphisme ne dépend pas du repère choisi : la notion d'*application polynomiale* de E dans K, ou encore de *fonction polynomiale* sur E, est définie intrinsèquement (indépendamment du choix d'un repère). Nous noterons $\mathrm{A}(E)$ la K-algèbre des fonctions polynomiales sur E.

Exemple 4.1.1 Sur l'espace vectoriel $E := \mathrm{Mat}_n(K)$, on a la base canonique des matrices élémentaires, d'où une identification de $\mathrm{A}(E)$ avec $K[(X_{i,j})_{1\le i,j\le n}]$. Chaque fonction coefficient $M \mapsto (M)_{i,j}$ est une fonction polynomiale sur E, ainsi que la trace, le déterminant, et, plus généralement, les coefficients du polynôme caractéristique. Nous noterons :

$$\chi_M(T) := \det(TI_n - M) = T^n + c_1(M)T^{n-1} + \cdots + c_n(M),$$

et considèrerons chaque $c_i(M)$ comme un élément aussi bien de $\mathrm{A}\big(\mathrm{Mat}_n(K)\big)$ que de $K[(X_{i,j})_{1\le i,j\le n}]$.

Pour toute partie F de l'algèbre $\mathrm{A}(E)$, on définit le *lieu des zéros de* F comme :

$$\mathcal{V}(F) := \{x \in E \mid \forall f \in F\ ,\ f(x) = 0\}.$$

Dans le cas d'une partie finie $F = \{f_1, \ldots, f_k\}$, on notera simplement $\mathcal{V}(F) = \mathcal{V}(f_1, \ldots, f_k)$. Dans le cas général, l'idéal I de $\mathrm{A}(E)$ engendré par F est de type fini (noetherianité de $\mathrm{A}(E)$), on a donc $I =< f_1, \ldots, f_k >$ et :

$$\mathcal{V}(F) = \mathcal{V}(I) = \mathcal{V}(f_1, \ldots, f_k) = \mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_k).$$

Formulaire. On ne considère ici que des $\mathcal{V}(I)$, I idéal de $\mathrm{A}(E)$.

$$\begin{array}{rcl}
\mathcal{V}(I) = E & \iff & I = \{0\}, \\
\mathcal{V}(I) = \emptyset & \iff & I = \mathrm{A}(E), \\
I \subset J & \implies & \mathcal{V}(J) \subset \mathcal{V}(I), \\
\mathcal{V}(I) & = & \mathcal{V}\left(\sqrt{I}\right), \\
\bigcap \mathcal{V}(I_k) & = & \mathcal{V}\left(\sum I_k\right), \\
\mathcal{V}(I) \cup \mathcal{V}(J) & = & \mathcal{V}(IJ), \\
 & = & \mathcal{V}(I \cap J).
\end{array}$$

Exercice 4.1.2 Quelle est l'unique affirmation non triviale du formulaire ci-dessus ?

Il résulte de ces formules que les $\mathcal{V}(I)$ sont les fermés d'une certaine topologie sur E.

Définition 4.1.3 (Topologie de Zariski) (i) On appelle *topologie de Zariski* sur E la topologie dont les fermés sont les $\mathcal{V}(I)$, I idéal de $\mathrm{A}(E)$.
(ii) On appelle *fermé de Zariski* ou *fermé algébrique* de E un tel fermé.
(iii) On appelle *ensemble algébrique affine* un fermé algébrique d'un espace affine de dimension finie.

Exemples 4.1.4 (i) Les fermés d'une droite affine E sont ses parties finies et E.
(ii) Dans E quelconque, toute partie finie est un fermé.
(iii) Les fermés d'un plan affine E sont les unions finies de points et de courbes $\mathcal{V}(f)$ (f non constant), et E lui-même.

Exercice 4.1.5 Montrer que les points sont des fermés, mais que la topologie de Zariski n'est pas séparée. Plus précisément deux ouverts non vides quelconques se rencontrent.

4.1.2 Correspondance entre fermés et idéaux

Soit $X \subset E$ une partie quelconque. L'*idéal (des équations) de* E est :

$$\mathfrak{I}_E(X) := \{f \in \mathrm{A}(E) \mid \forall x \in X\ ,\ f(x) = 0\}.$$

S'il n' a pas de risque de confusion, on notera parfois pour simplifier $\mathfrak{I}(X) := \mathfrak{I}_E(X)$.

Formulaire.

$$\begin{aligned}
\mathfrak{I}(\emptyset) &= \mathrm{A}(E),\\
\mathfrak{I}(E) &= \{0\},\\
\mathfrak{I}(X) &= \sqrt{\mathfrak{I}(X)},\\
X \subset Y &\implies \mathfrak{I}(Y) \subset \mathfrak{I}(X),\\
\mathfrak{I}\Big(\bigcup X_k\Big) &= \bigcap \mathfrak{I}(X_k).
\end{aligned}$$

Exemples 4.1.6 (i) Si $E = K^n$ et $X = \{a\}$, $a = (a_1, \ldots, a_n)$, alors $\mathfrak{I}(X)$ est l'idéal maximal :

$$\mathfrak{M}_a := < X_1 - a_1, \ldots, X_n - a_n > .$$

(ii) Si X est un sous-espace vectoriel d'un espace vectoriel E, l'idéal $\mathfrak{I}(X)$ est engendré par l'orthogonal $X^\perp \subset E^*$ (dual de E, qui est évidemment inclus dans $\mathrm{A}(E)$).

Exercice 4.1.7 Quel est l'idéal d'un sous-espace affine d'un espace affine E ?

Voici une équivalence extrêmement utile :

$$\forall I \subset \mathrm{A}(E)\ ,\ \forall X \subset E\ ,\ \big(I \subset \mathfrak{I}(X)\big) \Longleftrightarrow \big(X \subset \mathcal{V}(I)\big). \tag{4.1.7.1}$$

On en déduit immédiatement l'adhérence de Zariski d'une partie quelconque :

$$\forall X \subset E\ ,\ \overline{X} = \mathcal{V}\big(\mathfrak{I}(X)\big), \tag{4.1.7.2}$$

et un critère de *Zariski-densité, i.e.* de densité au sens de la topologie de Zariski :

$$(X \text{ est Zariski-dense}) \Longleftrightarrow (\mathfrak{I}(X) = \{0\}), \tag{4.1.7.3}$$

autrement dit : X est Zariski-dense si, et seulement si, toute identité polynomiale vérifiée sur X l'est sur E tout entier.

Proposition 4.1.8 (Principe de prolongement des identités algébriques) *Si $f \in A(E)$ est non nulle, $E \setminus \mathcal{V}(f)$ est Zariski-dense.*

Preuve. - Si g s'annulle sur $E \setminus \mathcal{V}(f)$, alors gf s'annule sur E, donc $gf = 0$, donc $g = 0$ puisque $\mathrm{A}(E)$ est intègre et f non nulle. □

Remarque 4.1.9 Une formulation topologique de cet énoncé est que deux ouverts non vides quelconques se rencontrent (exercice 4.1.5), et donc que tout ouvert non vide est dense : comme on va le voir en 4.1.3, on dit alors que E est irréductible (définition 4.1.16).

Exemple 4.1.10 En prenant $E = \mathrm{Mat}_n(K)$ et $f = \det$, on voit que $\mathrm{GL}_n(K)$ est Zariski-dense dans $\mathrm{Mat}_n(K)$. On va en déduire que, pour deux matrices A, B quelconques, $\chi_{AB} = \chi_{BA}$. Fixons A et considérons B comme un élément variable de $\mathrm{Mat}_n(K)$. Pour $i = 1, \ldots, n$, l'application $B \mapsto c_i(AB) - c_i(BA)$ est polynomiale (les c_i ont été définis dans l'exemple 4.1.1). Lorsque B est inversible, AB est semblable à $B(AB)B^{-1} = BA$; on a donc $\chi_{AB} = \chi_{BA}$ dans ce cas. Les fonctions polynomiales $c_i(AB) - c_i(BA)$ en les coefficients de B sont donc nulles sur la partie Zariski-dense $\mathrm{GL}_n(K)$, donc partout, autrement dit, $\chi_{AB} = \chi_{BA}$ dans tous les cas. À noter cependant que AB et BA ne sont pas toutjours semblables ; par exemple, on peut avoir $AB = 0 \neq BA$.

Exercice 4.1.11 (i) Démontrer que les matrices diagonalisables forment une partie Zariski-dense de $\mathrm{Mat}_n(K)$. (Leur ensemble contient le lieu de non annulation du discriminant du polynôme caractéristique.)
(ii) En déduire une preuve simple du théorème de Cayley-Hamilton sur un corps algébriquement clos.

4.1.3 Le nullstellensatz

Il est *a priori* évident que, pour tout idéal I de $\mathrm{A}(E)$, on a l'inclusion $\sqrt{I} \subset \mathfrak{I}\big(\mathcal{V}(I)\big)$.

Théorème 4.1.12 (Nullstellensatz (ou théorème des zéros) de Hilbert) *(i) Pour tout idéal I de $A(E)$, on a l'égalité :*

$$\mathfrak{I}\big(\mathcal{V}(I)\big) = \sqrt{I}.$$

(ii) En particulier :

$$\big(\mathcal{V}(I) = \emptyset\big) \Longleftrightarrow \big(I = A(E)\big).$$

Pour la preuve, voir [21].

Corollaire 4.1.13 *Les applications $I \mapsto \mathcal{V}(I)$ et $X \mapsto \mathfrak{I}(X)$ induisent deux bijections réciproques l'une de l'autre entre l'ensemble des idéaux radiciels de $A(E)$ (ce sont les idéaux I tels que $I = \sqrt{I}$) et l'ensemble des fermés de Zariski de E.*

Exercice 4.1.14 Démontrer que, si X et Y sont des fermés : $\mathfrak{I}(X \cap Y) = \sqrt{\mathfrak{I}(X) + \mathfrak{I}(Y)}$.

Le cas des idéaux maximaux

Soit I un idéal propre de $\mathrm{A}(E)$. D'après le nullstellensatz, $\mathcal{V}(I) \neq \emptyset$, il existe $a \in \mathcal{V}(I)$, d'où l'inclusion $I \subset \mathfrak{M}_a := \mathfrak{I}(\{a\})$. Ainsi, les seuls idéaux maximaux de $\mathrm{A}(E)$ sont les $\mathfrak{M}_a$ et, par les bijections du corollaire 4.1.13, se correspondent les idéaux maximaux de $\mathrm{A}(E)$ et les points de E.

Le morphisme $\mathrm{A}(E) \to \mathrm{A}(E)/\mathfrak{M}_a$ s'identifie en fait au *morphisme d'évaluation* $P \mapsto P(a)$ de $\mathrm{A}(E)$ sur K. c'est un morphisme de K-algèbres, et il n'est pas difficile de voir que tout morphisme de K-algèbres de $\mathrm{A}(E)$ dans K s'obtient de cette manière (voir là dessus page 47 la "dualité de Gelfand").

Exercice 4.1.15 En prenant $E = K^n$ et donc $\mathrm{A}(E) = K[X_1, \ldots, X_n]$, vérifier cette dernière assertion et expliciter une bijection de E sur l'ensemble $\mathrm{Hom}_{\mathcal{A}lg_K}$ des morphismes de K-algèbres de $\mathrm{A}(E)$ dans K.

Le cas des idéaux premiers

On va voir que les idéaux premiers acquièrent, par la correspondance du corollaire 4.1.13, une signification topologique.

Définition 4.1.16 (Fermés irréductibles) Le fermé X de E est dit *irréductible* s'il est non vide et s'il n'est pas la réunion de deux fermés strictement plus petits, *i.e.* si l'égalité $X = X_1 \cup X_2$ (avec X_1, X_2 fermés) entraîne $X = X_1$ ou $X = X_2$.
De manière équivalente : $X \neq \emptyset$ et l'inclusion $X \subset X_1 \cup X_2$ (avec X_1, X_2 fermés) entraîne $X \subset X_1$ ou $X \subset X_2$.

Exemples 4.1.17 (i) Les ensembles finis irréductibles sont les singletons.
(ii) L'ensemble E est irréductible (remarque 4.1.9).

Proposition 4.1.18 *Le fermé X est irréductible si, et seulement si, l'idéal $\mathfrak{I}(X)$ est premier.*

Preuve. - La condition $X \neq \emptyset$ équivaut à $\mathfrak{I}(X) \neq \mathrm{A}(E)$.
Supposons X irréductible. Si $f_1 f_2 \in \mathfrak{I}(X)$, alors $X \subset \mathcal{V}(f_1) \cup \mathcal{V}(f_2)$, donc $X \subset \mathcal{V}(f_1)$ ou $X \subset \mathcal{V}(f_2)$ (irréductibilité), *i.e.* $f_1 \in \mathfrak{I}(X)$ ou $f_2 \in \mathfrak{I}(X)$ et l'idéal $\mathfrak{I}(X)$ est premier.
Supposons $\mathfrak{I}(X)$ premier. Si $X \subset X_1 \cup X_2$, alors $\mathfrak{I}(X_1) \cap \mathfrak{I}(X_2) = \mathfrak{I}(X_1 \cup X_2) \subset \mathfrak{I}(X)$. Puisque $\mathfrak{I}(X)$ est premier, on en déduit (algèbre facile) que $\mathfrak{I}(X_1) \subset \mathfrak{I}(X)$ ou $\mathfrak{I}(X_2) \subset \mathfrak{I}(X)$, donc (puisque ce sont des fermés) que $X \subset X_1$ ou $X \subset X_2$. □

Corollaire 4.1.19 *Par les bijections du corollaire 4.1.13 se correspondent les idéaux premiers de $A(E)$ et les fermés irréductibles de E.*

Exemple 4.1.20 Tout sous-espace affine est un fermé irréductible.

Théorème 4.1.21 *Tout fermé non vide de E est réunion de ses fermés irréductibles maximaux, qui sont en nombre fini. On les appelle* composantes irréductibles *de X.*

Preuve. - C'est la finitude qui est non triviale ; elle découle de la noetherianité de $\mathrm{A}(E)$, pour la preuve voir [6]. □

Si $X = X_1 \cup \cdots \cup X_k$ est la *décomposition de X en composantes irréductibles*, c'est-à-dire l'écriture de X comme réunion de ses composantes irréductibles, cette réunion est minimale, au sens où l'on ne peut enlever aucun des X_i : sinon, ce dernier serait inclus dans la réunion des autres, donc (irréductibilité) dans l'un des autres, contredisant la maximalité.

Exercice 4.1.22 (i) Montrer que le fermé $\mathcal{V}(f)$ est irréductible si, et seulement si, f est puissance d'un polynôme irréductible avec un exposant non nul. (Invoquer la factorialité de $\mathrm{A}(E)$.)
(ii) En général, les composantes irréductibles du fermé $X = \mathcal{V}(f)$ sont les $\mathcal{V}(f_i)$, où les f_i sont les facteurs irréductibles de f.

4.2 Fonctions régulières

L'une des principales évolutions de la géométrie au XX$^{\mathrm{e}}$ siècle a été la découverte du fait que, pour connaitre un espace, il est essentiel de connaitre l'anneau des fonctions "adéquates" sur cet espace ; "adéquates" signifiant, selon le type de géométrie : continues, différentiables, analytiques ... et, pour la géométrie algébrique : régulières.

4.2.1 Fonctions régulières, algèbres affines

Définition 4.2.1 (Fonctions régulières, algèbres affines) Soit X un fermé de E. On appelle *fonction régulière* sur X la restriction d'une fonction polynomiale sur E. La K-algèbre des fonctions régulières sur X est notée $\mathrm{A}_E(X)$ et appelée *algèbre affine de* X. (On verra à la section 4.2.3 que la dépendance en E est inessentielle et que l'on peut aussi bien écrire $\mathrm{A}(X)$.)

Par définition, le morphisme $\mathrm{A}(E) \to \mathrm{A}_E(X)$ est surjectif de noyau l'idéal $\mathfrak{I}_E(X)$. On a donc un isomorphisme canonique de K-algèbres :

$$\mathrm{A}(E)/\mathfrak{I}_E(X) \simeq \mathrm{A}_E(X).$$

Exemples 4.2.2 (i) L'algèbre affine d'un sous-espace affine de dimension m est isomorphe à $K[X_1,\dots,X_m]$.
(ii) L'algèbre affine de X est un corps si, et seulement si, X est un point ; et dans ce cas $\mathrm{A}_E(X) = K$.
(iii) L'algèbre affine de X est intègre si, et seulement si, X est irréductible.

De manière générale, modulo identification de E avec K^n, l'algèbre affine d'un fermé de E est de la forme $K[X_1,\dots,X_n]/I$, où I est radiciel. C'est donc une K-algèbre de type fini réduite. Réciproquement, toute K-algèbre de type fini réduite est (isomorphe à une K-algèbre) de la forme $K[X_1,\dots,X_n]/I$, où I est radiciel, donc isomorphe à $\mathrm{A}_E(X)$, où $X = \mathcal{V}(I) \subset K^n$. (On a eu besoin de supposer I radiciel pour que $\mathfrak{I}(X)$ soit égal à I.)

Exercice 4.2.3 (i) Définir en toute généralité un morphisme injectif de K-algèbres :

$$\mathrm{A}_E(X_1 \cup X_2) \to \mathrm{A}_E(X_1) \times \mathrm{A}_E(X_2).$$

(ii) Montrer que c'est un isomorphisme si, et seulement si $X_1 \cap X_2 = \emptyset$. (C'est essentiellement le lemme chinois.)
(iii) En déduire que, pour que X soit connexe, il faut, et il suffit, que $\mathrm{A}_E(X)$ n'admette pas d'idempotents autres que 0 et 1.

La correspondance entre fermés de E et idéaux de $\mathrm{A}(E)$ (corollaire 4.1.13) se généralise en une correspondance fermés de X et idéaux de $\mathrm{A}_E(X)$ par la "chaine" suivante : un fermé Y de X est un fermé Y de E contenu dans X ; il correspond à un idéal radiciel $J := \mathfrak{I}(Y)$ qui contient $I := \mathfrak{I}(X)$; ce dernier correspond à un idéal radiciel J/I du quotient $\mathrm{A}(E)/I = \mathrm{A}_E(X)$. Par cette nouvelle correspondance bijective, les points (resp. les fermés irréductibles) de X correspondent aux idéaux maximaux (resp. aux idéaux premiers) de $\mathrm{A}_E(X)$.

On va d'ailleurs expliciter cette correspondance en étendant les notations $\mathcal{V}$ et $\mathfrak{I}$. Pour tout idéal L de l'algèbre $\mathrm{A}_E(X)$, le lieu d'annulation des éléments de L est un fermé de X :

$$\mathcal{V}_X(L) := \{x \in X \mid \forall f \in L\ ,\ f(x) = 0\}.$$

En fait, si J est l'image réciproque dans $\mathrm{A}(E)$ de $L \subset \mathrm{A}_E(X)$, on a $I \subset J$ et $\mathcal{V}_X(L) = \mathcal{V}(J)$. Les $\mathcal{V}_X(L)$ sont donc les fermés inclus dans X. On peut d'ailleurs définir $\mathcal{V}_X(L)$ pour un sous-ensemble quelconque $L \subset \mathrm{A}_E(X)$. Réciproquement, pour toute partie Y de X, l'ensemble des fonctions régulières sur X nulles sur Y est un idéal de $\mathrm{A}_E(X)$:

$$\mathfrak{I}_X(Y) := \{f \in \mathrm{A}_E(X) \mid \forall x \in Y\ ,\ f(x) = 0\}.$$

En fait, c'est l'image de l'idéal $\mathfrak{I}(Y) \supset \mathfrak{I}(X)$ par le morphisme canonique $\mathrm{A}(E) \to \mathrm{A}(E)/\mathfrak{I}(X) = \mathrm{A}_E(X)$.

Comme on l'a dit, $\mathcal{V}_X$ et $\mathfrak{I}_X$ induisent des bijections réciproques l'une de l'autre entre fermés de X et idéaux radiciels de $\mathrm{A}_E(X)$. De plus, si Y est un fermé de X, donc de E, le morphisme de restriction $\mathrm{A}_E(X) \to \mathrm{A}_E(Y)$ induit un isomorphisme de K-algèbres :

$$\mathrm{A}_E(Y) \simeq \mathrm{A}_E(X)/\mathfrak{I}_X(Y).$$

Exercice 4.2.4 (i) Soit (Y_α) une famille de fermés de X. Montrer l'équivalence :

$$\left(\bigcap Y_\alpha = \emptyset\right) \Longleftrightarrow \left(\sum \mathfrak{I}_X(Y_\alpha) = \mathrm{A}_E(X)\right).$$

(ii) En déduire que l'espace topologique X est quasi-compact. Est-il compact ?

4.2.2 Dimension d'un ensemble algébrique

Que signifie l'affirmation qu'une courbe est de dimension 1, qu'une surface est de dimension 2, etc ? Il y a beaucoup de définitions de la dimension en topologie, en géométrie différentielle ... Voici l'une de celles qui se sont imposées en géométrie algébrique.

Définition 4.2.5 (Dimension (de Krull) d'un espace topologique) La *dimension (de Krull)* $\dim X$ d'un espace topologique X est la borne supérieure des longueurs k des *chaines de fermés irréductibles de X*, une chaine de longueur k étant une suite $X_0 \subset \cdots \subset X_k$ de fermés irréductibles emboîtés, les inclusions étant supposées strictes. Par convention, l'ensemble vide est de dimension $-\infty$.

Exemples 4.2.6 Un ensemble fini non vide est de dimension 0. Une droite affine est de dimension de Krull 1.

Remarque 4.2.7 En fait, la dimension est souvent définie par l'intermédiaire du degré de transcendance (voir [6, 36]). Les deux approches sont équivalentes (théorème 4.2.12) mais celle qui précède se généralise mieux.

Proposition 4.2.8 *(i) Si X est de dimension finie,* $\dim X$ *est le maximum des dimensions des composantes irréductibles de X.*
(ii) On suppose X de dimension finie k. Pour toute chaine $X_0 \subset \cdots \subset X_k$ de fermés irréductibles de X, les fermés X_0 et X_k sont respectivement un point et une composante irréductible ; et la chaine est saturée *(on ne peut la raffiner).*
(iii) Si X, X' sont des fermés, $\dim(X \cup X') = \max(\dim X, \dim X')$.
(iv) Si $X \subset Y$ sont des fermés, $\dim X \leq \dim Y$. *Si de plus Y est irréductible et* $\dim X = \dim Y$, *alors $X = Y$.*

Preuve. - Facile et laissée au lecteur ! □

Définition 4.2.9 (Dimension de Krull d'un anneau commutatif) La *dimension de Krull* d'un anneau commutatif A est la borne supérieure des longueurs k des *chaines d'idéaux premiers* $\mathfrak{P}_0 \subset \cdots \subset \mathfrak{P}_k$ de A.

Proposition 4.2.10 *La dimension d'un fermé algébrique est égale à la dimension de Krull de son algèbre affine.*

Preuve. - C'est immédiat. □

Exercice 4.2.11 Le plan affine E est de dimension de Krull 2 et, si $f \in \mathrm{A}(E)$ est non constante, $\dim \mathcal{V}_E(f) = 1$.

Le théorème suivant est fondamental ; nous l'admettrons (voir [6, 36, 21]).

Théorème 4.2.12 *(i) La dimension de Krull de $K[X_1,\dots,X_n]$ est n. La dimension de Krull d'un espace affine E est égale à sa dimension.*
(ii) Si $f \in K[X_1,\dots,X_n]\setminus K$, la dimension de Krull de $K[X_1,\dots,X_n]/<f>$ est $n-1$. Si $f \in A(E)$ n'est pas constante, la dimension de Krull de l'hypersurface $\mathcal{V}(f)$ est $\dim E - 1$.
(iii) La dimension de Krull d'une algèbre affine intègre est égale au degré de transcendance sur K de son corps des fractions. La dimension de Krull d'un ensemble algébrique irréductible X est égale au degré de transcendance sur K du corps des fractions de $A(X)$.
(iv) Tout ensemble algébrique de dimension 0 est fini.

Exercice 4.2.13 Démontrer que tout ensemble algébrique est de dimension finie.

4.2.3 Qu'est-ce intrinsèquement qu'un ensemble algébrique ?

Deux difficultés vont se présenter, dûes à notre approche élémentaire et non intrinsèque[1] :

1. Notre définition d'un ensemble algébrique X, et tout ce qui s'en déduit, suppose X plongé dans un espace affine. Il n'est pas clair en l'état qu'une "même" courbe vue dans K^2 ou dans K^3 soit en effet le même objet.
2. Tous nos ensembles algébriques sont obtenus comme des fermés algébriques : rien de ce que nous avons fait ne semble s'appliquer à $\mathrm{GL}_n(K)$, qui est pourtant notre objet principal d'intérêt (dans ce cours).

Pour surmonter ces difficultés, nous allons adopter le point de vue (ou slogan) suivant : *ce qui caractérise la géométrie de X, c'est sa topologie de Zariski et son algèbre $A(X) = A_E(X)$ de fonctions régulières*. (Et l'on verra au passage que la dépendance en E est un artefact.)

Comment reconstituer X à partir de $\mathbf{A}(X)$: la "dualité de Gelfand"

Le "retour en arrière" de l'algèbre affine $A := \mathrm{A}(X)$ vers l'espace topologique X peut se réaliser à l'aide de la "dualité de Gelfand". Cette dernière est née dans la théorie des anneaux commutatifs normés, mais s'est étendue à l'ensemble de la géométrie[2]. Le lecteur est invité à vérifier tous les détails des arguments qui suivent.

[1] Les vraiment bonnes définitions reposent sur la notion de "schéma affine", qui n'est pas très difficile mais demande un peu de formalisme et masque (temporairement) la géométrie.

[2] L'avantage de cette construction est qu'elle garde un sens pour toute K-algèbre A, ce qui donne lieu à de vastes généralisations de la géométrie algébrique affine.

On pose d'abord :

$$\mathcal{X} := \mathrm{Mor}_{\mathcal{A}lg_K}(A, K).$$

Il y a une bijection $X \to \mathcal{X}$ qui, à $x \in X$ associe $\chi_x : f \mapsto f(x)$; la bijection réciproque associe à $\chi : A \to K$ l'unique point $x \in X$ tel que $\mathfrak{M}_x = \mathrm{Ker}\,\chi$.

Concrètement, prenons $A := K[X_1, \ldots, X_n]/I$, de sorte que X s'identifie à $\mathcal{V}(I) \subset K^n$. Un morphisme $\chi : A \to K$ est déterminé par les images $x_i := \chi(X_i) \in K$, soumises à la condition que $x := (x_1, \ldots, x_n) \in \mathcal{V}(I)$ (pour que le morphisme correspondant $K[X_1, \ldots, X_n] \to K$ se factorise via A). Le point x correspond à χ.

Pour tout idéal I de A, on pose ensuite :

$$\mathcal{V}_{\mathcal{X}}(I) := \{\chi \in \mathcal{X} \mid \mathrm{Ker}\,\chi \supset I\}.$$

On vérifie alors que les $\mathcal{V}(I)$ sont les fermés d'une topologie sur $\mathcal{X}$, puis que les bijections ci-dessus sont des homéomorphismes. Ainsi, si $a \in A$, l'ouvert de $\mathcal{X}$ qui correspond par ces homéomorphismes à l'ouvert $\mathcal{D}(a) \subset X$ est :

$$\mathcal{X} \setminus \mathcal{V}_{\mathcal{X}}(a) = \{\chi \in \mathcal{X} \mid \chi(a) \neq 0\}.$$

Fermés algébriques indépendamment du plongement

Proposition 4.2.14 *Soient E un espace affine et $E' \subset E$ un sous-espace affine.*
(i) Les fonctions polynomiales sur E' sont les restrictions à E' des fonctions polynomiales sur E. L'algèbre $A(E')$ des fonctions polynomiales sur l'espace affine E' est égale à l'algèbre $A(E)/\mathfrak{I}_E(E')$ des fonctions régulières sur le fermé E' de E.
(ii) Le sous-ensemble $X \subset E'$ est un fermé algébrique de E' si, et seulement si, c'est un fermé algébrique de E. Les idéaux correspondants sont alors liés par la relation suivante :

$$\mathfrak{I}_E(X) = \mathfrak{I}_{E'}(X)A(E) + \mathfrak{I}_E(E'),$$

et les algèbres affines par la relation suivante :

$$A_E(X) = A_{E'}(X).$$

Preuve. - Facile et laissée au lecteur. À noter que la dernière égalité dénote (abus courant) un isomorphisme canonique. L'égalité précédente est une vraie égalité et elle admet la forme concrète suivante. On prend $E = K^n$ muni des coordonnés $X_1, \ldots, X_n$ et $E' = K^{n'}$ muni des coordonnés $X_1, \ldots, X_{n'}$ ($n' < n$). Soient $f_1, \ldots, f_m \in K[X_1, \ldots, X_{n'}]$ des générateurs de $\mathfrak{I}_{E'}(X)$. Alors $f_1, \ldots, f_m, X_{n'+1}, \ldots, X_n$ sont des générateurs de $\mathfrak{I}_E(X)$. □

Corollaire 4.2.15 *La topologie et l'algèbre affine d'un ensemble algébrique X ne dépendent pas du plongement de X dans un espace affine.*

Extension de ce qui précède aux ouverts affines

L'ouvert $\mathrm{GL}_n(K)$ de $\mathrm{Mat}_n(K)$ est de nature particulière : son complémentaire est défini par une seule équation (det).

Définition 4.2.16 (Ouverts affines) Un *ouvert affine* d'un ensemble algébrique X est un ouvert de la forme $\mathcal{D}_X(f) := X \setminus \mathcal{V}_X(f)$, où $f \in \mathrm{A}(X)$.

L'intérêt des ouverts affines[3] est qu'ils s'identifient à des ensembles algébriques.

Proposition 4.2.17 *(i) Soit X un fermé algébrique de l'espace affine E. Alors $X' := X \times K$ est un fermé de l'espace affine $E' := E \times K$.*
(ii) La première projection $X' \to X$ est une application continue et ouverte.
(iii) La première projection $X' \to X$ induit un homéomorphisme :

$$\mathcal{V}_{X'}(1 - Tf) \simeq \mathcal{D}_X(f).$$

Preuve. - (i) La première assertion est facile et laissée au lecteur.
(ii) La projection $p : X' \to X$ est une application continue en vertu de la formule suivante, dont la preuve est facile et laissée au lecteur :

$$p^{-1}\big(\mathcal{V}_X(I)\big) = \mathcal{V}_{X'}\big(I\mathrm{A}_{E'}(X')\big).$$

La projection p est de plus une application ouverte ; en effet, pour tout ouvert $Y' := X' \setminus \mathcal{V}_{X'}(I')$ de X', les points $x \in X \setminus p(U')$ sont caractérisés par le fait que tout $(x,t) \in X'$ est dans $\mathcal{V}_{X'}(I')$. Notant I l'idéal des coefficients dans $\mathrm{A}(X)$ de tous les $f \in I'$ vus comme polynômes de $\mathrm{A}(X)[T]$, on a donc :

$$p(U') = X \setminus \mathcal{V}_X(I).$$

(iii) On a identifié $\mathrm{A}(E')$ à $\mathrm{A}(E)[T]$, d'où l'égalité $\mathrm{A}(X') = \mathrm{A}(X)[T]$. La bijectivité se ramène alors au fait que $f(x) \neq 0 \Leftrightarrow \exists t \ : \ tf(x) = 1$, et à l'unicité d'un tel t. La restriction $\mathcal{V}_{X'}(1 - Tf) \to \mathcal{D}_X(f)$de p est donc bijective, ouverte et continue, donc un homéomorphisme. □

La topologie sur l'ouvert affine $\mathcal{D}_X(f)$ est donc celle d'un ensemble algébrique. En vertu du paragraphe précédent (sur l'indépendance du plongement) et de la proposition, on peut donc définir *l'algèbre affine de l'ouvert affine* $\mathcal{D}_X(f)$ comme celle de l'ensemble algébrique $\mathcal{V}_{X'}(1 - Tf)$:

$$\begin{aligned} \mathrm{A}\big(\mathcal{D}_X(f)\big) &:= \mathrm{A}\big(\mathcal{V}_{X'}(1 - Tf)\big) \\ &= \mathrm{A}(X)[T]/ < 1 - Tf > \\ &= \mathrm{A}(X)_f \\ &= \mathrm{A}(X)[1/f]. \end{aligned}$$

Rappelons en effet que, pour tout anneau commutatif A et tout $f \in A$, l'anneau de fractions $A_f := S^{-1}A$, $S := \{f^n \mid n \in \mathbf{N}\}$ s'identifie canoniquement à $\mathrm{A}[T]/ < 1 - Tf >$. De plus, si A est intègre, A_f est le sous-anneau du corps des fractions de A engendré par A et $1/f$. (Cela s'applique

[3]Pour des ouverts plus généraux, l'algèbre des fonctions régulières ne suffit pas : il faut faire appel à un faisceau.

ici si X est irréductible.) On s'en autorise pour écrire en général, avec un léger abus : $A_f = A[1/f]$.

Les bijections habituelles entre fermés, resp. fermés irréductibles, resp. points de X et idéaux, resp. idéaux premiers, resp. idéaux maximaux de $\mathrm{A}(X)$ s'étendent directement au cas où X est un ouvert affine. Il en est de même de la théorie de la dimension. Nous considèrerons donc désormais les ouverts affines comme des ensembles algébriques.

Exemples 4.2.18 (i) Puisque $K^* = \mathcal{D}_K(X)$, on a :

$$\mathrm{A}(K^*) = K[X,T]/ < 1 - XT >= K[X,X^{-1}].$$

(ii) Puisque $\mathrm{GL}_n(K) = \mathcal{D}_K(\det)$, avec $E = \mathrm{Mat}_n(K)$, on trouve son algèbre affine :

$$\mathrm{A}\big(\mathrm{GL}_n(K)\big) = K[(X_{i,j})_{1\leq i,j\leq n}][T]/ < 1 - T\det(X_{i,j}) >= K[(X_{i,j})_{1\leq i,j\leq n}]\left[\frac{1}{\det(X_{i,j})}\right].$$

Exercice 4.2.19 (i) Soient E un espace affine de dimension n et $X := \mathcal{D}_E(f)$ où $f \in \mathrm{A}(E)$ n'est pas constante. Déduire du théorème 4.2.12, assertions (i) et (ii) que $\dim X = n$.
(ii) Montrer que X est irréductible et que le corps des fractions de son algèbre affine est égal au corps des fractions de $\mathrm{A}(E)$. En déduire à nouveau que $\dim X = n$.

4.3 La catégorie $\mathcal{A}ff_K$

La véritable manière de décider si deux courbes sont "essentiellement les mêmes" *du point de vue de la géométrie algébrique*, c'est de définir la notion d'isomorphisme ; et l'approche la plus efficace pour cela, c'est de définir une catégorie des ensembles algébriques (dans le cadre de ce cours : affines).

4.3.1 Morphismes

Soient E et F deux K-espaces affines de dimensions respectives n et p. Après choix de repères, on peut les identifier respectivement à K^n et à K^p, et donc identifier $\mathrm{A}(E)$ à $K[X_1,\ldots,X_n]$ et $\mathrm{A}(F)$ à $K[X_1,\ldots,X_p]$. Il est naturel de dire qu'une application $\phi : K^n \to K^p$ est *polynomiale* si elle est de la forme :

$$\phi = (Q_1,\ldots,Q_p), \quad Q_1,\ldots,Q_p \in K[X_1,\ldots,X_n].$$

Il est clair que cette définition ne dépend pas du choix des repères. On voit alors que les applications polynomiales admettent la caractérisation suivante :

$$\big(\phi : E \to F \text{ est polynomiale }\big) \Longleftrightarrow \big(\forall f \in \mathrm{A}(F)\ ,\ f\circ\phi \in \mathrm{A}(E)\big).$$

Exercice 4.3.1 Prouver cette équivalence en supposant que $E = K^n$, $F = K^p$, $\mathrm{A}(E) = K[X_1,\ldots,X_n]$ et $\mathrm{A}(F) = K[X_1,\ldots,X_p]$.

Il est tout aussi clair, si $\phi : E \to F$ est polynomiale, l'application $f \mapsto f\circ\phi$ de $\mathrm{A}(F)$ dans $\mathrm{A}(E)$ est un morphisme de K-algèbres. On note ϕ^* ce morphisme, et on l'appelle *comorphisme de* ϕ. On définit ainsi une bijection $\phi \mapsto \phi^*$ de l'ensemble des applications polynomiales de E dans F sur l'ensemble $\mathrm{Mor}_{\mathcal{A}lg_K}\big(\mathrm{A}(F),\mathrm{A}(E)\big)$.

Proposition 4.3.2 *Soit $\phi : E \to F$ une application polynomiale.*
(i) Soit $Y := \mathcal{V}_F(J) \subset F$ un fermé algébrique. Alors :

$$\phi^{-1}(Y) = \mathcal{V}_E\big(\phi^*(J)\big).$$

(ii) Soit $X \subset E$ un fermé algébrique. Alors :

$$\mathfrak{I}_F\big(\phi(X)\big) = \mathfrak{I}_F\left(\overline{\phi(X)}\right) = (\phi^*)^{-1}\big(\mathfrak{I}_E(X)\big).$$

Preuve. - (i) On a les équivalences :

$$x \in \phi^{-1}(Y) \Longleftrightarrow \phi(x) \in Y \Longleftrightarrow \forall f \in J\ ,\ f\big(\phi(x)\big) = 0 \Longleftrightarrow$$

$$\forall f \in J\ ,\ \phi^*(f)(x) = 0 \Longleftrightarrow \forall g \in \phi^*(J)\ ,\ g(x) = 0 \Longleftrightarrow x \in \mathcal{V}_F\big(\phi^*(J)\big).$$

(Noter cependant que $\phi^*(J)$ n'est en général pas un idéal.)
(ii) On a les équivalences :

$$f \in \mathfrak{I}_F\left(\overline{\phi(X)}\right) \Longleftrightarrow \forall y \in \phi(X)\ ,\ f(y) = 0 \Longleftrightarrow \forall x \in X\ ,\ f\big(\phi(x)\big) = 0 \Longleftrightarrow$$

$$\forall x \in X\ ,\ \phi^*(f)(x) = 0 \Longleftrightarrow \phi^*(f) \in \mathfrak{I}_E(X) \Longleftrightarrow f \in (\phi^*)^{-1}\big(\mathfrak{I}_E(X)\big).$$

□

Corollaire 4.3.3 *(i) Pour des fermés $X \subset E$, $Y \subset F$, l'inclusion $\phi(X) \subset Y$ équivaut à l'inclusion $\phi^*\big(\mathfrak{I}_F(Y)\big) \subset \mathfrak{I}_E(X)$, et cette dernière à l'existence d'un diagramme commutatif :*

$$\begin{array}{ccc} A(F) & \xrightarrow{\phi^*} & A(E) \\ \big\downarrow & & \big\downarrow \\ A(Y) & \longrightarrow & A(X) \end{array}$$

dans lequel les flèches verticales sont les surjections canoniques.
(ii) L'application induite $A(Y) \to A(X)$ est alors l'application $f \to f \circ \phi$.

Preuve. - (i) La première équivalence découle immédiatement de la proposition, la deuxième est de l'algèbre standard puisque $\mathrm{A}(Y) = \mathrm{A}(F)/\mathfrak{I}_F(Y)$ et $\mathrm{A}(X) = \mathrm{A}(E)/\mathfrak{I}_E(X)$. (ii) est immédiat. □

Nous dirons que l'application $\phi : X \to Y$ est *polynomiale* si c'est la restriction d'une application polynomiale de E dans F. Du corollaire, on déduit une caractérisation plus intrinsèque, que nous prendrons donc comme définition.

Définition 4.3.4 (Catégorie des ensembles algébriques affines) (i) Soient X, Y des ensembles algébriques. L'application $\phi : X \to Y$ est dite polynomiale si elle induit une application $\phi^* : f \mapsto f \circ \phi$ de $\mathrm{A}(Y)$ dans $\mathrm{A}(X)$. Le morphisme d'algèbres ϕ^* est appelé *comorphisme* de ϕ.
(ii) La catégorie $\mathcal{A}ff_K$ des ensembles algébriques affines sur K a pour objets les ensembles algébriques affines et pour morphismes les applications polynomiales.

Exemples 4.3.5 (i) L'application $i : x \mapsto x^{-1}$ de K^* dans lui-même est polynomiale. Pour le voir, on identifie K^* à $\mathcal{V}(1-XT) \subset K^2$ et l'on voit que le comorphisme de i est l'endomorphisme i^* de $\mathrm{A}(K^*) = K[X,T]/ < 1-XT >$ induit par l'endomorphisme $X \mapsto T, T \mapsto X$ de $K[X,T]$. Noter que cet endomorphisme envoie bien l'idéal $< 1-XT >$ dans lui-même.
(ii) L'application $A \mapsto A^{-1}$ de $\mathrm{GL}_n(K)$ dans lui-même est polynomiale. Pour le voir, on identifie $\mathrm{GL}_n(K)$ à $\mathcal{V}(1-T\det) \subset \mathcal{M}_n(K) \times K$. Le comorphisme est l'endomorphisme de l'algèbre $K[(X_{i,j})_{1\leq i,j\leq n}][T]/ < 1-T\det(X_{i,j}) >$ obtenu par passage au quotient de l'endomorphisme :

$$X_{i,j} \mapsto TK_{i,j}, \quad T \mapsto \det(X_{i,j}),$$

de l'algèbre $K[(X_{i,j})_{1\leq i,j\leq n}][T]$, où $K_{i,j}$ désigne le coefficient (i,j) de la transposée de la comatrice $(X_{i,j})$.

Exercice 4.3.6 Dans l'exemple précédent, vérifier que l'endomorphisme de l'algèbre $K[(X_{i,j})_{1\leq i,j\leq n}][T]$ envoie bien l'idéal $< 1-T\det(X_{i,j}) >$ dans lui-même.

Théorème 4.3.7 *Le foncteur contravariant $X \rightsquigarrow A(X), \phi \rightsquigarrow \phi^*$ de $\mathcal{A}ff_K$ dans $\mathcal{A}lg_K$ est pleinement fidèle et admet pour image essentielle la catégorie des algèbres affines réduites.*

Preuve. - C'est un résumé de la discussion ci-dessus. □

Exemple 4.3.8 Tout comme pour les espaces topologiques, un isomorphisme dans $\mathcal{A}ff_K$ est *ipso facto* un morphisme bijectif, mais la réciproque est fausse. Ainsi, l'application $t \mapsto (t^2,t^3)$ de K dans K^2 est un morphisme injectif d'image la courbe $\Gamma := \mathcal{V}(Y^2-X^3)$, et réalise donc un morphisme bijectif de K sur Γ. Mais ces deux ensembles algébriques ne sont pas isomorphes, car dans le cas contraire, leurs algèbres affines $K[T]$ et $K[X,Y]/ < Y^2-X^3 >$ le seraient.

Exercice 4.3.9 Démontrer que l'anneau $K[X,Y]/ < Y^2-X^3 >$ est intègre, de corps des fractions $K(X)[Y] < Y^2-X^3 >$; mais qu'il n'est pas intégralement clos, donc pas isomorphe à $K[T]$.

4.3.2 Aspects topologiques

Proposition 4.3.10 *Soit $\phi : X \to Y$ un morphisme entre ensembles algébriques.*
(i) Soit $Y' := \mathcal{V}_Y(J) \subset F$ un fermé algébrique. Alors :

$$\phi^{-1}(Y') = \mathcal{V}_X\big(\phi^*(J)\big).$$

(ii) Soit $X' \subset X$ un fermé algébrique. Alors :

$$\mathcal{I}_Y\big(\phi(X')\big) = \mathcal{I}_Y\left(\overline{\phi(X')}\right) = (\phi^*)^{-1}\big(\mathcal{I}_X(X')\big).$$

(iii) Le comorphisme ϕ^* est injectif si, et seulement si, le morphisme ϕ est dominant.
(iv) Le comorphisme ϕ^* est surjectif si, et seulement si, le morphisme ϕ est une immersion fermée, c'est-à-dire un isomorphisme de X avec un fermé de Y.

Preuve. - (i) et (ii) se démontrent exactement de la même que pour la proposition 4.3.2.
(iii) est une conséquence immédiate de (ii) appliqué à $X' := X$.
(iv) se voit ainsi : la surjectivité du comorphisme ϕ^* signifie qu'il se factorise par un isomorphisme d'un quotient $\mathrm{A}(Y)/J$ avec $\mathrm{A}(X)$, donc que ϕ se factorise par un isomorphisme de X avec un fermé $\mathcal{V}_Y(J)$. □

Corollaire 4.3.11 *Tout morphisme est continu.*

Exercice 4.3.12 Montrer que les projections de $X \times Y$ sur X, Y sont des morphismes et que ce sont des applications ouvertes.

Il n'y a aucune raison en général pour que l'image d'un morphisme entre ensembles algébriques soit un ouvert ou un fermé.

Exercice 4.3.13 Donner des contre-exemples.

Cependant, Chevalley a démontré que cette image est "constructible" (voir [6]). Nous allons prouver un théorème plus faible mais non trivial, et qui nous sera extrêmement utile dans l'étude des groupes algébriques.

Théorème 4.3.14 *Soit $\phi : X \to Y$ un morphisme d'ensembles algébriques. Alors $\phi(X)$ contient un ouvert dense de son adhérence $\overline{\phi(X)}$.*

Preuve. - On écrit $X = X_1 \cup \cdots \cup X_k$ (composantes irréductibles). On a donc $\overline{\phi(X)} = \overline{\phi(X_1)} \cup \cdots \cup \overline{\phi(X_k)}$, et, si $U_i \subset \phi(X_i)$ est un ouvert dense de $\overline{\phi(X_i)}$ pour $i = 1, \ldots, k$, alors $U := U_1 \cup \cdots \cup U_k \subset \phi(X)$ est un ouvert dense de $\overline{\phi(X)}$. Il suffit donc de démontrer le théorème dans le cas d'un ensemble irréductible.
Supposons donc d'emblée X irréductible. Quitte à remplacer Y par l'ensemble algébrique $\overline{\phi(X)}$, on peut même supposer que le morphisme ϕ est dominant. Ainsi, notant $A := \mathrm{A}(X)$ et $B := \mathrm{A}(Y)$, on voit que A est intègre et $\phi^* : B \to A$ injectif. (Donc B est intègre, et Y est irréductible, ce que l'on peut aussi prouver par un argument topologique.) On ne perd rien à identifier B avec son image et dire que $B \subset A$. Comme ce sont deux K-algèbres de type fini, A est elle-même une B-algèbre de type fini : il existe $f_1, \ldots, f_m \in A$ tels que $A = B[f_1, \ldots, f_m]$.
On va appliquer (et illustrer) la "dualité de Gelfand" (page 47). Si le point $x \in X$ correspond au morphisme $\chi : A \to K$, le point $\phi(x) \in Y$ correspond alors au morphisme $\chi \circ \phi^* = \chi_{|B} : B \to K$. Ainsi, pour que le point $y \in Y$ correspondant au morphisme $\chi' : B \to K$ soit dans l'image $\phi(X)$, il faut, et il suffit, que χ' s'étende en un morphisme $\chi : A \to K$.
D'après le lemme ci-dessous appliqué avec $a := 1$, il existe $b \in B \setminus \{0\}$ tel que tout $\chi' : B \to K$ tel que $\chi'(b) \neq 0$ s'étend en un $\chi : A \to K$. Dans les termes ci-dessus, cela signifie que $\phi(X)$ contient l'ouvert non vide $\mathcal{D}_Y(b) = Y \setminus \mathcal{V}_Y(b)$. Ce dernier est dense puisque Y est irréductible. □

Lemme 4.3.15 *Soient $B \subset A$ deux K-algèbres intègres et $f_1, \ldots, f_m \in A$ tels que $A = B[f_1, \ldots, f_m]$. Alors, pour tout $a \in A \setminus \{0\}$, il existe $b \in B \setminus \{0\}$ tel que tout $\chi' : B \to K$ tel que $\chi'(b) \neq 0$ s'étend en un $\chi : A \to K$ tel que $\chi(a) \neq 0$.*

Preuve. - Par récurrence, on peut se ramener au cas $m = 1$. (C'est dans l'optique d'une telle récurrence que le lemme fait intervenir a, alors que dans son application on prend $a = 1$.) On écrit donc $A = B[T]/I$, où l'idéal I de $B[T]$ est premier. Par hypothèse d'injectivité de $B \to A$, on a $I \cap B = \{0\}$ et l'on est conduit à distinguer deux cas.
Premier cas : $I = \{0\}$. Dans ce cas, X s'identifie à $Y \times K$ et le morphisme ϕ à la première projection, qui est ouverte (proposition 4.2.17) ; l'image de $\mathcal{D}_X(a)$ est donc un ouvert non vide, donc contient un ouvert affine non trivial $\mathcal{D}_Y(b)$.
Deuxième cas : $I =< P >$, où $P \in B[T]$ est unitaire non constant : $P = T^d + b_1 T^{d-1} + \cdots + b_d$, $d \geq 1$. Notons $f := T \pmod P \in A$. L'élément $a \in A$ est la classe modulo P d'un $Q \in B[T]$. Les morphismes de A dans K s'identifient aux morphismes de B dans K qui envoient P en 0, donc aux paires (χ', t) où $\chi' : B \to K$ est un morphisme et où $t \in K$ est racine du polynôme $\chi'(P) := T^d + \chi'(b_1)T^{d-1} + \cdots + \chi'(b_d)$. Étendre un morphisme $\chi' : B \to K$ en un morphisme $\chi : A \to K$ revient à choisir $\chi(f) \in K$ qui soit racine de $\chi'(P) \in K[T]$. C'est toujours possible puisque $\chi'(P)$ est non constant et K algébriquement clos. Comme nous étudions l'image dans Y de $\mathcal{D}_X(a)$, il faut maintenant voir si l'on peut choisir $t := \chi(f)$ tel que $\chi'(Q)(t) \neq 0$, *i.e.* non racine de $\chi'(Q)$. Mais le cas contraire signifie que toute racine de $\chi'(P)$ est racine de $\chi'(Q)$, autrement dit, puisque $\chi'(P)$ est de degré d, que $\chi'(P)$ divise $\big(\chi'(Q)\big)^d = \chi'(Q^d)$, autrement dit, que toutes les images dans B des coefficients de Q^d sont dans $\mathrm{Ker}\chi'$. Les χ' qui ne peuvent pas se relever dans $\mathcal{D}_X(a)$ forment donc le fermé d'équations ces images, donc un fermé, et l'image de $\mathcal{D}_X(a)$ est un ouvert. (Il est évident que ces touvert est non vide.)
Troisième cas : $I \neq \{0\}$. Notons L le corps des fractions de B. De l'égalité $I \cap B = \{0\}$ on déduit que $IL[T]$ est un idéal propre et non nul de $L[T]$, donc de la forme $< P >$, où l'on peut prendre $P \in B[T]$; et, par hypothèse, P n'est pas constant. (En fait, on peut prendre pour P n'importe quel polynôme non nul de degré minimal de $I \cap B[T]$.) Soit c le coefficient dominant de P. On va poser $X' := \mathcal{D}_X(c)$ et $Y' := \mathcal{D}_Y(c)$. L'application $X \to Y$ envoie X' dans Y' et il suffit de voir que l'image de $\mathcal{D}_{X'}(a) = \mathcal{D}_X(a) \cap X' = \mathcal{D}_X(ac)$ dans Y' contient un ouvert non vide $\mathcal{D}_{Y'}(b) = \mathcal{D}_Y(b) \cap Y'$. Mais l'algèbre affine de X', resp. de Y' est $A' := A_c$, resp. $B' := B_c$, et l'on a $A' = B'[T]/ < I' >$, où $I' := IB'[T]$ est principal, engendré par le polynôme unitaire $P' := c^{-1}P$. On est donc ramené au deuxième cas. □

Exercice 4.3.16 Montrer topologiquement que si X est irréductible et si $\phi : X \to Y$ est dominant, alors Y est irréductible.

4.3.3 Produits d'ensembles algébriques

Soient E et F deux espaces affines et $X \subset E$, $Y \subset F$ des fermés d'idéaux respectifs I, J. En appliquant les propriétés énoncées page 27 (section 2.2.3), on voit que $\mathrm{A}(E \times F) \simeq \mathrm{A}(E) \otimes_K \mathrm{A}(F)$. Pratiquement, $\sum f_i \otimes g_i \in \mathrm{A}(E) \otimes_K \mathrm{A}(F)$ s'interprète comme fonction sur $E \times F$ par la formule :

$$\forall (x,y) \in E \times F \ , \ \Big(\sum f_i \otimes g_i\Big)(x,y) = \sum f_i(x) g_i(y).$$

Exercice 4.3.17 Soient respectivement π_1, π_2 les projections de $E \times F$ sur E, F. Vérifier que leurs comorphismes sont respectivement $f \mapsto f \otimes 1$ et $g \mapsto 1 \otimes g$.

Théorème 4.3.18 *Soient $X \subset E$ et $Y \subset V$ des fermés, d'idéaux respectifs $I := \mathfrak{I}_E(X)$ et $J := \mathfrak{I}_F(Y)$. Notons $A := A(E)$ et $B := A(F)$.*

(i) Le produit $X \times Y$ est un fermé de $E \times F$ et l'idéal de ce fermé est $I \otimes B + A \otimes J \subset A \otimes B$. (Ce dernier est donc radiciel, ce qui ne se voit pas à l'oeil nu !)
(ii) L'algèbre affine de l'ensemble algébrique $X \times Y$ est :

$$A(X \times Y) = A(X) \otimes_K A(Y).$$

Preuve. - D'après les propriétés de la page 27, la seconde assertion découle de la première, sur laquelle nous allons donc nous concentrer.
Il est évident que $K := I \otimes B + A \otimes J$ s'annule sur $X \times Y$, d'où l'inclusion $K \subset \mathfrak{I}_{E \times F}(X \times Y)$. Pour démontrer l'inclusion réciproque, on identifie E, F à K^n, K^p et donc A, B à $K[X_1, \ldots, X_n]$, $K[Y_1, \ldots, Y_p]$. On introduit une base $(Q_i)_{i \in L}$ du K-espace vectoriel J, un supplémentaire J' de J dans le K-espace vectoriel $K[Y_1, \ldots, Y_p]$, et une base $(Q_i)_{i \in L'}$ de J'. Tout élément de $A \otimes B$ s'écrit comme une somme $f + f'$, où $f = \sum_{i \in L} P_i \otimes Q_i \in A \otimes J$ et $f' = \sum_{i \in L'} P_i \otimes Q_i \in A \otimes J'$. Si notre élément est nul sur $X \times Y$, alors f' aussi, et, pour tout $x \in X$, la fonction $\sum_{i \in L'} P_i(x) Q_i$ est nulle sur Y, donc élément de J : d'après le choix des bases, cela entraine que les $P_i(x)$ sont nuls ; comme c'est vrai pour tout $x \in X$, les P_i sont dans I et $f' \in I \otimes B$. □

Corollaire 4.3.19 *L'interprétation de $\sum f_i \otimes g_i \in A(X) \otimes_K A(Y)$ comme fonction sur $X \times Y$ est donnée par la formule :*

$$\forall (x,y) \in X \times Y \ , \ \left(\sum f_i \otimes g_i\right)(x,y) = \sum f_i(x) g_i(y).$$

La topologie sur un produit d'ensembles algébriques

Tout d'abord, ce n'est pas la topologie produit. Elle est aussi fine d'après le théorème, mais en général, elle est strictement plus fine. Par exemple, la diagonale de $X \times X$ est un fermé pour la topologie de Zariski, mais ne l'est pour la topologie produit que si X est séparé, ce qui est très rare.

Exercice 4.3.20 (i) Montrer que la diagonale de $X \times X$ en est un fermé de Zariski.
(ii) Quels ensembles algébriques sont séparés ?

Proposition 4.3.21 *(i) Le produit de deux irréductibles est irréductible.*
(ii) Soient $X = \bigcup_{i=1}^{k} X_i$ et $Y = \bigcup_{j=1}^{\ell} Y_j$ des décompositions en composantes irréductibles. Alors $X \times Y = \bigcup_{i,j=1}^{k,\ell} X_i \times Y_j$ est une décomposition en composantes irréductibles.

Preuve. - (i) Si $X \times Y = Z_1 \times Z_2$, on note $Y_i(x) := \{y \in Y \mid (x,y) \in Z_i\}$: donc $Y = Y_1(x) \cup Y_2(x)$, ce sont des fermés, et $Y = Y_1(x)$ ou $Y = Y_2(x)$. Notons $X_i := \{x \in X \mid Y = Y_i(x)\}$. Alors $X = X_1 \cup X_2$, ce sont des fermés, d'où $X = X_1$ ou $X = X_2$, d'où $Z = Z_1$ ou $Z = Z_2$.
(ii) découle de (i) puisque les $X_i \times Y_j$ sont deux à deux non comparables pour l'inclusion. □

On démontre enfin la formule suivante, que nous admettrons (voir [6, 36]) :

$$\dim(X \times Y) = (\dim X) + (\dim Y).$$

Deuxième partie

La suite

Chapitre 5

Groupes algébriques affines (théorie élémentaire)

Dans sa version idéale, la géométrie algébrique nécessite le langage des “schémas”, voir par exemple [25, 35, 16, 14]. Cependant, suivant l’exemple fondateur de Borel [6], ainsi que celui de ses successeurs [18, 36], on prendra ici le point de vue élémentaire de la géométrie algébrique affine sur un corps. Une introduction de niveau L3-M1 figure dans le chapitre correspondant du livre [27] ; voir aussi (et surtout) [15].

Bien que très efficace, ce point de vue s’avèrera trop étriqué lorsque nous introduirons des groupes “proalgébriques” au chapitre 7 : les propriétés de “fidèle platitude” et les passages à la limite inductive dont nous aurons alors besoin ne s’expriment commodément que dans le langage des “schémas en groupes”, voir par exemple [11, 37] (dont on a d’ailleurs plagié certaines démonstrations au paragraphe 7.2).

Pour pallier ces difficultés, on introduira quelques outils plus élémentaires que les schémas mais tout de même bien pratiques : point de vue fonctoriel au 5.1 ; algèbres de Hopf au 5.2 ; et l’on complètera cet attirail par un recours à la “dualité de Gelfand” (page 47).

Pour justifier cette attitude, citons *in extenso* Jean Giraud, dans l’introduction à son cours de “Géométrie algébrique élémentaire”, reproduit dans [15] :
Bien entendu, le manque d’un langage convenable est parfois gênant, mais beaucoup moins qu’on ne pourrait le croire et le pari est que le lecteur vraiment gêné est mûr pour assimiler le langage de la géométrie algébrique, celui des schémas de Grothendieck bien sûr, et les éléments d’algèbre commutative nécessaires pour cela.

5.1 Groupes dans une catégorie

5.1.1 Groupes et diagrammes

Un groupe peut être défini comme un ensemble G muni d’une loi de composition interne $\mu : G \times G \to G$, soumise à certains axiomes. Le premier axiome est l’associativité, que l’on peut

exprimer en disant que le diagramme suivant est commutatif :

(5.1.0.1)
$$\begin{array}{ccc} G\times G\times G & \xrightarrow{\mu\times \mathrm{Id}} & G\times G \\ {\scriptstyle \mathrm{Id}\times\mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ G\times G & \xrightarrow[\mu]{} & G \end{array}$$

À noter que les sources respectives de $\mu\times \mathrm{Id}$ et de $\mathrm{Id}\times\mu$ devraient être $(G\times G)\times G$ et $G\times(G\times G)$: on présuppose donc implicitement une identification de ces deux ensembles à $G\times G\times G$.

Pour les axiomes concernant le neutre et l'inverse, qui comportent des quantificateurs existentiels, il est commode d'introduire des objets nouveaux dans la structure. Commençons par le cas de l'élément neutre. C'est une constante de G, que l'on décide de représenter par une application $\varepsilon : \{\bullet\} \to G$, où $\{\bullet\}$ désigne un singleton indéterminé. Le neutre $1_G \in G$ est simplement l'image $\varepsilon(\bullet) \in G$. Le lecteur vérifiera que la neutralité de 1_G s'exprime par la commutativité des diagrammes suivants, dans lesquels on a noté pr_1, pr_2 les projections d'un produit sur ses facteurs :

(5.1.0.2)
$$\begin{array}{ccccc} G\times\{\bullet\} & \xrightarrow{\mathrm{Id}\times\varepsilon} & G\times G & \xleftarrow{\varepsilon\times\mathrm{Id}} & \{\bullet\}\times G \\ & {\scriptstyle pr_1}\searrow & \downarrow{\scriptstyle \mu} & \swarrow{\scriptstyle pr_2} & \\ & & G & & \end{array}$$

On représente enfin l'inverse par une application $\iota : G \to G$ telle que les diagrammes suivants commutent :

(5.1.0.3)
$$\begin{array}{ccccc} G & \xrightarrow{(\mathrm{Id},\iota)} & G\times G & \xleftarrow{(\iota,\mathrm{Id})} & G \\ {\scriptstyle \bullet}\downarrow & & \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle \bullet} \\ \{\bullet\} & \xrightarrow[\varepsilon]{} & G & \xleftarrow[\varepsilon]{} & \{\bullet\} \end{array}$$

On a noté $\bullet$ l'application constante $G \to \{\bullet\}$.

Remarque 5.1.1 Il est souvent commode de remplacer un axiome de la forme $\forall x\ ,\ \exists y\ :\ R(x,y)$ par l'introduction d'une fonction $y = f(x)$ telle que l'on ait $\forall x\ ,\ R\big(x, f(x)\big)$. Le quantificateur existentiel a disparu de l'axiome. Ce procédé s'appelle (en logique) *skolemisation* en l'honneur du logicien norvégien Thoralf Skolem. Les mathématiciens l'emploient tout particulièrement en théorie des catégories. Pour un axiome de la forme $\exists y\ :\ R(y)$, on introduira une constante, ou, ce qui revient au même, une fonction $y = f(\bullet)$ dépendant d'un argument constant $x \in \{\bullet\}$ (la source est un singleton arbitraire) ; l'axiome prend alors la forme $R\big(f(\bullet)\big)$.

Si l'on veut exprimer que le groupe est commutatif, on note $v : G\times G \to G$ la "volte" $(x,y) \mapsto (y,x)$ et l'on écrit le diagramme commutatif :

$$\begin{array}{ccc} G\times G & \xrightarrow{\ v\ } & G\times G \\ & {\scriptstyle \mu}\searrow \quad \swarrow{\scriptstyle \mu} & \\ & G & \end{array}$$

Exercice 5.1.2 Vérifier que les diagrammes ci-dessus traduisent bien les axiomes qui définissent un groupe, resp. un groupe commutatif.

5.1.2 Objets en groupe

Pas question ici de faire la théorie générale : nous renvoyons pour cela à [22, III.6]. Nous supposerons la catégorie $\mathcal{C}$ munie de "produits" ; autrement dit, étant donnés deux objets A_1, A_2 de $\mathcal{C}$, il y a un objet A muni de deux morphismes "projections" $p_i : A \to A_i$; de sorte que l'on a, pour tout objet B, une application :

$$f \mapsto (p_1 \circ f, p_2 \circ f),$$
$$\mathrm{Hom}_{\mathcal{C}}(B,A) \to \mathrm{Hom}_{\mathcal{C}}(B,A_1) \times \mathrm{Hom}_{\mathcal{C}}(B,A_2).$$

La propriété caractéristique du produit est que l'application ci-dessus est bijective. Le lecteur prendra la peine de formuler cette définition sous forme de propriété universelle et aussi de vérifier que tous les objets que nous avons nommés "produits" jusqu'ici en sont bien des cas particuliers. Dans ce qui suit, nous supposons que deux objets quelconques admettent un produit[1].

Remarque 5.1.3 Il est important de noter que les projections font partie intégrante de la notion de produit : c'est le triplet (A, p_1, p_2) qui est un produit.

Exercice 5.1.4 (i) Démontrer l'unicité du produit à isomorphisme près : si (A, p_1, p_2) et (A', p_1', p_2') sont tous deux des produits de A_1, A_2, il existe un unique isomorphisme $f : A \to A'$ tel que $p_i = p_i' \circ f$. On notera dorénavant $A_1 \times A_2$ muni des projections $pr_i : A_1 \times A_2 \to A_i$ "le" produit de A_1, A_2.
(ii) Démontrer l'existence, pour des morphismes (f_1, f_2) de B vers A_1, A_2 respectivement, d'un unique morphisme f de B vers $A_1 \times A_2$ tel que $f_i = pr_i \circ f$. Nous noterons (f_1, f_2) ce morphisme.
(iii) Soient des morphismes $f_i : A_i \to A_i'$. Démontrer l'existence, d'un unique morphisme f de $A_1 \times A_2$ dans $A_1' \times A_2'$ tel que $f_i \circ pr_i = pr_i' \circ f$. Nous noterons $f_1 \times f_2$ ce morphisme.
(iv) Démontrer l'existence d'un isomorphisme "canonique" (ce que l'on précisera) :

$$(A_1 \times A_2) \times A_3 \to A_1 \times (A_2 \times A_3).$$

On pourra donc utiliser la notation $A_1 \times A_2 \times A_3$.

On peut directement traduire la notion de loi de composition interne associative : on se donne un objet A de $\mathcal{C}$ et un morphisme μ de $A \times A$ dans A tel que le diagramme suivant soit commutatif :

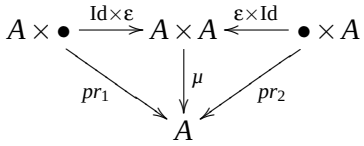
$$\begin{array}{ccc} A \times A \times A & \xrightarrow{\mu \times \mathrm{Id}} & A \times A \\ {\scriptstyle \mathrm{Id} \times \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ A \times A & \xrightarrow[\mu]{} & A \end{array}$$

Pour parler de neutre, il faut un substitut au singleton $\{\bullet\}$. La propriété la plus caractéristique de l'ensemble $\{\bullet\}$ est que, quelque soit l'ensemble E, il y a une et une seule application de E dans $\{\bullet\}$. Plus généralement, dans une catégorie $\mathcal{C}$, on appellera *(objet) terminal* un objet A tel que, pour tout objet B, l'ensemble $\mathrm{Hom}_{\mathcal{C}}(B,A)$ ait un et un seul élément. De même que, dans les diagrammes précédents, le choix du singleton arbitraire $\{\bullet\}$ n'avait pas d'importance, de même le choix d'un terminal n'a pas d'importance en vertu du principe suivant.

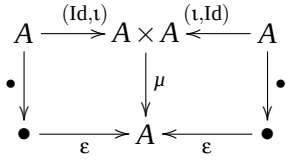
[1] Cela ne va pas de soi ; par exemple, il n'y a pas de produit dans la catégorie des corps commutatifs.

Exercice 5.1.5 Soient A, A' deux terminaux. Montrer qu'il existe un unique isomorphisme de A dans A'.

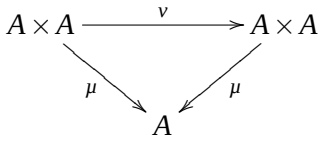
On suppose donc que $\bullet$ est un terminal de $\mathcal{C}$ et l'on appelle neutre de A un morphisme $\varepsilon : \bullet \to A$ tel que le diagramme suivant soit commutatif :



De même, on appelle inverse de A (ou, plus proprement, inversion sur A) un morphisme $\iota : A \to A$ tel que le diagramme suivant soit commutatif :



On a abusivement noté $\bullet$ l'unique morphisme de A dans $\bullet$. Enfin, on dit que la loi μ sur l'objet A est commutative si l'on a le diagramme commutatif suivant :



La volte $v : A \times A \to A \times A$ est simplement le morphisme (pr_2, pr_1).

On voit maintenant clairement ce qu'est un "groupe (éventuellement commutatif) dans $\mathcal{C}$" ; on parle également d'objet en groupe. Par exemple, un groupe dans la catégorie des espaces topologiques est tout simplement un groupe topologique. La notion de groupe de Lie est également un exemple de cette construction.

Exercice 5.1.6 Qu'est-ce qu'un groupe dans la catégorie des groupes ? (Attention : il y a vraiment une réponse sensée et non tautologique !)

Exercice 5.1.7 Soit $\mu : A \times A \to A$ une loi de composition sur l'objet A de $\mathcal{C}$. Elle définit donc, pour tout objet B, une application :

$$\begin{aligned} \mu_B : \mathrm{Hom}_{\mathcal{C}}(B,A) \times \mathrm{Hom}_{\mathcal{C}}(B,A) &\to \mathrm{Hom}_{\mathcal{C}}(B,A), \\ (f,g) &\mapsto \mu \circ (f,g). \end{aligned}$$

Démontrer que, pour que μ fasse de A un objet en groupe, il faut, et il suffit, que chaque μ_B fasse de $\mathrm{Hom}_{\mathcal{C}}(B,A)$ un groupe.

5.1.3 Groupes algébriques affines

Un groupe algébrique affine est simplement un ensemble algébrique affine qui est un groupe, avec compatibilité des deux structures : la multiplication et l'inversion sont des morphismes d'ensembles algébriques affines (pour l'application neutre, qui est constante, c'est automatique). Cette définition est équivalente à la suivante :

Définition 5.1.8 Un *groupe algébrique affine* sur le corps commutatif K est un groupe dans la catégorie $\mathcal{A}ff_K$ des ensembles algébriques affines sur K ; autrement dit, c'est un ensemble algébrique affine G sur K muni d'un morphisme $\mu : G \times G \to G$, d'un morphisme $\iota : G \to G$ et d'un élément $1_G \in G$, qui définit un morphisme constant $\varepsilon : \{\bullet\} \to G$, de telle sorte que les diagrammes (5.1.0.1), (5.1.0.2) et (5.1.0.3) soient commutatifs.

Cette définition est justifiée parce que nous avons défini au paragraphe 4.3.3 le produit dans $\mathcal{A}ff_K$, lequel est bien un produit au sens du paragraphe précédent ; et parce qu'il est évident que tout singleton $\{\bullet\}$ admet une unique structure d'espace affine (trivial) sur K, donc définit un objet de $\mathcal{A}ff_K$, lequel est terminal au sens du paragraphe précédent. On notera en général xy et x^{-1} plutôt que $\mu(x,y)$ et $\iota(x)$.

Si H est un sous-groupe du groupe algébrique affine G qui est fermé pour la topologie de Zariski, c'est un ensemble algébrique et ses applications de multiplication et d'inversion sont des morphismes, comme restrictions de morphismes. C'est donc un groupe algébrique affine.

Définition 5.1.9 Un *sous-groupe algébrique (affine)* du groupe algébrique affine G est un sous-groupe fermé H muni des structures induites (de groupe et d'ensemble algébrique).

Remarque 5.1.10 On a vu en 4.3.2 que tout morphisme d'ensembles algébriques est continu (pour les topologies de Zariski). On pourrait en déduire que tout groupe algébrique est un groupe topologique, *i.e.* dans lequel la multiplication et l'inversion sont des applications continues. Il faut toutefois prendre garde que, dans cette définition d'un groupe topologique, lorsque l'on impose la continuité de la multiplication $\mu : G \times G \to G$, la source $G \times G$ est munie de la topologie produit ; or la topologie de Zariski sur l'ensemble algébrique $G \times G$ n'est pas le produit des topologies de Zariski. En fait, il y a une manière simple de se rendre compte qu'un groupe algébrique n'est pas un groupe topologique : ses singletons sont fermés, et il n'est pourtant pas séparé (sauf exception).

Cependant, le très utile résultat suivant est valable :

Proposition 5.1.11 *Soit G un groupe algébrique affine.*
(i) Soit $a \in G$. Alors la translation à gauche $x \mapsto ax$ et la translation à droite $x \mapsto xa$ sont des homéomorphismes de G dans lui-même.
(ii) Soit H un sous-groupe arbitraire de G. Alors l'adhérence de Zariski $\overline{H}$ est un sous-groupe de G. En particulier, c'est un sous-groupe algébrique.

Preuve. - (i) L'application $x \mapsto ax$ est un morphisme donc continue, et son inverse est l'application $x \mapsto a^{-1}x$; même argument pour l'application $x \mapsto xa$.
(ii) L'application $x \mapsto ax$ est continue et, si $a \in H$, elle envoie H dans lui-même, donc $\overline{H}$ dans lui-même : on a donc $H\overline{H} \subset \overline{H}$. Ainsi, l'application continue $x \mapsto xa$ avec $a \in \overline{H}$ envoie H dans $\overline{H}$

donc $\overline{H}$ dans lui-même ; ce dernier est donc stable pour la multiplication. La stabilité pour l'inversion se prouve de façon similaire. □

Exercice 5.1.12 Démontrer la stabilité de $\overline{H}$ pour l'inversion.

5.2 Algèbres de Hopf commutatives réduites

Selon le théorème 4.3.7, la catégorie $\mathcal{A}ff_K$ des ensembles algébriques sur K est *antiéquivalente* (paragraphe 2.1.3) à celle des algèbres affines réduites. D'après le 4.3.3, dans cette antiéquivalence, se correspondent le produit des ensembles algébriques dans $\mathcal{A}ff_K$ et le produit tensoriel des algèbres affines (réduites).

Soient donc G un ensemble algébrique et A son algèbre affine. Nous pouvons traduire les axiomes des groupes algébriques en termes de propriétés de A. Il suffit de remplacer les morphismes dans $\mathcal{A}ff_K$ par leurs comorphismes et de renverser le sens des flèches dans les diagrammes commutatifs (le foncteur $G \rightsquigarrow A$ étant contravariant). L'existence d'une loi de composition μ sur G, d'un neutre $\varepsilon : \{\bullet\} \to G$, d'une inversion $\iota : G \to G$, se traduisent respectivement par l'existence de morphismes d'algèbres :

$$\begin{aligned} \Delta := \mu^* &: A \to A \otimes_K A, \\ e := \varepsilon^* &: A \to K, \\ i := \iota^* &: A \to A. \end{aligned}$$

Pour des raisons évidentes, nous appellerons *comultiplication* le morphisme Δ. En revanche, le morphisme de "coünité" e est plutôt appelé *augmentation* et le morphisme de "coïnversion" i *antipode*. Il sera utile de décrire leur effet concret. Tout d'abord, si l'on note $x.y := \mu(x,y)$ la multiplication dans G, on a la relation suivante avec Δ :

$$\Delta(f) = \sum f_i \otimes g_i \iff \forall x,y \in G\ ,\ f(xy) = \sum f_i(x) g_i(y).$$

Si l'on note 1_G le neutre de G, image de l'application constante ε, le comorphisme $e = \varepsilon^* : A \to K$ n'est autre que le morphisme de K-algèbres $f \mapsto f(1_G)$:

$$\forall f \in A\ ,\ e(f) = f(1_G).$$

Enfin, si l'on note x^{-1} l'inverse dans le groupe G :

$$i(f) = g \iff \forall x \in G\ ,\ g(x) = f(x^{-1}).$$

Les diagrammes commutatifs qui font de G un groupe se traduisent comme suit. Il y a d'abord la *coassociativité* :

$$\begin{array}{ccc} A & \xrightarrow{\Delta \otimes_K \mathrm{Id}} & A \otimes_K A \\ {\scriptstyle \mathrm{Id}\otimes_K \Delta}\downarrow & & \downarrow{\scriptstyle \Delta} \\ A \otimes_K A & \xrightarrow[\Delta]{} & A \otimes_K A \otimes_K A \end{array}$$

Il n'est pas très facile (principalement à cause des notations) de traduire concrètement la commutativité de ce diagramme. Pour ce faire, on utilise parfois la *notation de Sweedler* :

$$\Delta(f) = \sum_{(f)} f_1 \otimes f_2.$$

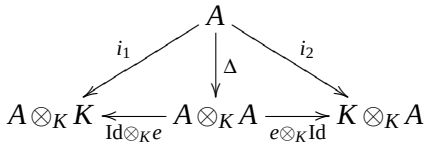
Avec cette convention, on a alors :

$$(\Delta \otimes_K \mathrm{Id}) \circ \Delta(f) = \sum_{(f)} f_{1,1} \otimes f_{1,2} \otimes f_2 = \sum_{(f)} f_1 \otimes f_{2,1} \otimes f_{2,2} = (\mathrm{Id} \otimes_K \Delta) \circ \Delta(f).$$

On peut alors alléger la notation et désigner cet élément de $A \otimes_K A \otimes_K A$ comme suit :

$$(\Delta \otimes_K \mathrm{Id}) \circ \Delta(f) = (\mathrm{Id} \otimes_K \Delta) \circ \Delta(f) =: \sum_{(f)} f_1 \otimes f_2 \otimes f_3.$$

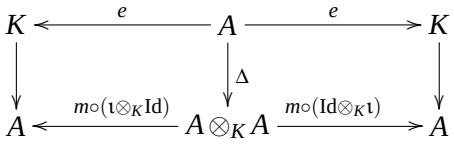
La coneutralité de e se traduit par le diagramme commutatif suivant :



Ici, i_1, i_2 sont les comorphismes respectifs de pr_1, pr_2, définis par $i_1(f) = f \otimes 1$, $i_2(f) = 1 \otimes f$. Grâce aux identifications canoniques $A \otimes_K K \simeq K \otimes_K A \simeq A$ et $f \otimes 1 = 1 \otimes f = f$, on peut traduire la commutativité du diagramme concrètement comme suit :

$$\Delta(f) = \sum f_i \otimes g_i \Longrightarrow \forall x \in G\ ,\ f(x) = \sum f_i(x) g_i(1_G) = \sum f_i(1_G) g_i(x).$$

Enfin, la propriété caractéristique de l'antipode (traduisant celle de l'inverse dans G) s'exprime par la commutativité du diagramme :



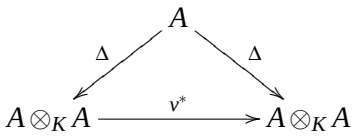
On a noté $m : A \otimes_K A \to A$ la multiplication dans l'algèbre A. Les flèches verticales $K \to A$ sont les inclusions canoniques. La commutativité du diagramme ci-dessus admet la traduction concrète :

$$\Delta(f) = \sum f_i \otimes g_i \Longrightarrow \forall x \in G\ ,\ f(1_G) = \sum f_i(x) \otimes g_i(x^{-1}) = \sum f_i(x^{-1}) \otimes g_i(x).$$

Une K-algèbre A, non nécessairement commutative ni réduite, munie d'une comultiplication Δ, d'une augmentation e et d'une antipode i vérifiant les diagrammes commutatifs ci-dessus est appelée une *algèbre de Hopf*[2]. Nous avons donc obtenu une correspondance entre groupes algébriques affines et algèbres de Hopf commutatives réduites. (Pour en faire une antiéquivalence de catégories, il faudra attendre d'avoir défini des morphismes, *cf.* 5.4.)

[2]les algèbres de Hopf non nécessairement commutatives interviennent en particulier en topologie algébrique (où elles sont apparues), en géométrie non commutative et dans la théorie des groupes quantiques.

Signalons enfin le diagramme d'algèbres affines dont la commutativité traduit le fait que le groupe algébrique G est commutatif :



On a encore utilisé une "volte" $v^* : x \otimes y \mapsto y \otimes x$. Une algèbre de Hopf vérifiant cette condition est dite *cocommutative*.

Exercice 5.2.1 (i) Traduire le fait que le K-espace vectoriel A est une K-algèbre par l'existence d'applications linéaires $m : A \otimes_K A \to A$ et $u : K \to A$. L'associativité et la neutralité de $u(1)$ s'expriment par des diagrammes commutatifs.
(ii) Traduire le fait que l'application K-linéaire $f : (A,m,u) \to (A',m',u')$ est un morphisme de K-algèbres par des diagrammes commutatifs où interviennent f, m, m', u, u'.
(iii) Appliquer ces diagrammes au cas de Δ, e, i.

5.3 Groupes algébriques linéaires

Proposition 5.3.1 *Le goupe $GL_n(K)$ est un groupe algébrique affine.*

Preuve. - C'est en tant qu'ouvert affine de $\mathrm{Mat}_n(K)$ (voir la fin du paragraphe 4.2.3, en particulier le deuxième des exemples 4.2.18 page 50) que $\mathrm{GL}_n(K)$ est un ensemble algébrique affine. Son algèbre affine est donc :

$$A := \mathrm{A}\big(\mathrm{GL}_n(K)\big) = K[(X_{i,j})_{1\le i,j\le n}]\left[\frac{1}{\det(X_{i,j})}\right] = K[(X_{i,j})_{1\le i,j\le n}][T]/ < 1 - T\det(X_{i,j}) > .$$

Autrement dit, $\mathrm{GL}_n(K)$ est vu comme le fermé de l'espace vectoriel $E := \mathrm{Mat}_n(K) \times K$ défini par l'idéal $I :=< 1 - T\det(X_{i,j}) >$ de $B := \mathrm{A}(E) = K[(X_{i,j})_{1\le i,j\le n}][T]$. On va d'abord décrire une loi de composition sur E qui induit celle de $\mathrm{GL}_n(K)$; cette loi est donnée par la formule :

$$(M',t')(M'',t'') := (M'M'', t't'').$$

(Il est bien clair qu'elle induit la loi μ de $\mathrm{GL}_n(K)$!) En tant qu'application de $E \times E$ dans E, c'est un morphisme d'ensembles algébriques ; pour décrire son comorphisme, on convient que $B \otimes_K B = K[(X'_{i,j}, X''_{i,j})_{1\le i,j\le n}][T', T'']$ et l'on a :

$$X_{i,j} \mapsto \sum_{k=1}^{n} X'_{i,k} X''_{k,j},$$
$$T \mapsto T'T''.$$

L'image de $1 - T\det(X_{i,j})$ par cette application est :

$$1 - T'T''\det(X'_{i,j})\det(X''_{i,j}) = \big(1 - T'\det(X'_{i,j})\big) + T'\det(X'_{i,j})\big(1 - T''\det(X''_{i,j})\big).$$

L'idéal I est donc envoyé dans $I \otimes_K B + B \otimes_K I$ et le comorphisme passe au quotient en :

$$\Delta : (B/I) \to (B/I) \otimes_K (B/I), \text{ c'est-à-dire } \Delta : A \to A \otimes_K A.$$

L'application constante ε de valeur $I_n \in \mathrm{Mat}_n(K)$ est évidemment un morphisme d'ensembles algébriques. Son comorphisme est défini par $X_{i,j} \mapsto \delta_{i,j}$, $T \mapsto 1$, qui envoie I dans $\{0\}$, donc passe au quotient en une augmentation $e : A = B/I \to K$. Il reste à voir que l'application d'inversion $\iota : M \to M^{-1}$ est un morphisme de l'ensemble algébrique $\mathrm{GL}_n(K)$ dans lui-même. C'est essentiellement dû à l'égalité :

$$M^{-1} = \frac{1}{\det M}\,{}^t\mathrm{com}(M)$$

(transposée de la comatrice), et au fait que la fonction $\dfrac{1}{\det M}$ est ici polynomiale : c'est le rôle de la coordonnée T. Plus précisément, on notera $P_{i,j}$ les coefficients de ${}^t\mathrm{com}(M)$ considérés comme polynômes en les coefficients de M, *i.e.* comme éléments de $K[(X_{i,j})_{1\leq i,j\leq n}]$. On a alors un morphisme de E dans E :

$$(M,t) \mapsto \left(t\,{}^t\mathrm{com}(M), \det M\right),$$

de comorphisme :

$$\begin{aligned} X_{i,j} &\mapsto TP_{i,j}, \\ T &\mapsto \det(X_{i,j}). \end{aligned}$$

L'image de $1 - T\det(X_{i,j})$ par cette application est $1 - T^n \det^n(X_{i,j})$ (exercice amusant) ; elle envoie donc I dans I et passe au quotient en une antipode $i : A \to A$, dont il est facile de vérifier que c'est bien le comorphisme de l'application d'inversion ι. □

Définition 5.3.2 On appelle *groupe algébrique linéaire* un sous-groupe fermé de $\mathrm{GL}_n(K)$.

Corollaire 5.3.3 *Tout groupe algébrique linéaire est un groupe algébrique affine.*

Preuve. - En effet, multiplication et inversion dans ce sous-groupe sont induits par ceux de $\mathrm{GL}_n(K)$, donc sont des morphismes d'ensembles algébriques (car induits sur un fermé algébrique par des itou). □

Nous verrons au 5.6 que réciproquement *tout groupe algébrique affine est un groupe algébrique linéaire*.

Exemples 5.3.4

1. Le groupe spécial linéaire $\mathrm{SL}_n(K)$, le groupe des matrices triangulaires supérieures inversibles, son sous-groupe formé des matrices unipotentes, le groupe des matrices diagonales inversibles sont des sous-groupes fermés de $\mathrm{GL}_n(K)$, donc des groupes algébriques linéaires.
2. Le groupe orthogonal d'une forme quadratique est un groupe algébrique linéaire ; mais le groupe unitaire sur $\mathbf{C}$ ne l'est pas, car ce n'est pas un ensemble algébrique : même pour $n = 1$ la condition $z\bar{z} = 1$ ne définit pas un fermé algébrique de $\mathbf{C}^*$.
3. Le *groupe multiplicatif* $G_m := \mathrm{GL}_1(K)$, autrement dit, K^* est un groupe algébrique linéaire.
4. Le *groupe additif* $G_a := (K,+)$ est évidemment un groupe algébrique affine, d'algèbre de Hopf $K[X]$. Comultiplication $X \mapsto X' + X''$; augmentation $X \mapsto 0$; antipode $X \mapsto -X$. C'est même un groupe algébrique linéaire, car il est isomorphe (comme groupe et comme ensemble algébrique) au groupe des matrices triangulaires supérieures unipotentes de $\mathrm{GL}_2(K)$,

l'isomorphisme étant défini par la formule : $a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. (La notion d'isomorphisme sera précisée à la section suivante.)

Exercice 5.3.5 Parmi les exemples ci-dessus, lesquels sont des fermés de $\mathrm{Mat}_n(K)$? Quelles sont leurs dimensions ?

5.4 Morphismes de groupes algébriques affines

Définition 5.4.1 Soient G, G' deux groupes algébriques affines sur K. Un *morphisme de groupes algébriques affines* de G dans G' est une application $\phi : G \to G'$ qui est à la fois un morphisme de groupes et un morphisme d'ensembles algébriques.

Il s'agit donc d'un morphisme dans $\mathcal{A}ff_K$ qui est compatible avec les lois de groupes μ, μ', autrement dit, tel que :

$$\forall x, y \in G \ , \ \phi\big(\mu(x,y)\big) = \mu'\big(\phi(x), \phi(y)\big).$$

Cette relation se traduit par la commutativité du diagramme suivant :

$$\begin{array}{ccc} G \times G & \xrightarrow{\phi \times \phi} & G' \times G' \\ {\scriptstyle \mu}\downarrow & & \downarrow{\scriptstyle \mu'} \\ G & \xrightarrow[\phi]{} & G' \end{array}$$

En passant aux algèbres affines A, A' de G, G', cela s'exprime par la compatibilité du comorphisme ϕ^* avec les comultiplications Δ, Δ', sous la forme du diagramme commutatif suivant :

$$\begin{array}{ccc} A' & \xrightarrow{\phi^*} & A \\ {\scriptstyle \Delta'}\downarrow & & \downarrow{\scriptstyle \Delta} \\ A' \otimes_K A' & \xrightarrow[\phi^* \otimes \phi^*]{} & A \otimes_K A \end{array}$$

Si l'on appelle *morphisme d'algèbres de Hopf* un morphisme d'algèbres $\psi : A \to A'$ tel que de plus $\Delta \circ \psi = (\psi \otimes \psi) \circ \Delta'$, on voit que l'on a obtenu une *antiéquivalence entre la catégorie des groupes algébriques affines et la catégorie des algèbres de Hopf commutatives réduites*.

Exercice 5.4.2 Vérifier que l'application contragrédiente $A \mapsto {}^tA^{-1}$ est un automorphisme de $\mathrm{GL}_n(K)$.

Remarque 5.4.3 Il ne va pas de soi qu'un morphisme bijectif entre groupes algébriques affines soit un isomorphisme (c'est-à-dire un morphisme dont l'inverse est un morphisme). C'est faux en caractéristique $p > 0$ comme le montre l'exemple de l'endomorphisme de Frobenius $x \mapsto x^p$ de $(K, +)$ (ici K est algébriquement clos de caractéristique p). Mais c'est vrai en caractéristique nulle, bien que loin d'être évident : cela découle en effet des propriétés du *quotient* d'un groupe algébrique G par un sous-groupe fermé invariant (*cf.* [6]). Nous admettrons ce fait dans les rares cas où nous en aurons besoin, en signalant les résultats qui en dépendent.

On a vu au 4.3.2 que la structure topologique de l'image d'un morphisme d'ensembles algébriques n'est en général pas simple. Dans le cas des groupes algébriques, la situation est bien meilleure.

Théorème 5.4.4 *L'image d'un morphisme de groupes algébriques affines est fermée.*

Preuve. - Soit $\phi : G \to G'$ ce morphisme. Selon le théorème 4.3.14, $\phi(G)$ contient un ensemble ouvert dense dans $\overline{\phi(G)}$. Comme $\phi(G)$ est un sous-groupe de G', la conclusion découle immédiatement du lemme suivant. □

Lemme 5.4.5 *Soient H un groupe algébrique affine et H' un sous-groupe quelconque.*
(i) L'adhérence de Zariski $\overline{H'}$ est un sous-groupe fermé de H.
(ii) Si H' contient un ouvert non vide de $\overline{H'}$, il est fermé : $H' = \overline{H'}$.

Preuve. - (i) a déjà été démontré (proposition 5.1.11).
(ii) Soit $U \subset H'$ un ouvert non vide de $\overline{H'}$. De la simple inclusion $U \subset H'$ et du fait que U est non vide, on déduit la relation :

$$H' = \bigcup_{h \in H} hU,$$

d'où il s'ensuit que H' est ouvert dans $\overline{H'}$. Il y a alors deux manières d'achever la démonstration.
Le groupe $\overline{H'}$ est réunion disjointe des classes à gauche selon son sous-groupe H', les hH' avec $h \in \overline{H'}$, qui sont des ouverts, donc des fermés (car chacun est le complémentaire de la réunion des autres). Ainsi, H' est fermé dans $\overline{H'}$, donc fermé.
Variante du raisonnement : une fois que l'on sait que H' est ouvert dans $\overline{H'}$, tous les hH' avec $h \in \overline{H'}$ le sont, et ils sont denses ; donc chaque hH' avec $h \in \overline{H'}$ rencontre H', ce qui entraine que $h \in H'$. □

Corollaire 5.4.6 *Tout morphisme $G \to G'$ de groupes algébriques affines se décompose en un morphisme surjectif $G \to H$ et une immersion fermée $H \to G'$ (de groupes algébriques affines).*

Rappelons (proposition 4.3.10) qu'une immersion fermée $H \to G'$ est un isomorphisme de H avec un fermé de G' (ici, un sous-groupe fermé).

Si maintenant nous admettons que tout morphisme bijectif est un isomorphisme (remarque 5.4.3), nous obtenons :

Corollaire 5.4.7 *En caractéristique nulle, tout morphisme injectif de groupes algébriques affines est une immersion fermée.*

Exercice 5.4.8 (i) Vérifier que l'application $a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ est un morphisme du groupe algébrique affine $(K, +)$ dans le groupe linéaire $\mathrm{GL}_2(K)$, et que c'est une immersion fermée.
(ii) Utiliser ce morphisme pour déterminer l'adhérence de Zariski du sous-groupe de $\mathrm{GL}_2(K)$ engendré par la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

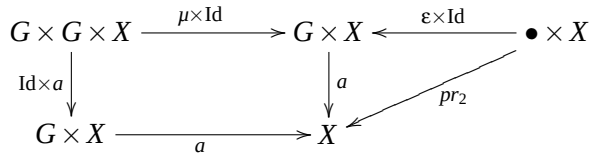
5.5 Action (ou opération) d'un groupe algébrique affine sur un ensemble algébrique affine

5.5.1 Vocabulaire

Définition 5.5.1 Soient G un groupe algébrique affine et X un ensemble algébrique affine. Une *action* ou *opération* de G sur X est un morphisme d'ensembles algébriques $a : G \times X \to X$ qui est de plus une action de groupe, autrement dit, tel que, notant $g.x := a(g,x)$, on ait :

$$\forall g,g' \in G\ ,\ \forall x \in X\ ,\ g'.(g.x) = (g'g).x \text{ et } \forall x \in X\ ,\ 1_G.x = x.$$

Ces deux règles se traduisent par les diagrammes commutatifs suivants :



Les *translations* de X (pour cette action) sont alors les $\tau_g : x \mapsto g.x$ (donc, des automorphismes de l'ensemble algébrique X).

Une *application orbite* est une application $a_x : g \mapsto g.x$ (donc un morphisme d'ensembles algébriques de G dans X), et l'*orbite de x* est son image $G(x) := \mathrm{Im}\, a_x = \{g.x \mid g \in G\} \subset X$.

Exercice 5.5.2 Pourquoi les translations sont-elles des automorphismes de X ?

Exemples 5.5.3
1. Le groupe G opère sur lui-même par automorphismes intérieurs : ici, $a(g,h) := ghg^{-1}$. Les orbites sont les classes de conjugaison.
2. Le groupe $\mathrm{GL}_n(K)$ opère sur $\mathrm{Mat}_n(K)$ par conjugaison.

Exercice 5.5.4 Dans ce dernier cas, quelles sont les orbites fermées ? (Voir par exemple [23, 24].)

5.5.2 Approche topologique

On suppose donnée une action a du groupe algébrique affine G sur l'ensemble algébrique affine X.

Proposition 5.5.5 *Soient $M,N \subset X$. Notons :*

$$Trans_G(M,N) := \{g \in G \mid g.M \subset N\} \subset G.$$

(i) On a $Trans_G(M,N) \subset Trans_G(\overline{M},\overline{N})$.
(ii) Si N est fermé dans X, il y a égalité et $Trans_G(M,N)$ est fermé dans G.

Preuve. - (i) Soit $g \in Trans_G(M,N)$. De l'inclusion $g.M \subset N$ et de la continuité des translations (ce sont des morphismes), on déduit :

$$g.\overline{M} = \overline{g.M} \subset \overline{N}.$$

(ii) On a évidemment $Trans_G(\overline{M},N) \subset Trans_G(M,N)$ sans condition, du simple fait que $M \subset \overline{M}$. Si N est fermé, c'est l'inclusion réciproque de la précédente. De plus, dans ce cas :

$$Trans_G(M,N) = \bigcap_{x\in M} a_x^{-1}(N)$$

est une intersection de fermés (chaque morphisme a_x étant continue) donc un fermé. □

Exemples 5.5.6 1. Tout stabilisateur $G_x := Trans_G(\{x\},\{x\})$ est un sous-groupe fermé de G.

2. Dans le cas de l'action de G sur lui-même par automorphismes intérieurs, on en déduit que chaque *centralisateur* $Z_G(h) := \{g \in G \mid gh = hg\}$ est fermé dans G.

La nature topologique des orbites est plus délicate à élucider.

Lemme 5.5.7 *Soient F un fermé non vide d'un ensemble algébrique X et U un ouvert dense de F. Alors* $\dim(F \setminus U) < \dim F$.

Preuve. - Soient $F_1,\ldots,F_k$ les composantes irréductibles de F. L'hypothèse de densité sur F entraine que chaque $U \cap F_i$ est non vide (sinon U serait inclus dans l'union des autres F_j, qui est un fermé strictement inclus dans F). Ainsi, $F_i \setminus U$ est un fermé strictement inclus dans F_i, donc de dimension $\dim(F_i \setminus U) < \dim F_i$ (par définition de la dimension de Krull). Comme $F \setminus U$ est la réunion des $F_i \setminus U$, sa dimension est $< \dim F$ (assertion (iii) de la proposition 4.2.8). □

Théorème 5.5.8 *(i) Toute orbite $G(x)$ est un ouvert dense de son adhérence.*
(ii) La frontière d'une orbite :

$$\partial G(x) := \overline{G(x)} \setminus G(x)$$

est une réunion d'orbites de dimensions $< \dim G(x)$.

Preuve. - (i) D'après le théorème 4.3.14, on sait que $G(x)$ contient un ouvert non vide U de son adhérence. Le raisonnement est alors semblable à celui utilisé lors de la démonstration du lemme 5.4.5 : par stabilité de l'orbite sous l'action de G, on a $G(x) = \bigcup_{g\in G} g.U$, et $G(x)$ est bien un ouvert de $\overline{G(x)}$; la densité va de soi.
(ii) L'adhérence $\overline{G(x)}$ est G-stable par continuité, donc la frontière $\partial G(x) = \overline{G(x)} \setminus G(x)$ aussi, et elle est donc réunion d'orbites. Ces dernières sont de dimensions $< \dim G(x)$ en vertu du lemme ci-dessus. □

Corollaire 5.5.9 *Il y a des orbites fermées.*

Preuve. - Il suffit de choisir $G(x)$ de dimension minimale, car alors $\partial G(x)$ est vide. □

Exercice 5.5.10 (i) Démontrer que toute suite décroissante de fermés d'un ensemble algébrique est stationnaire. (Invoquer la noetherianité de l'algèbre affine.)
(ii) En déduire une nouvelle démonstration de l'existence d'orbites fermées qui ne fasse pas intervenir la dimension.

5.5.3 Approche algébrique : la coaction

Du morphisme $a : G \times X \to X$ (action de G sur X) on déduit la *coaction*, c'est-à-dire le comorphisme $a^* : \mathrm{A}(X) \to \mathrm{A}(G) \otimes \mathrm{A}(X)$. On peut caractériser ce dernier comme suit. Soient $f \in \mathrm{A}(X)$ et $a^* f = \sum u_i \otimes f_i \in \mathrm{A}(G) \otimes \mathrm{A}(X)$. Alors :

$$\forall g \in G\ ,\ \forall x \in X\ ,\ f(g.x) = a^* f(g,x) = \sum u_i(g) \otimes f_i(x).$$

Exercice 5.5.11 Vérifier le "coaxiome" de l'axiome $g'.(g.x) = (g'g).x$:

$$(\mathrm{Id} \otimes a^*) \circ a^* = (\Delta \circ \mathrm{Id}) \circ a^*$$

Énoncer et vérifier le coaxiome de l'axiome $1_G.x = x$.

On va faire agir linéairement G sur l'espace vectoriel $\mathrm{A}(X)$. En vue d'obtenir une action *à gauche* (ce qui est l'usage le plus répandu), on pose :

$$\forall g \in G\ ,\ \forall f \in \mathrm{A}(X)\ ,\ g.f := f \circ \tau_g^{-1}\ \ \textit{i.e.}\ \ \forall x \in X\ ,\ g.f(x) := f(g^{-1}x).$$

(Il s'agit d'un analogue de la contragrédiente rencontrée dans l'exercice 5.4.2.) On vérifie facilement que $1_G.f = f$ et $g'.(g.f) = (g'g).f$. Pour tout $g \in G$, l'application $f \mapsto g.f$ est un automorphisme linéaire de $\mathrm{A}(X)$. On a bien une représentation linéaire de G, mais dimension infinie. Nous allons pallier cet inconvénient.

Proposition 5.5.12 *La représentation linéaire de G dans $A(X)$ ainsi obtenue est* localement finie, *autrement dit, tout sous-espace de dimension finie de $A(X)$ est inclus dans un sous-espace G-stable et de dimension finie.*

Preuve. - De la relation $\phi(E+F) \subset \phi(E) + \phi(F)$, valable pour deux sous-espaces et un endomorphisme arbitraires, on déduit que la somme de deux sous-espaces G-stables de dimension finie de $\mathrm{A}(X)$ est elle-même un sous-espace G-stable de dimension finie. Il suffit donc de voir que tout élément de $\mathrm{A}(X)$ est inclus dans un sous-espace G-stable de dimension finie.
Soit donc $f \in \mathrm{A}(X)$ et notons $a^* f = \sum u_i \otimes f_i$, qui est bien entendu une somme finie. De la formule vue plus haut, on tire :

$$g.f = \sum u_i(g^{-1})\, f_i. \tag{5.5.12.1}$$

Ainsi, le sous-espace de E de $\mathrm{A}(X)$ engendré par tous les $g.f$, où g parcourt G, est inclus dans le sous-espace engendré par les f_i : il est donc de dimension finie. Mais E est également G-stable par construction. □

On peut formuler la proposition en disant que la représentation de G dans $\mathrm{A}(X)$ est limite inductive de représentations de dimension finie.

Exemple 5.5.13 Fixons un vecteur $(a_1, \ldots, a_n) \in K^n$. Le groupe additif $G_a := (K, +)$, d'algèbre affine $\mathrm{A}(G) = K[T]$, agit sur l'espace $X := K^n$, d'algèbre affine $\mathrm{A}(X) = K[X_1, \ldots, X_n]$, par translations de vecteurs $t(a_1, \ldots, a_n)$ (où $t \in K$). La coaction est le morphisme $K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n][T]$ défini par :

$$P(X_1, \ldots, X_n) \mapsto P(X_1 + a_1 T, \ldots, X_n + a_1 T).$$

L'orbite de $P \in K[X_1, \ldots, X_n]$ sous cette action est l'ensemble des polynômes de la forme $P(X_1 + a_1 t, \ldots, X_n + a_1 t)$, où $t \in K$. D'après la formule de Taylor, cette orbite est incluse dans l'espace E engendré par les dérivées partielles de P, et celui-ci est stable et de dimension finie.

Exercice 5.5.14 (i) Dans l'exemple, l'orbite de P est-elle E ?
(ii) L'exemple n'est valable qu'en caractéristique nulle, puisqu'il fait appel à la formule de Taylor. Comment l'adapter en caractéristique positive ?

La (subtile) proposition suivante sera utile plus tard.

Proposition 5.5.15 *Pour que le sous-espace vectoriel F de $A(X)$ soit G-stable, il faut, et il suffit, que l'on ait l'inclusion*

$$a^*F \subset A(G) \otimes F.$$

Preuve. - Supposons d'abord que F est G-stable. Soit (f_i) une base de F que l'on complète en une base de $\mathrm{A}(X)$ en la juxtaposant avec une famille libre (f'_j) (laquelle est donc une base d'un supplémentaire F' de F dans $\mathrm{A}(X)$). Pour tout $f \in F$, on peut écrire :

$$a^* f = \sum u_i \otimes f_i + \sum u'_j \otimes f'_j,$$

avec les u_i, u'_j dans $\mathrm{A}(G)$. Même si les familles (f_i) et (f'_j) sont infinies, les familles (u_i) et (u'_j) n'ont qu'un nombre fini de termes non nuls. Pour tout $g \in G$, d'après la relation (5.5.12.1) :

$$g.f = \sum u_i(g^{-1})\, f_i + \sum u'_j(g^{-1})\, f'_j \in F,$$

ce qui entraine nécessairement que tous les $u'_j(g^{-1})$ sont nuls. Puisque $u'_j(g^{-1}) = 0$ pour tout $g \in G$, on a $u'_j = 0$. (Ce point est non tautologique, il utilise le fait que le corps de base est infini !) On a donc bien :

$$a^* f = \sum u_i \otimes f_i \in \mathrm{A}(X) \otimes F.$$

Supposons réciproquement l'inclusion vérifiée. Pour tout $f \in F$, on peut écrire $a^* f = \sum u_i \otimes f_i$, avec les u_i dans $\mathrm{A}(G)$ et les f_i dans F. De la formule (5.5.12.1) $g.f = \sum u_i(g^{-1}) f_i$ on déduit alors que $g.f \in F$ pour tout $g \in G$, d'où la stabilité. □

5.6 Tout groupe algébrique affine est linéaire

Soit G un groupe algébrique affine. On peut le faire agir sur son algèbre affine $\mathrm{A}(G)$ de deux manières. Tout d'abord, pour tous $g, h \in G$, notons $L_g(h) := g^{-1}h$ et $R_g(h) := hg$. On définit ainsi, pour tout $g \in G$, deux automorphismes L_g, R_g de l'ensemble (pas du groupe !) algébrique affine G. Leurs comorphismes $\lambda_g := L_g^*$ et $\rho_g := R_g^*$ sont donc des automorphismes de l'algèbre affine $\mathrm{A}(G)$. Des égalités évidentes $L_{gg'} = L_{g'} \circ L_g$ et $R_{gg'} = R_{g'} \circ R_g$ on déduit par contravariance les égalités :

$$\lambda_{g'g} = \lambda_{g'} \circ \lambda_g \text{ et } \rho_{g'g} = \rho_{g'} \circ \rho_g.$$

Nous avons donc deux représentations $\rho : g \mapsto \rho_g$ et $\lambda : g \mapsto \lambda_g$ de G dans $\mathrm{A}(G)$. Ce sont bien entendu ces formules agréables qui justifient l'étrange définition de L_g, R_g.

Lemme 5.6.1 *Ces deux représentations sont localement finies ; autrement dit, tout sous-espace vectoriel de $A(G)$ de dimension finie est inclus dans un sous-espace de dimension finie stable par ρ, resp. par λ.*

Preuve. - Cela découle de la proposition 5.5.12 appliquée à chacune des deux actions de G sur lui-même : par translations à gauche ou à droite. □

Théorème 5.6.2 *Il existe un sous-espace de dimension finie $V \subset A(G)$, stable par la représentation ρ, et tel que la représentation induite $G \to GL(V)$ soit une immersion fermée*, i.e. *un isomorphisme de G avec un sous-groupe fermé de $GL(V)$.*

Preuve. - L'algèbre affine $\mathrm{A}(G)$ est de type fini : soient $f_1, \ldots, f_m$ des générateurs. On prend pour V un sous-espace de dimension finie de $\mathrm{A}(G)$, contenant $f_1, \ldots, f_m$ et stable par ρ (c'est possible d'après le lemme). Soit $(\phi_1, \ldots, \phi_n)$ une base de V. En adaptant la proposition 5.5.15 à cette action par translations *à droite*, on voit que (μ désignant la multiplication de G) :

$$\mu^* V \subset V \otimes \mathrm{A}(G).$$

Il existe donc des $u_{i,j} \in \mathrm{A}(G)$ tels que :

$$\forall j \in \{1, \ldots, n\} \ , \ \mu^* \phi_j = \sum_{i=1}^{n} \phi_i \otimes u_{i,j} \Longrightarrow \forall g, h \in G \ , \ \phi_j(hg) = \sum_{i=1}^{n} \phi_i(h) u_{i,j}(g),$$

autrement dit :

$$\forall j \in \{1, \ldots, n\} \ , \ \forall g \in G \ , \ \rho_g(\phi_j) = \sum_{i=1}^{n} u_{i,j}(g) \phi_i.$$

La matrice de ρ_g dans la base des ϕ_i est donc $\big(u_{i,j}(g)\big) \in \mathrm{GL}_n(K)$ Cela entraine déjà que le morphisme de groupes $g \mapsto \rho_g$ de G dans $\mathrm{GL}(V)$ est un morphisme de groupes algébriques. Le choix de la base (ϕ_i) permet d'identifier V à K^n (isomorphisme d'ensembles algébriques) et $\mathrm{GL}(V)$ à $\mathrm{GL}_n(K)$ (isomorphisme de groupes algébriques). Dans ce modèle, le morphisme de groupes algébriques ci-dessus devient $g \mapsto \big(u_{i,j}(g)\big) \in \mathrm{GL}_n(K)$.

Le comorphisme de ce dernier est le morphisme d'algèbres de $\mathrm{A}\big(\mathrm{GL}_n(K)\big) = K[(X_{i,j})_{1 \le i,j \le n}] \left[\dfrac{1}{\det(X_{i,j})}\right]$ dans $\mathrm{A}(G)$ défini par $X_{i,j} \mapsto u_{i,j}$. Mais nous allons voir que ce morphisme d'algèbres est surjectif ; d'après la proposition 4.3.10, il en découlera que $G \to \mathrm{GL}(V)$ est bien une immersion fermée.

De l'égalité $\phi_j(hg) = \sum_{i=1}^{n} \phi_i(h) u_{i,j}(g)$, on tire $\phi_j = \sum_{i=1}^{n} \phi_i(1_G) u_{i,j}$. Les ϕ_j sont donc éléments de l'espace vectoriel engendré par les $u_{i,j}$, donc de l'image du morphisme d'algèbres $\mathrm{A}\big(\mathrm{GL}_n(K)\big) \to \mathrm{A}(G)$; comme les ϕ_j engendrent l'algèbre $\mathrm{A}(G)$, ce morphisme est bien surjectif. □

Corollaire 5.6.3 *Tout groupe algébrique affine est un groupe linéaire.*

Exemple 5.6.4 Le groupe additif $G_a = (K, +)$ a pour algèbre affine $K[X]$. L'action de $a \in K$ sur $\mathrm{A}(G) = K[X]$ est $P(X) \mapsto P(X + a)$. Le générateur X de l'algèbre a pour orbite la famille des $X + a$, qui engendre l'espace vectoriel $K + KX$. La matrice de la translation ρ_a dans cette base est $M_a := \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ et l'on voit que l'application $a \mapsto M_a$ est un isomorphisme de groupes algébriques de G_a sur le sous-groupe fermé de $\mathrm{GL}_2(K)$ formé des matrices triangulaires supérieures unipotentes.

Exercice 5.6.5 (i) Obtenir de même une description matricielle de $(K^n, +)$.
(ii) La même méthode permet d'identifier G_m à $\mathrm{GL}_1(K)$.

Chapitre 6

Représentations rationnelles d'un groupe algébrique

6.1 Généralités sur les représentations rationnelles

Définition 6.1.1 Une *représentation rationnelle* du groupe algébrique affine G est un morphisme de groupes algébriques affines $\rho : G \to \mathrm{GL}(V)$, où V est un K-espace vectoriel de dimension finie ; ou bien un morphisme de groupes algébriques affines $\rho : G \to \mathrm{GL}_n(K)$. On parle au choix de *représentation (de G) dans V* ou *dans GL*(V) ou encore *dans GL*$_n(K)$. La représentation ρ est dite *fidèle* si c'est une immersion fermée[1].

Soit ρ une représentation linéaire arbitraire de G dans V. Du choix d'une base de V, on déduit un isomorphisme f de $\mathrm{GL}(V)$ sur $\mathrm{GL}_n(K)$ et il est clair que l'on a équivalence entre les conditions suivantes :
(i) $\rho : G \to \mathrm{GL}(V)$ est rationnelle ;
(ii) $f \circ \rho : G \to \mathrm{GL}_n(K)$ est rationnelle ;
(iii) chacun des n^2 coefficients de $f \circ \rho$ est élément de $\mathrm{A}(G)$.
Ainsi, si $\rho : G \to \mathrm{GL}(V)$ et $\rho' : G \to \mathrm{GL}(V')$ sont rationnelles, la représentation $g \mapsto \rho(g) \oplus \rho'(g)$ de G dans $V \oplus V'$ est rationnelle : par choix d'une base adaptée de $V \oplus V'$, ses matrices sont diagonales de blocs rationnels.

On déduit de la définition que l'action du groupe G sur l'ensemble V, égale au composé :

$$G \times V \to \mathrm{GL}(V) \times V \to \mathrm{End}(V) \times V \to V$$

est un morphisme d'ensembles algébriques, donc une action de groupe algébrique au sens de la section 5.5. (Il faut invoquer le fait que l'inclusion d'un ouvert affine $\mathcal{D}_X(f)$ dans un ensemble algébrique X est un morphisme : exercice facile laissé au lecteur !) Supposons réciproquement donnée une représentation linéaire du groupe G dans l'espace vectoriel de dimension finie V, telle que l'application $G \times V \to V$ soit un morphisme d'ensembles algébriques, donc une action de groupe algébrique. Choisissons une base $(v_1, \ldots, v_n)$ de V, donc un isomorphisme $f \mapsto \big(f(v_1), \ldots, f(v_n)\big)$ de $\mathrm{End}(V)$ sur V^n (isomorphisme d'espaces vectoriels, donc d'ensembles algébriques).

[1] Si l'on admet que tout morphisme bijectif est un isomorphisme (remarque 5.4.3), on voit que la représentation est fidèle si, et seulement si, c'est un morphisme injectif, ce qui est la définition classique.

Le morphisme composé $G \to \mathrm{End}(V) \to V^n$ est donné par $g \mapsto (g.v_1, \ldots, g.v_n)$: c'est donc un morphisme d'ensembles algébriques (car chaque $g \mapsto g.v_i$ l'est, c'est une application orbite au sens de 5.5.1). On retrouve donc le fait que $G \to \mathrm{GL}(V)$ est un morphisme de groupes algébriques affines.

6.1.1 Représentations localement finies rationnelles

En vue d'étendre la définition d'une représentation rationnelle au cas d'un espace vectoriel de dimension infinie, quelques sorites :

Lemme 6.1.2 *(i) Soit $\rho : G \to GL(V)$ une représentation rationnelle. Soit $W \subset V$ un sous-espace stable sous l'action de G. Les représentations induites $G \to GL(W)$ et $G \to GL(V/W)$ sont alors rationnelles. (Au sujet de la réciproque,* cf. *l'exercice ci-dessous.)*
(ii) Soit $\rho : G \to GL(V)$ une représentation arbitraire du groupe algébrique affine G dans l'espace de dimension finie V. On suppose que $V = \sum V_i$, les V_i étant des sous-espaces stables sous l'action de G ; et que chaque représentation induite $G \to GL(V_i)$ est rationnelle ; alors ρ est rationnelle.

Preuve. - (i) Soient $i : W \to V$ l'inclusion et $p : V \to W$ une projection. Le morphisme $\phi \mapsto p \circ \phi \circ i$ est une projection de $\mathrm{End}(V)$ sur $\mathrm{End}(W)$ et la représentation induite $G \to \mathrm{End}(W)$ est la composition de $G \to \mathrm{End}(V)$ et de cette projection. Soient de même $\pi : V \to V/W$ la surjection canonique et $\sigma : V/W \to V$ une section linéaire quelconque de π. Le morphisme $\phi \mapsto \pi \circ \phi \circ \sigma$ est une surjection de $\mathrm{End}(V)$ sur $\mathrm{End}(V/W)$ et la représentation induite $G \to \mathrm{End}(V/W)$ est la composition de $G \to \mathrm{End}(V)$ et de cette surjection.
(ii) Puisque $\dim V < \infty$, on peut se ramener au cas d'une somme finie de sous-espaces ; et, moyennant une récurrence sur leur nombre, il suffit de considérer le cas de deux sous-espaces : $V = V' + V''$. On applique alors (i) à $V \cap V' \subset V \oplus V'$, dont le quotient est $V + V'$. (On a vu plus haut que la représentation de G dans $V \oplus V'$ était bien rationnelle.) □

Exercice 6.1.3 Décrire matriciellement la projection $\phi \mapsto p \circ \phi \circ i$ de $\mathrm{End}(V)$ sur $\mathrm{End}(W)$ utilisée dans la démonstration du (i) ci-dessus.

Exercice 6.1.4 Soit $\rho : G \to \mathrm{GL}(V)$ une représentation arbitraire du groupe algébrique affine G dans l'espace de dimension finie V. Soit W un sous-espace de V tel que les représentations induites $G \to \mathrm{GL}(W)$ et $G \to \mathrm{GL}(V/W)$ sont rationnelles. La représentation ρ est-elle nécessairement rationnelle ? (La réponse est non.)

Rappelons que, dans l'énoncé du lemme 5.6.1, nous avons appelé *localement finie* une représentation $\rho : G \to \mathrm{GL}(V)$ telle que V est union de sous-espaces stables de dimension finie.

Proposition 6.1.5 *Soit $\rho : G \to GL(V)$ une représentation du groupe algébrique affine G dans l'espace vectoriel V que l'on ne suppose pas de dimension finie. On suppose ρ localement finie. Les conditions suivantes sont alors équivalentes :*
(i) L'espace V est union de sous-espaces stables de dimension finie tels que les représentations induites soient rationnelles.
(ii) Tout sous-espace de dimension finie de V est inclus dans un sous-espace stable tel que la représentation induite soit rationnelle.
(iii) Pour tout sous-espace stable de dimension finie de V, la représentation induite est rationnelle.

Preuve. - Soit $V = \bigcup V_i$, les V_i étant supposés stables de dimension finie et les $G \to \mathrm{GL}(V_i)$ étant rationnelles. Tout sous-espace stable de dimension finie est inclus dans une somme finie de V_i et l'on peut appliquer le lemme, ce qui démontre que (i) implique (iii). Le fait que (iii) implique (ii) est trivial ; le fait que (ii) implique (i) l'est également puisque l'on a supposé au départ ρ localement finie. □

Définition 6.1.6 Une telle représentation est dite *(localement finie) rationnelle*.

6.1.2 La représentation régulière

Définition 6.1.7 La *représentation régulière* du groupe algébrique affine G est la représentation $g \mapsto \rho_g := R_g^*$ de G dans $\mathrm{A}(G)$ définie au début de la section 5.6.

Rappelons que, pour tout $f \in \mathrm{A}(G)$ et pour tout $g \in G$:

$$\rho_g(f) = \big(h \mapsto f(hg)\big) \in \mathrm{A}(G).$$

Pour simplifier, notons $V := \mathrm{A}(G)$. Soient $v \in V$ et $\mu^* v = \sum v'_i \otimes v''_i$. Alors :

$$\forall g \in G\ ,\ \rho_g v = \sum v''_i(g) v'_i.$$

Ainsi, l'orbite de v est incluse dans le sous-espace vectoriel de dimension finie engendré par les v'_i : on retrouve le fait que la représentation régulière est localement finie (lemme 5.6.1).

Théorème 6.1.8 *La représentation régulière est localement finie rationnelle. Elle admet une sous-représentation de dimension finie fidèle.*

Preuve. - Soit $W \subset V$ un sous-espace stable de dimension finie. Pour tout $w \in W$, notant $\mu^* w = \sum w'_i \otimes w''_i$, l'égalité $\rho_g w = \sum w''_i(g) w'_i$ montre que l'application orbite $g \mapsto \rho_g w$ de G dans W (puisque ce dernier est stable) est un morphisme d'ensembles algébriques. Soit $(w_1, \ldots, w_n)$ une base de W et soit $(w_1^*, \ldots, w_n^*)$ sa base duale. On a $\rho_g w = \sum w_i^*(\rho_g w) w_i$, qui est une fonction régulière de g, w. L'action $G \times W \to W$ est donc un morphisme, et la représentation induite de G dans W est rationnelle, d'où la première assertion. Par ailleurs, on a vu dans la démonstration du théorème 5.6.2 que, si W contient un système générateur de la K-algèbre $\mathrm{A}(G)$, alors cette représentation est fidèle. □

Proposition 6.1.9 *(i) Pour qu'un sous-espace W de $V = A(G)$ soit stable par la représentation régulière, il faut, et il suffit, que $\mu^* W \subset W \otimes A(G)$.*
(ii) Soient $H \subset G$ un sous-groupe fermé et $I \subset A(G)$ son idéal. Alors :

$$H = \{g \in G \mid \rho_g I \subset I\} = \{g \in G \mid \rho_g I = I\}.$$

Preuve. -

Démonstration de (i). Supposons d'abord que $\mu^* W \subset W \otimes \mathrm{A}(G)$. On prend $w \in W$ et l'on écrit $\mu^* w = \sum w_i \otimes v_i$, avec les $w_i \in W$ et les $v_i \in V$, d'où (formule vue plus haut) $\rho_g w = \sum v_i(g) w_i \in W$ pour tout $g \in G$, d'où la stabilité de W.
Supposons réciproquement que W est stable. Soient (w_i) une base de W et (w'_j) une base d'un supplémentaire de W dans V. Pour tout $w \in W$, on a :

$$\mu^* w = \sum w_i \otimes v_i + \sum w'_j \otimes v'_j,$$

d'où, pour tout $g \in G$:

$$\rho_g w = \sum v_i(g) w_i + \sum v'_j(g) w'_j.$$

Comme W est stable, $\rho_g w \in W$, donc les $v'_j(g)$ sont nuls. Comme ils le sont pour tout g, les v'_j sont nuls et $\rho_g w$ est bien élément de $W \otimes \mathrm{A}(G)$.

Démonstration de (ii). La condition $\rho_g I \subset I$ équivaut à l'existence d'un diagramme commutatif :

$$\begin{array}{ccc} \mathrm{A}(G) & \xrightarrow{\rho_g} & A(G) \\ \downarrow & & \downarrow \\ \mathrm{A}(H) & \longrightarrow & A(H) \end{array}$$

les flèches verticales représentant le passage au quotient par I. Par équivalence contravariante, cela équivaut à l'existence d'un diagramme commutatif :

$$\begin{array}{ccc} H & \longrightarrow & H \\ \downarrow & & \downarrow \\ G & \xrightarrow{R_g} & G \end{array}$$

les flèches verticales représentant l'inclusion. Ce diagramme équivaut à son tour à l'inclusion $R_g H \subset H$, *i.e.* $Hg \subset H$, *i.e.* $g \in H$. On a donc l'équivalence logique :

$$\forall g \in G \ , \ g \in H \Longleftrightarrow \rho_g I \subset I.$$

Pour obtenir la relation $\rho_g I = I$, utiliser l'inverse de g. □

6.2 Théorème de Tannaka et décomposition de Jordan

Nous revenons à la question posée en 3.3.1 : peut-on reconstituer un groupe à partir de ses représentations ? Nous allons voir que l'on peut reconstituer un groupe *algébrique affine* à partir de la catégorie *tensorielle* de ses représentations *rationnelles*. C'est un aspect de la *dualité de Tannaka*. Outre son aspect satisfaisant, la dualité de Tannaka est un outil efficace et nous en déduirons très facilement l'un des théorèmes de base sur les groupes algébriques affines, la *décomposition de Jordan*, qui généralise ce qu'en France on appelle "décomposition de Dunford".

6.2.1 Le petit théorème de Tannaka

Soit donc G un groupe algébrique affine sur K. On a déjà défini les morphismes entre représentations arbitraires du groupe abstrait G (ici, "abstrait" signifie que l'on ne prend pas en compte la structure d'ensemble algébrique affine). Cette définition des morphismes s'applique en particulier aux représentations rationnelles, qui forment donc une sous-catégorie pleine (2.1.1) de la catégorie $\mathcal{R}ep_K(G)$ (3.1). Nous noterons $\mathcal{R}ep_K^{rat}(G)$ cette catégorie.

Nous avons également défini un produit tensoriel sur $\mathcal{R}ep_K(G)$. Cette opération se restreint à $\mathcal{R}ep_K^{rat}(G)$. En effet, pour voir que le produit tensoriel de deux représentations rationnelles est une représentation rationnelle, il suffit de vérifier (le lecteur fournira lui-même l'autre partie du raisonnement) que l'application naturelle $\mathrm{GL}(V)\times\mathrm{GL}(V')\to\mathrm{GL}(V\otimes V')$ est un morphisme d'ensembles algébriques affines. Or, cela découle du diagramme commutatif suivant :

$$\begin{array}{ccc} \mathrm{GL}(V)\times\mathrm{GL}(V') & \longrightarrow & \mathrm{GL}(V\otimes V') \\ \downarrow & & \downarrow \\ \mathrm{End}(V)\times\mathrm{End}(V') & \longrightarrow & \mathrm{End}(V\otimes V') \end{array}$$

Les flèches verticales sont des inclusions d'ouverts affines dans des espaces vectoriels, la flèche horizontale basse est une application bilinéaire, donc polynomiale, donc un morphisme.

Enfin, $\mathcal{R}ep_K(G)$ était munie d'un foncteur oubli ω (3.3.2) compatible au produit tensoriel, et la restriction de ω à $\mathcal{R}ep_K^{rat}(G)$ vérifie encore cette propriété. Dans toute la suite de ce chapitre, c'est cette restriction que nous noterons ω. Comme en 3.3.3, c'est le groupe $\mathrm{Aut}^{\otimes}(\omega)$ des $\otimes$-automorphismes de ω qui nous intéresse.

Un élément de ce groupe admet la description suivante. C'est une famille (ϕ_X) où, pour chaque objet X de $\mathcal{R}ep_K^{rat}(G)$, on se donne un automorphisme ϕ_X de l'espace vectoriel $\omega(X)$, la famille étant collectivement soumise aux contraintes suivantes :

1. Fonctorialité. Soit $f : X \to X'$ un morphisme dans $\mathcal{R}ep_K^{rat}(G)$. Alors le diagramme suivant est commutatif :
$$\begin{array}{ccc} \omega(X) & \xrightarrow{\omega(f)} & \omega(X') \\ {\scriptstyle\phi_X}\downarrow & & {\scriptstyle\phi_{X'}}\downarrow \\ \omega(X) & \xrightarrow{\omega(f)} & \omega(X') \end{array}$$
2. Compatibilité avec le produit tensoriel, en abrégé $\otimes$-compatibilité. On a l'égalité suivante entre automorphismes de $\omega(X\otimes X') = \omega(X)\otimes\omega(X')$:
$$\phi_{X\otimes X'} = \phi_X \otimes \phi_{X'}.$$

Exemple 6.2.1 Soit $g \in G$. Pour tout $X = (V,\rho)$, on pose $\phi_X := \rho(g)$. C'est un automorphisme de $V = \omega(X)$. La famille (ϕ_X) est fonctorielle et $\otimes$-compatible, donc définit un élément de $\mathrm{Aut}^{\otimes}(\omega)$, que nous noterons $\Phi(g)$. De plus, Φ est un morphisme de groupes.

Exercice 6.2.2 Vérifier soigneusement ces assertions (*cf.* 3.3.3).

Théorème 6.2.3 (Mini Tannaka) *L'application Φ est un isomorphisme de groupes de G sur $Aut^{\otimes}(\omega)$.*

Preuve. - L'injectivité se voit en choisissant une représentation rationnelle fidèle $X = (V,\rho)$ (il en existe d'après le théorème 6.1.8) ; si g est dans le noyau de Φ, la composante $\phi_X = \rho(g)$ de $\Phi(g)$ est l'identité de $\omega(X) = V$, donc $g = 1_G$, puisque ρ est fidèle.
Soit donc (ϕ_X) un élément de $\mathrm{Aut}^{\otimes}(\omega)$. Pour toute sous-représentation $X' = (V',\rho')$ de $X = (V,\rho)$, l'inclusion $V' \subset V$ est un morphisme de représentations et, par fonctorialité, on voit que la restriction à V' de $\phi_X \in \mathrm{GL}(V)$ est $\phi_{X'} \in \mathrm{GL}(V')$. On en déduit le fait suivant : pour toute représentation localement finie rationnelle (ce que l'on abrègera dans cette démonstration en RLFR) $X = (V,\rho)$, les $\phi_{X'} \in \mathrm{GL}(V')$ associés à toutes les sous-représentations rationnelles de dimension finie $X' = (V',\rho')$ de X sont compatibles ; comme V est la réunion de ses sous-espaces stables de dimension finie V', les $\phi_{X'}$ définissent un automorphisme $\phi_X \in \mathrm{GL}(V)$. On va montrer que la famille (ϕ_X) ainsi étendue à toutes les RLFR est encore fonctorielle et $\otimes$-compatible.
Pour la fonctiorialité, cela découle du fait suivant ; si f est un morphisme de RLFR de X dans Y, pour tout sous-espace de dimension finie V' de $\omega(X)$, le sous-espace $W' := f(V')$ de $\omega(Y)$ est de dimension finie. L'hypothèse de fonctorialité s'applique donc à la restriction $f : V' \to W'$, ce qui signifie que l'égalité $\phi_Y \circ f = f \circ \phi_X$ a lieu en restriction à V'. Puisque les V' recouvrent V, cette égalité a lieu sur V, ce qui exprime bien la fonctorialité.
En ce qui concerne le produit tensoriel de deux RLFR X et Y, on voit d'abord que, si V', W' sont des sous-espaces stables de dimension finie de $V := \omega(X)$, $W := \omega(Y)$, les sous-représentations associées X', Y' satisfont la relation $\phi_{X'\otimes Y'} = \phi_{X'} \otimes \phi_{Y'}$, ce qui signifie que l'égalité $\phi_{X\otimes Y} = \phi_X \otimes \phi_Y$ a au moins lieu en restriction à $V' \otimes W'$; mais le lecteur vérifiera que les V' recouvrant V et les W' recouvrant W, les $V' \otimes W'$ recouvrent $V' \otimes W'$, d'où l'égalité $\phi_{X\otimes Y} = \phi_X \otimes \phi_Y$ sans restriction, d'où la $\otimes$-compatibilité.
On prendra maintenant pour X la représentation régulière $g \mapsto \rho_g$ de G dans $\mathrm{A} := \mathrm{A}(G)$, ce qu'autorise le théorème 6.1.8. La multiplication dans A peut être vue comme un morphisme de K-algèbres $m : A \otimes A \to A$ (la commutativité de A intervient ici) et la relation $(f_1 f_2)(hg) = f_1(hg) f_2(hg)$, autrement dit $\rho_g(f_1 f_2) = \rho_g(f_1)\rho_g(f_2)$, implique que m est un morphisme de représentations. Par fonctorialité et $\otimes$-compatibilité de la famille étendue (ϕ_X), on a donc :

$$\phi_A \circ m = m \circ \phi_{A\otimes A} = m \circ (\phi_A \otimes \phi_A),$$

ce qui signifie que $\phi_A : A \to A$ est un morphisme d'algèbres (donc le comorphisme d'un certain endomorphisme de l'ensemble algébrique G).
Par ailleurs, le comorphisme[2] λ_h de l'endomorphisme $L_h : g \mapsto hg$ de l'ensemble algébrique G commute avec ρ_g puisque L_h commute avec R_g (cette commutation traduit en effet l'associativité dans G). C'est donc un endomorphisme de la représentation régulière et, par fonctorialité, on a $\lambda_h \circ \phi_A = \phi_A \circ \lambda_h$. Ainsi, le morphisme d'algèbres $\phi_A : A \to A$ commute avec tous les λ_h. D'après le lemme ci-dessous, il existe $g_0 \in G$ tel que $\phi_A = \rho_{g_0}$. Nous allons voir que notre famille (ϕ_X) de départ, élément de $\mathrm{Aut}^{\otimes}(\omega)$, n'est autre que $\Phi(g_0)$.
Soit donc $X = (V,\rho)$ une représentation rationnelle arbitraire. Fixons une forme linéaire $\pi \in V^*$. L'application $U_\pi : V \to \mathrm{A}(G)$ qui, à $v \in V$ associe la fonction $g \mapsto \pi(g.v)$ (cette fonction est bien régulière sur G) satisfait la relation :

$$\forall g \in G\ ,\ U_\pi(h.v)(g) = \pi(gh.v) = U_\pi(v)(gh) \Longrightarrow U_\pi(h.v) = \rho_h\big(U_\pi(v)\big);$$

[2] Attention, nous avons changé ici la définition de λ_h et L_h par rapport à la section 5.6.

autrement dit, U_π est un morphisme de représentations de X dans la représentation régulière et, par fonctorialité :

$$\phi_A \circ U_\pi = U_\pi \circ \phi_X \Longrightarrow \rho_{g_0} \circ U_\pi = U_\pi \circ \rho_{g_0} \Longrightarrow \forall g \in G\ ,\ \forall v \in V\ ,\ \pi(gg_0v) = \pi\big(g\phi_X(v)\big).$$

Comme c'est vrai pour tout $\pi \in V^*$, on a :

$$\forall v \in V\ ,\ g_0v = \phi_X(v),$$

ce qui signifie bien que $(\phi_X) = \Phi(g_0)$. □

Lemme 6.2.4 (lemme utile) *Soit $f : A(G) \to A(G)$ un morphisme d'algèbres qui commute avec tous les λ_h. Alors il existe $g_0 \in G$ tel que $f = \rho_{g_0}$.*

Preuve. - Par anti-équivalence, f est le comorphisme d'un morphisme d'ensembles algébriques $\phi : G \to G$ qui commute avec tous les L_h. L'égalité $\phi \circ L_h = L_h \circ \phi$, c'est-à-dire $\phi(hg) = h\phi(g)$ entraine $\phi(h) = hg_0$, où $g_0 := \phi(1_G)$, donc $\phi = R_{g_0}$, donc $f = \rho_{g_0}$. □

Remarque 6.2.5 Le "mini-théorème de Tannaka" permet de reconstituer la structure du groupe *abstrait* G, mais pas sa géométrie, *i.e.* sa structure d'ensemble (et donc de groupe) algébrique. Ce dernier problème sera résolu au chapitre 7.

6.2.2 Rappels sur la décomposition de Dunford

Tout le contenu de ce numéro peut être considéré, au choix, comme un résumé de faits "bien connus" (et que l'on peut sans doute trouver dans les cinq premiers chapitres du livre d'Algèbre de Bourbaki), soit comme une série d'exercices de niveau L3-M1. Les espaces sont supposés de dimension finie (mais une partie des énoncés reste valide sans cette hypothèse).

Niplotents

Soit V un K-espace vectoriel. Si $f, g \in \mathrm{End}(V)$ commutent et sont nilpotents, alors $f+g$ et fg sont nilpotents. On en déduit directement que, si $f \in \mathrm{End}(V)$ et $g \in \mathrm{End}(W)$ sont nilpotents, alors $f \oplus g \in \mathrm{End}(V \oplus W)$, $f \otimes g \in \mathrm{End}(V \otimes W)$, $f \otimes \mathrm{Id}_W + \mathrm{Id}_V \otimes g \in \mathrm{End}(V \otimes W)$ et $f \otimes \mathrm{Id}_W + \mathrm{Id}_V \otimes g + f \otimes g \in \mathrm{End}(V \otimes W)$ sont nilpotents.

De plus, si $f \in \mathrm{End}(V)$ est nilpotent et si $V' \subset V$ est f-stable, alors la restriction $f_{|V'} \in \mathrm{End}(V')$ et l'endomorphisme induit $\overline{f} \in \mathrm{End}(V/V')$ sont nilpotents.

Unipotents

L'endomorphisme f de V est unipotent si $f - \mathrm{Id}_V$ est nilpotent ; f est donc un automorphisme. On déduit de ce qui précède que, si $f \in \mathrm{GL}(V)$ et $g \in \mathrm{GL}(W)$ sont unipotents, alors $f \oplus g \in \mathrm{GL}(V \oplus W)$ et $f \otimes g \in \mathrm{GL}(V \otimes W)$ sont unipotents.

De plus, si $f \in \mathrm{GL}(V)$ est unipotent et si $V' \subset V$ est f-stable, alors la restriction $f_{|V'} \in \mathrm{GL}(V')$ et l'automorphisme induit $\overline{f} \in \mathrm{GL}(V/V')$ sont unipotents.

Semi-simples

L'endomorphisme f de V est dit semi-simple s'il est diagonalisable. (La distinction intervient dans le cas d'un corps non algébriquement clos.) Si $f, g \in \mathrm{End}(V)$ commutent et sont semi-simples, alors $f+g$ et fg sont semi-simples. On en déduit que, si $f \in \mathrm{End}(V)$ et $g \in \mathrm{End}(W)$ sont semi-simples, alors $f \oplus g \in \mathrm{End}(V \oplus W)$ et $f \otimes g \in \mathrm{End}(V \otimes W)$ sont semi-simples.

De plus, si $f \in \mathrm{End}(V)$ est semi-simple et si $V' \subset V$ est f-stable, alors la restriction $f_{|V'} \in \mathrm{End}(V')$ et l'endomorphisme induit $\overline{f} \in \mathrm{End}(V/V')$ sont semi-simples.

Décompositions de Dunford

Tout endomorphisme $f \in \mathrm{End}(V)$ s'écrit de manière unique $f = f_s + f_n$, où f_s est semi-simple, f_n est nilpotent, et f_s, f_n commutent (décomposition de Dunford "additive"). On a alors $f_s, f_n \in K[f]$, de sorte que tout endomorphisme de V qui commute avec f commute également avec f_s et f_n.

Tout automorphisme $f \in \mathrm{GL}(V)$ s'écrit de manière unique $f = f_s f_u$, où f_s est semi-simple inversible, f_u est unipotent, et f_s, f_u commutent (décomposition de Dunford "multiplicative"). On a alors $f_s, f_u \in K[f]$, de sorte que tout endomorphisme de V qui commute avec f commute également avec f_s et f_u.

À noter que les composantes semi-simples f_s qui interviennent respectivement dans les décompositions de Dunford additive et multiplicative d'un automorphisme f sont les mêmes, et que l'on a $f_u = \mathrm{Id}_V + f_s^{-1} f_n$.

Stabilité de la décomposition de Dunford multiplicative

Théorème 6.2.6 *(i) Soient $f \in GL(V)$ et $g \in GL(W)$. Alors :*

$$\begin{aligned}(f \oplus g)_s &= f_s \oplus g_s \in GL(V \oplus W),\\ (f \oplus g)_u &= f_u \oplus g_u \in GL(V \oplus W),\\ (f \otimes g)_s &= f_s \otimes g_s \in GL(V \otimes W),\\ (f \otimes g)_u &= f_u \otimes g_u \in GL(V \otimes W).\end{aligned}$$

(ii) Soient $f \in GL(V)$ et $V' \subset V$ un sous-espace f-stable. Alors :

$$\begin{aligned}(f_{|V'})_s &= (f_s)_{|V'} \in GL(V'),\\ (f_{|V'})_u &= (f_u)_{|V'} \in GL(V'),\\ (\overline{f})_s &= \overline{f_s} \in GL(V/V'),\\ (\overline{f})_u &= \overline{f_u} \in GL(V/V')\end{aligned}$$

(iii) Soient $f \in GL(V)$ et $g \in GL(W)$ et soit $\phi : V \to W$ tel que $g \circ \phi = \phi \circ f$. Alors :

$$\begin{aligned}g_s \circ \phi &= \phi \circ f_s,\\ g_u \circ \phi &= \phi \circ f_u.\end{aligned}$$

Preuve. - Seul (iii) ne découle pas de ce qui précède, mais on le déduit de (ii) en composant $V \to V \oplus W \to W$. □

Exercice 6.2.7 Quels énoncés restent valides en dimension infinie ?

6.2.3 La décomposition de Jordan dans un groupe algébrique

Soit G un groupe algébrique affine et soit $g \in G$. Pour toute représentation rationnelle $X = (V, \rho)$ de G, notons $S_X := \big(\rho(g)\big)_s$ et $U_X := \big(\rho(g)\big)_u$ la décomposition de Dunford multiplicative de $\rho(g) \in \mathrm{GL}(V)$.

Lemme 6.2.8 *Les familles (S_X) et (U_X) sont des éléments de $Aut^{\otimes}(\omega)$.*

Preuve. - C'est immédiat d'après le théorème 6.2.6. □

Théorème 6.2.9 (Décomposition de Jordan dans un groupe algébrique) *Tout $g \in G$ admet une unique décomposition $g = g_s g_u$ telle que, pour toute représentation $X = (V, \rho)$ de G, on ait : $\rho(g_s) = \big(\rho(g)\big)_s$ et $\rho(g_u) = \big(\rho(g)\big)_u$.*

Preuve. - C'est immédiat d'après le lemme et le théorème 6.2.3. □

Remarque 6.2.10 D'après la démonstration du théorème 6.2.3, si $\rho : G \to \mathrm{GL}\big(\mathrm{A}(G)\big)$ désigne la représentation régulière de G, on a $\rho(g) = \rho(g_s)\rho(g_u)$, les deux facteurs étant respectivement semi-simple et unipotent dans le sens où leurs restrictions à tout sous-espace stable de dimension finie le sont ; et cela s'étend d'ailleurs à toute représentation localement finie rationnelle de G.

Définition 6.2.11 L'élément $g \in G$ est dit *semi-simple* si $g = g_s$ et *unipotent* si $g = g_u$.

Pour que g soit semi-simple, resp. unipotent, il suffit évidemment que son image par une représentation fidèle arbitraire le soit.

Corollaire 6.2.12 *Soit $\phi : G \to G'$ un morphisme de groupes algébriques affines. Alors, pour tout $g \in G$:*

$$\big(\phi(g)\big)_s = \phi(g_s),$$
$$\big(\phi(g)\big)_u = \phi(g_u).$$

Preuve. - Pour toute représentation $\rho' : G' \to \mathrm{GL}(V)$, appliquer le théorème à $\rho := \rho' \circ \phi$. □

Corollaire 6.2.13 *Si G est un sous-groupe fermé de $GL(V)$, la décomposition de Jordan dans le groupe algébrique G coïncide avec la décomposition de Jordan dans $GL(V)$.*

Preuve. - Appliquer le théorème à la représentation de G définie par l'inclusion de G dans $\mathrm{GL}(V)$. □

Corollaire 6.2.14 *Si $g, g' \in G$ commutent, alors :*

$$(gg')_s = g_s g'_s,$$
$$(gg')_u = g_u g'_u.$$

Preuve. - Immédiat d'après les théorèmes 6.2.6 et 6.2.9. □

Remarque 6.2.15 Si G est un groupe algébrique affine commutatif, il s'ensuit que les éléments unipotents de G forment un sous-groupe G_u et que les éléments semi-simples de G forment un sous-groupe G_s. Il est démontré dans [6] que l'application naturelle $G_s \times G_u \to G$ est un isomorphisme de groupes algébriques.

Exercice 6.2.16 Démontrer que c'est un isomorphisme de groupes et un morphisme d'ensembles algébriques. Que manque-t-il pour conclure ?

Exercice 6.2.17 Donner des contre-exemples aux égalités $(gg')_s = g_s g'_s$ et $(gg')_u = g_u g'_u$ dans $\mathrm{GL}_2(\mathbf{C})$.

6.3 Les théorèmes de Chevalley

Il s'agit de caractérisations des sous-groupes fermés d'un groupe algébrique affine particulièrement adaptées à la dualité de Tannaka.

6.3.1 La forme de base du théorème de Chevalley

Soient V un espace vectoriel de dimension finie et $W \subset V$ un sous-espace. Le sous-groupe :

$$\{\phi \in \mathrm{GL}(V) \mid \phi(W) \subset W\} = \{\phi \in \mathrm{GL}(V) \mid \phi(W) = W\}$$

de $\mathrm{GL}(V)$ en est un sous-groupe fermé. Il est en effet évident que c'en est un sous-groupe, et, notant p une projection arbitraire de V sur W, on a :

$$\forall \phi \in \mathrm{GL}(V)\ ,\ \phi(W) \subset W \Longleftrightarrow (\mathrm{Id}_V - p) \circ \phi \circ p = 0,$$

qui définit l'intersection avec $\mathrm{GL}(V)$ d'un sous-espace vectoriel de $\mathrm{End}(V)$.

Exercice 6.3.1 Est-ce que $\{\phi \in \mathrm{End}(V) \mid \phi(W) = W\}$ est un fermé de $\mathrm{End}(V)$?

Si par conséquent $\rho : G \to \mathrm{GL}(V)$ est une représentation rationnelle du groupe algébrique affine G, et si $W \subset V$ est un sous-espace de V, le sous-groupe :

$$H := \{g \in G \mid gW \subset W\} = \{g \in G \mid gW = W\}$$

de G en est un sous-groupe fermé : en effet, H est l'image réciproque par le morphisme ρ du sous-groupe fermé vu plus haut.

Théorème 6.3.2 (Chevalley) *Soient G un groupe algébrique affine et $H \subset G$ un sous-groupe fermé de G. Il existe alors une représentation rationnelle $\rho : G \to GL(V)$ et un sous-espace vectoriel $W \subset V$ tels que :*

$$H = \{g \in G \mid gW \subset W\} = \{g \in G \mid gW = W\}.$$

Preuve. - Soit $I \subset \mathrm{A}(G)$ l'idéal du fermé H dans G. Soient $f_1, \ldots, f_r$ des générateurs de l'idéal I (l'anneau $\mathrm{A}(G)$ est noetherien). Soit $V \subset \mathrm{A}(G)$ un sous-espace vectoriel de dimension finie, stable sous l'action de la représentation régulière de G, et contenant les f_i (*cf.* la première assertion du théorème 6.1.8). Nous noterons ρ la représentation induite de G dans V et $W := V \cap I$, qui est donc un sous-espace de V contenant les f_i.
Si $g \in H$, on a par hypothèse $\rho_g V = V$ et, d'après la proposition 6.1.9, $\rho_g I = I$, donc (ρ_g étant injective) $\rho_g W = W$, *i.e.* $gW = W$.
Supposons réciproquement $gW = W$, *i.e.* $\rho_g W = W$: alors $\rho_g f_i \in I$ pour $i = 1, \ldots, r$; comme ρ_g est un endomorphisme de l'algèbre $\mathrm{A}(G)$ et I l'idéal de $\mathrm{A}(G)$ engendré par les f_i, on a $\rho_g I \subset I$. De même, de $g^{-1}W = W$ (qui découle de $gW = W$), on déduit que $\rho_g^{-1} I \subset I$, donc, en fin de compte, que $\rho_g I = I$. Appliquant à nouveau la proposition 6.1.9, on voit que $g \in H$. □

Exemple 6.3.3 Considérons le groupe spécial linéaire $\mathrm{SL}_n(K) \subset \mathrm{GL}_n(K)$. Son idéal est $I := <1 - \det>$. (C'est un exercice classique d'algèbre commutative : cet idéal est premier, donc égal à son radical.) Prenons $V := K.1 + K\det \subset \mathrm{A}\big(\mathrm{GL}_n(K)\big)$. Ce sous-espace est bien stable par la représentation régulière et l'action de $G := \mathrm{GL}_n(K)$ est décrite par les formules :

$$\rho_g 1 = 1 \text{ et } \rho_g \det = (\det g) \det.$$

La représentation induite de G s'identifie donc à la représentation matricielle $G \to \mathrm{GL}_2(K)$ définie par :

$$g \mapsto \begin{pmatrix} 1 & 0 \\ 0 & \det g \end{pmatrix}.$$

Cette représentation provient de l'identification de V avec K^2 associée à la base $(1, \det)$ de V. Sous cette même identification, $W := V \cap I = K(1 - \det)$ correspond au à la droite engendrée par $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$. Le stabilisateur de cette droite par la représentation $G \to \mathrm{GL}_2(K)$ est :

$$\left\{ g \in G \;\middle|\; \begin{pmatrix} 1 & 0 \\ 0 & \det g \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} /\!/ \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\} = \{g \in G \mid \det g = 1\} = \mathrm{SL}_n(K).$$

6.3.2 Compléments d'algèbre multilinéaire

Encore une fois, il s'agit de faits "bien connus" d'algèbre linéaire, pour lesquels on pourra au choix consulter Bourbaki ou chercher soi-même à titre d'exercice.

Formes k-linéaires

Soit V un K-espace vectoriel de dimension n. Nous noterons respectivement $M_k(V)$, $S_k(V)$ et $A_k(V)$, l'espace des formes k-linéaires, l'espace des formes k-linéaires symétriques et l'espace des

formes k-linéaires alternées[3] sur V. Leurs dimensions sont respectivement n^k, $\binom{n+k-1}{k}$ et $\binom{n}{k}$. Plus précisément, si $(e_1,\dots,e_n)$ est une base de V,

1. une forme k-linéaire quelconque $\phi \in M_k(V)$ est déterminée de manière unique par les scalaires $\phi(e_{i_1},\dots,e_{i_k}) \in K$, où $i_1,\dots,i_k \in \{1,\dots,n\}$: donc par n^k scalaires ;
2. une forme k-linéaire symétrique $\phi \in S_k(V)$ est déterminée de manière unique par les scalaires $\phi(e_{i_1},\dots,e_{i_k}) \in K$, où $1 \leq i_1 \leq \cdots \leq i_k \leq n$: donc par $\binom{n+k-1}{k}$ scalaires ;
3. une forme k-linéaire alternée $\phi \in S_k(V)$ est déterminée de manière unique par les scalaires $\phi(e_{i_1},\dots,e_{i_k}) \in K$, où $1 \leq i_1 < \cdots < i_k \leq n$: donc par $\binom{n}{k}$ scalaires.

Enfin, M_k, S_k et A_k sont des foncteurs contravariants de la catégorie $\mathcal{E}vf_K$ des K-espaces vectoriels de dimension finie dans elle-même, et les inclusions $S_k(V) \subset M_k(V)$ et $A_k(V) \subset M_k(V)$ définissent des transformations naturelles entre ces foncteurs.

Puissances tensorielles

La propriété universelle du produit tensoriel fournit un isomorphisme :

$$(V \otimes \cdots \otimes V)^* \simeq M_k(V)$$

qui, à la forme linéaire λ sur $V \otimes \cdots \otimes V$ (produit tensoriel de k facteurs égaux à V) associe la forme k-linéaire $(v_1,\dots,v_k) \mapsto \lambda(v_1 \otimes \cdots \otimes v_k)$ sur V. Comme ces espaces sont de dimension finie, on en déduit par bidualité un isomorphisme :

$$\begin{aligned} V \otimes \cdots \otimes V &\simeq \big(M_k(V)\big)^*, \\ v_1 \otimes \cdots \otimes v_k &\mapsto \big(\phi \mapsto \phi(v_1,\dots,v_k)\big). \end{aligned}$$

L'espace $T^k(V) := V \otimes \cdots \otimes V$ est la *puissance tensorielle k^e de V*.

Soit maintenant $(e_1,\dots,e_n)$ une base de V. Alors les $e_{i_1} \otimes \cdots \otimes e_{i_k}$, où $i_1,\dots,i_k \in \{1,\dots,n\}$, forment une base de $T^k(V)$, qui est donc de dimension n^k (comme son dual $M_k(V)$).

Enfin, T^k est un foncteur covariant de la catégorie $\mathcal{E}vf_K$ dans elle-même. Plus précisément, si $f : V \to W$ est une application linéaire, $T^k(f)$ est l'application linéaire de $T^k(V)$ dans $T^k(W)$ définie par $v_1 \otimes \cdots \otimes v_k \mapsto f(v_1) \otimes \cdots \otimes f(v_k)$.

Puissances symétriques

On appelle *puissance symétrique k^e de V* et l'on note $S^k(V)$ le dual de l'espace $S_k(V)$ des formes k-linéaires symétriques. Comme $S_k(V)$ est un sous-espace de $M_k(V)$, on voit en passant au dual que $S^k(V)$ est un quotient de $T^k(V)$. On obtient donc une applications linéaire surjective :

$$T^k(V) \to S^k(V) \to 0.$$

L'image par cette surjection de $v_1 \otimes \cdots \otimes v_k$ est notée $v_1 \cdots v_k$. Le noyau de la surjection est le sous-espace vectoriel de $T^k(V)$ engendré par les $v_1 \otimes \cdots \otimes v_k - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(k)}$, où σ parcourt le groupe symétrique sur k éléments.

[3] Puisque nous nous sommes placés en caractéristique 0, il n'y a pas lieu de distinguer "alternée" et "antisymétrique".

Soit maintenant $(e_1,\dots,e_n)$ une base de V. Alors les $e_{i_1}\cdots e_{i_k}$, où $1\leq i_1\leq\ldots\leq i_k\leq n$, forment une base de $S^k(V)$, qui est donc de dimension $\binom{n+k-1}{k}$ (comme son dual $S_k(V)$).

Enfin, S^k est un foncteur covariant et les surjections $T^k(V)\to S^k(V)$ définissent une transformation naturelle entre ces deux foncteurs.

Remarque 6.3.4 Si l'on choisit une base $(e_1,\dots,e_n)$ de V et si l'on note $(X_1,\dots,X_n)$ la base duale de V^*, les éléments de la base de $S^k(V^*)$ décrite ci-dessus s'identifient aux monômes de degré k en les X_i et les éléments de $S^k(V^*)$ aux polynômes homogènes de degré k en les X_i. La somme directe $S^\bullet(V^*):=\bigoplus_{k\geq 0}S^k(V^*)$, que l'on appelle "algèbre symétrique sur V^*", s'identifie à $K[X_1,\dots,X_n]$, donc à $\mathrm{A}(V)$. On obtient ainsi une définition intrinsèque de $\mathrm{A}(V)$.

Puissances extérieures

On appelle *puissance extérieure k^e de V* et l'on note $\Lambda^k(V)$ le dual de l'espace $A_k(V)$ des formes k-linéaires alternées. Comme $A_k(V)$ est un sous-espace de $M_k(V)$, on voit en passant au dual que $\Lambda^k(V)$ est un quotient de $T^k(V)$. On obtient donc une applications linéaire surjective :

$$T^k(V)\to\Lambda^k(V)\to 0.$$

L'image par cette surjection de $v_1\otimes\cdots\otimes v_k$ est notée $v_1\wedge\cdots\wedge v_k$. Le noyau de la surjection est le sous-espace vectoriel de $T^k(V)$ engendré par les $v_1\otimes\cdots\otimes v_k-\varepsilon(\sigma)v_{\sigma(1)}\otimes\cdots\otimes v_{\sigma(k)}$, où σ parcourt le groupe symétrique sur k éléments et où l'on note $\varepsilon(\sigma)$ la signature de σ.

Soit maintenant $(e_1,\dots,e_n)$ une base de V. Alors les $e_{i_1}\wedge\cdots\wedge e_{i_k}$, où $1\leq i_1<\ldots<i_k\leq n$, forment une base de $\Lambda^k(V)$, qui est donc de dimension $\binom{n}{k}$ (comme son dual $A_k(V)$).

Enfin, Λ^k est un foncteur covariant et les surjections $T^k(V)\to\Lambda^k(V)$ définissent une transformation naturelle entre ces deux foncteurs.

Exercice 6.3.5 Déduire de la fonctorialité que, si $f:V\to W$ est injective, resp. surjective, $T^k(f)$, $S^k(f)$ et $\Lambda^k(f)$ le sont également. (Selon le cas, il existe g ou h tel que gf ou fh soit l'identité.)

Lien avec les groupes linéaires

Par pure fonctorialité (voir l'exercice ci-dessus), tout automorphisme f de V définit des automorphismes $T^k(f)$, $S^k(f)$ et $\Lambda^k(f)$ de $T^k(V)$, $S^k(V)$ et $\Lambda^k(V)$. On définit ainsi des morphismes de groupes :

$$\begin{aligned}\mathrm{GL}(V)&\to\mathrm{GL}\big(T^k(V)\big),\\ \mathrm{GL}\big(T^k(V)\big)&\to\mathrm{GL}\big(S^k(V)\big),\\ \mathrm{GL}\big(T^k(V)\big)&\to\mathrm{GL}\big(\Lambda^k(V)\big).\end{aligned}$$

Il suffit d'écrire les effets sur des bases de $T^k(f)$, $S^k(f)$ et $\Lambda^k(f)$ pour voir que les applications ci-dessus sont définies par des formules polynomiales : ce sont donc des morphismes de groupes algébriques.

6.3.3 Deuxième version du théorème de Chevalley

Lemme 6.3.6 *Soient W, W' deux sous-espaces vectoriels de l'espace vectoriel V, et soit $k := \dim W$. Alors :*

$$W \subset W' \Longleftrightarrow \Lambda^k W \subset \Lambda^k W'.$$

Preuve. - L'implication directe est immédiate, par fonctorialité ou par description explicite de l'effet sur les bases.
Supposons que $\Lambda^k W \subset \Lambda^k W'$. Dualement, cette hypothèse signifie que toute forme k-linéaire alternée sur V qui s'annule sur W' s'annule sur W. On va alors démontrer par l'absurde que $W \subset W'$. Dans le cas contraire, il existe une base $(e_1, \ldots, e_n)$ de V et des entiers ℓ et m tels que $m > k$ et que : $(e_1, \ldots, e_k)$ est une base de W ; et $(e_\ell, \ldots, e_m)$ est une base de W'. On peut alors construire $\phi \in A_k(V)$ telle que $\phi(e_1, \ldots, e_k) = 0$ et $\phi(e_{m-k+1}, \ldots, e_m) \neq 0$ (les autres valeurs étant arbitraires), de sorte que ϕ est nulle sur W mais pas sur W', contradiction. □

Lemme 6.3.7 *Soit W un sous-espace vectoriel de l'espace vectoriel V, soit $k := \dim W$ et soit $\phi \in GL(V)$. Alors :*

$$\phi(W) = W \Longleftrightarrow (\Lambda^k \phi)(\Lambda^k W) = \Lambda^k W.$$

Preuve. - Soit $W' = \phi(W)$. Alors $\Lambda^k W' = (\Lambda^k \phi)(\Lambda^k W)$ (fonctorialité ou effet sur les bases) et l'on peut appliquer le lemme précédent. □

Théorème 6.3.8 (Chevalley) *Soient G un groupe algébrique affine et H un sous-groupe fermé de G. Il existe alors une représentation rationnelle $\rho : G \to GL(E)$ et une droite $D \subset E$ telles que :*

$$H = \{g \in G \mid gD = D\}.$$

Preuve. - Il suffit d'appliquer le théorème 6.3.2, puis le lemme ci-dessus en posant $E := \Lambda^k V$ et $D := \Lambda^k W$. □

Remarque 6.3.9 Un vecteur v non nul de D vérifie :

$$\forall g \in H \ , \ g.v = \chi(g)v,$$

où $\chi : H \to K^*$ est un morphisme de groupes, et même un morphisme de groupes algébriques $H \to G_m$, qui ne dépend que de D (et non du choix de v). On dit que v est un *semi-invariant* et que χ est un *caractère de H*. Si le groupe $X(H)$ des caractères de H est trivial (par exemple si H est unipotent), v est invariant.

Exercice 6.3.10 Démontrer les assertions de la remarque.

Chapitre 7

L'enveloppe proalgébrique et ses représentations

Ce chapitre est le but du cours : on *tente* d'y démontrer les principaux théorèmes relatifs à l'enveloppe proalgébrique d'un groupe, et ce, uniquement avec de la géométrie algébrique élémentaire. S'agissant du dernier chapitre d'un cours de M2 de deuxième semestre, le rédacteur s'est autorisé à laisser un peu plus de travail non trivial au lecteur !

7.1 Enveloppe proalgébrique d'un "groupe abstrait"

On désignera par Γ un "groupe abstrait", c'est-à-dire sans structure supplémentaire. Les lettres $G, G', H, \ldots$ seront réservées aux groupes algébriques. La lettre K dénote toujours notre bon vieux corps algébriquement clos de caractéristique nulle.

7.1.1 La catégorie tensorielle des représentations de Γ sur K

Commençons par quelques redites, pour la commodité du lecteur. La catégorie $\mathcal{R}ep_K(\Gamma)$ des représentations de Γ sur K a pour objets les couples (V,ρ) où V est un K-espace vectoriel de dimension finie et $\rho : \Gamma \to \mathrm{GL}(V)$ une représentation ; et pour morphismes $(V,\rho) \to (V',\rho')$ les applications K-linéaires $u : V \to V'$ telles que $\forall g \in \Gamma\ ,\ \rho'(g) \circ u = u \circ \rho(g)$. La catégorie $\mathcal{R}ep_K(\Gamma)$ est également munie d'un produit tensoriel : on pose $(V,\rho) \otimes_K (V',\rho') := (V \otimes_K V', \rho \otimes_K \rho')$, où, par définition : $(\rho \otimes_K \rho')(g) := \rho(g) \otimes_K \rho'(g) \in \mathrm{GL}(V \otimes_K V')$. (On omettra le plus souvent de préciser la base K.) Enfin, $\mathcal{R}ep_K(\Gamma)$ est munie d'un foncteur oubli. C'est le foncteur covariant ω de $\mathcal{R}ep_K(\Gamma)$ dans $\mathcal{E}vf_K$ qui, à (V,ρ), associe V et, à $u : (V,\rho) \to (V',\rho')$, associe $u : V \to V'$. Ce foncteur est fidèle et $\otimes$-compatible, *i.e.* $\omega(X \otimes X') = \omega(X) \otimes \omega(X')$.

On note $\underline{1}$ l'*objet unité* de $\mathcal{R}ep_K(\Gamma)$, à savoir la représentation triviale de Γ dans K. De l'existence d'isomorphismes fonctoriels $K \otimes V \simeq V \otimes K \simeq V$, on déduit sans peine l'existence d'isomorphismes fonctoriels :

$$\underline{1} \otimes X \simeq X \otimes \underline{1} \simeq X.$$

Exercice 7.1.1 Montrer que les morphismes de $\underline{1}$ dans (V,ρ) sont les applications $\lambda \mapsto \lambda v$, où $v \in V$ est stable par ρ, *i.e.* $\forall g \in G\ ,\ \rho(g)(v) = v$.

Remarque 7.1.2 Soit F un foncteur covariant de la catégorie $\mathcal{E}vf_K$ dans elle-même. Pour tout $X := (V, \rho)$, l'application $g \mapsto F(\rho(g))$ est un morphisme de Γ dans $\mathrm{GL}(F(V))$, donc une représentation. On définit ainsi un objet (abusivement noté) $F(X)$ de $\mathcal{R}ep_K(\Gamma)$, que l'on étend sans problème en un foncteur de la catégorie $\mathcal{R}ep_K(\Gamma)$ dans elle-même. À titre d'application, on peut définir les puissances tensorielles, symétriques, extérieures (6.3.2) d'un objet de $\mathcal{R}ep_K(\Gamma)$.

La représentation duale

Soit $X := (V, \rho)$ un objet de $\mathcal{R}ep_K(\Gamma)$. Notons V^* le dual de l'espace vectoriel V et, pour tout automorphisme ϕ de V :

$$\phi^\vee := {}^t\phi^{-1}$$

la *contragrédiente* de ϕ, qui est un automorphisme de V^*. De l'égalité aisément vérifiée :

$$(\phi \circ \psi)^\vee = \phi^\vee \circ \psi^\vee,$$

on déduit que l'application :

$$\rho^\vee : \begin{cases} g \mapsto \big(\rho(g)\big)^\vee, \\ G \to \mathrm{GL}(V^*), \end{cases}$$

est une représentation de Γ dans V^*, appelée *représentation contragrédiente* de ρ. L'objet :

$$X^\vee := (V^*, \rho^\vee)$$

de $\mathcal{R}ep_K(\Gamma)$ est appelé *dual* de X. Par exemple, $\underline{1}^\vee$ s'identifie canoniquement à $\underline{1}$.

Par construction, on a donc :

$$\omega(X^\vee) = \big(\omega(X)\big)^*.$$

Si u est un morphisme de $X := (V, \rho)$ dans $X' := (V', \rho')$, il est facile de vérifier que l'application linéaire transposée ${}^t u : V'^* \to V^*$ est compatible avec les deux représentations contragrédientes et définit donc un morphisme de $X'^\vee$ dans $X^\vee$. En effet, pour tout $g \in G$:

$$\rho'(g) \circ u = u \circ \rho(g) \Longrightarrow \rho^\vee(g) \circ {}^t u = {}^t u \circ \rho'^\vee(g).$$

On définit ainsi un foncteur contravariant $X \rightsquigarrow X^\vee$ de la catégorie $\mathcal{R}ep_K(\Gamma)$ dans elle-même. Ce foncteur est "involutif". Plus rigoureusement, on a (tout comme dans $\mathcal{E}vf_K$) des isomorphismes $X \simeq X^{\vee\vee}$ qui définissent un isomorphisme du foncteur identité de $\mathcal{R}ep_K(\Gamma)$ sur le foncteur "bi-dual" $X \rightsquigarrow X^{\vee\vee}$ (qui est covariant).

Proposition 7.1.3 (Rigidité) *On a un isomorphisme canonique et fonctoriel en chaque argument :*

$$(X \otimes X')^\vee \simeq X^\vee \otimes X'^\vee.$$

Preuve. - L'assertion correspondante pour les espaces vectoriels et pour les applications linéaires figure (par exemple) dans [7, chap. 2,§4.4] ; et l'application aux représentations est alors immédiate. □

Exercice 7.1.4 (i) Définir un morphisme canonique de $V^* \otimes V'$ dans le K-espace vectoriel $\mathrm{Hom}_K(V,V')$ des applications K-linéaires de V dans V' et démontrer qu'il est bijectif en dimension finie, et fonctoriel en chaque argument.
(ii) Soient $X := (V,\rho)$ et $X' := (V',\rho')$ deux objets de $\mathcal{R}ep_K(\Gamma)$. Décrire la représentation R de Γ dans $\mathrm{Hom}_K(V,V')$ qui correspond à $\rho^\vee \otimes \rho'$ par l'isomorphisme de la question précédente. En déduire une description de $X^\vee \otimes X'$ sous la forme $\big(\mathrm{Hom}_K(V,W),R\big)$. Cet objet est alors appelé "Hom interne" et noté $\underline{\mathrm{Hom}}(X,X')$; on a un isomorphisme fonctoriel : $\underline{\mathrm{Hom}}(X,X') \simeq X^\vee \otimes X'$. En particulier, $X^\vee$ s'identifie à $\underline{\mathrm{Hom}}(X,\underline{1})$.
(iii) Montrer que $\mathrm{Hom}(X,X')$ est l'espace des points fixes de la représentation $\underline{\mathrm{Hom}}(X,X')$.
(iv) Expliciter et démontrer l'isomorphisme "d'adjonction", fonctoriel en chaque argument :

$$\underline{\mathrm{Hom}}(X \otimes Y, Z) \simeq \underline{\mathrm{Hom}}\big(X, \underline{\mathrm{Hom}}(Y,Z)\big).$$

(On commencera par l'isomorphisme analogue pour des espaces vectoriels.)

Le groupe $\mathbf{Aut}^\otimes(\omega)$

Les éléments du groupe $\mathrm{Aut}^\otimes(\omega)$ des automorphismes $\otimes$-compatibles du foncteur ω sont les familles $(\phi_X)_X$ indexées par les objets X de $\mathcal{R}ep_K(\Gamma)$, où chaque ϕ_X attaché à $X := (V,\rho)$ est un automorphisme de l'espace vectoriel V, où $\phi_{X\otimes X'} = \phi_X \otimes \phi_{X'}$ et où, pour tout morphisme $u : X \to X'$, on a $\phi_{X'} \circ u = u \circ \phi_X$. Ils forment un groupe pour la loi $(\phi_X)_X(\psi_X)_X := (\phi_X \circ \psi_X)_X$. L'élément neutre est la famille $(\mathrm{Id}_X)_X$, l'inverse de $(\phi_X)_X$ est la famille $(\phi_X^{-1})_X$.

À tout $g \in \Gamma$, on associe un élément $(\phi_X)_X$ de $\mathrm{Aut}^\otimes(\omega)$ défini en posant, pour tout $X := (V,\rho)$, $\phi_X := \rho(g)$. On définit ainsi un morphisme de groupes de Γ dans $\mathrm{Aut}^\otimes(\omega)$.

Définition 7.1.5 On note Γ^{alg} le groupe $\mathrm{Aut}^\otimes(\omega)$. Le groupe Γ^{alg}, muni du morphisme structural $\Gamma \to \Gamma^{alg}$, est appelé *enveloppe proalgébrique de* Γ.

On prendra garde que cette définition est liée au corps K, bien que ce dernier ne soit pas explicitement mentionné. On verra dans ce chapitre que l'enveloppe proalgébrique peut être caractérisée par une propriété universelle (c'est même sa raison d'être).

Il n'est nullement garanti que le morphisme $\Gamma \to \Gamma^{alg}$ soit injectif. C'est évidemment le cas si le groupe Γ admet au moins une représentation fidèle de dimension finie (voir les exercices pour des exemples). À l'opposé, on peut démontrer qu'un groupe simple infini de type fini (et il en existe !) n'admet aucune représentation non triviale de dimension finie[1] : son enveloppe proalgébrique est donc triviale !

Exercice 7.1.6 Démontrer que le morphisme $\mathbf{Z} \to \mathbf{Z}^{alg}$ est injectif. (Déterminer une représentation fidèle de dimension finie.)

[1] L'argument est essentiellement le suivant : si $\Gamma \to \mathrm{GL}(V)$ n'était pas triviale, elle serait injective (simplicité de Γ) et le groupe Γ serait "résiduellement fini" d'après un résultat de Malcev ; or, c'est impossible pour un groupe simple infini. Le lecteur intéressé pourra consulter "Introduction to Group Theory, chap. 29" de Oleg Bogopolski, ainsi que, pour le résultat de Malcev, le volume 37 de l'Encyclopaedia of Mathematical Sciences intitulé "Infinite Groups, Linear Groups", p. 152.

Exercice 7.1.7 (i) Soit Γ un groupe fini. Démontrer que le morphisme $\Gamma \to \Gamma^{alg}$ est injectif. (Utiliser la représentation dans $K[\Gamma]$.)
(ii) Démontrer que ce morphisme est en fait bijectif. (Utiliser le théorème 6.2.3.)

7.1.2 Les groupes de Galois et l'enveloppe proalgébrique

Constructions

Soient $X := (V, \rho)$ un objet de $\mathcal{R}ep_K(\Gamma)$ et $P(s,t) := \sum a_{k,\ell} s^k t^\ell \in \mathbf{N}[s,t]$ un polynôme à coefficients entiers naturels. On pose alors (avec les notations de 6.3.2) :

$$P(X, X^\vee) := \bigoplus \left(T^k(X) \otimes T^\ell(X^\vee)\right)^{\oplus a_{k,\ell}}.$$

(L'exposant $\oplus a_{k,\ell}$ signifie que le terme correspondant figure $a_{k,\ell}$ fois dans la somme directe.) Une *construction* sur X est un sous-quotient[2] d'un tel $P(X, X^\vee)$. Le lemme suivant va alors de soi :

Lemme 7.1.8 *La sous-catégorie pleine de $\mathcal{R}ep_K(\Gamma)$ dont les objets sont les constructions sur X est stable par passage au sous-quotient, et aussi par produit tensoriel et dual.*

□

On la note $< X >$ (parfois $\{\{X\}\}$) et on l'appelle *sous-catégorie tannakienne de $\mathcal{R}ep_K(\Gamma)$ engendrée par X*. C'est donc la plus petite sous-catégorie pleine de $\mathcal{R}ep_K(\Gamma)$ contenant $\underline{1}$ et X et stable par produit tensoriel, dualisation, et passage aux sous-objets et aux quotients. (L'unité $\underline{1}$ est présente comme puissance tensorielle d'exposant 0.) Ainsi, les puissances symétriques et extérieures (remarque 7.1.2) d'une construction sont des constructions. En particulier, les puissances symétriques et extérieures de X sont des constructions.

La restriction $\omega_{|<X>}$ du foncteur oubli ω à la sous-catégorie $< X >$ est encore un foncteur fidèle et $\otimes$-compatible.

Exemples 7.1.9
1. Si Y et Z sont des constructions, $\underline{\mathrm{Hom}}(Y,Z)$ aussi, par identification avec $Y^\vee \otimes Z$. Par exemple, $\underline{\mathrm{End}}(X) \simeq X^\vee \otimes X$ est une construction.
2. Si $X = (V, \rho)$, la représentation "déterminant" $g \mapsto \det \rho(g) \in \mathrm{GL}_1(K)$ s'identifie à la construction $\Lambda^{\dim V}(X)$. La représentation $g \mapsto 1/\det \rho(g)$ est la construction duale de la précédente.
3. Si l'on fait agir G linéairement sur E, pour chaque g, l'automorphisme g de E s'étend en un unique automorphisme d'algèbre de $S^\bullet(E)$. La restriction $g^{(r)}$ au sous-espace $S^r(E)$ est la r^{e} puissance symétrique de la représentation de G dans E. Si, comme dans la remarque 6.3.4, on prend $E = V^*$, on voit que les polynômes homogènes de degré r sur V donnent lieu à une représentation qui est une construction sur X.

Le groupe de Galois tannakien

Définition 7.1.10 Le *groupe de Galois (tannakien) de X* est le groupe $\mathrm{Aut}^\otimes(\omega_{|<X>})$ des automorphismes $\otimes$-compatibles du foncteur $\omega_{|<X>}$. On le notera $\mathrm{Gal}(X)$.

[2] Un sous-quotient d'un objet X est par définition un sous-objet d'un quotient de X. Cela entraine évidemment que c'est un quotient d'un sous-objet, mais la réciproque est fausse.

Un élément de $\mathrm{Gal}(X)$ est une famille $(\phi_Y)_Y$, où Y parcourt les constructions sur X, et soumise aux contraintes habituelles : pour chaque Y, $\phi_Y \in \mathrm{GL}(\omega(Y))$; fonctorialité ; $\otimes$-compatibilité.

Lemme 7.1.11 *On a alors* $\phi_{\underline{1}} = Id_K$ *et* $\phi_{X^\vee} = (\phi_X)^\vee$.

Preuve. - Pour la première égalité, on remarque d'abord que $\underline{1}$ est bien un objet de $< X >$ (puissance tensorielle d'exposant 0) et qu'il est idempotent, donc l'automorphisme $\phi_{\underline{1}}$ de K aussi ($\otimes$-compatibilité).
Pour la seconde égalité, commençons par un peu d'algèbre linéaire (*cf.* par exemple [7, chap. 2]). L'isomorphisme canonique $V^* \otimes V' \to Hom_K(V,V')$ associe à $\pi \otimes v'$ le morphisme $x \mapsto \pi(v)v'$ de V dans V'. En particulier, si $V = V'$, l'antécédent de Id_V par l'isomorphisme $V^* \otimes V \to \mathrm{End}(V)$ se calcule ainsi : on choisit une base arbitraire (e_i) de V, on note (e_i^*) sa base duale ; et l'antécédent recherché est $\sum e_i \otimes e_i^*$. Ce dernier élément est donc indépendant de la base (e_i) choisie. Il donne lieu à un morphisme canonique :

$$\begin{cases} K \to V \otimes_K V^*, \\ 1 \mapsto \sum e_i \otimes e_i^*. \end{cases}$$

Pour tout automorphisme f de V, la base duale de la base (e_i) est la base $\left(f^\vee(e_i^*)\right)$, d'où l'égalité :

$$\sum e_i \otimes e_i^* = \sum f(e_i) \otimes f^\vee(e_i^*).$$

Cette égalité dit que l'élément $\sum e_i \otimes e_i^*$ est laissé invariant par l'automorphisme $f \otimes f^\vee$ de $V \otimes_K V^*$. En particulier, si ρ est une représentation de Γ dans V, cet élément est un point fixe de la représentation $\rho \otimes \rho^\vee$, et induit donc (d'après l'exercice 7.1.1) un morphisme canonique :

$$\underline{1} \to X \otimes X^\vee.$$

Revenant à notre famille $(\phi_Y)_Y$, par fonctorialité et $\otimes$-compatibilité, le morphisme ci-dessus fournit le diagramme commutatif suivant :

$$\begin{array}{ccc} K & \longrightarrow & V \otimes V^* \\ {\scriptstyle \phi_{\underline{1}}}\downarrow & & \downarrow{\scriptstyle \phi_X \otimes \phi_{X^\vee}} \\ K & \longrightarrow & V \otimes V^* \end{array}$$

Comme $\phi_{\underline{1}} = \mathrm{Id}_K$, on est ramené à voir que, si $f \in \mathrm{GL}(V)$ et $g \in \mathrm{GL}(V^*)$ rendent commutatif le diagramme suivant :

$$\begin{array}{ccc} & K & \\ \swarrow & & \searrow \\ V \otimes V^* & \xrightarrow{f \otimes g} & V \otimes V^*, \end{array}$$

alors $g = f^\vee$. Mais, (e_i) désignant une base arbitraire de V et (e_i^*) la base duale de V^*, la base duale de $(f(e_i))$ est $(f^\vee(e_i^*))$ et l'image de $1 \in K$ dans $V \otimes V^*$ est $\sum e_i \otimes e_i^* = \sum f(e_i) \otimes f^\vee(e_i^*)$ (*cf.* [7, chap 2,§4.2]), d'où les égalités :

$$\sum f(e_i) \otimes g(e_i^*) = \sum e_i \otimes e_i^* = \sum f(e_i) \otimes f^\vee(e_i^*) \Longrightarrow \forall i\ ,\ g(e_i^*) = f^\vee(e_i^*).$$

□

En particulier, pour tout $g \in \Gamma$, en posant pour $Y := (W, \sigma)$, $\phi_Y := \sigma(g)$, on définit un élément de $\mathrm{Gal}(X)$; et l'on obtient ainsi un morphisme de Γ dans $\mathrm{Gal}(X)$. Enfin, pour tout élément $(\phi_X)_X$ de $\mathrm{Aut}^{\otimes}(\omega)$, la sous-famille $(\phi_Y)_Y$, où Y parcourt les constructions sur un X fixé est un élément de $\mathrm{Gal}(X)$; et l'on obtient ainsi un morphisme de $\mathrm{Aut}^{\otimes}(\omega)$ dans $\mathrm{Gal}(X)$, d'où enfin un triangle commutatif :

$$\begin{array}{ccc} & & \Gamma^{alg} \\ & \nearrow & \downarrow \\ \Gamma & \longrightarrow & \mathrm{Gal}(X) \end{array}$$

Nous noterons Γ_X l'image de Γ dans $\mathrm{Gal}(X)$.

Une autre façon d'aborder l'étude de $\mathrm{Gal}(X)$ est de regarder la composante de $(\phi_Y)_Y$ en la plus simple des constructions sur X, à savoir X lui-même. Par définition, cette composante ϕ_X est un automorphisme de $\mathrm{GL}(X)$. On a donc une application :

$$\begin{cases} \mathrm{Gal}(X) \to \mathrm{GL}\big(\omega(X)\big), \\ (\phi_Y)_Y \mapsto \phi_X. \end{cases}$$

Cette application est un morphisme de groupes.

Proposition 7.1.12 *Le morphisme $(\phi_Y)_Y \mapsto \phi_X$ de $Gal(X)$ dans $GL\big(\omega(X)\big)$ est injectif.*

Preuve. - En vertu du lemme 7.1.11 et de la $\otimes$-compatibilité, ϕ_X détermine tous les ϕ_Y pour les objets Y de la forme $T^k(X) \otimes T^\ell(X^\vee)$; puis la fonctorialité permet d'étendre cela aux sous-quotients des sommes directes de tels objets. □

Le triangle commutatif précédent s'enrichit donc en un diagramme commutatif :

$$\begin{array}{ccccccc} & & & & \Gamma^{alg} & & \\ & \nearrow & & \swarrow & \downarrow & \searrow & \\ \Gamma & \twoheadrightarrow & \Gamma_X & \hookrightarrow & \mathrm{Gal}(X) & \hookrightarrow & \mathrm{GL}\big(\omega(X)\big) \end{array}$$

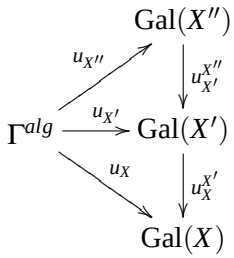
(Injections et surjections respectivement visualisées par $\hookrightarrow$ et $\twoheadrightarrow$.)

Théorème 7.1.13 *L'enveloppe proalgébrique est (en tant que groupe) la limite projective filtrante des groupes de Galois :*

$$\Gamma^{alg} = \varprojlim Gal(X).$$

Preuve. - Nous allons d'abord préciser de quel système projectif il s'agit. Disons que $X \leq X'$ s'il existe un Y tel que $X' = X \oplus Y$. La classe des objets X munie de cette relation n'est pas vraiment un ensemble ordonné : ce n'est pas un ensemble, et la relation est un préordre (elle n'est pas antisymétrique). Pour pallier cela, on pourrait considérer l'ensemble des classes d'équivalence (c'en est bien un !) et la relation d'ordre correspondante (c'en est bien une). Ce n'est pas absolument nécessaire, la notion de système projectif s'étendant sans peine à notre contexte, où les indices sont les objets d'une catégorie (*cf.* par exemple [22, III.4]). Notons que notre catégorie d'indexation est filtrante puisque X et Y sont dominés par $X \oplus Y$.

Lorsque $X \leq X'$, toute construction sur X en est une sur X', donc $< X >$ est une sous-catégorie de $< X' >$ et le foncteur $\omega_{|<X>}$ est la restriction de $\omega_{|<X'>}$ à $< X >$. Tout $\otimes$-automorphisme de $\omega_{|<X'>}$ induit par restriction un $\otimes$-automorphisme de $\omega_{|<X>}$, ce qui nous donne un morphisme de groupes de $\mathrm{Gal}(X')$ dans $\mathrm{Gal}(X)$. Naturellement, si $X' \leq X''$, les morphismes $\mathrm{Gal}(X') \to \mathrm{Gal}(X)$ et $\mathrm{Gal}(X'') \to \mathrm{Gal}(X')$ ont pour composé le morphisme $\mathrm{Gal}(X'') \to \mathrm{Gal}(X)$. On a donc bien, au sens étendu, un système projectif (filtrant) $X \rightsquigarrow \mathrm{Gal}(X)$.
La définition par restriction de ces morphismes de groupes est similaire à celle du morphisme $\Gamma^{alg} \to \mathrm{Gal}(X)$, et l'on a en fait des diagrammes commutatifs :



Dire que ces flèches font de Γ^{alg} la limite projective des $\mathrm{Gal}(X)$, c'est dire que, pour chaque famille d'éléments $\gamma_X \in \mathrm{Gal}(X)$ telle que $u_X^{X'}(\gamma_{X'}) = \gamma_X$ pour tous $X \leq X'$, il existe un unique $\gamma \in \Gamma^{alg}$ tel que $u_X(\gamma) = \gamma_X$ pour tout X.
Pour le voir, on rappelle que, d'après la proposition ci-dessus, chaque $\gamma_X = (\phi_{X,Y})_Y \in \mathrm{Gal}(X)$ est entièrement déterminée par son image $\phi_{X,X} \in \mathrm{GL}\big(\omega(X)\big)$. (Pour être rigoureux, nous avons introduit un premier indice X dans la notation car il y a *a priori* une telle famille pour chaque X.) La condition de compatibilité des γ_X est exactement équivalente au fait que la famille des $\phi_{X,X}$ définit un élément γ de Γ^{alg} ; ce dernier est l'unique antécédent possible pour la famille des γ_X. □

7.2 Les théorèmes de structure

7.2.1 Structure algébrique des groupes de Galois Gal(X)

Notons d'abord que, pour $P \in \mathbf{N}[s,t]$ et pour tout K-espace vectoriel V, on peut définir comme précédemment $P(V,V^*)$; et que tout automorphisme $\phi \in \mathrm{GL}(V)$ définit un automorphisme $P(\phi,\phi^\vee)$ de $P(V,V^*)$. Le lecteur vérifiera que l'on obtient ainsi un morphisme de groupes algébriques[3] :

$$\mathrm{GL}(V) \to \mathrm{GL}\big(P(V,V^*)\big).$$

Pour tout sous-espace $W \subset P(V,V^*)$, on en déduit que les $\phi \in \mathrm{GL}(V)$ dont l'image $P(\phi,\phi^\vee)$ stabilise W (c'est-à-dire le laisse globalement invariant) forment un sous-groupe algébrique de $\mathrm{GL}(V)$. On en tire facilement :

Proposition 7.2.1 *(i) Le morphisme injectif de la proposition 7.1.12 fait de Gal(X) un sous-groupe algébrique de GL$\big(\omega(X)\big)$.*
*(ii) Si $X \leq X'$ (*cf. *la preuve du théorème 7.1.13), le morphisme Gal$(X') \to$ Gal(X) est un morphisme de groupes algébriques.*

[3] Cette construction ne relève pas de la remarque 7.1.2 car $V \rightsquigarrow P(V,V^*)$ n'est pas un foncteur.

□

Pour préciser le lien entre Γ_X et $\mathrm{Gal}(X)$, nous avons besoin d'une nouvelle forme (!) du théorème de Chevalley. Cette dernière repose à son tour sur une meilleure compréhension de la représentation régulière.

Représentation régulière et constructions

Soient V un K-espace vectoriel de dimension finie et G un sous-groupe fermé de $\mathrm{GL}(V)$. Pour tout $P \in \mathbf{N}[s,t]$, on en déduit une représentation rationnelle de G dans $P(V,V^*)$.

D'autre part, G opère à gauche sur son algèbre affine $\mathrm{A}(G)$ par $g \mapsto \rho_g$, où $\rho_g(f) := \big(h \mapsto f(hg)\big)$. (Le lecteur ravivera cette vieille connaissance en vérifiant que l'on a bien une opération à gauche.) Cette action est une représentation localement finie rationnelle.

L'action à droite de G sur lui-même définie par $R_g(h) := hg$ s'étend immédiatement en une action à droite de G sur $\mathrm{GL}(V)$ définie de même pour $g \in G$ et $h \in \mathrm{GL}(V)$. Dualement, l'action à gauche de G sur $\mathrm{A}(G)$ définie par ρ_g se relève le long du morphisme surjectif $\mathrm{A}\big(\mathrm{GL}(V)\big) \to \mathrm{A}(G)$ en une action à gauche de G sur $\mathrm{A}\big(\mathrm{GL}(V)\big)$, que nous noterons encore $g \mapsto \rho_g$, où l'on emploie la même formule $\rho_g(f) := \big(h \mapsto f(hg)\big)$ mais pour $g \in G$ et $f \in \mathrm{A}\big(\mathrm{GL}(V)\big)$. Le morphisme d'algèbres $\mathrm{A}\big(\mathrm{GL}(V)\big) \to \mathrm{A}(G)$ est alors un morphisme de représentations (localement finies).

Lemme 7.2.2 *Soit $V' \subset A(G)$ un sous-espace G-stable de dimension finie (donc une sous-représentation de dimension finie). La représentation de G dans V' est un sous-quotient d'une représentation $P(V,V^*)$, $P \in \mathbf{N}[s,t]$.*

Preuve. - Elle vient de [37, p. 25], dont l'énoncé est cependant plus général. On peut la formuler de manière intrinsèque, mais nous prendrons $V = K^n$ et $G \subset \mathrm{GL}(V) = \mathrm{GL}_n(K)$, de sorte que :

$$\mathrm{A}\big(\mathrm{GL}(V)\big) = \mathrm{A}\big(\mathrm{GL}_n(K)\big) = K[(X_{i,j})_{1\le i,j\le n}]\left[\frac{1}{\det X}\right].$$

On a noté X la matrice $(X_{i,j})$. Si l'on voulait une formulation intrinsèque, on remplacerait les $X_{i,j}$ par des formes linéaires sur $\mathrm{End}(V)$ et l'on écrirait :

$$\mathrm{A}\big(\mathrm{GL}(V)\big) = \mathrm{A}\big(\mathrm{End}(V)\big)[1/\det] = S^\bullet\big((\mathrm{End}V)^*\big)[1/\det].$$

L'algèbre $\mathrm{A}\big(\mathrm{GL}_n(K)\big)$ est la réunion filtrante de ses sous-espaces vectoriels stables de dimension finie :

$$E_{r,s} := \{F/\det{}^t \mid F \in K[(X_{i,j})_{1\le i,j\le n}], \deg F \le r \text{ et } t \le s\}.$$

La représentation correspondante est un quotient du produit tensoriel $E_r \otimes E'_s$, où :

$$E_r := \{F \mid F \in K[(X_{i,j})_{1\le i,j\le n}], \deg F \le r\} \quad \text{et} \quad E'_s := \bigoplus_{t=0}^{s} K\det{}^{-t}.$$

Nous allons étudier chacune de ces deux représentations.
Soit $g := (g_{i,j}) \in G \subset \mathrm{GL}_n(K)$. Son action ρ_g sur $\mathrm{A}\big(\mathrm{GL}_n(K)\big)$ est décrite par les formules :

$$X_{i,j} \mapsto (X.g)_{i,j} = \sum_{k=1}^{n} X_{i,k} g_{k,j},$$
$$\det X \mapsto (\det g) \det X.$$

Notons $E := \mathrm{Vect}(X_{1,1}, \ldots, X_{n,n})$ le sous-espace vectoriel de $K[(X_{i,j})_{1\leq i,j\leq n}]$ engendré par les $X_{i,j}$. En termes intrinsèques, il correspond donc au sous-espace $(\mathrm{End}V)^* = S^1\big((\mathrm{End}V)^*\big)$ de $S^\bullet\big((\mathrm{End}V)^*\big)$. L'espace E est la somme directe des $E_i := \mathrm{Vect}(X_{i,1}, \ldots, X_{i,n})$. Chaque E_i est stable par G et l'action de $g \in G$ sur sa base $(X_{i,1}, \ldots, X_{i,n})$ de E_i est donnée par la matrice g (car $X_{i,j} \mapsto \sum X_{i,k} g_{k,j}$). La représentation correspondante est donc isomorphe à la représentation de G sur V, et l'on a un isomorphisme de représentations $E \simeq V^n$.
Le sous-espace vectoriel des polynômes homogènes de degré r de $K[(X_{i,j})_{1\leq i,j\leq n}]$ est également stable par G, et la sous-représentation correspondante est $S^r(E) \simeq S^r(V^n)$ (remarque 6.3.4 et le troisième des exemples 7.1.9). Nous avons noté E_r le sous-espace des polynômes de degré $\leq r$ et la représentation associée, qui est donc un quotient d'un $Q(V)$, $Q \in \mathbf{N}[s]$.
La représentation E'_s est somme directe des $K\det^{-t}$ pour $t = 0, \ldots, s$. Chaque $K\det^{-t}$ est égale à la puissance tensorielle t^{e} de $K\det^{-1}$, *i.e.*, d'après le deuxième des exemples 7.1.9, du dual de $\Lambda^{\dim V}(X)$ Ainsi, E'_s est un sous-quotient d'un $R(V^*)$, $R \in \mathbf{N}[t]$ et $E_{r,s}$ est un sous-quotient d'un $P(V,V^*)$, $P \in \mathbf{N}[s,t]$.
Comme tout sous-espace de dimension finie de $\mathrm{A}(G)$ est inclus dans l'image par la surjection $\mathrm{A}\big(\mathrm{GL}(V)\big) \to \mathrm{A}(G)$ d'un $E_{r,s}$, le lemme est démontré. □

Remarque 7.2.3 Le rôle du passage au dual est ici clair : il a uniquement servi à inverser le déterminant. L'exercice ci-dessous le confirme.

Exercice 7.2.4 Notons X la représentation $x \mapsto x \in \mathrm{GL}_1(K)$ du groupe K^* dans l'espace vectoriel K. Déterminer tous les sous-quotients des $P(X)$, $P \in \mathbf{N}[s]$. Y trouve-t-on la représentation $x \mapsto x^{-1} \in \mathrm{GL}_1(K)$ (autrement dit, la représentation duale $X^\vee$) ?

Exercice 7.2.5 Reconstituer la démonstration différente du lemme fournie dans [9, p. 40], basée sur l'identification de $\mathrm{GL}(V)$ au fermé de $\mathrm{End}V \times \mathrm{End}V^*$ d'équations $gh^\vee = \mathrm{Id}_V$.

Exercice 7.2.6 Décrire matriciellement l'isomorphisme $S^\bullet(V^* \otimes V) \simeq \mathrm{A}\big(\mathrm{End}(V)\big)$.

Une troisième version du théorème de Chevalley

Soient V un K-espace vectoriel de dimension finie et $H \subset G$ des sous-groupes fermés de $\mathrm{GL}(V)$. On reprend les mêmes notations que précédemment pour les opérations de G sur $\mathrm{A}(G)$ et sur les $P(V,V^*)$.

Théorème 7.2.7 (Chevalley) *Il existe un sous-quotient V' d'une représentation $P(V,V^*)$ de G et un sous-espace $W \subset V'$ tels que G soit le stabilisateur de W dans V' :*

$$H = \{g \in G \mid gW \subset W\} = \{g \in G \mid gW = W\}.$$

Preuve. - Selon la démonstration du théorème 6.3.2, il existe un sous-espace $V' \subset \mathrm{A}(G)$ de dimension finie et stable sous G, et un sous-espace $W \subset V'$ tels que G soit le stabilisateur de W dans V'. Il suffit alors d'appliquer le lemme 7.2.2. □

La forme pratique la plus courante de ce théorème est le critère de densité suivant :

Corollaire 7.2.8 *Soient V un K-espace vectoriel de dimension finie, G un sous-groupe fermé de $GL(V)$ et H un sous-groupe* arbitraire *(pas nécessairement fermé) de G. On suppose que pour tout sous-quotient V' d'une représentation $P(V,V^*)$ de G, tout sous-espace $W \subset V'$ qui est stabilisé par H l'est par G. Alors H est Zariski-dense dans G.*

Preuve. - Il suffit d'invoquer le théorème de Chevalley pour le sous-groupe fermé $\overline{H}$ de G, puis d'appliquer l'hypothèse du corollaire'aux espaces $W \subset V'$ fournis par le théorème. □

Remarque 7.2.9 Comme dans théorème 6.3.8, on peut se ramener au cas où W est une droite.

Application au groupe de Galois

Soit $X := (V,\rho)$ un objet de $\mathcal{R}ep_K(\Gamma)$. On a vu que l'image Γ_X de Γ dans $\mathrm{GL}\big(\omega(X)\big) = \mathrm{GL}(V)$ est incluse dans le sous-groupe fermé $\mathrm{Gal}(X)$ de $\mathrm{GL}(V)$.

Théorème 7.2.10 (de densité) *Le groupe de Galois $Gal(X)$ est l'adhérence de Zariski de Γ_X dans $GL\big(\omega(X)\big)$.*

Preuve. - D'après le critère de densité 7.2.8, il suffit de prouver que pour tout sous-quotient V' d'un $P(V,V^*)$, et pour tout sous-espace $W \subset V'$, si W est stabilisé par Γ_X, *i.e.* par Γ, il l'est par $\mathrm{Gal}(X)$; mais un tel W définit une représentation de Γ et un objet de $< X >$: la propriété à vérifier est donc exactement la définition de $\mathrm{Gal}(X)$. □

Corollaire 7.2.11 *Si $X \leq X'$, le morphisme $Gal(X') \to Gal(X)$ est surjectif.*

Preuve. - Son image contient l'image de $\Gamma_{X'}$, qui est Γ_X ; et elle est fermée (théorème 5.4.4). □

7.2.2 Structure proalgébrique du groupe tannakien Γ^{alg}

Énoncé et conséquences du théorème

Puisque Γ^{alg} est la limite projective d'un système projectif filtrant dont tous les morphismes sont surjectifs, on peut se demander si les morphismes $\Gamma^{alg} \to \mathrm{Gal}(X)$ sont surjectifs. C'est bien le cas, *mais pas pour des raisons ensemblistes* : voir l'annexe A pour un exemple de système projectif filtrant d'ensembles non vides dont toutes les applications sont surjectives et dont la limite projective est vide. Le théorème qui suit est donc un résultat de géométrie algébrique. Sa preuve en est un peu plus fatigante que celle de la plupart des résultats de ce cours, et il faut bien reconnaitre que le langage des schémas en groupes serait ici plus adapté que celui de la géométrie algébrique "élémentaire".

Théorème 7.2.12 *Les morphismes $\Gamma^{alg} \to Gal(X)$ sont surjectifs.*

Avant de démontrer ce théorème, donnons-en des conséquences frappantes. Notons I l'ensemble des classes d'isomorphie d'objets de $\mathcal{R}ep_K(\Gamma)$ (il est ordonné filtrant). Pour chaque $i \in I$, notons $G_i := \mathrm{Gal}(X)$, où X est un objet arbitrairement choisi dans la classe i ; et H_i le noyau du morphisme surjectif de groupes $\Gamma^{alg} \to G_i$. Le premier corollaire est immédiat :

Corollaire 7.2.13 *Le groupe Γ^{alg} admet une famille filtrante décroissante de sous-groupes distingués H_i telle que :*
(i) chaque Γ^{alg}/H_i est muni d'une structure de groupe algébrique ;
(ii) lorsque $H_j \subset H_i$, la projection canonique $\Gamma^{alg}/H_j \to \Gamma^{alg}/H_i$ est un morphisme de groupes algébriques ;
(iii) les projections canoniques $\Gamma^{alg} \to \Gamma^{alg}/H_i$ font du groupe Γ^{alg} la limite projective des groupes Γ^{alg}/H_i.

Par définition, ces propriétés font de Γ^{alg} un *groupe proalgébrique* au sens de [32]. Le corollaire suivant est à peine moins immédiat :

Corollaire 7.2.14 *Tout morphisme de groupes de Γ dans un groupe algébrique G se factorise par $\Gamma \to \Gamma^{alg} \to G$. Cette factorisation est unique si l'on impose de plus au morphisme de groupes $\Gamma^{alg} \to G$ d'être algébrique dans le sens suivant : il se factorise à travers un $\Gamma^{alg} \to \Gamma^{alg}/H_i$ du corollaire précédent.*

On peut alors introduire la catégorie des représentations "rationnelles" de Γ^{alg}, définies comme celles telles que $\Gamma^{alg} \to \mathrm{GL}(V)$ est algébrique dans le sens précédent ; on a alors :

Corollaire 7.2.15 *Le morphisme canonique $\Gamma \to \Gamma^{alg}$ induit une équivalence $\otimes$-compatible de catégories de $\mathcal{R}ep_K(\Gamma)$ avec la catégorie des représentations rationnelles de Γ^{alg}.*

Un groupe proalgébrique est visiblement un objet plus général qu'un groupe algébrique. Pour pouvoir y appliquer les méthodes de la géométrie algébrique, nous allons introduire une K-algèbre qui jouera le rôle d'algèbre affine de ce groupe ; ce sera bien entendu une algèbre de Hopf. Cette K-algèbre de Hopf ne sera pas de type fini (sauf si le groupe est algébrique), mais on verra que c'est une réunion filtrante de K-algèbres de Hopf de type fini, ce qui palliera la difficulté.

Remarque 7.2.16 Nos K-algèbres sont toutes réduites. En levant cette restriction, on arrive au concept général de "schéma en groupes" (affine).

Dualité de Gelfand pour les groupes algébriques

Avant de passer à la démonstration du théorème 7.2.12, nous allons expliquer comment la dualité de Gelfand s'enrichit dans le cas des groupes algébriques affines. Rappelons (page 47) que l'on a noté, pour tout ensemble algébrique affine X d'algèbre affine $A := \mathrm{A}(X)$:

$$\mathcal{X}(A) := \mathcal{X} := \mathrm{Mor}_{\mathcal{A}lg_K}(A, K).$$

L'application $x \in X \mapsto \big(\chi_x : f \mapsto f(x)\big)$ est une bijection $X \to \mathcal{X}$, dont la bijection réciproque associe à $(\chi : A \to K)$ l'unique $x \in X$ tel que $\mathfrak{M}_x = \mathrm{Ker}\,\chi$. Pour tout idéal I de A, le fermé $\mathcal{V}_X(I)$ de

X correspond ainsi à $\mathcal{V}_X(I) := \{\chi \in \mathcal{X} \mid \text{Ker}\,\chi \supset I\}$.

Si l'on note maintenant G un groupe algébrique affine, $A := \mathrm{A}(G)$ est une algèbre de Hopf (section 5.2). Nous noterons respectivement Δ, e, S sa comultiplication, son augmentation et son antipode. Les opérations du groupe G correspondent alors, par la bijection ci-dessus, aux opérations suivantes sur $\mathcal{X} := \mathcal{X}(A)$:

- la multiplication sur $\mathcal{X}$ est donnée par $(\chi, \chi') \mapsto m_K \circ (\chi \otimes \chi') \circ \Delta$, où $m_K : K \otimes K \to K$ est la multiplication ;
- le neutre de $\mathcal{X}$ est l'augmentation e ;
- l'inversion dans $\mathcal{X}$ est donnée par $\chi \mapsto \chi \circ S$.

On obtient ainsi une antiéquivalence entre la catégorie des groupes algébriques affines et la catégorie des algèbres de Hopf commutatives réduites qui sont de type fini sur K. Nous appellerons *affines* ou *algébriques* ces dernières et nous dirons simplement "algèbre de Hopf" pour "algèbre de Hopf commutative réduite" (sans hypothèse de finitude).

Si A est une algèbre de Hopf (commutative réduite) quelconque (*i.e.* pas nécessairement affine), on peut encore définir l'ensemble $\mathcal{X}(A) := \mathrm{Mor}_{\mathcal{A}lg_K}(A, K)$ et le munir de deux structures :

- une structure d'espace topologique dont les fermés sont définis comme les $\mathcal{V}_{\mathcal{X}}(I)$ ci-dessus ;
- une structure de groupe dont les opérations sont encore définies comme ci-dessus.

Les mêmes calculs que dans le cas des groupes algébriques permettent de voir que tout morphisme $A \to B$ d'algèbres de Hopf induit un morphisme de groupes $\mathcal{X}(B) \to \mathcal{X}(A)$ qui est de plus une application continue. De même, si $A \to B$ est injectif, resp. surjectif, alors $\mathcal{X}(B) \to \mathcal{X}(A)$ est une application dominante, resp. une immersion fermée (*i.e.* un isomorphisme avec un fermé de l'espace d'arrivée).

Lemme 7.2.17 *Soient A une algèbre de Hopf et (A_i) une famille de sous-algèbres de Hopf de A telle que $A = \bigcup A_i$. Les morphismes $\mathcal{X}(A) \to \mathcal{X}(A_i)$ induisent un isomorphisme de groupes de $\mathcal{X}(A)$ sur la limite projective des $\mathcal{X}(A_i)$.*

Preuve. - Les $\mathcal{X}(A_i)$ forment un système projectif filtrant et un élément de la limite projective est la donnée d'une famille (f_i) de morphismes $f_i : A_i \to K$, compatibles par restrictions ; ce qui est bien la même chose qu'un morphisme $f : A \to K$, d'où une bijection de $\mathcal{X}(A)$ sur la limite projective des $\mathcal{X}(A_i)$, et même un isomorphisme de groupes, vue la description générale des limites projectives de groupes. (Nous ne nous occupons pas ici de l'aspect topologique afin d'éviter la description de la topologie limite, qui n'est pas une chose simple.) □

Nous allons "réaliser" Γ^{alg} sous la forme $\mathcal{X}(A)$ pour une certaine algèbre de Hopf A obtenue comme réunion filtrante d'algèbres de Hopf affines.

Compléments sur les algèbres de Hopf

Nous dirons qu'une sous-algèbre B d'une algèbre de Hopf A de comultiplication Δ et d'antipode S en est une *sous-algèbre de Hopf* si $S(B) \subset B$ et $\Delta(B) \subset B \otimes B$. (Il n'y a pas de condition imposée sur l'augmentation, elle se réalise automatiquement.)

Lemme 7.2.18 *Si B, C sont des sous-algèbres de Hopf (resp. des sous-algèbres de Hopf affines) de l'algèbre de Hopf A, la sous-algèbre BC qu'elles engendrent l'est aussi.*

Preuve. - Soit $D := BC$. Alors $\Delta^{-1}(D\otimes D)$ est une sous-algèbre de A puisque Δ est un morphisme d'algèbres. Cette sous-algèbre contient $\Delta^{-1}(B\otimes B)$ qui contient B, puisque B est une sous-algèbre de Hopf ; et $\Delta^{-1}(D\otimes D)$ contient de même C, donc $BC = D$, donc $\Delta(D) \subset D\otimes D$. On vérifie de la même manière que $S(D) \subset D$.
Pour la propriété d'être affine, il suffit de remarquer que, si les K-algèbres B et C sont respectivement engendrées par les parties finies E et F, alors BC est engendrée par la partie finie $E\cup F$. □

Lemme 7.2.19 *Toute algèbre de Hopf A est réunion filtrante de sous-algèbres de Hopf affines.*

Preuve. - (On la tire de [37, p. 24].) Grâce au lemme précédent, il suffit, pour tout $v \in A$, de construire une sous-algèbre de Hopf affine B de A contenant v. Soit (a_i) une base de A. Pour tout K-espace vectoriel M, tout élément de $M\otimes A$ admet donc une unique écriture de la forme $\sum m_i \otimes a_i$. Par exemple, prenant $M = A$, on a $\Delta(a_i) = \sum a_{i,j}\otimes a_j$. De même, on peut écrire $\Delta(v) = \sum v_i \otimes a_i$. Notons V le sous-espace vectoriel de A engendré par v et les v_i. Nous allons voir que $\Delta(V) \subset V\otimes A$. Il est clair par construction que $\Delta(v) \in V\otimes A$. Par coassociativité :

$$\sum \Delta(v_i)\otimes a_i = (\Delta\otimes \mathrm{Id}_A)\circ\Delta(v) = (\mathrm{Id}_A\otimes\Delta)\circ\Delta(v) = \sum v_i \otimes \Delta(a_i) = \sum v_i \otimes a_{i,j}\otimes a_j.$$

Par le principe d'unicité ci-dessus appliqué à $M := A\otimes A$:

$$\Delta(v_i) = \sum v_j \otimes a_{j,i} \in V\otimes A,$$

d'où la conclusion. On peut poser $v_0 := v$ et $a_{j,0} := a_j$, de sorte que cette égalité est encore vraie pour $i = 0$.
Considérons maintenant le sous-espace vectoriel U de A engendré par les v_i et les $a_{i,j}$. Un calcul similaire (et laissé au lecteur) permet de voir que $\Delta(U) \subset U\otimes U$. Soit ensuite L le sous-espace vectoriel de A engendré par U et $S(U)$. On voit en appliquant la propriété caractéristique de l'antipode (section 5.2) que $\Delta(L) \subset L\otimes L$ et que $S(L) \subset L$. Les mêmes calculs que dans la démonstration du lemme précédent entrainent que la K-algèbre B engendrée par L est une sous-algèbre de Hopf ; et il est évident qu'elle est affine. □

Ce lemme dit que le groupe $\mathcal{X}(A)$ est limite projective filtrante de groupes algébriques affines. Pour les deux lemmes qui suivent, nous introduirons une terminologie non standard. Nous dirons qu'une extension d'algèbres $B \subset C$ est "fidèle" si, pour tout idéal maximal $\mathfrak{M}$ de B, l'idéal $\mathfrak{M}C$ de C est propre, *i.e.* $\mathfrak{M}C \neq C$, *i.e.* $1 \notin \mathfrak{M}C$. Cette notion est motivée par la notion d'extension "fidèlement plate" en algèbre commutative, et l'on peut d'ailleurs démontrer [37, p. 109] que toute extension d'algèbres de Hopf (sur un corps, mais pas nécessairement réduites) $B \subset C$ est "fidèlement plate" (ce qui renforce le lemme 7.2.21 ci-dessous).

Lemme 7.2.20 *Soit B une sous-algèbre de Hopf de l'algèbre de Hopf C. On suppose que C est une extension fidèle de type fini de B. Alors le morphisme de groupes $\mathcal{X}(C) \to \mathcal{X}(B)$ est surjectif.*

Preuve. - Soit $\chi : B \to K$ un morphisme d'algèbre ; son noyau $\mathfrak{M}$ est un idéal maximal de corps résiduel K. La K-algèbre $C/\mathfrak{M}C = (B/\mathfrak{M})\otimes_B C$ est de type fini sur $K = B/\mathfrak{M}$, et elle est non triviale. D'après le nullstellensatz, il existe un morphisme d'algèbre $C/\mathfrak{M}C \to K$, autrement dit, un morphisme d'algèbre $\chi' : C \to K$ dont le noyau contient $\mathfrak{M}C$. La restriction de χ' à B a donc pour noyau $\mathfrak{M}$, d'où l'on déduit que χ appartient à l'image de $\mathcal{X}(C) \to \mathcal{X}(B)$. □

Lemme 7.2.21 *Soit B une sous-algèbre de Hopf de l'algèbre de Hopf C. Alors C est une extension fidèle de B.*

Preuve. - Soit $\mathfrak{M}$ un idéal maximal de B et supposons que $\mathfrak{M}C = C$. On a donc $1 = \sum m_i c_i$, où les $m_i \in \mathfrak{M}$ et les $c_i \in C$. D'après le lemme 7.2.19, les m_i appartiennent tous à un idéal maximal d'une sous-algèbre de Hopf affine B' de B, et les c_i appartiennent tous à une sous-algèbre de Hopf affine C' de C, dont on peut supposer qu'elle contient B'. L'application $\mathcal{X}(C') \to \mathcal{X}(B')$ est alors un morphisme dominant de groupes *algébriques*, donc surjective d'après le théorème 5.4.4[4]. Mais la relation $1 = \sum m_i c_i$ entraine qu'aucun $\chi \in \mathcal{X}(B')$ dont le noyau contient les m_i (et il en existe) n'est dans l'image, TILT. □

Remarque 7.2.22 Les algèbres de Hopf ont des propriétés beaucoup plus "rigides" que les simples algèbres. Il est par exemple démontré dans [1, th. 4.2.7, p. 180] que toute sous-algèbre de Hopf d'une algèbre de Hopf intègre affine est elle-même affine. L'exercice ci-dessous montre que rien d'équivalent ne se produit pour une simple algèbre. (La propriété de fidèle platitude évoquée plus haut est un autre exemple de cette rigidité.)

Exercice 7.2.23 (i) Soient $A := K + XK[X,Y]$ et $I := XK[X,Y]$. Vérifier que A est une sous-algèbre de $K[X,Y]$, que I en est un idéal maximal de corps résiduel K, que $I^2 = X^2K[X,Y]$ et que le K-espace vectoriel I/I^2 admet pour base les classes des XY^n, donc est de dimension infinie.
(ii) En déduire que I n'est pas un idéal de type fini, que A n'est pas un anneau noetherien, et donc pas une K-algèbre de type fini.

Démonstration du théorème 7.2.12

Preuve. - On notera G_i les $\mathrm{Gal}(X)$ et I l'ensemble ordonné filtrant de leurs indices, *i.e.* les classes d'isomorphie de $\mathcal{R}ep_K(\Gamma)$. Puisque, pour $j > i$, le morphisme $G_j \to G_i$ est surjectif, on peut identifier l'algèbre $A_i := \mathrm{A}(G_i)$ à une sous-algèbre de Hopf de $A_j := \mathrm{A}(G_j)$.

Par dualité de Gelfand (page 97) chaque G_i s'identifie à $\mathcal{X}(A_i) := \mathrm{Mor}_{\mathcal{A}lg_K}(A_i, K)$, donc leur limite projective Γ^{alg} à :

$$\Gamma^{alg} = \varprojlim G_i = \varprojlim \mathrm{Mor}_{\mathcal{A}lg_K}(A_i,K) = \mathrm{Mor}_{\mathcal{A}lg_K}(A,K), \text{ où } A := \varinjlim A_i = \bigcup A_i.$$

Les morphismes $\left(\Delta_i : A_i \to A_i \otimes A_i, e_i : A_i \to K, S_i : A_i \to A_i\right)$ qui font des A_i des algèbres de Hopf (et qui correspondent aux structures de groupes sur les G_i, *cf.* page 97) passent à la limite inductive en des morphismes $\left(\Delta : A \to A \otimes A, e : A \to A, S : A \to K\right)$ qui font de A une algèbre de Hopf et qui fournissent une structure de groupe sur $G := \mathcal{X}(A)$. Ce dernier hérite de plus (par dualité de Gelfand) de la topologie de Zariski. Noter que chaque morphisme $G \to \mathcal{X}(A_i)$ est dominant.
On raisonne en partant de $x_0 \in G_0 := \mathrm{Gal}(X_0)$ (on note ici 0 l'un des indices). Par dualité de Gelfand, ce x_0 correspond à un morphisme d'algèbre $\chi_0 : A_0 \to K$, que l'on veut étendre en $\chi : A \to K$. Pour cela, on considère l'ensemble des couples (A', χ'), où A' est une sous-algèbre de Hopf de A contenant A_0 et où $\chi' : A' \to K$ est un morphisme d'algèbre qui étend χ. On ordonne cet ensemble

[4] C'est ici que l'on voit qu'il s'agit bien de géométrie algébrique et pas simplement d'algèbre !

en posant $(A',\chi') \prec (A'',\chi'')$ si $A' \subset A''$ et si χ'' étend χ'. Cet ensemble est stable par réunion filtrante, donc inductif, et, d'après le lemme de Zorn, il admet donc un élément maximal (A',χ'). Il s'agit de voir que $A' = A$.
Dans le cas contraire, l'une des A_i n'est pas incluse dans A. La sous-algèbre de Hopf $B' := A'A_i$ de A (lemme 7.2.18) contient strictement A', et il suffira d'y étendre χ' pour contredire la maximalité de (A',χ'). Or, l'extension $A' \subset B'$ est fidèle (lemme 7.2.21) et de type fini (parce que A_i est de type fini sur K), et il découle du lemme 7.2.20 que $\mathcal{X}(B') \to \mathcal{X}(A')$ est surjectif, ce qui achève la démonstration. □

7.3 L'enveloppe proalgébrique de Z sur C et ses incarnations

Voici maintenant un exemple non trivial d'enveloppe proalgébrique, qui a de plus le charme de posséder une interprétation topologique.

7.3.1 Rappels et compléments sur $\mathcal{R}ep_{\mathbf{C}}(\mathbf{Z})$

À une représentation (V,ρ) de $\mathbf{Z}$ dans un $\mathbf{C}$-espace vectoriel de dimension finie V, on a associé d'une part le couple (V,ϕ), où $\phi := \rho(1) \in \mathrm{GL}(V)$; et d'autre part le R-module de groupe additif sous-jacent V, où R est l'anneau principal $\mathbf{C}[X,X^{-1}]$ et où la multiplication externe est définie par $P.v := P(\phi)(v)$. On a ainsi obtenu des équivalences de catégories :

$$\mathcal{R}ep_{\mathbf{C}}(\mathbf{Z}) \rightsquigarrow \{\text{couples } (V,\phi)\} \rightsquigarrow \{R\text{-modules de torsion de type fini}\}.$$

Dans la catégorie du milieu, les morphismes de (V,ϕ) dans (V',ϕ') sont les applications linéaires $u : V \to V'$ telles que $\phi' \circ u = u \circ \phi$.

Descriptions de la structure tannakienne

Le foncteur d'oubli ω se décrit ainsi dans chaque catégorie : à un objet (V,ρ) de la première, il associe V ; à un objet (V,ϕ) de la deuxième, il associe V ; à un R-module de torsion de type fini, il associe l'espace vectoriel sous-jacent (donc obtenu par restriction des scalaires de R à $\mathbf{C}$).

Le produit tensoriel et le dual se décrivent très bien dans la première catégorie :

$$(V,\rho)\otimes(V',\rho') = (V\otimes V',\rho\otimes\rho') \text{ et } (V,\rho)^\vee = (V^*,\rho^\vee);$$

et dans la seconde catégorie :

$$(V,\phi)\otimes(V',\phi') = (V\otimes V',\phi\otimes\phi') \text{ et } (V,\phi)^\vee = (V^*,\phi^\vee).$$

Mais ils n'admettent pas de description simple dans la troisième catégorie.

Exercice 7.3.1 Décrire l'unité dans chacune des trois catégories.

Description “axiomatique” du groupe tannakien

Ici, nous préférons la catégorie du milieu. Un élément de $\mathrm{Aut}^{\otimes}(\omega)$ est la donnée, pour tout (V,ϕ), d'un $\overline{\phi} \in \mathrm{GL}(V)$, donnée assujettie aux deux contraintes :

1. Fonctorialité : pour tout $u : V \to V'$ tel que $\phi' \circ u = u \circ \phi$, on a $\overline{\phi'} \circ u = u \circ \overline{\phi}$.
2. $\otimes$-compatibilité : $\overline{\phi \otimes \phi'} = \overline{\phi} \otimes \overline{\phi'}$.

En prenant pour u un isomorphisme dans la première relation, on voit que, si $(V,\phi) \simeq (V',\phi')$, alors $\overline{\phi}$ et $\overline{\phi}$ sont semblables. En prenant (toujours dans la première relation) $(V',\phi') = (V,\phi)$ et $u := \phi$, on voit que :

$$\overline{\phi} \circ \phi = \phi \circ \overline{\phi}.$$

Ces conséquences de la première relation s'appliquent donc à tout élément $(V,\phi) \mapsto \overline{\phi}$ du groupe $\mathrm{Aut}(\omega)$ des automorphismes (non nécessairement tensoriels) de ω.

Exercice 7.3.2 Dans la troisième catégorie, $\overline{\phi}$ est un automorphisme de R-modules.

7.3.2 Calcul de Aut(ω)

Pour commencer, on ne s'occupera pas des conséquences de la contrainte de $\otimes$-compatibilité.

Composante semi-simple

Pour étudier l'effet de l'action de $\mathrm{Aut}(\omega)$ sur les éléments propres, on prendra pour cadre la catégorie des (V,ϕ). On veut décrire au mieux un élément $(V,\phi) \mapsto \overline{\phi}$ de $\mathrm{Aut}(\omega)$. Les conséquences explicitées ci-dessus de la contrainte de fonctorialité s'appliquent donc.

Pour toute droite D, le groupe $\mathrm{GL}(D)$ est canoniquement isomorphe à $\mathbf{C}^*$ et l'on écrira plutôt (D,λ) avec $\lambda \in \mathbf{C}^*$. Soient donc D,D' deux droites et $\lambda,\lambda' \in \mathbf{C}^*$. Pour que les objets (D,λ) et (D',λ') soient isomorphes, il faut, et il suffit, que $\lambda = \lambda'$ (exercice facile et amusant pour le plaisir du lecteur). Si c'est le cas, on a vu que $\overline{\lambda}$ et $\overline{\lambda'}$ sont semblables, autrement dit égaux puisque $\mathbf{C}^*$ est commutatif. On a donc, pour tout élément de $\mathrm{Aut}(\omega)$, une application bien définie $\lambda \mapsto \overline{\lambda}$ de $\mathbf{C}^*$ dans lui-même telle que notre élément de $\mathrm{Aut}(\omega)$ envoie (D,λ) sur $\overline{\lambda}$.

Soit $\phi \in \mathrm{GL}(V)$ et soit λ une valeur propre de ϕ. Notant $x \in V \setminus \{0\}$ un vecteur propre associé à λ, l'égalité $\phi(x) = \lambda x$ dit que l'application $t \mapsto tx$ de $\mathbf{C}$ dans V définit un morphisme de $(\mathbf{C},\lambda)$ dans (V,ϕ). La fonctorialité se traduit alors par la relation $\overline{\phi}(x) = \overline{\lambda}x$. Ainsi, tout vecteur propre de ϕ est un vecteur propre de $\overline{\phi}$.

Le produit $(V \times W, \phi \times \psi)$ est muni de projections p,q qui sont des morphismes vers (V,ϕ) et (W,ψ). Par fonctorialité, on a les relations :

$$p \circ \overline{\phi \times \psi} = \overline{\phi} \circ p \text{ et } q \circ \overline{\phi \times \psi} = \overline{\psi} \circ q,$$

d'où l'on tire :

$$\overline{\phi \times \psi} = \overline{\phi} \times \overline{\psi}.$$

La formation de $\overline{\phi}$ commute donc à la formation de blocs.

Supposons maintenant ϕ semi-simple, de valeurs propres $\lambda_1,\dots,\lambda_n$ et soit $x_1,\dots,x_n$ une base de vecteurs propres associés. On a $V=\bigoplus \mathbf{C}x_i$ et même $(V,\phi)=\bigoplus(\mathbf{C}x_i,\lambda_i)$. On déduit alors de ce qui précède :

$$(V,\overline{\phi})=\bigoplus(\mathbf{C}x_i,\overline{\lambda_i}).$$

En termes matriciels, si $(V,\phi)=(\mathbf{C}^n,S)$ avec $S\in \mathrm{GL}_n(\mathbf{C})$, et si $S=P\,\mathrm{Diag}(\lambda_1,\dots,\lambda_n)P^{-1}$, alors $\overline{S}=P\,\mathrm{Diag}(\overline{\lambda_1},\dots,\overline{\lambda_n})P^{-1}$.

Exercice 7.3.3 Soit γ une application arbitraire de $\mathbf{C}^*$ dans lui-même.
(i) Soit $\phi\in \mathrm{GL}(V)$ semi-simple, de valeurs propres $\lambda_1,\dots,\lambda_n$ et soit $x_1,\dots,x_n$ une base de vecteurs propres associés. Montrer que l'automorphisme de V défini par $x_i\mapsto \gamma(\lambda_i)x_i$ est indépendant du choix de la base de diagonalisation choisie. On le notera $\gamma(\phi)$.
(ii) Soit $S=P\,\mathrm{Diag}(\lambda_1,\dots,\lambda_n)P^{-1}\in \mathrm{GL}_n(\mathbf{C})$ une matrice diagonalisable. Montrer que la matrice $P\,\mathrm{Diag}\big(\gamma(\lambda_1),\dots,\gamma(\lambda_n)\big)P^{-1}$ ne dépend que de S et de γ, et non de la matrice de passage P. On notera $\gamma(S)$ cette matrice.

Composante unipotente

Pour étudier l'effet sur les blocs de Jordan, il sera plus commode d'adopter le point de vue des R-modules. Le bloc de Jordan cyclique de valeur propre $\alpha\in\mathbf{C}^*$ et de taille n est un objet bien défini à isomorphisme près. Le R-module correspondant s'identifie à $R/<\pi_\alpha^n>$, où $\pi_\alpha:=X-\alpha$ est premier dans R. D'après l'exercice 7.3.2, on doit lui associer un automorphisme du R-module $R/<\pi_\alpha^n>$. Ce dernier étant monogène, cet automorphisme est une homothétie de rapport :

$$y_n\in (R/<\pi_\alpha^n>)^*,$$

défini à conjugaison près, donc absolument (c'est-à-dire ne dépendant que de α et n) puisque R est commutatif. Par exemple, pour $n=1$, on retrouve la situation semi-simple vue plus haut et :

$$y_1=\gamma(\alpha)\in\mathbf{C}^*=(R/<\pi_\alpha>)^*.$$

Dans le cas général, la contrainte de fonctorialité appliquée aux surjections canoniques :

$$R/<\pi_\alpha^n>\to R/<\pi_\alpha^{n-1}>$$

entraine que la famille (y_n) est compatible avec ces surjections, donc appartient à la limite projective :

$$\lim_{\leftarrow}(R/<\pi_\alpha^n>)^*=\big(\lim_{\leftarrow}R/<\pi_\alpha^n>\big)^*=\big(\mathbf{C}[[X-\alpha]]\big)^*.$$

On a utilisé l'isomorphisme $\mathbf{C}[X,X^{-1}]/(X-\alpha)^n\simeq\mathbf{C}[X]/(X-\alpha)^n$ (valable pour $\alpha\neq 0$) et l'exemple 2.2.11. Puisque $\big(\mathbf{C}[[X-\alpha]]\big)^*$ code l'effet des éléments de $\mathrm{Aut}(\omega)$ sur les blocs de Jordan de valeur propre α, on obtient :

Théorème 7.3.4 *Le groupe $\mathrm{Aut}(\omega)$ des automorphismes (pas nécessairement $\otimes$-compatibles) du foncteur ω est isomorphe au groupe produit* $\prod_{\alpha\in\mathbf{C}^*}\big(\mathbf{C}[[X-\alpha]]\big)^*$.

Preuve. - Les raisonnements qui précèdent donnent une application injective de $\mathrm{Aut}(\omega)$ dans ce produit. La composition dans $\mathrm{Aut}(\omega)$ se traduit par des compositions d'homothéties, donc des produits de facteurs d'homothétie, ce qui montre que cette application est un morphisme de groupes. Pour la surjectivité, voir l'exercice qui suit. □

Exercice 7.3.5 Étant donné un élément $(\hat{y}_\alpha)$ de $\prod_{\alpha\in\mathbf{C}^*}\left(\mathbf{C}[[X-\alpha]]\right)^*$, décrire son effet $(V,\phi)\to\overline{\phi}$ comme élément de $\mathrm{Aut}(\omega)$ et en déduire que le morphisme ci-dessus est surjectif. Par exemple, l'effet sur les composantes semi-simples est décrit par l'application γ qui, à $\alpha\in\mathbf{C}^*$, associe le terme constant y_1 de $\hat{y}_\alpha\in\left(\mathbf{C}[[X-\alpha]]\right)^*$.

7.3.3 Calcul de $\mathbf{Z}^{alg}=\mathbf{Aut}^{\otimes}(\omega)$

On considère maintenant un élément de $\mathrm{Aut}^{\otimes}(\omega)$, sous sa forme $(V,\phi)\mapsto\overline{\phi}$. Outre la contrainte de fonctorialité, exploitée ci-dessus, il doit satisfaire la contrainte de $\otimes$-compatibilité :

$$\overline{\phi\otimes\phi'}=\overline{\phi}\otimes\overline{\phi'}.$$

Par exemple, le cas de $(\mathbf{C},\lambda)\otimes(\mathbf{C},\mu)$ donne :

$$\overline{\lambda\mu}=\overline{\lambda}\,\overline{\mu},$$

autrement dit, l'application $\gamma:\lambda\mapsto\overline{\lambda}$ est un morphisme de groupes :

$$\gamma\in\mathrm{Hom}_{gr}(\mathbf{C}^*,\mathbf{C}^*).$$

Décrivons les blocs de Jordan sous la forme $(\mathbf{C}^n,\xi_{\lambda,n})$, où :

$$\xi_{\lambda,n}:=\begin{pmatrix}\lambda&1&0&\dots&0\\0&\lambda&1&\dots&0\\0&0&\lambda&\dots&0\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\dots&\lambda\end{pmatrix}.$$

De l'isomorphisme :

$$(\mathbf{C}^n,\xi_{\lambda,n})\simeq(\mathbf{C}^n,\xi_{1,n})\otimes(\mathbf{C},\lambda),$$

on déduit qu'il suffira de déterminer les $\overline{\xi_{1,n}}$. Pour cela, on remarque que sa base canonique $(f_1,\dots,f_n)$ vérifie $\xi_{1,n}(f_i)=f_i+f_{i-1}$ (par convention $f_0=0$). De même, la base canonique $(g_1,\dots,g_{n+1})$ de $\mathbf{C}^{n+1}$ vérifie $\xi_{1,n+1}(g_i)=g_i+g_{i-1}$ et la base canonique (e_1,e_2) de $\mathbf{C}^2$ vérifie $\xi_{1,2}(e_i)=e_i+e_{i-1}$.

Lemme 7.3.6 *Il y a un unique morphisme :*

$$u:(\mathbf{C}^{n+1},\xi_{\lambda,n+1})\to(\mathbf{C}^n,\xi_{1,n})\otimes(\mathbf{C}^2,\xi_{1,2})$$

tel que $u(g_{n+1})=f_n\otimes e_2$, et ce morphisme est injectif.

Preuve. - Puisque $(\mathbf{C}^{n+1},\xi_{\lambda,n+1})$ est cyclique, il suffit de voir que :

$$(\xi_{1,n}\otimes\xi_{1,2}-\mathrm{Id})^p(f_n\otimes e_2)=0\Longleftrightarrow p\geq n+1.$$

Mais on vérifie par récurrence que c'est une combinaison linéaire de $f_i\otimes e_j$ tels que $i+j\leq n+2-p$, les termes tels que $i+j=n+2-p$ ayant des coefficients non nuls. □

On a donc :

$$\left(\overline{\xi_{1,n}} \otimes \overline{\xi_{1,2}}\right) \circ u = u \circ \overline{\xi_{1,n+1}}.$$

On sait déjà que $\overline{\xi_{1,1}} = 1$ (c'est dû au fait que γ est un morphisme de groupes). Comme u est injectif, la connaissance de $\overline{\xi_{1,2}}$ et de $\overline{\xi_{1,n}}$ détermine $\overline{\xi_{1,n+1}}$. Autrement dit, il y a au plus une suite $(\overline{\xi_{1,n}})$ correspondant à un $\overline{\xi_{1,2}}$ donné.

De la suite exacte :

$$0 \to (\mathbf{C}, \xi_{1,1}) \to (\mathbf{C}^2, \xi_{1,2}) \to (\mathbf{C}, \xi_{1,1}) \to 0,$$

on déduit que $\overline{\xi_{1,2}}$ est triangulaire supérieure unipotente :

$$\overline{\xi_{1,2}} = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = \xi_{1,2}^{\lambda}.$$

On vérifie facilement qu'en posant pour tout n :

$$\overline{\xi_{1,n}} := \xi_{1,n}^{\lambda},$$

on définit une suite $\left(\overline{\xi_{1,n}}\right)$ telle que toutes les contraintes (fonctorialité et $\otimes$-compatibilité) sont satisfaites. C'est la seule possible pour un $\lambda \in \mathbf{C}$, donc pour un $\overline{\xi_{1,2}}$ donné. Ainsi, notre élément de $\mathrm{Aut}^{\otimes}(\omega)$ est totalement caractérisé, outre $\gamma \in \mathrm{Hom}_{gr}(\mathbf{C}^*, \mathbf{C}^*)$, par un $\lambda \in \mathbf{C}$.

Théorème 7.3.7 *L'enveloppe proalgébrique de* $\mathbf{Z}$ *est le groupe :*

$$\mathbf{Z}^{alg} = Aut^{\otimes}(\omega) = Hom_{gr}(\mathbf{C}^*, \mathbf{C}^*) \times \mathbf{C}.$$

Preuve. - La bijection résulte de ce qui précède. La multiplication dans $\mathbf{Z}^{alg}$ correspond à la composition des homothéties en ce qui concerne l'effet sur les valeurs propres, comme on l'avait déjà dit en étudiant $\mathrm{Aut}(\omega)$: donc à la multiplication dans $\mathrm{Hom}_{gr}(\mathbf{C}^*, \mathbf{C}^*)$ définie par la structure de groupe de l'ensemble d'arrivée, *i.e.* $(\gamma_1\gamma_2)(\alpha) := \gamma_1(\alpha)\gamma_1(\alpha)$. En ce qui concerne l'effet sur les blocs unipotents, on doit effectuer le produit des $\overline{\xi_{1,2}}$, donc additionner les coefficients λ. □

Exercice 7.3.8 Comment se plonge concrètement le groupe $\mathrm{Aut}^{\otimes}(\omega) = \mathrm{Hom}_{gr}(\mathbf{C}^*, \mathbf{C}^*) \times \mathbf{C}$ dans le groupe $\mathrm{Aut}(\omega) = \prod_{\alpha \in \mathbf{C}^*} \left(\mathbf{C}[[X - \alpha]]\right)^*$?

Incarnation et structure proalgébrique de $\mathbf{Z}^{alg}$

Nous ne faisons ici que synthétiser les conséquence de l'étude précédente, sans détailler les arguments.

Soit $(\gamma, \lambda) \in \mathrm{Hom}_{gr}(\mathbf{C}^*, \mathbf{C}^*) \times \mathbf{C}$ un élément de $\mathbf{Z}^{alg}$. Soit (V, ϕ) un objet associé à une représentation de $\mathbf{Z}$ et soit $\phi = \phi_s\phi_u$ la décomposition de Dunford de $\phi \in \mathrm{GL}(V)$. L'automorphisme $\overline{\phi}$ de V correspondant est alors :

$$\overline{\phi} = \gamma(\phi_s)\phi_u^{\lambda}.$$

(La notation $\gamma(\phi_s)$ a été introduite dans l'exercice 7.3.3.) Ainsi, la représentation $\rho : \mathbf{Z} \to \mathrm{GL}(V)$ qui à n associe ϕ^n donne lieu à la représentation $\mathbf{Z}^{alg} :\to \mathrm{GL}(V)$ qui à (γ, λ) associe $\gamma(\phi_s)\phi_u^{\lambda}$.

On sait *a priori* que le morphisme $\mathbf{Z} \to \mathbf{Z}^{alg}$ détermine une équivalence entre $\mathcal{R}ep_{\mathbf{C}}(\mathbf{Z})$ et la catégorie des représentations rationnelles de $\mathbf{Z}^{alg}$ (au sens de la section 7.2.2). On déduit donc de la description ci-dessus que le morphisme $\mathbf{Z} \to \mathbf{Z}^{alg}$ est donné par :

$$n \mapsto \big((z \mapsto z^n), n\big).$$

Dans une représentation (V, ϕ) donnée, l'effet de l'élément (γ, λ) est trivial si, et seulement si, les valeurs propres de ϕ appartiennent au noyau de γ ; et, soit $\lambda = 0$, soit $\phi_u = \mathrm{Id}_V$. Le groupe de Galois correspondant admet donc comme composante unipotente soit 0 soit $\mathbf{C}$ selon que ϕ est ou non semi-simple ; et comme composante semi-simple $\mathrm{Hom}_{gr}(S, \mathbf{C}^*)$, où S est le sous-groupe de $\mathbf{C}^*$ engendré par les valeurs propres $\lambda_1, \ldots, \lambda_n$ de ϕ. C'est bien un groupe algébrique, que l'on peut identifier au sous-groupe de $(\mathbf{C}^*)^n$ formé par les images de $(\lambda_1, \ldots, \lambda_n)$ par tous les $\gamma \in \mathrm{Hom}_{gr}(\mathbf{C}^*, \mathbf{C}^*)$. Pour une description plus précise, voir l'examen (annexe B). Comme $\mathbf{C}^*$ est la réunion filtrante de ses sous-groupes S de type fini, le groupe proalgébrique $\mathrm{Hom}_{gr}(\mathbf{C}^*, \mathbf{C}^*)$ est la limite projective des groupes algébriques $\mathrm{Hom}_{gr}(S, \mathbf{C}^*)$.

Annexe A

Un exemple bizarre

Objectif. On va construire un système projectif (E_i, f_i^j) d'ensembles et d'applications tel que :
- l'ensemble ordonné I des indices est filtrant ;
- les $f_i^j : E_j \to E_i, j \geq i$ sont surjectifs ;
- notant E la limite projective du système et $f_i : E \to E_i$ ses applications structurales, les f_i ne sont pas surjectifs.

En fait, les E_i seront non vides et leur limite projective E sera vide.

La construction. On prend pour I l'ensemble des parties dénombrables de $\mathbf{R}$, ordonné par inclusion ; il est bien clair qu'il est filtrant. Pour tout $i \in I$, on pose :

$$E_i := \{\phi : i \to \mathbf{R} \mid \phi \text{ est injective d'image discrète}\}.$$

Si $j \geq i$, c'est-à-dire si $i \subset j$, l'application $f_i^j : E_j \to E_i$ est simplement l'application de restriction : en effet, si $\phi : j \to \mathbf{R}$ est injective d'image discrète, c'est *a fortiori* vrai de sa restriction au sous-ensemble i. On vérifie immédiatement qu'aucun E_i n'est vide : il suffit de prendre pour $\phi \in E_i$ une bijection de i sur $\mathbf{N}$.

Pour voir que chaque f_i^j est surjectif, on remarque que, si $\phi : X \to \mathbf{R}$ est injective d'image discrète et si Y est la réunion disjointe de X et de X', ce dernier étant dénombrable, on peut étendre ϕ en $\psi : Y \to \mathbf{R}$ en envoyant X' dans un intervalle ouvert non vide du complémentaire de $\mathrm{Im}\phi$; cela peut être fait de telle sorte que ψ soit injective d'image discrète.

Lemme A.0.9 *La limite projective des E_i est vide.*

Preuve. - Un élément de la limite projective E est une famille (ϕ_i) telle que chaque ϕ_i est injective d'image discrète et telle que, si $i \subset j$, ϕ_i est la restriction de ϕ_j. En comparant i et j quelconques à $i \cup j$, on voit que deux quelconques de ces applications coïncident sur leur domaine commun et définissent donc une application $\phi : \mathbf{R} \to \mathbf{R}$ (puisque les partie dénombrables de $\mathbf{R}$ ont pour réunion $\mathbf{R}$). L'application ϕ est telle que sa restriction à toute partie dénombrable de $\mathbf{R}$ est injective ; elle est donc injective. Elle est aussi telle que l'image de toute partie dénombrable de $\mathbf{R}$ est discrète. Cela implique que $\mathrm{Im}\phi$ est discrète : sinon, une suite d'éléments $\phi(x_n)$ deux à deux distincts aurait une limite $\phi(x)$, et, prenant pour i l'ensemble formé de x et des x_n, on aurait une contradiction. Nous avons donc en fin de compte une partie $\phi(\mathbf{R})$ discrète non dénombrable de $\mathbf{R}$, ce qui n'existe pas. □

Annexe B

Examen de M2 sur “Équations fonctionnelles et représentations des groupes algébriques”, 5 juin 2009

L’épreuve dure quatre heures. L’usage des documents (notes de cours, polycopié) est autorisé.

Dans tout le problème, la lettre K désigne un corps algébriquement clos de caractéristique nulle. On dira abusivement “algébrique” pour “algébrique affine”. Les réponses doivent être justifiées sauf celles pour lesquelles cela est expressément indiqué. Dans chaque section, les premières questions sont élémentaires. *Les questions difficiles sont en italiques.*

Le but du problème est de décrire $\mathbf{Z}^{alg}$, l’enveloppe proalgébrique de $\mathbf{Z}$, par des méthodes directes, c’est-à-dire sans dualité tannakienne.

B.1 Groupes algébriques en dimension 1

1) Soient X un ensemble algébrique affine et $A := A(X)$ son algèbre affine. Soit $f \in A \setminus \{0\}$. On note U l’ouvert affine $\mathcal{D}_X(f) := X \setminus \mathcal{V}_X(f)$. Rappeler sans justification quelle est l’algèbre affine B de U. Démontrer que l’inclusion $U \to X$ est un morphisme d’ensembles algébriques. Quel est son comorphisme ? On prend dorénavant $X := K$ et $U := K^*$. Préciser sans justification ce que sont ici A, f et B. Déterminer les fermés de $X = K$ et ceux de $U = K^*$.

2) Décrire tous les morphismes d’ensembles algébriques $K^* \to K$ et leurs comorphismes $A \to B$. Décrire de même tous les morphismes d’ensembles algébriques $K \to K^*$ et leurs comorphismes $B \to A$.

3) On note $\mathbb{G}_a$ le groupe algébrique $(K, +)$ (“groupe additif”). Déterminer ses sous-groupes fermés. Décrire sans justification le comorphisme $A \to A \otimes A$ de l’addition. On note $\mathbb{G}_m$ le groupe algébrique $(K^*, \times)$ (“groupe multiplicatif”). Déterminer ses sous-groupes fermés. Décrire sans justification le comorphisme $B \to B \otimes B$ de la multiplication.

4) Décrire tous les morphismes de groupes algébriques de $\mathbb{G}_m$ dans $\mathbb{G}_a$ et leurs comorphismes $A \to B$. Décrire de même tous les morphismes de groupes algébriques de $\mathbb{G}_a$ dans $\mathbb{G}_m$ et leurs comorphismes $B \to A$.

B.2 Morphismes de $\mathbb{G}_a$ dans $\mathrm{GL}_n(K)$

1) Soit $U \in \mathrm{GL}_n(K)$ une matrice unipotente. On rappelle que $(U - I_n)^n = 0$. Pour tout $\lambda \in K$, on pose :

$$f(\lambda) := \sum_{k=0}^{n-1} \binom{\lambda}{k} (U - I_n)^k, \quad \text{où } \binom{\lambda}{0} := 1 \text{ et } \binom{\lambda}{k} := \frac{1}{k!} \prod_{0 \le i \le k-1} (\lambda - i).$$

Vérifier que $f(p) = U^p$ pour $p \in \mathbf{N}, p \ge n$, puis que $f(p+q) = f(p)f(q)$ pour $p, q \in \mathbf{N}, p, q \ge n$.

2) En déduire que f définit un morphisme de groupes algébriques de $\mathbb{G}_a$ dans $\mathrm{GL}_n(K)$. On notera $U^\lambda := f(\lambda)$.

3) Montrer que l'adhérence de Zariski de $\{U^p \mid p \in \mathbf{Z}\}$ est le plus petit sous-groupe fermé de $\mathrm{GL}_n(K)$ contenant U. On note $G(U)$ ce groupe.

4) Déduire de ce qui précède et de la question 3 de la première section l'égalité : $G(U) = \{U^\lambda \mid \lambda \in K\}$. Ce groupe algébrique est-il isomorphe au groupe algébrique $\mathbb{G}_a$?

B.3 Caractères d'un groupe algébrique

Pour tout groupe algébrique G, on note $\mathbb{X}(G)$ l'ensemble des morphismes de groupes algébriques de G dans $\mathbb{G}_m$. Les éléments de $\mathbb{X}(G)$ sont appelés *caractères* de G. (Par définition, on a donc $\mathbb{X}(G) \subset A(G)$.)

1) Vérifier qu'en posant $(\chi.\chi')(g) := \chi(g)\chi'(g)$ (autrement dit, la multiplication sur $\mathbb{X}(G)$ est la restriction de celle de $A(G)$), on fait de $\mathbb{X}(G)$ un groupe[1]. Soit H un sous-groupe fermé de G. Vérifier que la surjection canonique $A(G) \to A(H)$ induit un morphisme de groupes $\mathbb{X}(G) \to \mathbb{X}(H)$.

2) On dit que le groupe algébrique G est *multiplicatif* si $\mathbb{X}(G)$ engendre la K-algèbre $A(G)$. Vérifier que cela revient à dire que $\mathbb{X}(G)$ engendre le K-espace vectoriel $A(G)$. Soit H un sous-groupe fermé du groupe multiplicatif G. Montrer H est multiplicatif.

3) Pour tout groupe algébrique G, démontrer que $\mathbb{X}(G)$ est une partie libre de $A(G)$ (théorème d'indépendance linéaire des caractères, de Artin-Dedekind). On pourra pour cela considérer une relation linéaire non triviale la plus courte possible entre les caractères : $L := \sum_{i=1}^{m} \lambda_i \chi_i = 0$, où les χ_i sont deux à deux distincts, puis en tirer une relation plus courte $L(g_0 g) - \chi_1(g_0)L(g)$.

[1] En général, $\mathbb{X}(G)$ *n'est pas* un groupe algébrique.

4) Déduire de la question 3 que, si H est un sous-groupe fermé du groupe algébrique multiplicatif G, le morphisme de groupes $\mathbb{X}(G) \to \mathbb{X}(H)$ est surjectif. Soit alors E le noyau de ce morphisme. Démontrer la formule :

$$H = \{g \in G \mid \forall \chi \in E \ , \ \chi(g) = 1\}.$$

B.4 Groupes multiplicatifs monogènes

1) On note $\mathbb{T}_n$ le groupe algébrique $((K^*)^n, \times)$; autrement dit, $\mathbb{T}_n = (\mathbb{G}_m)^n$. Décrire sans justification son algèbre affine, que l'on notera B_n, et le comorphisme de la multiplication. Pour tout $\lambda := (\lambda_1, \ldots, \lambda_n) \in \mathbf{Z}^n$, on notera $X^\lambda := X_1^{\lambda_1} \cdots X_n^{\lambda_n} \in B_n$. Montrer que $\mathbb{X}(\mathbb{T}_n)$ est l'ensemble des monômes X^λ.

2) À l'aide des résultats de la section précédente, montrer que tout sous-groupe algébrique G de $\mathbb{T}_n$ est multiplicatif et qu'il existe un sous-groupe Λ de $\mathbf{Z}^n$ tel que :

$$G = \{(x_1, \ldots, x_n) \in (K^*)^n \mid \forall \lambda \in \Lambda \ , \ x^\lambda = 1\} = \bigcap_{\lambda \in \Lambda} \mathrm{Ker} X^\lambda.$$ On notera $\mathbb{T}(\Lambda)$ ce groupe.

3) Soit $x := (x_1, \ldots, x_n) \in (K^*)^n$. On note Λ_x le groupe des relations multiplicatives entre les x_i :

$$\Lambda_x := \{\lambda \in \mathbf{Z}^n \mid \prod x_i^{\lambda_i} = 1\}.$$

Démontrer que le plus petit sous-groupe algébrique de $\mathbb{T}_n$ contenant x est $\mathbb{T}(\Lambda_x)$. Ce groupe sera noté $G(x)$. On dit que $y := (y_1, \ldots, y_n) \in (K^*)^n$ est une *réplique* de x si toute relation multiplicative entre les x_i est également satisfaite par les y_i :

$$\forall \lambda \in \mathbf{Z}^n \ , \ \prod x_i^{\lambda_i} = 1 \Longrightarrow \prod y_i^{\lambda_i} = 1.$$

Autrement dit, $\Lambda_x \subset \Lambda_y$. Vérifier que $G(x)$ est l'ensemble des répliques de x.

4) Montrer que les répliques de $x := (x_1, \ldots, x_n) \in (K^*)^n$ sont exactement les $\big(\phi(x_1), \ldots, \phi(x_n)\big)$, où ϕ est un morphisme de groupes de K^* dans lui-même. Pour montrer l'implication difficile, on pourra utiliser le fait[2] *que, Γ étant un groupe arbitraire et $\Gamma' \subset \Gamma$ un sous-groupe, tout morphisme $\Gamma' \to K^*$ s'étend en un morphisme $\Gamma \to K^*$.*

B.5 Groupes monogènes dans $\mathbf{GL}_n(K)$

1) Soit $S \in \mathrm{GL}_n(K)$ une matrice semisimple et soit $f : K \to K$ une application arbitraire. On écrit $S = P\,\mathrm{Diag}(d_1, \ldots, d_n)\,P^{-1}$ et l'on pose $f(S) := P\,\mathrm{Diag}\big(f(d_1), \ldots, f(d_n)\big)\,P^{-1}$. Montrer que cette définition ne dépend pas du choix de la diagonalisation de S.

[2] Ce "fait" vient de ce que le $\mathbf{Z}$-module K^* est *divisible*, donc *injectif*, voir par exemple Lang.

2) On note $Hom_{gr}(K^*,K^*)$ l'ensemble des morphismes de groupes de K^* dans K^*. Déduire de la question 4 de la section précédente que le plus petit sous-groupe algébrique de $\mathrm{GL}_n(K)$ contenant S est :

$$G(S) = \{\phi(S) \mid \phi \in Hom_{gr}(K^*,K^*)\}.$$

3) Soit $A \in GL_n(K)$ et soit $A = A_s A_u$ sa décomposition de Dunford multiplicative. Déduire des sections précédentes l'égalité :

$$G(A) = \{\phi(A_s)A_u^{\lambda} \mid (\phi,\lambda) \in Hom_{gr}(K^*,K^*) \times K\}.$$

En déduire que l'enveloppe proalgébrique $\mathbf{Z}_K^{alg}$ de $\mathbf{Z}$ sur K s'identifie à $Hom_{gr}(K^*,K^*) \times K$. On pourra utiliser le fait que $\mathbf{Z}_K^{alg}$ est la limite projective des groupes $G(A)$, en spécifiant bien le système projectif concerné. Les morphismes $\mathbf{Z}_K^{alg} \to G(A)$ sont-ils surjectifs ?

B.6 Pour se préparer à la deuxième session

Ce qui suit ne fait pas partie de l'examen du vendredi 5 octobre !

1) On note $\mathbb{V}_n$ le groupe algébrique $(K^n,+)$; autrement dit, $\mathbb{V}_n = (\mathbb{G}_a)^n$. Décrire sans justification son algèbre affine, que l'on notera A_n, et le comorphisme de l'addition. Vérifier que tout sous-espace vectoriel de K^n définit un sous-groupe algébrique de $\mathbb{V}_n$.

2) Pour tout $x \in K^n$, montrer que l'application $\lambda \mapsto \lambda x$ définit un morphisme de groupes algébriques de $\mathbb{G}_a$ dans $\mathbb{V}_n$ et en décrire le comorphisme.

3) Soit G un sous-groupe algébrique de $\mathbb{V}_n$. À l'aide de la question précédente et de la question 3 de la première section démontrer que, quelque soit $x \in K^n$, soit $Kx \subset G$, soit $Kx \cap G = \{0\}$. En déduire que $G = \sum_{x \in G} Kx$, puis une réciproque à la question 1.

4) Montrer que tout morphisme de groupes algébriques de $\mathbb{G}_a$ dans $GL_n(K)$ est de la forme $\lambda \mapsto U^{\lambda}$ pour une certaine matrice unipotente U. On pourra trigonaliser simultanément tous les $f(\lambda)$ et utiliser la question 4 de la première section.

Annexe C

Corrigé succinct de l'examen

C.1 Groupes algébriques en dimension 1

1)

Solution :
$B = A[T]/\langle 1 - Tf\rangle = A[1/f] = A_f$.
U s'identifie au fermé $\mathcal{V}_X(1-Tf)$ de $X \times K$ et l'inclusion $U \to X$ à la composée de la seconde projection (qui est un morphisme) avec l'inclusion de ce fermé (qui est un morphisme).
Le comorphisme est donc le composé de $A \to A[T]$ et de $A[T] \to A[T]/\langle 1 - Tf\rangle$, donc le morphisme canonique $A \to A_f$.
$A = K[X]$, $f = X$, $B = K[X, 1/X]$. (On peut aussi prendre pour f n'importe quel cX^m, $c \in K^*$, $m \in \mathbf{N}^*$.)
Tout fermé de K distinct de lui-même est inclus dans un $\mathcal{V}(P)$, $P \in K[X]$ non nul, donc est fini ; réciproquement, tout ensemble fini est fermé (c'est vrai dans tout ensemble algébrique). Les fermés de K sont donc K et ses sous-ensembles finis.
Pour la même raison (avec $P \in K[X, 1/X]$), les fermés de K^* sont K^* et ses sous-ensembles finis.

---

2)

Solution :
Pour décrire un morphisme $K^* \to K$, on part du comorphisme $K[X] \to K[X, 1/X]$ qui est de la forme $\Phi \mapsto \Phi \circ P$, où $P \in K[X, 1/X]$ est quelconque (c'est l'image de X) ; le morphisme correspondant est $x \mapsto P(x)$. (On peut aussi remarquer qu'un morphisme $K^* \to K$ est tout simplement une fonction régulière sur K^* !)
Pour décrire un morphisme $K \to K^*$, on part du comorphisme $K[X, 1/X] \to K[X]$ qui est de la forme $\Phi \mapsto \Phi \circ P$, où $P \in K[X]$ est inversible, donc une constante non nulle arbitraire $a \in K$; le morphisme correspondant est constant $x \mapsto a$.

---

3)

Solution :
Parmi les sous-groupes fermés de $\mathbb{G}_a$, il y a $\{0\}$ et $\mathbb{G}_a$. Tout sous-groupe non trivial est infini (car K est de caractéristique nulle) ; s'il est fermé, c'est donc $\mathbb{G}_a$ d'après la question 2. Les seuls sous-groupes fermés de $\mathbb{G}_a$ sont donc $\{0\}$ et $\mathbb{G}_a$.

Le comorphisme de l'addition est, au choix, $\begin{cases} K[X] \to K[X] \otimes K[X], \\ X \mapsto X \otimes 1 + 1 \otimes X \end{cases}$, ou $\begin{cases} K[X] \to K[X', X''], \\ X \mapsto X' + X'' \end{cases}$.
Parmi les sous-groupes fermés de $\mathbb{G}_m$, il y a $\{1\}$ et $\mathbb{G}_m$. Tout sous-groupe propre fermé est fini (question 2), donc de la forme $\mu_n := \{x \in K \mid x^n = 1\}$ (tous les sous-groupes du groupe multiplicatif d'un corps sont de cette forme, et cycliques). Ces groupes étant finis sont fermés.
Le comorphisme de la multiplication est, au choix, $\begin{cases} K[X, 1/X] \to K[X, 1/X] \otimes K[X, 1/X], \\ X \mapsto X \otimes X \end{cases}$, ou $\begin{cases} K[X] \to K[X', X'', 1/X', 1/X''], \\ X \mapsto X'X'' \end{cases}$.

---

4)

Solution :
Les morphismes de K^* dans K sont de la forme $x \mapsto P(x)$, où $P \in K[X, 1/X]$. Les morphismes de $\mathbb{G}_m$ dans $\mathbb{G}_a$ correspondent aux P tels que $P(xy) = P(x) + P(y)$. La dérivation par rapport à x suivie de $x := 1$ donne $P' = C/X$ ce qui n'est possible que si $C = 0$, donc P constant. Le seul morphisme de $\mathbb{G}_m$ dans $\mathbb{G}_a$ est donc le morphisme trivial et son comorphisme est $P \mapsto P(0)$.
Les morphismes de K dans K^* sont constants ; le seul morphisme de $\mathbb{G}_a$ dans $\mathbb{G}_m$ est donc le morphisme trivial et son comorphisme est $P \mapsto P(1)$.

C.2 Morphismes de $\mathbb{G}_a$ dans $\mathbf{GL}_n(K)$

1)

Solution :
En appliquant la formule du binôme à $\big(I_n + (U - I_n)\big)^p$ et en tenant compte de la nilpotence, on trouve $f(p) = U^p$ pour $p \geq n$.
L'égalité $f(p+q) = f(p)f(q)$ pour $p, q \geq n$ en découle immédiatement.

---

2)

Solution :
La forme de f montre que c'est une fonction polynomiale, donc un morphisme d'ensembles algébriques. Fixons $p \geq n$. Alors les fonctions polynomiales $f(p+\mu)$ et $f(p)f(\mu)$ sont égales pour une infinité de valeurs de $\mu \in K$, donc égales. En réitérant le raisonnement avec p, λ au lieu de q, μ, on obtient l'égalité $f(\lambda + \mu)$ et $f(\lambda)f(\mu)$ pour tous $\lambda, \mu \in K$, d'où la conclusion.

---

3)

Solution :
Soit $\Gamma := \{U^p \mid p \in \mathbf{Z}\}$: c'est un sous-groupe de $\mathrm{GL}_n(K)$, son adhérence est donc un sous-groupe fermé de $\mathrm{GL}_n(K)$ contenant U. Par ailleurs, tout sous-groupe fermé de $\mathrm{GL}_n(K)$ contenant U contient Γ (car sous-groupe) donc son adhérence (car fermé). La conclusion est alors immédiate.

---

4)

Solution :
L'image réciproque $f^{-1}\big(G(U)\big)$ est un sous-groupe fermé de $\mathbb{G}_a$ contenant $\mathbf{Z}$, c'est donc $\mathbb{G}_a$, et $G(U)$ contient $\{U^\lambda \mid \lambda \in K\}$. Mais ce dernier est un sous-groupe fermé de $\mathrm{GL}_n(K)$, car image d'un morphisme de groupes algébriques : c'est donc $G(U)$ par minimalité de celui-ci.
Le noyau de f est égal à $\{0\}$ ou $\mathbb{G}_a$. Dans le premier cas, qui se produit si $U \neq I_n$, on a un isomorphisme de $\mathbb{G}_a$ sur $G(U)$. Dans le deuxième cas, qui se produit si $U = I_n$, on a bien entendu $G(U) = \{I_n\}$.

C.3 Caractères d'un groupe algébrique

1)

Solution :
Il est clair que $\chi\chi' \in A(G)$ et que c'est un morphisme de groupes, donc un élément de $\mathbb{X}(G)$: on a donc bien une loi de composition interne, qui est évidemment associative. L'application constante 1 est le neutre. Il faut vérifier que $\chi^{-1} := (g \mapsto \chi(g)^{-1})$ est dans $\mathbb{X}(G)$, car ce sera alors l'inverse de χ. Mais il est évident que c'est un morphisme de groupes, et c'est aussi un morphisme d'ensembles algébriques comme composé de χ et de l'inversion dans K^*.
L'image de $\chi \in \mathbb{X}(G)$ dans $A(H)$ est un morphisme de groupes donc un élément de $\mathbb{X}(H)$; et la restriction à H est compatible avec la multiplication.

2)

Solution :
Toute partie qui engendre le K-espace vectoriel $A(G)$ engendre *a fortiori* la K-algèbre $A(G)$. Dire que $\mathbb{X}(G)$ engendre la K-algèbre $A(G)$, c'est dire que les produits d'éléments de $\mathbb{X}(G)$ engendrent le K-espace vectoriel $A(G)$; mais ces produits sont eux-mêmes éléments de $\mathbb{X}(G)$.
Puisque $\mathbb{X}(G)$ est une partie génératrice du K-espace vectoriel $A(G)$, son image par l'application linéaire surjective $A(G) \to A(H)$ est une partie génératrice du K-espace vectoriel $A(H)$; mais cette image est contenue dans $\mathbb{X}(H)$, qui est donc également une partie génératrice de $A(H)$.

3)

Solution :
Supposons par l'absurde que $\mathbb{X}(G)$ n'est pas libre. Il existe donc une combinaison linéaire non triviale $L := \sum_{i=1}^{m} \lambda_i \chi_i$, avec $m \geq 1$, tous les $\lambda_i \in K^*$, les $\chi_i \in \mathbb{X}(G)$ deux à deux distincts et telle que $L(g) = 0$ pour tout $g \in G$. On choisit une telle relation avec m minimum. Puisque les χ_i sont non nuls, $m \geq 2$. Soit $g_0 \in G$ tel que $\chi_1(g_0) \neq \chi_m(g_0)$ (possible puisque $\chi_1 \neq \chi_m$). Alors $L(g_0 g) - \chi_m(g_0) L(g) = L'(g)$, où $L' := \sum_{i=1}^{m-1} \big(\chi_i(g_0) - \chi_m(g_0)\big)\lambda_i \chi_i$ est identiquement nul, et fournit donc une relation linéaire du même type que la précédente mais strictement plus courte, TILT.

4)

Solution :
L'image de la base $\mathbb{X}(G)$ de $A(G)$ est incluse dans la base $\mathbb{X}(H)$ de $A(H)$, dont c'est une partie génératrice ; elle est donc égale à $\mathbb{X}(H)$.
Une inclusion est évidente. Pour prouver l'autre, on va démontrer que l'idéal $I_G(H)$ de H dans G est engendré par les $\chi - 1$ avec $\chi \in E$, ce qui suffira évidemment. Soit donc $P \in A(G)$ nul sur H. On écrit P comme combinaison linéaire de caractères, en regroupant ces derniers par classes modulo E, autrement dit, par famille de caractères ayant même restriction à H :

$$P = \sum_{\chi' \in \mathbb{X}(G)} \sum_{\chi \mapsto \chi'} \lambda_\chi \chi. \quad \text{d'où, par restriction à } H : \quad \sum_{\chi' \in \mathbb{X}(G)} \left(\sum_{\chi \mapsto \chi'} \lambda_\chi \right) \chi' = 0.$$

Par indépendance linéaire des caractères de $\mathbb{X}(H)$, on en tire $\sum_{\chi \mapsto \chi'} \lambda_\chi = 0$ pour tout $\chi' \in \mathbb{X}(H)$.
Ainsi, si l'on note $\overline{\chi'} \in \mathbb{X}(G)$ un relèvement arbitraire de chaque $\chi' \in \mathbb{X}(H)$:

$$P = \sum_{\chi' \in \mathbb{X}(G)} \sum_{\chi \mapsto \chi'} \lambda_\chi (\chi - \overline{\chi'}).$$

Il ne reste plus qu'à remarquer que $\chi - \overline{\chi'}$ est de la forme $\overline{\chi'}(\rho - 1)$ avec $\rho \in E$.

C.4 Groupes multiplicatifs monogènes

1)

Solution :
$B_n = K[X_1, \ldots, X_n, 1/X_1, \ldots, 1/X_n]$.
Le comorphisme de la multiplication est, au choix, $X_i \mapsto X_i \otimes X_i$ de $K[X_1, \ldots, X_n, 1/X_1, \ldots, 1/X_n]$ dans $K[X_1, \ldots, X_n, 1/X_1, \ldots, 1/X_n] \otimes K[X_1, \ldots, X_n, 1/X_1, \ldots, 1/X_n]$, ou bien : $X_i \mapsto X_i' X_i''$ de $K[X_1, \ldots, X_n, 1/X_1, \ldots, 1/X_n]$ dans $K[X_1', \ldots, X_n', 1/X_1', \ldots, 1/X_n', X_1'', \ldots, X_n'', 1/X_1'', \ldots, 1/X_n'']$.
Parmi les éléments de $\mathbb{X}(\mathbb{T}_n)$, il y a évidemment les X^λ. Comme ces derniers engendrent $A(\mathbb{T}_n)$, par indépendance linéaire, il n'y a qu'eux.

---

2)

Solution :
Comme on vient de le voir, $\mathbb{X}(\mathbb{T}_n)$ engendre $A(\mathbb{T}_n)$ qui est donc multiplicatif, ainsi que tous ses sous-groupes fermés (question 2 de la section 3).
Remplaçons, dans les notations de la section 3, G par $\mathbb{T}_n$ et H par G. Notant $\Lambda := \{\lambda \in \mathbf{Z}^n \mid X^\lambda \in E\}$ (c'est un sous-groupe de $\mathbf{Z}^n$), on a $E = \{X^\lambda \mid \lambda \in E\}$ donc, d'après la question 4 de la section 3, $G = \mathbb{T}(\Lambda)$.

---

3)

Solution :
On a $x \in \mathbb{T}(\Lambda) \Leftrightarrow \Lambda \subset \Lambda_x$. Les sous-groupes fermés de $\mathbb{T}_n$ contenant x sont donc les $\mathbb{T}(\Lambda)$ tels que $\Lambda \subset \Lambda_x$, et le plus petit est bien $\mathbb{T}(\Lambda_x)$.

Dire que $y \in G(x)$ c'est dire que $y \in \mathbb{T}(\Lambda_x)$, autrement dit (comme ci-dessus), que $\Lambda_x \subset \Lambda_y$, autrement dit, que y est une réplique de x.

---

4)

Solution :
Il est très facile de voir que, si ϕ est un morphisme de groupes de K^* dans lui-même, alors $\big(\phi(x_1),\dots,\phi(x_n)\big)$ est une réplique de $x := (x_1,\dots,x_n) \in (K^*)^n$, puisque $\prod x_i^{\lambda_i} = 1 \Rightarrow \prod \phi(x_i)^{\lambda_i} = \phi\left(\prod x_i^{\lambda_i}\right) = 1$. Réciproquement, soit $y := (y_1,\dots,y_n)$ une réplique de $x := (x_1,\dots,x_n)$. Notant Γ le sous-groupe de K^* engendré par les x_i, on peut définir une application ψ de Γ dans K^* par la formule : $\psi\left(\prod x_i^{\lambda_i}\right) := \prod y_i^{\lambda_i}$. En effet, tout élément de Γ s'écrit sous la forme $\prod x_i^{\lambda_i}$; et s'il s'écrit de deux manières, le résultat est le même parce que y est une réplique de x. Il est immédiat que ψ est un morphisme de groupes. On peut donc le prolonger en $\phi : K^* \to K^*$, qui répond à la question. (Le principe de prolongement invoqué est le lemme 8.2 de III §8 de Lang.)

C.5 Groupes monogènes dans $\mathbf{GL}_n(K)$

Solution :
Personne ne l'ayant abordée, je ne corrige pas ici cette section : elle pourra servir pour la deuxième session. Le corrigé complet du problème figurera dans la version complète du poly (sur ma page web fin juillet).

Bibliographie

[1] **Abe E., 2004.** *Hopf Algebras*, Cambridge Tracts in Mathematics, no 74, Cambridge University Press.

[2] **Ahlfors L., 1979.** *Complex analysis*, McGraw-Hill.

[3] **Anosov D.V. and Bolibrukh A.A., 1994.** *The Riemann-Hilbert Problem, Aspects of Mathematics*, vol. E22, Vieweg.

[4] **Arnold V.I. and Ill'yashenko Yu.S., 1988.** *Ordinary differential equations*, in *Dynamical Systems I*, D.V. Anosov & V.I. Arnold (Eds.), Encyclopaedia of Mathematical Sciences, Vol. 1, Springer Verlag.

[5] **Beauville A., 1993.** Monodromie des systèmes différentiels linéaires à pôles simples sur la sphère de Riemann [d'après A. Bolibruch], Séminaire Bourbaki no 765, Astérisque 216, Société Mathématique de France.

[6] **Borel A., 1991.** *Linear Algebraic Groups*, Graduate Texts in Mathematics 126, Springer Verlag.

[7] **Bourbaki N., 1970.** *Algèbre, chapitres 1 à 3*, Diffusion C.C.L.S.

[8] **Deligne P., 1970.** *Equations différentielles à points singuliers réguliers*, Lecture notes in Mathematics 163, Springer Verlag.

[9] **Deligne P. and Milne J. S., 1982.** *Tannakian categories* in *Hodge Cycles, Motives and Shimura Varieties*, Lecture Notes in Mathematics 900, Springer Verlag.

[10] **Deligne P., 1990.** *Catégories tannakiennes* in *The Grothendieck Festschrift vol. II*, Progress in Mathematics 87, Birkhäuser.

[11] **Demazure M. et Gabriel P., 1970.** *Groupes Algébriques*, Masson et North-Holland.

[12] **Douady R. et Douady A., 2005.** *Algèbre et théories galoisiennes*, Nouvelle bibliothèque mathématique 4, Cassini.

[13] **Godement R., 1964.** *Topologie algébrique et théorie des faisceaux*, Actualités scientifiques et industrielles (*sic*) XIII, Hermann.

[14] **Grothendieck A. et Dieudonné J., 1971.** *Éléments de Géométrie Algébrique I*, Grundlehren der mathematischen Wissenschaften 166, Springer Verlag.

[15] **Jean Giraud.** *Cours de géométrie algébrique*, à paraître dans la collection « Tableau noir », aux éditions Calvage et Mounet.

[16] **Hartshorne R., 1977.** *Algebraic geometry*, Graduate Texts in Mathematics 52, Springer Verlag.

[17] **Hilbert D., 1976.** *Mathematical developments arising from Hilbert problems*, Proceedings of symposia in pure mathematics, vol. XXVIII, part 1 and 2, American Mathematical Society.

[18] **Humphreys J.E., 1975.** *Linear Algebraic Groups*, Graduate Texts in Mathematics 21, Springer Verlag.

[19] **Iwasaki K., Kimura H., Shimomura S. et Yoshida M., 1990.** *From Gauss to Painlevé, Aspects of Mathematics*, vol. E16, Vieweg.

[20] **Kirillov, A., 1974** *Éléments de la théorie des représentations* Éditions Mir.

[21] **Lang S., 1984.** *Algebra (second edition)*, Addison-Wesley.

[22] **Mac Lane S., 1971.** *Categories for the Working Mathematician*, Graduate Texts in Mathematics no 5, Springer Verlag.

[23] **Mneimné R., 2006.** *Réduction des endomorphismes*, Calvage & Mounet.

[24] **Mneimné R. et Testard F., 1986.** *Introduction à la théorie des groupes de Lie classiques*, Hermann.

[25] **Mumford D., 1988.** *The red book of varieties and schemes*, Lecture Notes in Mathematics 1358, Springer Verlag.

[26] **van der Put M. and Singer M.F., 2003.** *Galois theory of linear differential equations*, Springer Verlag.

[27] **Ramis J.-P. et Warusfel A. (sous la direction de), 2009.** *Cours de Mathématiques pures et appliquées L3-M1, vol I*, De Boeck.

[28] **Riemann B., 1968.** *Oeuvres mathématiques*, Librairie Albert Blanchard.

[29] **Riemann B., 1851.** Principes fondamentaux pour une théorie générale des fonctions d'une grandeur variable complexe, *in* [28].

[30] **Riemann B., 1854.** Contribution à la théorie des fonctions représentables par la série de Gauss $F(\alpha,\beta,\gamma;x)$. *in* [28].

[31] **Sauloy J., 2005.** *Équations fonctionnelles analytiques dans le champ complexe*, Cours de DEA 2004-2005, URL `http://www.math.univ-toulouse.fr/~sauloy/`.

[32] **Serre J.-P., 1960.** *Groupes proalgébriques*, Publications Mathématiques de l'I.H.E.S no 7.

[33] **Serre J.-P., 1967.** *Représentations linéaires des groupes finis*, Collection Méthodes, Hermann.

[34] **Serre J.-P., 1970.** *Cours d'arithmétique*, Presses Universitaires de France.

[35] **Shafarevitch I.R., 1970** *Basic Algebraic Geometry*, Grundlehren der mathematischen Wissenschaften 213, Springer Verlag.

[36] **Springer T. A., 1991.** *Linear Algebraic Groups*, Progress in Mathematics 9, Birkhäuser.

[37] **Waterhouse W.C., 1979.** *Introduction to Affine Group Schemes*, Graduate Texts in Mathematics 66, Springer Verlag.

[38] **Whittaker E.T. and Watson G.N., 1927.** *A course of modern analysis*, Cambridge.