Une introduction aux Groupes algébriques

Bernard Le Stum
Université de Rennes 1

Version du 30 mars 2007

Table des matières

Introduction

Un système hamiltonien est un système différentiel de la forme

$$x_i' = \partial H/\partial y_i \qquad y_i' = -\partial H/\partial x_i$$

ou H est ce qu'on appelle l'énergie totale (mouvement d'une toupie par exemple). Liouville avait montré qu'un tel système est intégrable s'il y a « suffisamment d'intégrales premières qui commutent ». A un système différentiel, on peut associer un groupe algébrique, son groupe de Galois (une fois fixée une solution). Le théorème de Ramis et Morales formalise le théorème de Liouville en montrant que le système est intégrable si et seulement si la composante neutre (composante connexe de l'unité) du groupe de Galois est un groupe commutatif. Ce n'est qu'un exemple de l'utilité des groupes algébriques en mathématiques.

Le but de ce cours est de présenter la théorie des groupes algébriques dans un cours de Master. Nous voulons comprendre comment les propriétés géométriques et les propriété algébriques s'interpénètrent. Nous verrons par exemple qu'un groupe affine connexe est résoluble (propriété algébrique) s'il n'a pas de sous-groupe fermé parabolique (propriété géométrique). Mais les notions de groupes réductif ou semi-simple ne seront pas étudiées, pas plus que celle de systèmes de racines. Ce ne serait pas raisonnable dans un cours sans prérequis.

On introduira le vocabulaire de la géométrie algébrique au fur et à mesure qu'il apparaîtra. L'étudiant pourra en parallèle lire la première partie du livre de Hartshorne ([2]). Nous utiliserons le vocabulaire des catégories qui sera introduit progressivement dans le premier chapitre du cours. L'étudiant pourra en parallèle lire le début du livre de Strooker ([6]) par exemple. En fait, on pourrait se limiter aux groupes affines et à leur action sur des variétés quasi-projectives, mais ce cours est aussi aussi un tremplin vers la géométrie algébrique, voire même arithmétique.

L'ouvrage de référence pour ce cours est le livre de Springer ([5]) qui lui même s'inspire de celui de Humphreys ([3]). Il y a aussi le livre de Borel ([1]) et celui de Waterhouse ([7]).

Nous illustrerons nos résultats à l'aide des groupes classiques (spécial, orthogonal, symplectique, etc.). Ceux-ci sont étudiés en détail dans le cours de Jacobson ([4]) par exemple.

1 Définitions

1.1 Le groupe linéaire

Si k est un corps et $n \in N$, on note $\mathbf{GL}_n(k)$ le groupe des matrices carrées inversibles d'ordre n. Si E est un espace vectoriel de dimension finie sur un corps k, on note $\mathbf{GL}(E)$ le groupes des applications linéaires bijectives de E dans E (automorphismes). Si $\dim_k E = n$, on a un isomorphismes de groupes $\mathbf{GL}(E) \simeq \mathbf{GL}_n(k)$ qui correspond au choix d'une base de E. Plus généralement, si A est un anneau commutatif et M un A-module libre de rang n, on définit $\mathbf{GL}_n(A)$ et $\mathbf{GL}(M)$ de la même manière et on a encore $\mathbf{GL}(M) \simeq \mathbf{GL}_n(A)$.

On peut considérer des sous groupes remarquables du *groupe linéaire* $\mathbf{GL}_n$:

- Le *groupe spécial linéaire* $\mathbf{SL}_n$ des matrices à déterminant 1.
- Le groupe $\mathbf{D}_n$ des matrices diagonales inversibles.
- Le groupe $\mathbf{T}_n$ des matrices triangulaires supérieures inversibles.
- Le groupe $\mathbf{U}_n$ des matrices triangulaires supérieures avec des 1 sur la diagonale.

Remarquons dès maintenant que la méthode du pivot de Gauss permet de montrer que $\mathbf{SL}_n(k)$ est engendré par les matrices $I + \lambda \mathbf{1}_{ij}$ avec $\lambda \in k$ avec $(\mathbf{1}_{ij})$ désignant la base canonique de $M_n(k)$ (exercice).

On note $\mathbf{G}_m$ le *groupe multiplicatif* défini par $\mathbf{G}_m(A) := A^*$. Bien sûr, on a tout simplement $\mathbf{G}_m = \mathbf{GL}_1$ et on voit que, plus généralement, $\mathbf{G}_m^n \simeq \mathbf{D}_n$.

On note de même $\mathbf{G}_a$ le *groupe additif* où $\mathbf{G}_a(A)$ n'est autre que le groupe additif de l'anneau A. On a alors un isomorphisme

$$\mathbf{G}_a \simeq \mathbf{U}_2, \quad f \mapsto \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}.$$

Un autre groupe intéressant est le groupe μ_n des racines n-ièmes de l'unité, qui est défini comme le noyau de la puissance n dans $\mathbf{G}_m$. On a donc

$$\mu_n(A) := \{f \in A, \quad f^n = 1\}.$$

On peut remarquer que l'application

$$\mathbf{Z}/n\mathbf{Z} \to \mu_n(\mathbf{C}), \quad r \mapsto e^{2ir\pi/n}$$

est un isomorphisme. Si A est une $\mathbf{C}$-algèbre intègre, on peut généraliser cet isomorphisme en $\mathbf{Z}/n\mathbf{Z} \simeq \mu_n(A)$. Cet isomorphisme est valide plus généralement pour les k-algèbres intègres si la caractéristique de k ne divise pas n mais on a

$$\mu_p(k) = 1 \neq \mathbf{Z}/p\mathbf{Z}$$

si car$k = p$.

On rappelle qu'une *k-algèbre* est tout simplement un anneau A muni d'un morphisme d'anneaux $k \to A$ (nécessairement injectif si $A \neq 0$).

1.2 Le groupe orthogonal et le groupe symplectique

Soit E un espace vectoriel de dimension finie sur k. Une *forme bilinéaire non dégénérée* sur E est une application

$$\begin{aligned} E \times E &\longrightarrow k \\ (v, w) &\longmapsto \langle v, w \rangle \end{aligned}$$

induisant un isomorphisme

$$\begin{aligned} E &\xrightarrow[b]{\simeq} \check{E} \\ v &\longmapsto \langle v, . \rangle \end{aligned}$$

ou $\check{E} := L(E, k)$ est l'espace vectoriel *dual* de E (espace des formes linéaires sur E).

Un morphisme $\phi : E \to E'$ est *compatible* avec des formes bilinéaire non-dégénérées b et b' respectivement si le diagramme

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[d, "b"', "\simeq"] & E' \arrow[d, "b'"', "\simeq"] \\ \check{E} & \check{E}' \arrow[l, "\check{\phi}"] \end{tikzcd} ,$$

ou $\check{\phi} : \check{E}' \to \check{E}$ est l'application duale de ϕ donnée par $\check{\phi}(f')(v) = f'(\phi(v))$, est commutatif, i.e. $\check{\phi} \circ b' \circ \phi = b$. Notons que ϕ est alors nécessairement bijective.

En particulier, un endomorphisme (autrement appelé opérateur) ϕ de E est compatible à une forme bilinéaire non-dégénérée b si et seulement si $\check{\phi} \circ b \circ \phi = b$. Ceux-ci forment un sous-groupe de $\mathbf{GL}(E)$.

Une forme bilinéaire non dégénérée b sur E est dite *alternée* si

$$\forall v \in E, \quad \langle v, v \rangle = 0.$$

On dit alors que (E, b) est un espace *symplectique*. Un opérateur compatible à b est dit *symplectique*. Les opérateurs symplectiques forment donc un groupe $\mathbf{Sp}(E, b)$ appelé *groupe symplectique* de (E, b). On peut montrer que ce groupe est engendré par les *transvections symplectiques*

$$v \mapsto v + c\langle v, u \rangle u$$

avec $c \in k$ et $u \in E$. En fait, si $\dim E = 2n$, on a un isomorphisme

$$\mathbf{Sp}(E) \simeq \mathbf{Sp}_{2n}(k) := \{M \in \mathbf{GL}_{2n}(k), \quad {}^tMJM = J\}$$

avec

$$J := \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

On peut remarquer que cette dernière définition a aussi un sens sur n'importe quel anneau A.

Une forme bilinéaire non dégénérée b sur E est dite *symétrique* si

$$\forall v, w \in E, \quad \langle v, w \rangle = \langle w, v \rangle.$$

Un opérateur compatible à b est dit *orthogonal*. Les opérateurs orthogonaux forment un groupe $\mathbf{O}(E)$ appelé *groupe orthogonal* de E. On peut montrer (théorème de Cartan-Dieudonné) que ce groupe est engendré par les *symétries orthogonales*

$$v \mapsto v - 2\frac{\langle v, u \rangle}{\langle u, u \rangle} u$$

avec $c \in k$ et $u \in E$ (si car $k \neq 2$). Lorsque k est algébriquement clos, si $\dim E = n$, on a un isomorphisme

$$\mathbf{O}(E) \simeq \mathbf{O}_n(k) := \{M \in \mathbf{GL}_n(k), \quad {}^tMM = I\}$$

et on peut remarquer à nouveau que cette dernière définition a aussi un sens sur n'importe quel anneau A.

1.3 Groupes classiques et variétés algébriques

Remarquons tout d'abord que $\mathbf{M}_n$ est un espace affine muni des coordonnées

$$T_{ij} : \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \mapsto a_{ij}.$$

et on a

$$\det = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_i T_{i\sigma(i)}.$$

Il suit que $\mathbf{GL}_n$ est un *ouvert affine* de $\mathbf{M}_n$: par définition, un *fermé (de Zariski)* de $\mathbf{M}_n$ est le lieu des zéros d'une famille de polynômes. Et un *ouvert (de Zariski)* est le complémentaire d'un fermé (de Zariski). Ici, c'est un *ouvert principal*, c'est à dire le complémentaire d'une *hypersurface* (lieu des zéros d'un seul polynôme).

Pour expliquer ce qu'on entend par *affine*, il faut en faire un peu plus. Pour simplifier, on se place sur un corps algébriquement clos k (pour disposer du NullStellenSatz) et on définit une *variété affine* comme la donnée d'un ensemble X, une k-algèbre réduite de type fini $A := A(X)$ et une bijection

$$\begin{array}{ccc} X & \xrightarrow{\simeq} & \mathrm{Hom}_{k-alg}(A, k) \\ x & \longmapsto & \pi_x \end{array}.$$

L'exemple de base est la variété affine $\mathbf{A}_k^n$ définie par

$$X = k^n, \quad A = k[T_1, \dots T_n], \quad (a_1, \dots a_n) \mapsto (P \mapsto P(a_1, \cdots, a_n)).$$

En général, l'isomorphisme $X \simeq \mathrm{Hom}_{k-alg}(A, k)$ induit un accouplement

$$\begin{array}{ccc} A \times X & \longrightarrow & k \\ (f, x) & \longmapsto & f(x) := \pi_x(f) \end{array}.$$

et donc aussi une application, en fait injective, $A \hookrightarrow \mathrm{Hom}_{Ens}(X, k)$ qui permet d'identifier A avec une sous-algèbre de l'algèbre des fonctions sur k.

J'aurais dû rappeler plus tôt qu'un anneau A est *réduit* si $f^n = 0$ implique $f = 0$ et qu'une k algèbre est *de type fini* elle est engendrée par une partie finie (en général, la sous-algèbre *engendrée* par une partie est la plus petite sous-algèbre contenant cette partie). En fait, si A est n'importe quelle k-algèbre réduite, on peut prendre pour X le spectre maximal de A, c'est à dire l'ensemble $\mathrm{Spm}(A)$ des idéaux maximaux de A. En effet, si $\mathfrak{m} \in \mathrm{Spm}A$, l'application canonique $k \to A \to A/\mathfrak{m}$ est un isomorphisme et on prend $\pi_{\mathfrak{m}} : A \to A/\mathfrak{m} \simeq k$.

En général, on munit une variété affine X de sa *topologie de Zariski* pour laquelle les fermés sont les

$$V := V(E) := \{x \in X, \quad \forall f \in E, \quad f(x) = 0\}$$

avec $E \subset A$. Un tel fermé est de manière naturelle une variété affine d'anneau $A(V) := A/I(V)$ ou

$$I = I(Z) := \{f \in A, \quad \forall x \in Z, \quad f(x) = 0\}$$

pour $Z \subset X$. On obtient ainsi une bijection entre les fermés V de X et les idéaux *radicaux* I de A (satisfaisant $f^n \in I \Leftrightarrow f \in I$). Mais les ouverts ne *sont* pas des variétés affines en général, l'exemple le plus simple étant $\mathbf{A}_k^2 \setminus 0$. Mais is E est réduit à un élément f (on dit alors que $V(f)$ est une *hypersurface* d'équation $f = 0$), alors le complémentaire de $V(f)$ est ce qu'on appelle un *ouvert spécial*

$$U := D(f) = \{x \in X, \quad f(x) \neq 0\}.$$

qui *est* affine. On pose alors

$$A(U) = A_f := \{\frac{g}{f^n}, \quad g \in A, \quad n \in \mathbf{N}\} \simeq A[S]/(Sf - 1)$$

et bien sûr

$$\frac{g}{f^n}(x) = \frac{g(x)}{f(x)^n}$$

(vérifier que c'est bien défini !).

On voit donc que $\mathbf{GL}_{n,k}$ est une variété affine d'anneau

$$k[T_{ij}]_{\det} \simeq k[T_{ij}, T]/(S \det -1).$$

De même, on a

- $\mathbf{SL}_{n,k}$ est l'hypersurface de $\mathbf{M}_{n,k}$ d'équation $\det = 1$ et donc d'anneau

$$k[T_{ij}]/(\det -1).$$

- $\mathbf{D}_{n,k}$ est le fermé de $\mathbf{GL}_{n,k}$ défini par $T_{ij} = 0$ pour $i \neq j$ et donc d'anneau

$$k[T_{ij}]_{\det}/(T_{ij})_{i \neq j} \simeq k[T_i, S]/(S \prod T_i - 1).$$

- $\mathbf{T}_{n,k}$ est le fermé de $\mathbf{GL}_{n,k}$ défini par $T_{ij} = 0$ pour $i > j$ et donc d'anneau

$$k[T_{ij}]_{\det}/(T_{ij})_{i>j} \simeq k[(T_{ij})_{i \leq j}, S]/(S \prod T_{ii} - 1).$$

- $\mathbf{U}_{n,k}$ est le fermé de $\mathbf{M}_{n,k}$ défini par $T_{ij} = 0$ pour $i > j$ et $T_{ii} = 1$, donc d'anneau

$$k[T_{ij}]/((T_{ij})_{i>j}, T_{ii} - 1) \simeq k[(T_{ij})_{i<j}].$$

- $\mathbf{Sp}_{2n,k}$ est le fermé de $\mathbf{M}_{2n,k}$ défini par les équations déduites de ${}^tMJM = J$.
- $\mathbf{O}_{n,k}$ est le fermé de $\mathbf{M}_{n,k}$ défini par les équations déduites de ${}^tMM = I$.
- La variété affine sous-jacente à $\mathbf{G}_{m,k}$ n'est autre que la droite affine privée de 0 et son anneau est donc $k[T]_T \simeq k[T, S]/ST - 1$.
- La variété affine sous-jacente à $\mathbf{G}_{a,k}$ n'est autre que la droite affine et son anneau est donc $k[T]$.
- $\mu_{n,k}$ est défini par $T^n = 1$ dans la droite affine et son anneau est donc

$$k[T]/(T^n - 1) \quad (\mathrm{car} k | n).$$

- $\mathbf{Z}/n\mathbf{Z}$ est aussi une variété affine d'anneau $k^n := k \times \cdots \times k$ et plus généralement, si E est un ensemble fini, c'est une variété affine d'anneau $\mathrm{Hom}_{Ens}(E, k)$.

1.4 Groupes algébriques

Toute application $\phi : Y \to X$ entre deux (ensembles sous-jacent de) variétés affines induit un homomorphisme de k-algèbres

$$\begin{aligned} \phi^* : \mathrm{Hom}_{Ens}(X,k) &\longrightarrow \mathrm{Hom}_{Ens}(Y,k) \ . \\ f &\longmapsto f \circ \phi \end{aligned}$$

On dit que ϕ est un *morphisme* si ϕ^* envoie $A := A(X)$ dans $B := A(Y)$ et on note encore $\phi^* : A \to B$ le morphisme induit. Le morphisme ϕ est alors nécessairement continu (pour les topologies de Zariski). Réciproquement, tout homomorphisme de k-algèbres $u : A \to B$ induit une application

$$\phi : X \simeq \mathrm{Hom}_{k-alg}(B,k) \to \mathrm{Hom}_{k-alg}(A,k) \simeq Y$$

donnée par

$$y = \phi(x) \Leftrightarrow \pi_y = \pi_x \circ u$$

et on obtient ainsi une bijection entre les morphismes de variétés affines et les homomorphismes de k-algèbres.

Avant d'aller plus loin, il est peut-être nécessaire de revoir la notion de produit tensoriel. Si R est un anneau commutatif et M, N deux R-modules, leur produit tensoriel est un R-module $M \otimes_A N$ muni d'une application bilinéaire :

$$\begin{aligned} M \times N &\longrightarrow M \otimes_R N \\ (m,n) &\longmapsto m \otimes n \end{aligned}$$

qui factorise de manière unique toutes les application bilinéaire

$$\begin{tikzcd} M \times N \arrow[rr] \arrow[dr] & & P \ . \\ & M \otimes_R N \arrow[ur, dashed] & \end{tikzcd}$$

Par exemple, $R^n \otimes_R R^m \simeq R^{mn}$.

Si A est une R-algèbre commutative et M un R module, alors $A \otimes_R M$ a une structure naturelle de A-module par multiplication à gauche. Il est universel pour les morphismes R-linéaires dans les A-modules :

$$\begin{tikzcd} M \arrow[rr] \arrow[dr] & & N \ . \\ & A \otimes_R N \arrow[ur, dashed] & \end{tikzcd}$$

On a par exemple, $B \otimes A^n \simeq B^n$. Enfin, si B est une autre$R$-algèbre commutative, alors $A \otimes_R B$ a une structure naturelle de R-algèbre commutative par multiplication terme à terme. Celle-ci est universelle pour les applications dans des R-algèbres :

$$\begin{tikzcd} & A \arrow[d] \arrow[ddr] & \\ B \arrow[r] \arrow[drr] & A \otimes_R B \arrow[dr, dashed] & \\ & & C \end{tikzcd} .$$

Par exemple, $A \otimes_R R[T] \simeq A[T]$ et $A \otimes_R B/J \simeq (A \otimes_R B)/(A \otimes_R J)$.

On en déduit immédiatement que si X et Y sont deux variétés affines, alors $X \times Y$ est naturellement muni d'une structure de variété affine avec

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

Attention cependant, la topologie n'est pas la topologie produit !

On voit facilement que l'application

$$\begin{array}{rcl} \mathbf{GL}_{n,k} \times \mathbf{GL}_{n,k} & \xrightarrow{\mu} & \mathbf{GL}_{n,k} \\ (M, N) & \longmapsto & MN \end{array}$$

est un morphisme de variétés affines. Ici, on a évidemment

$$\mu^* : T_{ij} \mapsto \sum_k T_{ik} \otimes_k T_{kj}.$$

De même, l'application

$$\begin{array}{rcl} \mathbf{GL}_{n,k} & \xrightarrow{\sigma} & \mathbf{GL}_{n,k} \\ M & \longmapsto & M^{-1} \end{array}$$

est un morphisme comme on s'en convainc aisément en rappelant que l'on peut écrire

$$M^{-1} = \frac{1}{\det M} {}^t M^*$$

ou M^* est la comatrice de M : ses entrées sont les cofacteurs $m_{ij} := (-1)^{i+j} \det M_{ij}$ ou M_{ij} est le mineur correspondant (la matrice déduite de M en effaçant la i-ème ligne et la j-ème colonne). Enfin, il est bon de noter que l'application

$$\begin{array}{rcl} 0 & \xrightarrow{\epsilon} & \mathbf{GL}_{n,k} \\ 0 & \longmapsto & I \end{array}$$

est aussi un morphisme. L'homomorphisme de k-algèbres correspondant est donnée par l'application de Dirac :

$$\epsilon^* : X_{ij} \mapsto \delta_{ij} := \left\{ \begin{array}{ll} 1 & \text{sit} \quad i = j \\ 0 & \text{sinon} \end{array} \right. .$$

Bien sûr, on a les propriétés analogues pour les sous-groupes de $\mathbf{GL}_{n,k}$ considérés plus haut. On peut aussi considérer de $\mathbf{G}_{a,k}$ qui n'est pas à proprement parler un sous-groupe de $\mathbf{GL}_{n,k}$ même si on peut l'identifier à $\mathbf{U}_{2,k}$. On a alors

$$\mu^*(T) = 1 \otimes T + T \otimes 1, \quad \sigma^*(T) = -T, \quad \epsilon^*(T) = 0.$$

Enfin, on vérifie aisément que si G est un groupe fini, la multiplication, l'inverse et l'unité sont bien des morphismes : toute application entre ensembles finis est un morphisme de variétés algébriques.

La notion de variété affine se généralise en *variété algébrique*. Moralement une variété algébrique est localement une variété affine et un morphisme est localement un morphisme de variétés affines. L'exemple le plus simple est donné par l'espace projectif $\mathbf{P}_k^n$ dont l'espace sous-jacent est $(k^{n+1} \setminus 0)/k^*$. Si on note $T_0, \ldots, T_n$ les coordonnées homogènes associés, on voit que $\mathbf{P}_k^n$ s'obtient en recollant les espaces affines $T_i \neq 0$. Tout ouvert et tout fermé d'une variété algébrique reçoit une structure naturelle de variété algébrique. Une variété algébrique est dite *projective* si elle est (isomorphe à une partie) fermée de $\mathbf{P}_k^n$ et *quasi-projective* si elle est ouverte dans une variété projective.

Dans ce qui suit, on pourra se limiter au cas affine. En d'autres termes, on pourra remplacer partout « algébrique »par « affine ». Ce sera largement suffisant pour ce cours.

Définition 1.4.1 *Soit k un corps algébriquement clos. Un* groupe algébrique *sur k est une variété algébrique G sur k munie d'une structure de groupe telle que la multiplication*

$$\begin{aligned} G \times G &\xrightarrow{\mu} G \\ (g,h) &\longmapsto gh \end{aligned}$$

et l'inversion

$$\begin{aligned} G &\xrightarrow{\sigma} G \\ g &\longmapsto g^{-1} \end{aligned}$$

soient des morphismes de variétés algébriques.

On considérera aussi l'unité

$$\begin{aligned} 0 &\xrightarrow{\epsilon} G \\ 0 &\longmapsto 1 \end{aligned}$$

qui est automatiquement un morphisme.

L'exemple le plus simple de groupe algébrique non affine (mais projectif) est la courbe elliptique d'équation affine $y^2 = x^3 - x$ à laquelle on rajoute la direction verticale comme point à l'infini (l'équation projective est donc $y^2z = x^3 - xz^2$). On en fait un groupe abélien en prenant le point à l'infini comme zéro et demandant que $P + Q + R = 0$ lorsque les points sont alignés (et $2P + R = 0$ si la tangente en P passe aussi par R, et $P + Q = 0$ si la droite (PQ) est verticale).

On peut donner une autre définition équivalente d'un groupe algébrique :

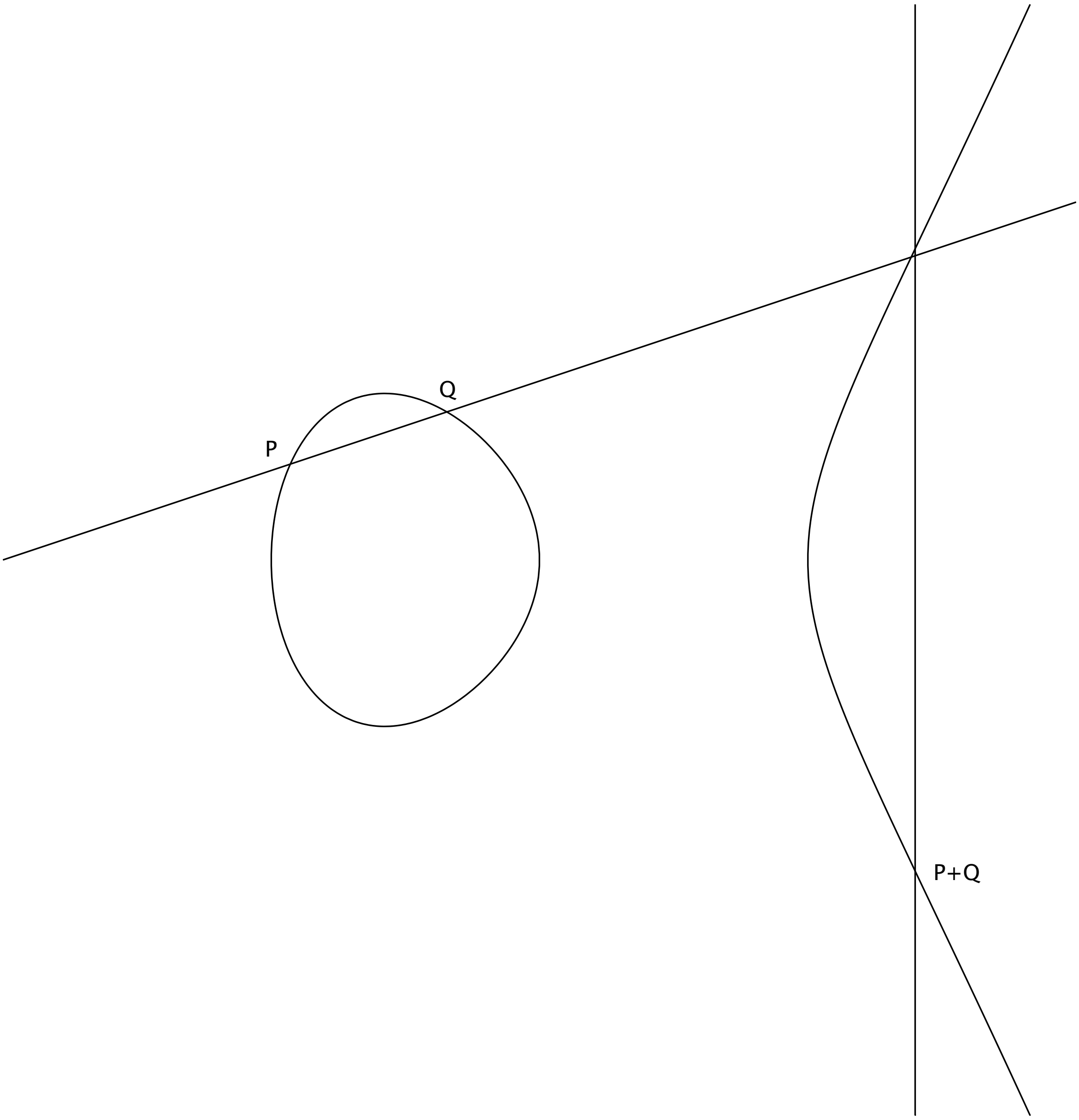

FIG. 1 – La loi de groupe sur une courbe elliptique

Définition 1.4.2 *Un* groupe algébrique *sur k est une variété algébrique G munie de morphismes*

$$\mu : G \times G \to G, \quad \sigma : G \to G, \quad \epsilon : 0 \to G$$

tels que les diagrammes suivants soient commutatifs :

$$\begin{tikzcd} G \times G \times G \arrow[r, "\mu\times \mathrm{Id}_G"] \arrow[d, "\mathrm{Id}_G\times\mu"] & G \times G \arrow[d, "\mu"] \\ G \times G \arrow[r, "\mu"] & G \end{tikzcd}, \qquad \begin{tikzcd} G \arrow[r, "(\epsilon,\mathrm{Id}_G)"] \arrow[dr, equal] & G \times G \arrow[d, "\mu"] \\ & G \end{tikzcd},$$

$$\begin{tikzcd} G \arrow[r, "(\mathrm{Id}_G,\epsilon)"] \arrow[dr, equal] & G \times G \arrow[d, "\mu"] \\ & G \end{tikzcd}, \quad \begin{tikzcd} G \arrow[r, "(\sigma,\mathrm{Id}_G)"] \arrow[d] & G \times G \arrow[d, "\mu"] \\ 0 \arrow[r, "\epsilon"] & G \end{tikzcd}, \quad \begin{tikzcd} G \arrow[r, "(\mathrm{Id}_G,\sigma)"] \arrow[d] & G \times G \arrow[d, "\mu"] \\ 0 \arrow[r, "\epsilon"] & G \end{tikzcd}.$$

Bien sûr, cela signifie que G est muni d'une loi de groupe définie par des morphismes. La commutativité des diagrammes correspond à l'associativité, l'unité et l'inversion. Les deux définitions sont bien équivalentes.

Cette dernière définition se généralise aisément. On rappelle qu'une *catégorie* $\mathcal{C}$ est formée d'*objets* X et de *morphismes* $\phi : Y \to X$ entre ces objets. On dispose de la composition des morphismes qui n'est définie que si le but du premier est identique à la source du second. Cette composition est associative et possède un élément neutre Id_X pour chaque objet X. Si on peu faire des produits finis dans $\mathcal{C}$, on définit alors un *objet en groupe* de $\mathcal{C}$ exactement comme dans la définition 1.4.2.

Par exemple,
- Dans la catégorie des ensembles (et des applications), un objet en groupe est tout simplement ce qu'on appelle un groupe d'habitude. On dira *groupe abstrait.*
- Dans la catégorie des variétés algébriques (et des morphismes de variétés), on obtient justement les groupes algébriques.
- Dans la catégorie des variétés affines, on trouve les groupes affines.
- Dans la catégorie des espaces topologiques (et applications continues), on trouve les groupes topologiques.
- Si on travaille avec les variétés analytiques, on trouve les *groupes de Lie.*

On peut renverser formellement les flèches dans la définition d'un groupe et on trouve alors la notion de *cogroupe* dans une catégorie $\mathcal{C}$ avec sommes finies. Nous allons nous limiter au cas qui nous intéressera par la suite.

Définition 1.4.3 *Une* algèbre de Hopf *est une k-algèbre (réduite de type fini) A munie d' homomorphismes de k-algèbres*

$$\delta : A \to A \otimes_k A, \quad \iota : A \to A, \quad \alpha : A \to k$$

tels que les diagrammes suivants soient commutatifs :

$$\begin{tikzcd} A \arrow[r, "\delta"] \arrow[d, "\delta"] & A \otimes_k A \arrow[d, "\mathrm{Id}_A\otimes_k\delta"] \\ A \otimes_k A \arrow[r, "\delta\otimes\mathrm{Id}A"] & A \otimes_k A \otimes_k A \end{tikzcd}, \qquad \begin{tikzcd} A \arrow[r, "\delta"] \arrow[dr, equal] & A \otimes_k A \arrow[d, "\alpha\otimes\mathrm{Id}_A"] \\ & A \end{tikzcd},$$

$$
\begin{tikzcd}
A \arrow[r, "\delta"] \arrow[dr, equal] & A \otimes_k A \arrow[d, "\mathrm{Id}_A \otimes \alpha"] \\
& A
\end{tikzcd}
,\qquad
\begin{tikzcd}
A \arrow[r, "\alpha"] \arrow[d, "\delta"] & k \arrow[d] \\
A \otimes_k A \arrow[r, "{(\iota, \mathrm{Id}_A)}"] & A
\end{tikzcd}
,\qquad
\begin{tikzcd}
A \arrow[r, "\alpha"] \arrow[d, "\delta"] & k \arrow[d] \\
A \otimes_k A \arrow[r, "{(\mathrm{Id}_A, \iota)}"] & A
\end{tikzcd}
.
$$

Il revient donc au même de se donner une structure de groupe affine sur une variété affine ou une structure d'algèbre de Hopf sur son anneau. En termes savant, on dit qu'on a une équivalence de catégories entre les variétés affines sur k et les k-algèbres réduites de type fini et que celle-ci induit une équivalence entre les groupes d'un coté et les algèbres de Hopf de l'autre.

1.5 Foncteurs en groupes

Nous pouvons donner une troisième définition d'un groupe algébrique :

Définition 1.5.1 *Un groupe algébrique est une variété algébrique G munie pour chaque variété algébrique X, d'une structure de groupe sur*

$$G(X) := \mathrm{Hom}_{VarAlg}(X, G)$$

telle que si $\phi : Y \to X$ est un morphisme de variétés algébriques, alors, l'application induite

$$
\begin{aligned}
G(\phi) : \ G(X) &\longrightarrow G(Y) \\
g &\longmapsto g \circ \phi
\end{aligned}
$$

soit un homomorphisme de groupes.

Bien sûr, la même définition fonctionne avec un objet en groupe dans une catégorie $\mathcal{C}$ qui a des produits finis. On va d'ailleurs vérifier l'équivalence avec la seconde définition dans ce cadre plus général.

Supposons donc donné un objet en groupe G d'une catégorie $\mathcal{C}$ comme dans la définition 1.4.2. Si $X \in \mathcal{C}$, on peut poser poser pour $g, h \in G(X)$,

$$gh : X \xrightarrow{(g,h)} G \times G \xrightarrow{\mu} G\ ,$$

$$1 : X \longrightarrow 0 \xrightarrow{\epsilon} G\ , \qquad g^{-1} : X \xrightarrow{g} G \xrightarrow{\sigma} G\ .$$

On vérifie alors facilement que $G(X)$ est est un groupe et que $G(\phi)$ est un homomorphisme de groupes si $\phi : Y \to X$ est un morphisme de $\mathcal{C}$.

Réciproquement, si on se donne G comme dans la dernière définition, on peut considérer pour tout $X \in \mathcal{C}$, la multiplication

$$
\begin{aligned}
(G \times G)(X) = G(X) \times G(X) &\longrightarrow G(X) \\
(g, h) &\longmapsto gh
\end{aligned}
$$

et l'appliquer au cas particulier $X = G \times G$, ce qui donne un morphisme

$$(G \times G)(G \times G) \longrightarrow G(G \times G)$$

et on note $\mu : G \times G \to G$ l'image de Id_G. De même, on peut considérer pour $X \in \mathcal{C}$, l'unite $1 : X \to G$ et l'appliquer au cas particulier $X = 0$ pour obtenir $\epsilon : 0 \to G$. Enfin, l'inversion

$$\begin{aligned} G(X) &\longrightarrow G(X) \\ g &\longmapsto g^{-1} \end{aligned}$$

appliquée à $X = G$, donne un morphisme $G(G) \to G(G)$ et on note $\sigma : G \to G$ l'image de Id_G. On vérifie aisément que les diagrammes de la définition 1.4.2 sont bien commutatifs.

On a donc maintenant trois définitions équivalentes d'un groupe algébrique. On peut formaliser un peu mieux la troisième en introduisant la notion de foncteur.

Un *foncteur (contravariant)* F entre deux catégories $\mathcal{C}$ et $\mathcal{D}$ associe à tout objet X de $\mathcal{C}$ un object $F(X)$ de $\mathcal{D}$ et à tout morphisme $\phi : Y \to X$ dans $\mathcal{C}$ un morphisme

$$F(\phi) : F(X) \to F(Y)$$

dans $\mathcal{D}$. On demande de plus que les identités et la composition soient préservés. On dit aussi que F est un *préfaisceau* à valeurs dans D. Si on prend pour $\mathcal{D}$ la catégorie des ensembles , groupes, etc., on dit que F est un *foncteur en ensembles, en groupes, etc.*. Enfin, on peut aussi considérer des foncteurs covariants, c'est à dire qui ne changent pas le sens des flèches.

Si Z et un objet de $\mathcal{C}$, on dispose d'un foncteur en ensembles

$$X \mapsto Z(X) := \mathrm{Hom}_{\mathcal{C}}(X, Z).$$

On dit que ce foncteur est *représenté* par Z (plus généralement, un foncteur représentable est un foncteur *équivalent* à un foncteur représenté). Pour les variétés algébriques, on regarde plutôt le foncteur covariant induit sur sur la catégorie des k-algèbres (réduites de type fini) :

$$A \mapsto Z(A) := Z(\mathrm{SpmA}).$$

Par exemple, pour l'espace affine, on a

$$\mathbf{A}^n_k(A) = \mathrm{Hom}_{k-alg}(k[T_i], A) \simeq A^n.$$

et on voit de même que

$$\mathbf{M}_{n,k}(A) = \mathrm{Hom}_{k-alg}(k[T_{ij}], A) \simeq \{(f_{ij}), f_{ij} \in A\}$$

s'identifie bien à l'algèbre des matrices carrées d'ordre n à coefficients dans A.

En général, avec le vocabulaire introduit précédemment, on voit qu'un groupe d'une catégorie (avec produits finis) $\mathcal{C}$ n'est autre qu'un objet de $\mathcal{C}$ qui représente un foncteur en groupes. Dans le cas des variétés algébriques, ça donne :

Définition 1.5.2 *Un groupe algébrique est une variété algébrique qui représente un foncteur en groupes.*

– Bien sûr,

$$\begin{aligned}\mathbf{GL}_{n,k}(A) &= \mathrm{Hom}_{k-alg}(k[T_{ij}]_{\det}, A)\\ &= \{M \in \mathbf{M}_n(A) = \mathrm{Hom}_{k-alg}(k[T_{ij}], A), \quad \det M \in A^*\}\end{aligned}$$

est le groupe des matrices inversibles d'ordre n à coefficients dans A. En général, si E est un espace vectoriel de dimension finie on montre (en choisissant une base) que

$$\mathbf{GL}_k(E)(A) = \mathbf{GL}_A(A \otimes_k E)$$

est le groupe des automorphismes du A-module $A \otimes_k E$.

– De même,
  – $\mathbf{SL}_{n,k}(A) = \{M \in \mathbf{M}_n(A), \quad \det M = 1\}$,
  – $\mathbf{D}_{n,k}(A) = \{(f_1, \ldots, f_n) \in A^n, f_1 \cdots f_n \in A^*\}$,
  – $\mathbf{T}_{n,k}(A) = \{M = [f_{ij}] \in \mathbf{M}_n(A), f_{ij} = 0 \text{ si } i > j \text{ et } f_1 \cdots f_n \in A^*\}$,
  – $\mathbf{U}_{n,k}(A) = \{M = [f_{ij}] \in \mathbf{M}_n(A), f_{ij} = 0 \text{ si } i > j \text{ et } f_{ii} = 1\}$.
– Et bien sûr $\mathbf{Sp}_{2n,k}(A)$ est le sous-groupe des $M \in \mathbf{M}_n(A)$ telles que ${}^tMJM = J$. De même, $\mathbf{O}_{n,k}(A)$ est le sous-groupe des $M \in \mathbf{M}_n(A)$ telles que ${}^tMM = I$.
– On a $\mathbf{G}_{a,k}(A) = A$, $\mathbf{G}_{m,k}(A) = A^*$ et $\mu_{n,k}(A)$ est bien l'ensemble des $f \in A$ tels que $f^n = 1$.
– Enfin, si G est un groupe fini, on a $G(A) = G^{\pi_0(A)}$ ou $\pi_0(A) := \pi_0(X)$ est l'ensemble des composantes connexes de $X := \mathrm{Spm}A$. En fait, comme G est un espace topologique discret fini, on a,

$$\mathrm{Hom}_{VarAlg}(X, G) = \mathrm{Hom}_{cont}(X, G) = G^{\pi_0(X)},$$

Pour finir, il faut dire ce qu'on entend par morphisme de groupes algébriques. On peut donner autant de définitions équivalentes qu'on a de définitions équivalentes de groupes algébriques.

Définition 1.5.3 *Un* morphisme $\Phi : G \to G'$ *entre deux groupes algébriques est (de manière équivalente)*

1. *une application qui est à la fois un homomorphisme de groupe et un morphisme de variétés algébriques.*
2. *un morphisme de variétés algébriques tel que les diagrammes*

$$\begin{tikzcd} G \times G \arrow[r, "\mu"] \arrow[d, "\Phi\times\Phi"] & G \arrow[d, "\Phi"] \\ G' \times G' \arrow[r, "\mu'"] & G' \end{tikzcd}, \quad \begin{tikzcd} G \arrow[r, "\sigma"] \arrow[d, "\Phi"] & G \arrow[d, "\Phi"] \\ G' \arrow[r, "\sigma'"] & G' \end{tikzcd}, \quad \begin{tikzcd} 0 \arrow[r, "\epsilon"] \arrow[d, equal] & G \arrow[d, "\Phi"] \\ 0 \arrow[r, "\epsilon'"] & G' \end{tikzcd}$$

   soient commutatifs.
3. *la donnée, pour toute variété algébrique X sur k, d'un homomorphismes de groupes*

$$\Phi(X) : G(X) \to G'(X)$$

tel que si $\Psi = Y \to X$ *est un morphisme de variétés algébriques, le diagramme*

$$\begin{tikzcd} G(Y) \arrow[r, "G(\Psi)"] \arrow[d, "\Phi(Y)"] & G(X) \arrow[d, "\Phi(X)"] \\ G'(Y) \arrow[r, "G'(\Psi)"] & G'(X) \end{tikzcd}$$

soit commutatif.

4. *Un morphisme entre les faisceaux en groupes représentés.*

La première condition est clairement équivalente à la seconde. Notons aussi que les trois dernières définitions ont un sens dans toute catégorie avec produits. Enfin, il est nécessaire de dire ce qu'est un morphisme entre deux foncteurs $F, F' : \mathcal{C} \to \mathcal{D}$: c'est la donnée, pour tout objet $X \in \mathcal{C}$ d'un morphisme

$$\Phi(X) : F(X) \to F'(X)$$

dans $\mathcal{D}$ tel que si $\Psi = Y \to X$ est un morphisme dans $\mathcal{C}$, le diagramme

$$\begin{tikzcd} F(Y) \arrow[r, "F(\Psi)"] \arrow[d, "\Phi(Y)"] & F(X) \arrow[d, "\Phi(X)"] \\ F'(Y) \arrow[r, "F'(\Psi)"] & F'(X) \end{tikzcd}$$

soit commutatif. On en déduit immédiatement l'équivalence des deux dernières définitions. Il reste à s'assurer que la seconde et la troisième sont équivalentes, ce que je laisserai en exercice. C'est basé sur le *lemme de Yoneda* qui dit que dans une catégorie quelconque $\mathcal{C}$, l'ensemble des morphismes entre deux objets X, Y sont en bijection avec les morphismes entre les foncteurs en ensembles qu'ils représentent.

Comme exemples de morphismes de groupes algébriques, on peut considérer les différentes inclusions de groupes classiques, les isomorphismes qu'on a déjà rencontrés et finalement, le déterminant

$$\det : \mathbf{GL}_{n,k} \to \mathbf{G}_{m,k}.$$

Nous avons utilisé sans vraiment les définir les notions d'isomorphisme et d'équivalence. Dans une catégorie $\mathcal{C}$, un *isomorphisme* est un morphisme qui possède un inverse à droite et à gauche. Une *équivalence* entre deux catégories est un foncteur qui possède un « quasi-inverse »à droite et à gauche.

2 Propriétés élémentaires

2.1 Variétés algébriques

On fixe donc un corps algébriquement clos k et on considère les variétés algébriques (séparées réduites de type fini) sur k. Même si nous sommes essentiellement intéressés par les variétés affines et que nous pouvons facilement nous restreindre au cas quasi-projectif, il vaut mieux traiter le cas général. Et nous n'avons pas encore vraiment dit ce qu'était une variété algébrique.

Tout d'abord, si X est un espace topologique, les ouverts de X forment une catégorie (avec les inclusions comme morphismes). Un *préfaisceau* sur X est un préfaisceau (foncteur contravariant) sur la catégorie des ouverts de X : on a donc pour tout ouvert U un objet $F(U)$ et chaque fois que $V \subset U$, un morphisme de *restriction*

$$\begin{array}{ccc} F(U) & \longrightarrow & F(V) \, . \\ s & \longmapsto & s_{|V} \end{array}$$

Et ces morphismes doivent être compatibles. Notons dès à présent que si U est un ouvert d'un espace topologique X, tout préfaisceau F sur X induit par restriction un préfaisceau $F_{|U}$ sur U.

On dit qu'un préfaisceau F est un faisceau si on a la *propriété de recollement* :

- si $U = \cup_{i \in I} U_i$ est un recouvrement ouvert d'un ouvert de X, et pour tout $i \in I$, $s_i \in F(U_i)$ avec $s_{i|U_i \cap U_j} = s_{j|U_i \cap U_j}$, alors il existe un unique $s \in F(U)$ tel que $s_{|U_i} = s_i$.

Par exemple, si X est une variété affine, il existe un unique faisceau de k-algèbres $\mathcal{O}_X$ sur X valant $A(U)$ si U est un ouvert spécial. On définit une *variété algébrique* comme un espace topologique X muni d'un faisceau de k-algèbres $\mathcal{O}_X$ tel qu'il existe un recouvrement ouvert $X = \cup X_i$ par des variétés affines (avec $\mathcal{O}_{X|U_i} = \mathcal{O}_{U_i}$ pour tout i). On dit que c'est une *carte affine*. On demandera en plus que le recouvrement soit fini et que les $X_i \cap X_j$ soient aussi affine.

Notons que toute partie localement fermée (intersection d'ouverts et de fermés) Y d'une variété algébrique X hérite naturellement d'une structure de variété algébrique. On dit que c'est une *sous-variété*.

Il faut aussi dire ce que l'on entend par morphisme entre deux variétés $\phi : Y \to X$. Le plus simple ici est de demander qu'il existe des cartes affines $X = \cup X_i$ et $Y = \cup Y_i$ telles que $\phi(Y_i) \subset X_i$ et les applications induites $Y_i \mapsto X_i$ sont des morphismes de variétés affines. Le morphisme ϕ est alors automatiquement continu.

2.2 Composantes connexes

On peut voir dès maintenant comment des propriétés géométriques et même topologiques (composantes connexes) des groupes algébriques influencent les propriétés algébriques (sous-groupe distingué).

Rappelons qu'un sous-groupe qui est aussi une sous-variété, par exemple, un sous-groupe fermé, d'un groupe algébrique est nécessairement aussi un groupe algébrique.

Proposition 2.2.1 *Si G est un groupe algébrique, la composante connexe G° de G contenant* 1 *est le plus petit sous-groupe fermé (donc algébrique) de G d'indice fini. Il est distingué dans G et irréductible.*

On rappelle qu'un sous-groupe est *distingué* si les classes à droites sont égales aux classes à gauche et qu'un espace topologique X est *irréductible* s'il est non vide et si tout ouvert non vide est dense. On rappelle aussi qu'il est dit *connexe* si $\emptyset$ et X sont ses seuls ouverts fermés. Nous aurons besoin des résultats suivants :
- Tout espace topologique irréductible est connexe.
- Si $\phi : Y \to X$ est une application continue, l'image d'une partie irréductible est irréductible. Et de même pour connexe.
- Toute variété algébrique est réunion finie de ses sous-variétés irréductibles maximales (composantes irréductibles). Et de même pour connexe.
- Si X et Y sont deux variétés irréductibles, $X \times Y$ (qui n'a pas la topologie produit) est aussi irréductible. Et idem pour connexe.

Remarquons qu'un espace affine X est irréductible si et seulement si $A(X)$ est intègre. On en déduit facilement qu'en général, les fermés irréductibles sont en bijection avec les idéaux premiers. On peut aussi voir que $\mathrm{Spm}A$ est connexe si et seulement si 0 et 1 sont les seuls *idempotents* (satisfaisant $f^2 = f$). Remarquons enfin que les composantes irréductibles (ou connexes) sont permutées par les automorphismes.

On utilisera les notations suivantes pour les parties d'un groupe algébrique G avec multiplication μ, et inversion σ :

$$XY = \mu(X \times Y), \quad X^{-1} = \sigma(X) \quad \text{et} \quad gX = t_g(X)$$

ou t_g est la translation à gauche par $g \in G$. C'est un morphisme de variétés algébriques car c'est la composée

$$t_g : G \xrightarrow{(g,\mathrm{Id}_G)} G \times G \xrightarrow{\mu} G\,.$$

On utilisera aussi la translation à droite. Revenons maintenant à notre proposition.

Démonstration : Tout d'abord, soient X et Y deux composantes irréductibles de G contenant 1. Comme X et Y sont irréductibles, on voit que $X \times Y$ est irréductible et il en va donc de même de XY. Puisque X et Y passent par 1, on a $X, Y \subset XY$ et, par maximalité, on voit que $X = Y = XY$. Il suit qu'il existe une unique composante irréductible X contenant 1. Comme σ est un automorphisme, X^{-1} est aussi une composante irréductible de G et $1 \in X^{-1}$. Il suit que $XX^{-1} = X$. On voit donc que X est un sous-groupe. Et celui-ci est fermé (car une composante irréductible est obligatoirement fermée) de G.

Ensuite, pour tout $g \in G$, gX est une composante irréductible de G (car t_g est un automorphisme) et G est somme disjointe des différents gX. Ceux-ci sont donc en nombre finis et ce sont des fermés ouverts (car leur complémentaire est fermé comme union finie de fermés). Il suit que $X = G^\circ$ et que G° est d'indice fini dans G.

Maintenant, si H est un sous-groupe fermé d'indice fini dans G, alors G est somme disjointe d'un nombre fini de gH qui sont nécessairement fermés et donc aussi ouverts. En particulier, H est ouvert et fermé et contient 1. On a donc $H \supset G^\circ$.

Finalement, si $g \in G$, alors $gG^\circ g^{-1}$ est aussi une composante irréductible qui contient 1 et on a donc nécessairement $G^\circ = gG^\circ g^{-1}$ qui est bien distingué. $\surd$

Définition 2.2.2 *On dit alors que G° est la* composante neutre *de G et que le groupe fini $\Phi := G/G^\circ$ est le* groupe des composantes connexes.

On voit en particulier qu'un groupe connexe est automatiquement irréductible. En général, on a une suite exacte de groupes

$$1 \longrightarrow G^\circ \longrightarrow G \longrightarrow \Phi \longrightarrow 1$$

avec G° connexe et Φ fini. C'est notre premier *dévissage* : on réduit ainsi l'étude des groupes algébriques à l'étude des groupes algébriques connexes et celle des groupes finis.

On va traiter quelques exemples. On rappelle que la *dimension de Krull* d'une variété algébrique est la longueur maximale n d'une suite strictement croissante

$$X_0 \subsetneq X_2 \subsetneq \cdots \subsetneq X_n$$

de fermés irréductibles. On a alors

- Tout ouvert dense à même dimension que la variété ambiante.
- La dimension d'un produit est la somme des dimensions.

Par exemple, il est clair qu'une variété finie est de dimension nulle. Plus sérieusement, $\mathbf{A}^1_k$ est de irréductible dimension 1 car $k[T]$ est principal. On en déduit que

$$\mathbf{A}^n_k = \mathbf{A}^1_k \times \cdots \times \mathbf{A}^1_k$$

est irréductible de dimension n et donc que $\mathbf{M}_{n,k}$ est irréductible de dimension n^2. Et il suit que $\mathbf{G}L_{n,k}$, qui est un ouvert non-vide et donc dense de $\mathbf{M}_{n,k}$ est un groupe algébrique connexe de dimension n^2.

On montre facilement que
- $\mathbf{D}_{n,k}$ est un groupe algébrique connexe de dimension n
- $\mathbf{T}_{n,k}$ est un groupe algébrique connexe de dimension $n(n+1)/2$
- $\mathbf{U}_{n,k}$ est un groupe algébrique connexe de dimension $n(n-1)/2$
- $\mathbf{G}_{a,k}$ est un groupe algébrique connexe de dimension 1
- $\mathbf{G}_{m,k}$ est un groupe algébrique connexe de dimension 1
- $\mu_{n,k}$ est un groupe algébrique à n composantes connexe de dimension 0 (si $\mathrm{car} k \not| n$)
- $Z/n\mathbf{Z}$ est un groupe algébrique à n composantes connexe de dimension 0

Le cas de $\mathbf{S}L_{n,k}$ est plus subtil. Pour montrer qu'il est connexe, on peut considérer la suite exacte

$$1 \longrightarrow \mathbf{SL}_{n,k} \longrightarrow \mathbf{GL}_{n,k} \xrightarrow{\det} \mathbf{G}_{m,k} \longrightarrow 1$$

et remarquer que le morphisme $\mathbf{G}_{m,k} \to \mathbf{GL}_{n,k}$ défini par

$$a \mapsto \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & 1 \end{pmatrix}$$

est une section de det et fournit donc un isomorphisme de groupes algébriques

$$\mathbf{GL}_{n,k} \simeq \mathbf{SL}_{n,k} \rtimes \mathbf{G}_{m,k}.$$

Il suit immédiatement que $\mathbf{SL}_{n,k}$ un un groupe algébrique connexe de dimension $n^2 - 1$. On en déduit une démonstration géométrique que $1 - \det$ est un polynôme irréductible.

Pour les groupes symplectiques et orthogonaux, c'est plus dur encore. Bien sûr, il suffit de considérer la suite exacte

$$1 \longrightarrow \mathbf{SO}_{n,k} \longrightarrow \mathbf{O}_{n,k} \xrightarrow{\det} \mu_{2,k} \longrightarrow 1$$

pour voir que si car$k \neq 2$, alors $\mathbf{O}_{n,k}$ n'est pas connexe. Nous montrerons plus tard que $\mathbf{Sp}_{n,k}$ et $\mathbf{SO}_{n,k}$ sont connexes. Nous pouvons cependant calculer leurs dimensions. Traitons le cas de $\mathbf{O}_{n,k}$ par exemple. On considère pour cela l'ouvert $\mathcal{U}$ de $\mathbf{M}_{n,k}$ défini par $\det(I + M) \neq 0$ et l'automorphisme

$$\begin{array}{ccc} \mathcal{U} & \xrightarrow{s} & \mathcal{U} \\ M & \longmapsto & (I+M)^{-1}(I-M) \end{array}.$$

Celui ci induit un isomorphisme

$$\mathcal{U} \cap \mathbf{O}_{n,k} \simeq \mathcal{U} \cap \mathfrak{o}_{n,k}$$

ou $\mathfrak{o}_{n,k}$ est *l'algèbre de Lie* de $\mathbf{O}_{n,k}$ définie par $M + {}^tM = 0$. On en déduit aisément que $\dim \mathbf{O}_{n,k} = \dim \mathfrak{o}_{n,k}$. Et ce dernier est une sous-variété linéaire de $\mathbf{M}_{n,k}$ de dimension $n(n-1)/2$. On montre de la même manière que $\dim \mathbf{Sp}_{n,k} = \frac{2n(2n+1)}{2}$.

Pour illustrer les méthodes ci-dessus, on peut aussi montrer le résultat suivant :

Proposition 2.2.3 *Si G est un groupe algébrique connexe, tout sous-groupe distingué fini N est contenu dans le centre de G.*

On rappelle que le *centre* d'un groupe G est

$$Z(G) := \{g \in G, \forall h \in G, gh = hg\}.$$

En d'autres termes, c'est l'ensemble des éléments qui sont fixés par tous les automorphismes intérieurs

$$\begin{array}{ccc} G & \longrightarrow & G \\ h & \longmapsto & ghg^{-1} \end{array}$$

Par exemple, on a

$$Z(\mathbf{GL}_{n,k}) \simeq \mathbf{G}_{m,k}, \quad Z(\mathbf{SL}_{n,k}) \simeq \mu_{n,k}, \quad Z(\mathbf{Sp}_{2n,k}) = Z(\mathbf{O}_{n,k}) \simeq \mu_{2,k}.$$

Démonstration : On fixe $h \in N$ et on considère le morphisme de variétés algébriques

$$\begin{array}{ccc} G & \xrightarrow{\phi} & N \\ g & \longmapsto & ghg^{-1} \end{array}$$

(qui est bien à valeurs dans N car N est distingué). Comme G est connexe, son image est aussi connexe et comme N est fini, ce ne peut être qu'un point. On a donc pour tout $g \in G$,

$$ghg^{-1} = \phi(g) = \phi(1) = h. \quad \surd$$

2.3 Sous-groupes, noyaux et images

On commence par un lemme.

Lemme 2.3.1 *Si X est une partie dense d'un groupe algébrique G et Y une partie contenant un ouvert non vide de G, alors $XY = G$.*

Démonstration : On peut bien sûr supposer que Y est un ouvert non vide de G. Si $g \in G$, alors gY^{-1} est aussi un ouvert non vide de G. Comme X est dense, on a $X \cap gY^{-1} \neq \emptyset$. On peut donc trouver $h \in X$ et $k \in Y$ tels que $h = gk^{-1}$, c'est à dire $g = hk$. $\surd$

Proposition 2.3.2 *Soit H un sous-groupe dense d'un groupe algébrique G qui contient un ouvert non vide de G. On a alors $H = G$.*

Démonstration : Comme H est un sous-groupe de G, on a $HH = H$. Et comme H est dense dans G et contient un ouvert non-vide de G, on a donc $HH = G$. $\surd$

Lemme 2.3.3 *Soit G un groupe algébrique. On notera $\overline{X}$ l'adhérence (de Zariski) d'une partie X de G. On a alors*

1. $\forall X \subset G, \quad \overline{X^{-1}} = \overline{X}^{-1}$
2. $\forall X, Y \subset G, \quad \overline{X}\,\overline{Y} \subset \overline{XY}$

Démonstration : Si $X \subset G$, on a $X \subset \overline{X}$ et donc $X^{-1} \subset \overline{X}^{-1}$ qui est fermé, si bien que $\overline{X^{-1}} \subset \overline{X}^{-1}$. En l'appliquant à X^{-1}, on trouve $\overline{X} \subset \overline{X^{-1}}^{-1}$ et donc $\overline{X}^{-1} \subset \overline{X^{-1}}$.

Soient maintenant $X, Y \subset G$. Si $g \in X$, on a $gY \subset XY$ et donc $g\overline{Y} = \overline{gY} \subset \overline{XY}$. Ceci étant vrai pour tout $g \in X$, on voit donc que $X\overline{Y} \subset \overline{XY}$. On continue : si $h \in \overline{Y}$, alors $Xh \subset \overline{XY}$ et on a donc $\overline{X}h = \overline{Xh} \subset \overline{XY}$. Et ceci étant vrai pour tout $h \in \overline{Y}$, on a bien $\overline{X}\,\overline{Y} \subset \overline{XY}$ comme annoncé. $\surd$

Proposition 2.3.4 *Soit H un sous-groupe d'un groupe algébrique G. Alors l'adhérence (de Zariski) $\overline{H}$ de H dans G est un sous-groupe (algébrique) de G.*

C'est ce qu'on appelle l'*enveloppe algébrique* de H dans G.

Démonstration : On sait qu'une partie non-vide H est un sous-groupe si et seulement si $HH^{-1} \subset H$ (et on a alors égalité). Il résulte alors du lemme que

$$\overline{H}\,\overline{H}^{-1} = \overline{H}\,\overline{H^{-1}} \subset \overline{HH^{-1}} = \overline{H}$$

et $\overline{H}$ est donc aussi un sous-groupe. $\surd$

Nous aurons besoin maintenant de la notion de *partie constructible* d'une variété algébrique X : c'est une combinaison bouléenne d'ouverts de X, c'est à dire, une union finie de sous-variétés. On voit aisément qu'une partie constructible est dense si et seulement si elle contient un ouvert dense et on en déduit :

Proposition 2.3.5 *Soit G un groupe algébrique.*

1. *Si X et Y sont deux parties constructibles denses de G, alors*

$$X \cap Y \neq \emptyset \quad \text{et} \quad XY = G.$$

2. *Si H est un sous-groupe constructible de G, alors H est nécessairement fermé.*

Démonstration : Pour la première assertion, comme X et Y sont constructibles et denses, elles contiennent chacune un ouvert non vide et dense et peut donc supposer qu'elles sont elles mêmes ouvertes. On a donc bien sûr $X \cap Y \neq \emptyset$ et grace au lemme 2.3.1, on a aussi $YY = G$.

En ce qui concerne la seconde assertion, on peut remplacer G par $\overline{H}$ et supposer que H est dense dans G. Comme H est constructible, il contient un ouvert non vide et il suffit alors d'invoquer la proposition 2.3.2. $\surd$

Nous aurons besoin du théorème suivant (dont la démonstration est assez difficile) :

Théorème 2.3.6 (Chevalley) *Si $\Phi : Y \to X$ est un morphisme de variétés algébriques et Z une partie constructible de Y alors, $\Phi(Z)$ est une partie constructible de X.*

On en déduit le résultat suivant :

Proposition 2.3.7 *Soit $\Phi : G \to G'$ un morphisme de groupes algébriques. Alors*

1. $\ker \Phi$ *est un sous-groupe fermé distingué de G.*
2. $\mathrm{im}\, \Phi$ *est un sous-groupe fermé de G'.*
3. *On a $\Phi(G^\circ) = \Phi(G)^\circ$.*

Démonstration : Comme les points sont fermés pour la topologie de Zariski et les morphismes sont continus, on voit que $\ker \Phi = \phi^{-1}(1)$ est bien fermé. Et il est bien sûr distingué.

Ensuite, on sait grâce au théorème de Chevalley que $\mathrm{im}\, \Phi$ est constructible et comme c'est un sous-groupe, il est fermé.

Pour la dernière assertion, on peut supposer que Φ est surjectif et alors $\Phi(G^\circ)$ est un sous-groupe fermé connexe d'indice fini et donc nécessairement égal à G'°. $\surd$

2.4 Sous-groupes engendrés

Proposition 2.4.1 *Soit $\mathcal{F}$ une famille de partie constructibles irréductibles passant par 1 dans G. Alors, le sous-groupe H de G engendré par les $X \in \mathcal{F}$ est fermé connexe et s'écrit*

$$H = X_1^{\pm} \cdots X_r^{\pm}.$$

avec $X_1, \ldots, X_r \in \mathcal{F}$.

Démonstration : On peut bien sûr supposer que $\mathcal{F}$ est stable par produits et les inverses en rajoutant les parties de la forme $X_1^{\pm} \cdots X_r^{\pm}$ qui sont constructibles grâce au théorème de Chevalley et bien sûr aussi irréductibles. On va montrer que $H \in \mathcal{F}$.

On prend un $X \in \mathcal{F}$ avec $\dim \overline{X}$ maximal. Soit $Y \in \mathcal{F}$, alors $X \subset XY$ car $1 \in Y$ et donc $\overline{X} \subset \overline{XY}$. Par maximalité, ces deux variétés ont même dimension et comme ils sont fermés et irréductibles, ils sont égaux. On a donc $\overline{X} = \overline{XY} \supset \overline{X}\,\overline{Y}$.

On en déduit tout d'abord que $Y \subset \overline{X}$, ce qui montre que $\overline{X}$ est un majorant pour $\mathcal{F}$. Mais on voit aussi que $\overline{X}$ est un sous-groupe (nécessairement fermé et donc algébrique) de G : en prenant $Y = X^{-1}$, on a

$$\overline{X}\,\overline{X}^{-1} = \overline{X}\,\overline{X^{-1}} \subset \overline{X}.$$

Comme $\overline{X}$ est un sous-groupe de G, on a $\overline{X} = XX \in \mathcal{F}$. Il suit que $\overline{X}$ est un plus grand élément de $\mathcal{F}$ et donc que $H = \overline{X}$. $\surd$

Grace à cette proposition, on peut montrer le résultat suivant.

Proposition 2.4.2 *Soit G un groupe algébrique. Si H et K sont deux sous-groupes fermés de G dont l'un est connexe, alors $[H, K]$ est un sous-groupe fermé connexe.*

On rappelle que $[H, K]$ désigne le sous-groupe *engendré* par les *commutateurs* $[g, h] := ghg^{-1}g^{-1}$ avec $g \in H$ et $h \in K$.

Démonstration On suppose H connexe et on regarde pour $h \in K$, l'image X_h du morphisme

$$\begin{array}{rcl} H & \longrightarrow & G \\ g & \longmapsto & [g, h] \end{array} .$$

Alors, $[H, K]$ est le sous-groupe engendré par les X_h qui sont des parties constructibles irréductibles passant par 1. C'est donc bien un sous-groupe fermé connexe. $\surd$

En utilisant la proposition, on peut aussi donner une nouvelle démonstration de la connexité de $\mathbf{SL}_{n,k}$. En effet, on regarde pour $i, j = 1, \ldots, n$, l'application

$$\begin{array}{rcl} \phi_{ij} : \mathbf{A}_k^1 & \longrightarrow & \mathbf{SL}_{n,k} \\ t & \longmapsto & I + t\mathbf{1}_{ij} \end{array}$$

C'est un morphisme de variétés algébriques et $\mathbf{A}_k^1$ est irréductible. Il suit que $X_{ij} :=$ im ϕ_{ij} est une partie constructible irréductible passant par 1. Comme $\mathbf{SL}_{n,k}$ est engendré par les X_{ij}, c'est un groupe connexe.

Le même genre d'argument montre que $\mathbf{Sp}_{2n,k}$ et $\mathbf{SO}_{n,k}$ sont connexes. En particulier, on peut en déduire que $\mathbf{Sp}_{2n,k} \subset \mathbf{SL}_{2n,k}$.

3 Action de groupe

3.1 Généralités

On rappelle qu'une action (à gauche) d'un groupe (abstrait) G sur un ensemble E est une application

$$\begin{aligned} G \times E &\xrightarrow{\mu} E \\ (g,x) &\longmapsto gx \end{aligned}$$

satisfaisant

$$\forall x \in E, 1x = x \quad \text{et} \quad \forall g,h \in G, x \in E, (gh)x = g(hx).$$

On en déduit un homomorphisme de groupes

$$\begin{aligned} \rho : G &\longrightarrow S(E) \\ g &\longmapsto (x \mapsto gx) \end{aligned}$$

ou $S(E)$ désigne le groupe des bijections de E dans E. Et réciproquement, tout homomorphisme de groupes $\rho : G \to S(E)$ induit une action ($gx = \rho(g)(x)$).

On peut faire les remarques suivantes :

- On peut remplacer *groupe* par *monoïde* ci-dessus à condition de remplacer $S(E)$ par le monoïde E^E des applications de E dans E.
- Une action à droite

  $$\begin{aligned} G \times E &\longrightarrow E \\ (g,x) &\longmapsto xg \end{aligned}$$

  satisfait

  $$\forall x \in E, x = x1 \quad \text{et} \quad \forall g,h \in G, x \in E, x(gh) = (xg)h.$$

  C'est équivalent à une action à gauche du *groupe opposé* G^{op} qui a les mêmes éléments que G mais avec la loi $g * h := hg$. Il existe en fait un isomorphisme de groupes

  $$\begin{aligned} G^{op} &\longrightarrow G \\ x &\longmapsto x^{-1} \end{aligned} .$$

  que nous utiliserons pour remplacer systématiquement les actions à droite par des actions à gauche.
- Cette notion passe mal aux catégories car l'analogue de $S(E)$ pour un objet X d'une catégorie $\mathcal{C}$ est le foncteur en groupes

  $$\mathcal{A}ut(X) : S \mapsto \mathrm{Aut}_S(X_S)$$

  qui n'est pas représentable en général.

Nous pouvons rappeler brièvement le vocabulaire utilisé dans la théorie. Le *stabilisateur* ou *groupe d'isotropie* d'un $x \in E$ est le sous-groupe

$$G_x : \{g \in G, \quad gx = g\}$$

et son *orbite* est la partie

$$Gx := \{gx, g \in G\}$$

de E. L'action est *fidèle* si $\ker \rho = 0$; elle est *simple* si $\forall x \in E, G_x = 0$. Comme $\ker \rho = \cap_{x \in E} G_x$, on voit qu'une action simple est toujours fidèle. L'action est *transitive* s'il existe une unique orbite :

$$E \neq \emptyset \quad \text{et} \quad \forall x, y \in E, \exists g \in G, y = gx.$$

On dit aussi que E est *homogène* sous G. Une action simple et transitive est dite *simplement transitive* :

$$E \neq \emptyset \quad \text{et} \quad \forall x, y \in E, \exists! g \in G, y = gx.$$

On dit aussi que E est *principal homogène* sous G. En général, on dit qu'une partie E' de E est *stable* si

$$\forall g \in G, \forall x \in E', gx \in E'.$$

Enfin, une application $\phi : E \to E'$ est *compatible aux actions* d'un groupe G si on a

$$\forall g \in G, \forall x \in E, \phi(gx) = g\phi(x).$$

On dit aussi que c'est un *G-morphisme* ou un morphisme *G-équivariant*.

Nous rencontrerons en particulier l'action par *conjugaison* de G sur un sous-groupe distingué N :

$$\begin{array}{rcl} G \times N & \longrightarrow & N \\ (g, h) & \longmapsto & \mathrm{int}_g(h) := ghg^{-1} \end{array}$$

Enfin, nous avons aussi l'action par *translation à gauche* d'un sous-groupe H de G sur G :

$$\begin{array}{rcl} H \times G & \longrightarrow & G \\ (h, g) & \longmapsto & hg \end{array} ,$$

ou par translation à droite (vu comme action à gauche !) :

$$\begin{array}{rcl} H \times G & \longrightarrow & G \\ (h, g) & \longmapsto & gh^{-1} \end{array} .$$

3.2 G-variétés

On rappelle qu'on travaille sur un corps algébriquement clos k.

Définition 3.2.1 *Soit G un groupe algébrique et X une variété algébrique. Une action de G sur X est une action du groupe abstrait G sur l'ensemble sous-jacent à X donnée par un morphisme*

$$\mu : G \times X \to X.$$

On dira aussi que X est une G-variété.

Notons en particulier, que si $g \in G$, la multiplication par g sur X est un morphisme

$$\begin{array}{rcl} g : X \xrightarrow{(g,\mathrm{Id}_X)} G \times X & \xrightarrow{\mu} & X \\ x & \longrightarrow & gx \end{array}.$$

et c'est même un automorphisme d'inverse g^{-1}. On notera gY l'image d'une partie $Y \subset X$.

Proposition 3.2.2 *Soit G un groupe algébrique. Si X est une G-variétés, les orbites sont des sous-variétés. De plus, si X est non-vide, il existe une orbite fermée.*

Démonstration : Soit $x \in X$. Comme Gx est l'image du morphisme

$$\begin{array}{rcl} G & \longrightarrow & X \\ g & \longmapsto & gx \end{array},$$

c'est une partie constructible de X. Donc, Gx contient un ouvert U non vide de $\overline{Gx}$. On a alors $Gx = \cup_{g \in G} gU$ qui est ouvert dans $\overline{Gx}$. C'est donc bien une sous-variété (ouvert d'un fermé).

Notons maintenant que $\overline{Gx}$ est stable sous l'action de G : comme la multiplication par g sur X est un automorphisme, on a

$$g\overline{Gx} = \overline{gGx} = \overline{Gx}.$$

Soit O une orbite de dimension minimale (on suppose donc X non vide). Comme $\overline{O}$ et O sont tous deux stables sous l'action de G, il en va de même de la frontière $\overline{O} \setminus O$. Si $\overline{O} \setminus O \neq \emptyset$, il existe une orbite O' contenue dedans et donc

$$\dim O' \leq \dim \overline{O} \setminus O < \dim O$$

ce qui contredit la minimalité de O (la frontière est toujours de dimension strictement inférieure). On a donc $\overline{O} \setminus O = \emptyset$ si bien que $O = \overline{O}$ est fermée dans X. $\surd$

Proposition 3.2.3 *Soit G un groupe algébrique et X une variété homogène sous G. Alors, les composantes connexes de X sont irréductibles, ce sont les orbites sous G° et elles sont toutes isomorphes.*

Démonstration : Soit X' une orbite fermée de X sous G°. Comme X est homogène sous G et que G° est d'indice fini, on voit facilement que X est l'union disjointe d'un nombre fini de gX'. Celles ci-sont fermées et toutes isomorphes. Comme elles sont en nombre fini, elles sont aussi ouvertes. Ce sont donc les composantes connexes.

Pour l'irréductibilité, on peut supposer que G est connexe. Comme X est homogène, si $x \in X$, on a un morphisme surjectif

$$\begin{array}{rcl} G & \longrightarrow & X \\ g & \longmapsto & gx \end{array}.$$

Puisque G est connexe, il est irréductible et son image X aussi. $\surd$

On rappelle qu'une action dun groupe abstrait G sur un k-espace vectoriel E est linéaire si le morphisme $\rho : G \to S(E)$ est à valeurs dans $\mathbf{GL}(E)$. Cela signifie que

$$\forall g \in G, v, w \in E, g(v + w) = gv + gw \quad \text{et} \quad \forall g \in G, v \in E, \lambda \in k, g(\lambda v) = \lambda gv$$

C'est aussi équivalent à une structure de $k^{(G)}$-module ou $k^{(G)}$ est l'algèbre du groupe G (souvent notée $k[G]$). On dit aussi que l'application

$$\rho : G \to \mathbf{GL}(E)$$

est une *représentation linéaire* du groupe G. On écrira parfois $g_E := \rho(g)$ et on parlera de *morphisme de représentations* au lieu d'application linéaire équivariante et de *sous-représentation* au lieu de sous-espace stable.

Dans la proposition suivante, on n'a pas besoin que G ou X soit affine, mais je ne vois pas d'applications intéressantes du cas général.

Proposition 3.2.4 *Soit G un groupe affine et X une G-variété affine. On a alors*

1. *L'application*
$$\begin{array}{ccc} G & \longrightarrow & \mathbf{G}L_k(A(X)) \\ g & \longmapsto & g^{-1*} \end{array}$$
est une représentation linéaire de G (de dimension infinie en général).
2. *Si F est un sous espace de $A(X)$ stable sous G et E est un sous-espace vectoriel de dimension finie de F, il existe un sous-espace vectoriel E' de dimension finie de F contenant E et stable sous l'action de G.*
3. *Si*
$$\mu^* : A(X) \to A(G) \otimes_k A(X).$$
désigne l'application induite par $\mu : G \times X \to X$ et E est un sous-espace vectoriel de dimension finie de $A(X)$, alors les conditions, suivantes sont équivalentes :
   - *(a) E et stable sous l'action de G*
   - *(b) $\mu^*(E) \subset A(G) \otimes_k E$.*

Par définition, on a donc pour $g \in G$, $\rho(g) = g^{-1*}$, ce qui signifie que si $f \in A(X)$, on a

$$gf := \rho(g)(f) = g^{-1*}(f) = f \circ g^{-1}$$

et donc finalement, si $x \in X$,

$$(gf)(x) = (f \circ g^{-1})(x) = f(g^{-1}x).$$

Démonstration : On vérifie immédiatement que ρ est bien une représentation (linéaire) : on a bien sûr pour $f \in A(X)$ et $x \in X$,

$$(1f)(x) = f(1x) = f(x),$$

et aussi si, de plus $g, h \in G$,

$$((gh)f)(x) = f((gh)^{-1}x) = f(h^{-1}g^{-1}x) = (hf)(g^{-1}x) = (g(hf))(x).$$

On montre maintenant la seconde assertion. Soit E' le sous-espace vectoriel de $A(X)$ engendré par tous les gf avec $g \in G$ et $f \in E$. Alors E' est clairement G-stable, contenu dans F, et contient E. Il reste à voir qu'il est de dimension finie. Comme E est de dimension finie, on voit immédiatement qu'il existe un sous-espace de dimension finie E'' de F tel que $\mu^*(E) \subset A(G) \otimes_k E''$. Pour $g \in G$, la décomposition de la multiplication par g^{-1}

$$\begin{array}{ccc} X \xrightarrow{(g,\mathrm{Id}_X)} G \times X \xrightarrow{\mu} X & . \\ x \xrightarrow{\qquad\qquad\qquad\qquad} g^{-1}x & \end{array}$$

permet de décomposer g^{-1*} :

$$\begin{tikzcd} E \arrow[r] \arrow[d, hook] & A(G) \otimes_k E'' \arrow[r] \arrow[d, hook] & E'' \arrow[d, hook] \\ A(X) \arrow[r, "\mu^*"] & A(G) \otimes_k A(X) \arrow[r] & A(X) \end{tikzcd} .$$

$$\varphi \otimes f \longmapsto \varphi(g^{-1})f$$

On en déduit que $g^{-1*}(E) \subset E'$. Ceci étant vrai pour tout g, on a $E \subset E' \subset E''$ et E' est donc bien de dimension finie.

Il reste à montrer la dernière assertion. Si la seconde condition est satisfaite, on peut prendre $E'' = E$ et on a donc aussi $E = E' = E''$. Réciproquement, supposons que E est stable sous l'action de G. On peut choisir une base $(f_1, \ldots, f_r)$ de E que l'on prolonge en une base $(f_i)_{i\in\mathbf{N}}$ de $A(X)$. Si $f \in E$, on peut écrire

$$\mu^*(f) = \sum \varphi_i \otimes f_i$$

et on a donc pour tout $g \in G$,

$$\sum \varphi_i(g^{-1})f_i = {g^{-1}}^*(f) = gf \in E.$$

On voit donc que $\varphi_i(g^{-1}) = 0$ pour $i \neq 1, \cdots, r$. Ceci étant vrai pour tout $g \in G$, on a nécessairement $\varphi_i = 0$. Ceci étant vrai pour tout $i \neq 1, \cdots, r$, on a

$$\mu^*(f) = \sum_{i=1}^{r} \varphi_i \otimes f_i \in A(G) \otimes_k E.$$

Et ceci étant vrai pour tout $f \in E$, on a bien $\mu^*(E) \subset A(G) \otimes_k E$.

3.3 Représentations de dimension finie

Avant d'aller plus loin, il est peut être pratique d'avoir une définition alternative d'une action linéaire d'un groupe algébrique.

On fait tout d'abord un petit rappel d'algèbre multilinéaire. Si E est un espace vectoriel de dimension finie sur k, on pose

$$T^r(E) = E \otimes_k \cdots \otimes_k E(r \text{ fois}).$$

L'*algèbre tensorielle* de E est l'algèbre graduée $T(E) = \oplus_{r \leq 0} T^r(E)$ avec et multiplication évidente

$$(v_1 \otimes \cdots v_r)(w_1 \otimes \cdots w_s) = v_1 \otimes \cdots v_r \otimes w_1 \otimes \cdots w_s.$$

L'*algèbre symétrique* (resp. *extérieure*) de E est l'algèbre graduée $S(E)$ (resp. $\Lambda(E)$), quotient de $T(E)$ par l'idéal

$$(v \otimes w - w \otimes v, v, w \in E) \quad \text{resp.} \quad (v \otimes v, v \in E).$$

On note $v_1 \cdots v_r$ (resp. $v_1 \wedge \cdots \wedge v_r$) l'image de $v_1 \otimes \cdots \otimes v_r$ dans $S(E)$ (resp. $\Lambda(E)$). L'algèbre $T(E)$ (resp. $S(E)$, resp. $\Lambda(E)$) est universelle dans la mesure ou toute application linéaire $E \to A$ ou A est une k-algèbre (resp. commutative, resp. alternée) se prolonge de manière unique en un morphisme de k-algèbres $T(E) \to A$ (resp. $S(E) \to A$, resp. $\Lambda(E) \to A$).

Notons alors que tout espace vectoriel de dimension finie E est de manière naturelle une variété affine dont l'algèbre est l'algèbre symétrique $S(\check{E})$ du dual de E, car bien sûr,

$$\mathrm{Hom}_{k-alg}(S(\check{E}), k) = L(\check{E}, k) \simeq E.$$

Le résultat suivant est vrai plus généralement pour un groupe algébrique quelconque mais nous n'en auront pas besoin.

Proposition 3.3.1 *Soit E un espace vectoriel muni d'une action linéaire d'un groupe affine G qui en fait une G-variété. Alors, l'homomorphisme de groupes*

$$\rho : G \to \mathbf{GL}(E)$$

est aussi un morphisme de variétés algébriques. Et réciproquement, un tel morphisme de groupes algébriques définit une action k-linéaire du groupe algébrique sur la variété E.

Démonstration : Se donner ρ revient à se donner, une famille compatible, pour toute k-algèbre réduite de type fini A, de morphismes de groupes

$$\rho(A) : G(A) \to GL(E)(A) = \mathbf{GL}_A(A \otimes_k E).$$

Or on a

$$E(A) = \mathrm{Hom}_{k-alg}(S(\check{E}), A) = L(\check{E}, A) \simeq A \otimes_k E.$$

Un tel morphisme de groupes correspond donc à une action

$$G(A) \times E(A) \to E(A)$$

et la compatibilité est conservée. Une telle famille correspond à un morphisme

$$\mu : G \times E \to E$$

qui fait donc de E une G-variété. Et l'action est bien sûr k-linéaire. Réciproquement, une telle action fournit une action A-linéaire pour tout A qui donne un morphisme de groupes comme ci-dessus. $\surd$

Définition 3.3.2 *On dit alors que ρ est une représentation linéaire algébrique de G.*

Le théorème suivant nous dit que les groupes affines sont essentiellement des groupes classiques :

Théorème 3.3.3 *Tout groupe affine est isomorphe à un sous-groupe fermé de $\mathbf{GL}_{n,k}$, pour n assez grand.*

Comme la plupart des groupes qu'on a vu sont déjà des sous-groupes de $\mathbf{GL}_{n,k}$, ou de $\mathbf{GL}(E)$ qui est isomorphe à $\mathbf{GL}_{n,k}$, nous avons peu d'exemples intéressants. Rappelons tout de même que $\mathbf{G}_{a,k} \simeq \mathbf{U}_{2,k}$. Notons aussi que tout sous-groupe fini est isomorphe à un sous-groupe d'un groupe symétrique $\mathbf{S}_n$ qui est lui même isomorphe à un sous-groupe de $\mathbf{GL}_{n,k}$ par

$$\sigma \mapsto M_\sigma := [\delta_{i\sigma(i)}].$$

Démonstration : Soit G un groupe affine que l'on fait agir sur lui même par translation *à droite* :

$$\mu : (g,h) \mapsto hg^{-1}$$

La proposition 3.3.1 nous fournit donc une action

$$\rho : G \to \mathbf{GL}_k(A)$$

avec $A := A(G)$ donnée par

$$(gf)(h) = f(hg)$$

pour $g, h \in G$ et $f \in A$. Soit S un ensemble fini de générateurs de A comme k-algèbre. Le sous-espace vectoriel engendré par S est de dimension finie. Grace à la seconde partie de la proposition 3.3.1, il existe un sous-espace vectoriel E de dimension finie de A qui contient S, et qui est stable par G. Soit $f_1, \dots, f_n$ une base de E. Par construction, ceux-ci engendrent A comme k-algèbre.

Comme E est stable sous l'action de G, μ^* induit une application linéaire

$$\begin{array}{ccc} E & \longrightarrow & A \otimes_k E \\ f_i & \longmapsto & \sum_{j=1}^n m_{ji} \otimes f_j \end{array} .$$

Si $g \in G$, l'action de G sur E s'obtient en composant avec l'application d'évaluation

$$\begin{array}{rcl} A \otimes_k E & \longrightarrow & E \\ m \otimes f & \longmapsto & m(g)f \end{array}$$

pour obtenir

$$\begin{array}{rcl} E & \xrightarrow{\quad g \quad} & E \\ f_i & \longmapsto & \sum_{j=1}^n m_{ji}(g) f_j \end{array} .$$

On peut alors considérer le morphisme de groupes ϕ :

$$\begin{array}{ccccc} G & \longrightarrow & \mathbf{GL}(E) & \xrightarrow{\simeq} & \mathbf{GL}_n(k) \\ g & \longmapsto & \rho(g)_{|E} & \longmapsto & [m_{ij}(g)] \end{array}$$

qui est bien un morphisme de groupes algébriques avec

$$\begin{array}{rcl} k[T_{ij}]_{\det} & \xrightarrow{\phi^*} & A \\ T_{ij} & \longmapsto & m_{ij} \end{array}$$

(on a pour tout $g \in G$, $(\det[m_{ij}])(g) = \det[m_{ij}(g)] \neq 0$ et donc $\det[m_{ij}] \in A^*$).

Il reste à montrer que ϕ est un isomorphisme sur un fermé (une immersion fermée), et c'est équivalent à avoir ϕ^* surjectif. Or, on a pour tout $g, h \in G$,

$$f_i(gh) = (gf_i)(h) = \sum_{j=1}^n m_{ji}(g) f_j(h)$$

et en prenant $h = 1$, on voit que

$$f_i(g) = \sum_{j=1}^n f_j(1) m_{ji}(g) = \phi^*(\sum_{j=1}^n f_j(1) T_{ji})(g)$$

et cela étant vrai pour tout g, on a

$$f_i = \phi^*(\sum_{j=1}^n f_j(1) T_{ji}).$$

Comme ϕ^* est un morphisme de k-algèbres et que les f_i engendrent A comme k-algèbre, on a fini. $\surd$

On termine avec une caractérisation des sous-groupes algébriques qui nous servira plus tard :

Proposition 3.3.4 *Soit H un sous-groupe fermé d'idéal J d'un groupe affine G d'algèbre A. On considère l'action induite sur A par la translation à droite ou à gauche. On a alors pour*

$$H = \{g \in G, \quad gJ \subset J\}$$

Démonstration : On traite le cas de le translation à droite, la translation à gauche s'obtenant en passant aux groupes opposés. Donnons nous tout d'abord $g \in H$ et $f \in J$. Comme H est un sous-groupe, on a pour tout $h \in H$,

$$(gf)(h) = f(hg) = 0$$

si bien que $gf \in J$.

Inversement, supposons qu'un élément $g \in G$ laisse J stable. Alors, si $f \in J$, on a $gf \in J$ et donc pour tout $h \in H$,

$$f(hg) = (gf)(h) = 0.$$

Il suffit alors de prendre $h = 1$ et on a $f(g) = 0$. Ceci étant vrai pour tout $f \in J$, on a bien $g \in H$. $\surd$

4 Décomposition de Jordan

On a vu que tout groupe affine est un sous-groupe d'un groupe linéaire. Or, pour étudier les matrices, l'outil fondamental est la décomposition de Jordan. Nous allons voir que la décomposition induite sur le groupe affine ne dépend pas de sa réalisation comme sous-groupe du groupe linéaire.

4.1 Rappels d'algèbre linéaire

On rappelle que k désigne un corps algébriquement clos et que les espaces vectoriels ne sont pas nécessairement de dimension finie.

Définition 4.1.1 *Soit E un espace vectoriel sur k et $g \in L(E)$. Alors, g est* essentiellement fini *si E est l'union de sous-espaces vectoriels g-stables de dimension finie. Elle est* essentiellement semi-simple *si sa restriction à tout sous-espace g-stable est diagonalisable. Elle est* essentiellement nilpotente *si sa restriction à tout sous-espace g-stable est nilpotente. Enfin, elle est* essentiellement unipotente *si $\mathrm{Id}_E - g$ est essentiellement nilpotente.*

Se donner un endomorphisme g d'un espace vectoriel E revient à se donner une structure de $k[T]$-module sur E (avec $Tu = g(u)$). On montre alors facilement que g est essentiellement fini si et seulement si E est un module de torsion :

$$\forall u \in E, \exists P \in k[T], P(g)(u) = 0.$$

Les notions introduites dans cette définition se comportent mal vis-à-vis de la composition. On peut remarquer tout de même que si g et h sont deux endomorphismes essentiellement finis de E *qui commutent*, alors, gh est aussi essentiellement fini. Plus précisément, E est l'union de sous espaces vectoriels de dimension finie stables à la fois par g et par h. Tout polynôme en g et h est donc essentiellement fini. Il est clair alors, que si l'un des deux endomorphisme est essentiellement nilpotent, alors gh aussi. On voit aussi facilement que si les deux endomorphismes sont essentiellement semi-simples, alors leur produit l'est aussi (les sous-espaces propres de l'un sont stables par l'autre et réciproquement).

Proposition 4.1.2 *Soit E un espace vectoriel sur k et $g \in L(E)$ essentiellement fini.*

1. *On peut alors écrire de manière unique $g = g_s + g_n$ avec g_s essentiellement semi-simple, g_n essentiellement nilpotente et $g_s g_n = g_n g_s$.*
2. *Si $\phi : E \to E'$ est une application linéaire et $g' \in L(E')$ localement finie telle que $g' \circ \phi = \phi \circ g$, alors*

$$g'_s \circ \phi = \phi \circ g_s \quad \text{et} \quad g'_n \circ \phi = \phi \circ g_n.$$

On énonce dès maintenant un corollaire que l'on démontrera en même temps que la proposition.

Corollaire 4.1.3 *Soit E un espace vectoriel sur k et $g \in L(E)$ essentiellement fini. Si E' est un sous-espace vectoriel g-stable, alors*

1. *$g_{|E'}$ est essentiellement finie et on a*

$$(g_{|E'})_s = g_{s|E'} \quad \text{et} \quad (g_{|E'})_n = g_{n|E'}.$$

2. *L'image $\overline{g}$ de g dans E/E' est essentiellement finie et on a*

$$(\overline{g})_s = \overline{g_s} \quad \text{et} (\overline{g})_n = \overline{g_n}.$$

Démonstration : Tout d'abord, le corollaire résulte immédiatement de la seconde partie de la proposition en considérant les applications d'inclusion $E' \to E$ et de projection $E \to E/E'$: en effet, il est clair que $g_{|E'}$ ainsi que $\overline{g}$ sont essentiellement finies.

En utilisant la première assertion du corollaire, on voit que l'on peut supposer que E est de dimension finie. Grace au théorème de structure pour les modules de type fini sur les anneaux principaux, on peut supposer que $g = \lambda \mathrm{Id}_E + n$ avec n nilpotent et $\lambda \in k$. La première assertion de la proposition en résulte immédiatement. On peut aussi supposer que $g' = \lambda' \mathrm{Id}_E + n'$ avec n' nilpotent et $\lambda' \in k$. La seconde assertion en découle. $\surd$

Je me permet de vous rappeler que si M est un module de type fini sur un anneau principal A, alors $M \simeq \oplus_i A/(p_i)^{N_i}$ avec (p_i) premier. Dans le cas $A = k[T]$ et $M = E$ avec structure induite par g, on a $p_i = T - \lambda_i$ avec $\lambda_i \in k$ et on voit donc que $E = \oplus E_i$ avec E_i stable sous l'action de g, et $(g_{|E_i} - \lambda_i \mathrm{Id}_{E_i})^{N_i} = 0$.

Définition 4.1.4 *On dit que g_s est la* partie semi-simple *de g et que g_n est la* partie nilpotente*.*

Lemme 4.1.5 *Si $g, h \in L(E)$ sont essentiellement finis et commutent, alors gh est essentiellement fini, g_n et g_s commutent avec h_s et h_n, et on a*

$$(gh)_s = g_s h_s \quad \text{et} \quad (gh)_n = g_s h_n + g_n h_s + g_n h_n.$$

Démonstration : On a vu plus haut que gh est essentiellement fini et les commutations résultent de seconde partie de la proposition. Enfin, on a

$$gh = g_s h_s + (g_s h_n + g_n h_s + g_n h_n)$$

et on a vu plus haut que le premier terme est essentiellement semi-simple et que les autres sont essentiellement nilpotents. Il en va de même de leur somme. On conclut par unicité de la décomposition. $\surd$

Proposition 4.1.6 *Soit E un espace vectoriel sur k et $G \in \mathbf{GL}(E)$ essentiellement finie.*

1. *On a alors $g_s \in \mathbf{GL}(E)$ et il existe une unique $g_u \in \mathbf{GL}(E)$ essentiellement unipotente telle que*
$$g = g_s g_u = g_u g_s.$$
2. *g^{-1} est essentiellement finie et on a $(g^{-1})_s = (g_s)^{-1}$ et $(g^{-1})_u = (g_u)^{-1}$*
3. *Si $\phi : E \to E'$ est une application linéaire et $g' \in \mathbf{GL}(E')$ localement finie telle que $g' \circ \phi = \phi \circ g$, alors*

$$g'_s \circ \phi = \phi \circ g_s \quad \text{et} \quad g'_u \circ \phi = \phi \circ g_u.$$

Démonstration : Si g laisse stable un sous-espace de dimension finie E', comme g est bijective sur E, g est injective sur E' et donc aussi bijective. Il suit que g^{-1} aussi laisse E' stable et on voit donc que g^{-1} est essentiellement finie. Comme g et g^{-1} commutent, il résulte du lemme que g_s est inversible et que son inverse est $(g^{-1})_s$. Les deux dernière assertions résulteront alors de la première (et de la proposition 4.1.2). D'autre part, l'unicité de g_u est triviale. Il suffit donc de poser

$$g_u := \mathrm{Id}_E + g_s^{-1} g_n,$$

ce qui donne bien sûr $g_s g_u = g$ mais aussi $g_u g_s = g$ car g_s^{-1} commute avec g_n grace au lemme. $\surd$.

Définition 4.1.7 *On dit que g_u est la* partie unipotente *de g.*

Pour future référence, notons que

Proposition 4.1.8 *Si g (resp. g') est un endomorphisme essentiellement fini de E (resp. E'), alors*

1. *$g \oplus g'$ est un endomorphisme essentiellement fini de $E \oplus E'$ et on a*

$$(g \oplus g')_s = g_s \oplus g'_s \quad \text{et} \quad (g \oplus g')_n = g_n \oplus g'_n$$

   et $(g \oplus g')_u = g_u \oplus g'_u$ si g est bijectif.
2. *$g \otimes g'$ est un endomorphisme essentiellement fini de $E \otimes_k E'$ et on a*

$$(g \otimes g')_s = g_s \otimes g'_s \quad \text{et} \quad (g \otimes g')_n = g_s \otimes g'_n + g_n \otimes g'_s + g_n \otimes g'_n$$

   et $(g \otimes g')_u = g_u \otimes g'_u$ si g est bijectif.

Démonstration : Laissé en exercice. $\surd$

4.2 Application aux groupes algébriques

Lemme 4.2.1 *Si G est un groupe affine d'algèbre A, alors la représentation*

$$\rho : G \to \mathbf{GL}(A)$$

induite par la translation à droite dans G est fidèle.

On a bien sûr le résultat analogue pour l'action par translation à gauche.

Démonstration : Comme la translation à droite définit l'action (à gauche)

$$\mu : (g, h) \mapsto hg^{-1},$$

on a

$$\rho(g)(f)(h) = (gf)(h) = f(hg)$$

pour $g, h \in G$ et $f \in A$. On voit donc que si $\rho(g) = \mathrm{Id}_A$, on a pour tous $h \in G$ et $f \in A$, $f(hg) = f(h)$. En prenant $h = 1$, on voit que $f(g) = f(1)$ et ceci étant vrai pour tout f, on a nécessairement $g = 1$. Il suit que $\ker \rho = \{1\}$. $\surd$

Théorème 4.2.2 *Soient G un groupe affine d'algèbre A et $\rho : G \to \mathbf{GL}(A)$ la représentation induite par la translation à droite dans G. Si $g \in G$, alors $\rho(g)$ est essentiellement fini et il existe $g_s, g_u \in G$ uniques tels que*

$$\rho(g_u) = \rho(g)_u \quad \textit{et} \quad \rho(g_s) = \rho(g)_s.$$

De plus on a

$$g = g_s g_u = g_u g_s.$$

Définition 4.2.3 *On dit que g_s est la* partie semi-simple *de g et que g_u est sa* partie unipotente. *Si $g_u = 1$, on dit que g est* semi-simple *et si $g_s = 1$, on dit que g est* unipotent.

Démonstration : L'unicité ainsi que la dernière assertion résultent de la fidélité de l'action. Et l'existence de g_u résultera de celle de g_s.

Considérons la multiplication

$$\begin{array}{ccc} A\otimes_k A & \xrightarrow{m} & A \\ f_1\otimes f_2 & \longmapsto & f_1f_2 \end{array} .$$

Comme, pour $g \in G$, $\rho(g)$ est un homomorphisme d'algèbres, on a

$$m \circ \rho(g) \otimes \rho(g) = \rho(g) \circ m.$$

On en déduit que

$$m \circ \rho(g)_s \otimes \rho(g)_s = \rho(g)_s \circ m.$$

et donc que $\rho(g)_s$ est aussi un morphisme d'algèbres. On π_g^s alors le morphisme composé

$$\begin{array}{ccccc} A & \xrightarrow{\rho(g)_s} & A & \longrightarrow & K \\ & & f & \longmapsto & f(1) \end{array}$$

et on note $g_s \in G$ le point correspondant. Par définition, on a donc

$$f(g_s) = \rho(g)_s(f)(1)$$

pour tout $f \in A$. Nous voulons montrer que $\rho(g_s) = \rho(g)_s$. Pour cela, nous aurons besoin du lemme suivant :

Lemme 4.2.4 *Si on note $\lambda : G \to \mathbf{GL}(A)$, l'action induite par la translation à gauche, on a*

$$\forall g, h \in G, \quad \rho(g) \circ \lambda(h) = \lambda(h) \circ \rho(g).$$

Démonstration : Par définition, on a pour $g, h \in G$ et $f \in A$:

$$\lambda(g)(f)(h) = f(g^{-1}h).$$

On voit ainsi que, pour $k \in G$ et $f \in A$,

$$(\rho(g) \circ \lambda(h))(f)(k) = \rho(g)(\lambda(h)(f))(k) = \lambda(h)(f)(kg) = f(h^{-1}kg)$$

et

$$(\lambda(h) \circ \rho(g))(f)(k) = \lambda(h)(\rho(g)(f))(k) = \rho(g)(f))(h^{-1}k) = f(h^{-1}kg). \quad \checkmark$$

Revenons à la démonstration du théorème. On a pour tout $g, h \in G$ et $f \in A$,

$$\rho(g_s)(f)(h) = f(hg_s) = \lambda(h^{-1})(f)(g_s)$$
$$= \rho(g)_s(\lambda(h^{-1})(f)(1) = (\rho(g)_s \circ \lambda(h^{-1}))(f)(1)$$

Grâce au lemme, on a

$$\rho(g)_s \circ \lambda(h^{-1}) = \lambda(h^{-1}) \circ \rho(g)_s,$$

et il suit que

$$\begin{aligned}\rho(g_s)(f)(h) &= (\lambda(h^{-1}) \circ \rho(g)_s)(f)(1) \\ &= \lambda(h^{-1})(\rho(g)_s)(f))(1) = \rho(g)_s(f)(h).\end{aligned}$$

On a donc bien $\rho(g_s) = \rho(g)_s$. $\surd$

Proposition 4.2.5 *Soit $\Phi : G \to G'$ un morphisme de groupes affines. Si $g \in G$, on a*

$$\Phi(g)_s = \Phi(g_s) \quad \text{et} \quad \Phi(g)_u = \Phi(g_u).$$

Démonstration : Bien sûr, il suffit de montrer que $\Phi(g)_s = \Phi(g_s)$.

On note A et A' les algèbres de G et G' respectivement, et

$$\rho : G \to \mathbf{GL}(A), \quad \rho' : G' \to \mathbf{GL}(A')$$

les représentations associées aux actions par translation à droite. On montre d'abord le lemme suivant :

Lemme 4.2.6 *Le diagramme*

$$\begin{tikzcd} A' \arrow[r, "\Phi^*"] \arrow[d, "\rho'(\Phi(g))"] & A \arrow[d, "\rho(g)"] \\ A' \arrow[r, "\Phi^*"] & A \end{tikzcd}$$

est commutatif.

Démonstration : Pour $h \in G$ et $f' \in A'$, on a

$$(\Phi^* \circ \rho'(\Phi(g)))(f')(h) = (\Phi^*(\rho'(\Phi(g))(f'))(h)$$

$$= \rho'(\Phi(g))(f')(\Phi(h) = f'(\Phi(h)\Phi(g)) = f'(\Phi(hg))$$

$$= \Phi^*(f')(hg) = \rho(g)(\Phi^*(f'))(h) = (\rho(g) \circ \Phi^*)(f')(h). \quad \surd$$

Nous revenons à notre proposition. Il résulte du lemme que

$$\Phi^* \circ \rho'(\Phi(g)_s) = \Phi^* \circ \rho'(\Phi(g))_s = \rho(g)_s \circ \Phi^*$$

$$= \rho(g_s) \circ \Phi^* = \Phi^* \circ \rho'(\Phi(g_s)).$$

On voit donc que si Φ^* est injectif, on a $\rho'(\Phi(g)_s) = \rho'(\Phi(g_s))$ et comme ρ' est fidèle, on a bien $\Phi(g)_s = \Phi(g_s)$. On vérifie aisément que si Φ est surjectif, alors, Φ^* est injectif. En général, on peut décomposer Φ en une suite de morphismes de groupes affines

$$G \to \operatorname{im} \Phi \hookrightarrow G'$$

ou le premier morphisme est surjectif, et le second, l'inclusion d'un sous-groupe fermé. On peut donc dorénavant supposer que $\Phi : G \hookrightarrow G'$ est l'inclusion d'un sous-groupe fermé défini par un idéal I. On considère alors le diagramme commutatif à lignes exactes :

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] \arrow[d, dotted] & A' \arrow[r, "\Phi^*"] \arrow[d, "\rho'(\Phi(g)_s)"] & A \arrow[r] \arrow[d, "\rho(g_s)"] & 0 . \\ 0 \arrow[r] & I \arrow[r] & A' \arrow[r, "\Phi^*"] & A \arrow[r] & 0 \end{tikzcd}$$

On a donc nécessairement $\rho'(\Phi(g)_s)(I) \subset I$ et la proposition 3.3.4 implique que $\Phi(g)_s \in G$. On peut donc écrire $\Phi(g)_s = \Phi(h)$ avec $h \in G$ et il reste à montrer que $h = g_s$. On utilise à nouveau le lemme qui nous donne

$$\Phi^* \circ \rho'(\Phi(g)_s) = \Phi^* \circ \rho'(\Phi(h)) = \rho(h) \circ \Phi^*$$

et en comparant avec le calcul ci-dessus, on peut voir que

$$\rho(h) \circ \Phi^* = \rho(g_s) \circ \Phi^*$$

et comme Φ^* est surjectif, on a bien $h = g_s$. $\surd$

Si G est un sous-groupe fermé de $\mathbf{GL}(E)$, alors tout $g \in G$ est aussi un automorphisme de l'espace vectoriel E et nous avons donc deux définitions différentes de g_s et de g_u selon que l'on voit g comme élément du groupe algébrique G ou comme automorphisme de E. En fait, on a :

Proposition 4.2.7 *Si G est un sous-groupe fermé de $\mathbf{GL}(E)$ et $g \in G$, les deux définitions de g_s et g_u coincident.*

Démonstration : Grace à la proposition précédente, il suffit de traiter le cas $G := \mathbf{GL}_{n,k}$. On note $g = g_s g_u$ la décomposition de g en tant qu'automorphisme de k^n et $g = g'_s g'_u$ la décomposition en tant qu'élément du groupe G. On veut montrer que $g'_s = g_s$. L'autre égalité suivra.

L'espace k^n est muni de l'action naturelle du groupe linéaire et l'algèbre $A := K[T_{ij}]_{\det}$ est munie comme d'habitude de l'action $\rho : G \to \mathbf{GL}(A)$ induit par la translation à droite. Imaginons que nous disposons d'une application linéaire G-équivariante

$$\phi : k^n \hookrightarrow K[T_{ij}]_{\det}.$$

Cela signifie que, pour tout $g \in G$, on a

$$\phi \circ g = \rho(g) \circ \phi.$$

On aura alors

$$\phi \circ g'_s = \rho(g'_s) \circ \phi = \rho(g)_s \circ \phi = \phi \circ g_s,$$

Si ϕ est injective, on pourra conclure que $g'_s = g_s$.

Il suffit donc de construire cette application ϕ. On veut donc pour tout $g, h \in G$ et tout $v \in k^n$,

$$\phi(g(v))(h) = \rho(g)(\phi(v))(h) = \phi(v)(hg).$$

Si on pose $f(v) = \phi(v)(1)$, on aura donc $\phi(v)(g) = f(g(v))$. Il suffit donc de choisir une forme linéaire $f : k^n \to k$. Mais nous voulons aussi que ϕ soit injective. S'il existe $v \in k^n \setminus 0$ tel que $\phi(v) = 0$, alors pour tout $g \in G$, on aura $f(gv) = \phi(v)(g) = 0$ et comme l'action de G est transitive sur $k^n \setminus 0$, on aura $f = 0$. Il suffit donc de prendre f non nulle. $\surd$

4.3 Groupes unipotents

On rappelle que si G est un groupe abstrait, on note

$$C^0(G) := D^0(G) := G, \quad C^1(G) := D^1(G) := G' := [G, G]$$

et par récurrence

$$C^{n+1}(G) = [G, C^n(G)] \quad \text{et} \quad D^{n+1}(G) = [D^n(G), D^n(G)].$$

On dit que G est *nilpotent* (resp. *résoluble*) s'il existe N tel que $C^{N+1}(G) = 0$ (resp. $D^{N+1}(G) = 0$).

Ce n'est pas évident mais on peut montrer que, par exemple, $\mathbf{U}_{n,k}$ est nilpotent et $\mathbf{T}_{n,k}$ est résoluble. On peut utiliser pour cela les décompositions suivantes en produits semi-directs :

$$\mathbf{T}_{n,k} = \mathbf{U}_{n,k} \ltimes \mathbf{D}_{n,k} \quad \text{et} \quad \mathbf{U}_{n,k} = \mathbf{U}_{n-1,k} \ltimes \mathbf{G}_{a,k}^{n-1}.$$

Définition 4.3.1 *Un groupe affine est* unipotent *si tous ses éléments sont unipotents.*

Proposition 4.3.2 1. *Un groupe affine est unipotent si et seulement si il est isomorphe à un sous-groupe de $\mathbf{U}_{n,k}$.*

2. *Si G est un groupe unipotent et $\Phi : G \to \mathbf{G}L(E)$ est un morphisme de groupes algébriques, il existe une base de E telle que* $\mathrm{im}\, \Phi \subset \mathbf{U}_{n,k}$.

Démonstration : La condition de la première assertion est bien sûr suffisante. Pour la réciproque, comme on peut réaliser G comme sous groupe d'une groupe linéaire, il suffit de montrer la seconde assertion. Nous allons procéder par récurrence sur $\dim E$.

Remarquons avant tout que si on a une suite exacte de représentations linéaires d'un groupe G

$$0 \to E' \to E \to E'' \to 0,$$

la matrice de l'action d'un élément g de G est de la forme

$$g_E = \begin{pmatrix} g_{E'} & \star \\ 0 & g_{E''} \end{pmatrix}.$$

On voit donc que $g_E \in \mathbf{U}_{\dim E,k}$ si et seulement si $g_{E'} \in \mathbf{U}_{\dim E',k}$ et $g_{E''} \in \mathbf{U}_{\dim E'',k}$ (et on a bien sûr le même résultat en remplaçant $\mathbf{U}$ par $\mathbf{T}$).

On peut donc supposer que E est irréductible, c'est à dire, n'a pas de sous-représentation non triviale. Bien sûr, comme l'image d'un unipotent est unipotent, on peut aussi remplacer G par im Φ et supposer que $G \subset \mathbf{GL}(E)$. On va montrer que, dans cette situation, on a en fait $G = \{1\}$.

Nous allons utiliser le théorème de Burnside qui est classique mais dont la démonstration est assez difficile :

Théorème 4.3.3 (Burnside) *Si E est une représentation linéaire irréductible d'un groupe abstrait G, l'application*

$$\begin{array}{rcl} k^{(G)} & \longrightarrow & L(E) \\ \sum a_i g_i & \longmapsto & \sum \lambda_i g_{i,E} \end{array}$$

est surjective.

On revient à notre démonstration. Soit $g \in G$. Si $h \in L(E)$, on peut écrire grâce au théorème de Burnside, $h = \sum \lambda_i h_i$ avec $h_i \in G$ et $\lambda_i \in k$. On voit donc que

$$\mathrm{tr}\ [(1-g)h] = \sum \lambda_i \mathrm{tr}\ [(1-g)h_i]$$

$$= \sum \lambda_i [\mathrm{tr}\ g - \mathrm{tr}\ gh_i] = \sum \lambda_i (\dim E - \dim E) = 0$$

car la trace d'un unipotent est égale à la dimension de l'espace et que g ainsi que les gh_i sont unipotents. Puisque tr $[(1-g)h] = 0$ pour tout $h \in L(E)$, on a nécessairement $1 - g = 0$, c'est à dire $g = 1$ comme annoncé. $\surd$

Corollaire 4.3.4 *Un groupe unipotent est nilpotent et donc résoluble.*

Démonstration : En effet, un sous-groupe d'un nilpotent est nilpotent et $\mathbf{U}_{n,k}$ est nilpotent. $\surd$

Corollaire 4.3.5 (Lie-Kochin) *Si E est une représentation linéaire non nulle d'un groupe unipotent G, il existe $v \in E$, non nul, stable sous G.*

Démonstration : Il suffit bien sûr de considérer la représentation naturelle de $\mathbf{U}_{n,k}$ et de prendre $v = (1, 0, \ldots, 0)$. $\surd$

Proposition 4.3.6 *Si un groupe unipotent G agit sur une variété affine X, toutes les orbites sont fermées.*

Démonstration : On choisit une orbite $\mathcal{O}$ de G dans X. Quitte à remplacer X par $\overline{\mathcal{O}}$, on peut supposer que $\mathcal{O}$ est (ouverte) et dense dans X. On note Y le complémentaire de $\mathcal{O}$ dans X et on désigne par I son idéal dans $A := A(X)$. On va alors utiliser alors la seconde assertion de la proposition 3.2.4. Comme Y est stable sous l'action de G, il ne va de même de I. Comme $\mathcal{O} \neq \emptyset$, I est non nul, et il existe un sous-espace vectoriel non nul E de dimension finie de I stable sous l'action de G. On utilise alors Lie-Kochin : Comme G est unipotent, il existe $f \in E \subset I$ non nul et stable sous G. Il suit que f est constant sur les orbites et donc en particulier sur $\mathcal{O}$ qui est dense. On voit donc que f est constant non nul. On a donc $I = A$ et alors $Y = \emptyset$. C'est ce que l'on voulait. $\surd$

Nous avons utilisé le fait que si $f \in A$ est G-stable, alors f est constant sur les orbites : c'est clair car alors pour tout $x \in X$ et $g \in G$, on aura

$$f(gx) = (g^{-1}f)(x) = f(x).$$

4.4 Groupes commutatifs

Théorème 4.4.1 *Soit G un groupe affine commutatif. Alors, l'ensemble G_s (resp. G_u) des éléments semi-simples (resp. unipotents) de G est un sous-groupe fermé et on a $G = G_u \times G_s$.*

Démonstration :

Nous commençons par un lemme.

Lemme 4.4.2 *Si $\Phi : G \to \mathbf{GL}(E)$ est une représentation linéaire d'un groupe commutatif G, il existe une base de E telle que*

$$\Phi(G) \subset \mathbf{T}_{n,k} \quad \text{et} \quad \Phi(G_s) = \mathbf{D}_{n,k} \cap \Phi(G).$$

Démonstration : On procède par récurrence sur $\dim E$. Si $\Phi(G) \subset \mathbf{G}_{m,k}\mathrm{Id}_E$, c'est clair. Sinon, on peut trouver $g \in G$ tel que $\Phi(g) \neq \lambda \mathrm{Id}_E$ pout tout $\lambda \in k$.

Supposons d'abord que $\Phi(G_s) \not\subset \mathbf{G}_{m,k}$. On peut alors supposer que $g \in G_s$ et décomposer E en somme de sous-espaces propres $E = \oplus E_i$. Comme G est commutatifs, chaque E_i est stable sous G, et on finit par récurrence.

Si on suppose maintenant que $\Phi(G_s) \subset \mathbf{G}_{m,k}$, la seconde condition sera automatiquement satisfaite. Pour montrer la première, on choisit un sous-espace propre E' de g et on regarde la suite exacte de représentations

$$0 \to E' \to E \to E/E' \to 0.$$

On finit alors par récurrence (on trigonalise sur le sous-espace et sur le quotient). $\surd$

Avant de revenir au théorème, on rappelle qu'on a un produit semi-direct

$$\mathbf{T}_{n,k} \simeq \mathbf{U}_{n,k} \ltimes \mathbf{D}_{n,k}.$$

En d'autres termes, on a une suite exacte scindée de groupes algébriques

$$\begin{tikzcd} 0 \arrow[r] & \mathbf{U}_{n,k} \arrow[r] & \mathbf{T}_{n,k} \arrow[r] & \mathbf{D}_{n,k} \arrow[r] \arrow[l, bend right] & 0 \end{tikzcd}$$

Grâce au lemme, on peut supposer que $G \subset \mathbf{T}_{n,k}$ et $G_s = \mathbf{D}_{n,k} \cap G$ et on en déduit immédiatement que $G_u = \mathbf{U}_{n,k} \cap G$. On a donc une suite exacte scindée de groupes algébriques commutatifs

$$0 \longrightarrow G_u \longrightarrow G \rightleftarrows G_s \longrightarrow 0$$

et notre assertion en découle formellement. $\surd$

Remarquons au passage que si G est connexe, alors G_s et G_u aussi.

Proposition 4.4.3 *Tout groupe affine connexe G de dimension 1 est commutatif.*

On voit en particulier que G est soit unipotent, soit composé d'éléments semi-simples. On peut montrer (mais ce n'est pas si facile) que dans le premier cas, on a $G \simeq \mathbf{G}_a$ et dans le second, $G \simeq \mathbf{G}_m$.

Démonstration : On raisonne par l'absurde.

Si G n'est pas commutatif, on peut alors trouver $g \in G$ tel que le morphisme

$$\begin{array}{rcl} G & \xrightarrow{\Phi} & G \\ h & \longmapsto & ghg^{-1} \end{array}$$

ne soit pas constant. Comme G est connexe, im Φ est une partie constructible infinie de G. Et comme G est irréductible de dimension 1, $G \setminus \operatorname{im} \Phi$ est nécessairement fini. Cela implique que presque tous les éléments de G sont conjugués.

On plonge G dans un groupe linéaire et on considère la suite de morphismes de variétés algébriques

$$\begin{array}{rcccl} G & \hookrightarrow & \mathbf{GL}_{n,k} & \longrightarrow & k[T]_{\leq n} \\ & & h & \longmapsto & \det(I - Th) \end{array}.$$

L'image de G est finie car presque tous les éléments de G sont conjugués. Comme G est connexe, cette image est réduite à un élément, l'image de 1 qui est donc $(1-T)^n$. Le théorème de Cayley-Hamilton implique donc que, pour tout $g \in G$, on a $(1-g)^n = 0$, et donc que g est unipotent. Il suit que G est un groupe unipotent, donc nilpotent, donc résoluble.

On considère maintenant $D(G)$ qui est un sous-groupe fermé connexe de G grâce à la proposition 2.4.2. Comme on a supposé que G n'est pas commutatif, on a $D(G) \neq 0$ et et donc $D(G) = G$ pour des raisons de dimension. Et G n'est donc pas résoluble ! Contradiction. $\surd$

4.5 Groupes diagonalisables

Un *caractère* d'un groupe abstrait G est une application $\chi : G \to k^*$. On dispose alors du théorème d'indépendance des caractères de Dedekind :

Théorème 4.5.1 (Dedekind) *Si G est un groupe abstrait G, alors* $\operatorname{Hom}_{Gr}(G, k^*)$ *est une partie libre de l'espace vectoriel* $\operatorname{Hom}_{Ens}(G, k)$.

La démonstration est classique : on considère une combinaison linéaire nulle

$$\sum_{i=1}^{n} \lambda_i \chi_i = 0.$$

On en déduit pour tous $g, h \in G$, que

$$\sum_{i=1}^{n} \lambda_i \chi_i(gh) = 0 \quad \text{et} \quad (\sum_{i=1}^{n} \lambda_i \chi_i(g))\chi_n(h) = 0$$

et une soustraction nous donne :

$$\sum_{i=1}^{n-1} \lambda_i [\chi_i(h) - \chi_1(h)]\chi_i = 0.$$

Définition 4.5.2 *Un caractère d'un groupe algébrique G est un morphisme de groupes algébriques $\chi : G \to \mathbf{G}_m$.*

Proposition 4.5.3 *1. Les caractères d'un groupe algébrique G forment un groupe abélien $M(G)$ pour*

$$(\chi_1 + \chi_2)(g) = \chi_1(g)\chi_2(g).$$

2. Si $\Phi : G \to H$ est un morphisme de groupes algébriques, l'application

$$\begin{array}{ccc} M(H) & \xrightarrow{M(\Phi)} & M(G) \\ \chi & \longmapsto & \chi \circ \Phi \end{array}$$

est un homomorphisme de groupes.

3. On a toujours $M(G \times H) = M(G) \oplus M(H)$.

4. On a $\mathbf{Z} \simeq M(\mathbf{G}_{m,k})$.

5. La composition avec l'inclusion $\mathbf{G}_{m,k} \hookrightarrow \mathbf{A}^1_k$ induit un homomorphisme injectif d'anneaux

$$k^{(M(G))} \hookrightarrow A(G).$$

Démonstration : Les homomorphismes d'un groupe vers un groupe abélien forment toujours un groupe abélien. Pour montrer la première assertion, il suffit donc de vérifier que $M(G)$ est un sous-groupe. En effet, $\chi_1 + \chi_2$ est le morphisme de variétés

$$G \xrightarrow{(\mathrm{Id},\mathrm{Id})} G \times G \xrightarrow{\chi_1 \times \chi_2} \mathbf{G}_{m,k} \times \mathbf{G}_{m,k} \xrightarrow{mult.} \mathbf{G}_{m,k}\ .$$

Et si χ est un caractère, alors $-\chi$ est le morphisme de variétés

$$G \xrightarrow{\chi} \mathbf{G}_{m,k} \xrightarrow{inv.} \mathbf{G}_{m,k}\ .$$

La seconde assertion est claire.

Pour la troisième assertion, on a une bijection par définition du produit et c'est compatible aux lois de groupes par construction. Les détails sont laissés en exercice.

On montre maintenant la quatrième assertion.

$$\mathrm{Hom}_{VarAlg}(\mathbf{G}_{m,k}, \mathbf{G}_{m,k}) \simeq \mathrm{Hom}_{k-alg}(k[T]_T, k[T]_T) \simeq k[T]_T^* = \{\lambda T^n, \lambda \in k, n \in \mathbf{Z})$$

Et l'application correspondante est $\alpha \mapsto \lambda\alpha^n$ qui est un morphisme de groupe si et seulement si $\lambda = 1$.

Pour la dernière assertion, la composition avec l'inclusion $\mathbf{G}_{m,k} \hookrightarrow \mathbf{A}^1_k$ fournit une injection

$$M(G) = \mathrm{Hom}_{GrAlg}(G, \mathbf{G}_{m,k}) \hookrightarrow \mathrm{Hom}_{VarAlg}(G, \mathbf{A}^1_k) \simeq A(G)$$

qui transforme par construction les sommes en produits. Par fonctorialité, on obtient un morphisme $k^{(M(G))} \to A(G)$ qui est injectif grace au théorème d'indépendance de Dedekind. $\surd$

On identifiera souvent $M(G)$ avec une partie de $A(G)$ et $k^{(M(G))}$ avec un sous-anneau de $A(G)$.

Définition 4.5.4 *Un groupe algébrique est diagonalisable s'il est est isomorphe à un sous groupe d'un groupe diagonal* $\mathbf{D}_{n,k}$.

On peut bien sûr, dans cette définition, remplacer $\mathbf{D}_{n,k}$ par $\mathbf{G}^n_{m,k}$ qui lui est isomorphe.

Théorème 4.5.5 *Le foncteur $G \mapsto M(G)$ induit une équivalence entre la catégorie des groupes diagonalisables et celle des groupes abéliens de type fini sans p-torsion (*car $k = p$*).*

On montrera au passage que l'on a des isomorphismes naturels

$$k^{(M(G))} \simeq A(G) \quad \text{et} \quad G \simeq \mathrm{Hom}_{Gr}(M(G), k^*),$$

et que la structure d'algèbre de Hopf de $A(G)$ est induite par

$$\mu^* : m \mapsto m \otimes m, \quad \epsilon^* : m \mapsto 1 \quad \text{et} \quad \sigma^* : m \mapsto m^{-1}.$$

Démonstration :

Soit $G \hookrightarrow \mathbf{G}^n_{m,k}$ une immersion fermée. On a alors un diagramme commutatif

$$\begin{tikzcd}
\mathbf{Z}^n \arrow[r, "\simeq"] \arrow[d, hook] & M(\mathbf{G}^n_{m,k}) \arrow[r] \arrow[d, hook] & M(G) \arrow[d, hook] \\
k[\underline{T}]_{\underline{T}} \arrow[r, "\simeq"] & A(\mathbf{G}^n_{m,k}) \arrow[r] & A(G)
\end{tikzcd}$$

ou la flèche du bas est surjective. On remarque alors que la première flèche verticale identifie $\mathbf{Z}^n$ avec la base canonique de $k[\underline{T}]_{\underline{T}}$. Il suit que l'image de $\mathbf{Z}^n$ dans $A(G)$ est un ensemble générateur et on sait que $M(G)$ est une partie libre de $A(G)$. Il suit que la flèche du haut est aussi surjective et que $M(G)$ est une base de $A(G)$. En particulier, on voit que $M(G)$ est bien un groupe abélien de type fini et que $k^{(M(G))} \simeq A(G)$. D'autre part, la structure d'algèbre de Hopf est induite par celle de $\mathbf{G}_{m,k}^n$ et est donc bien celle annoncée. Enfin, on vérifie aisément que $M(G)$ n'a pas de p-torsion : si $\chi \in M(G)$ satisfait $p\chi = 0$, alors pour tout $g \in G$, on a $\chi(g)^p = 1$ et donc $\chi(g) = 1$, ce qui montre que $\chi = 1$.

On montre maintenant notre foncteur est *pleinement fidèle*. On se donne un autre groupe diagonalisable H et un homomorphisme de groupes $\varphi : M(H) \to M(G)$. Celui-ci se prolonge de manière unique en un morphisme d'algèbres $A(H) \to A(G)$ qui est compatible avec les structures de Hopf. Ce dernier correspond à un unique morphisme de groupes algébriques $\Phi : G \to H$. De plus, par construction, on a donc pour $\chi \in M(H)$,

$$M(\Phi)(\chi) = \chi \circ \Phi = \Phi^*(\chi) = \varphi(\chi)$$

et donc $M(\Phi) = \varphi$.

On montre pour finir que notre foncteur est *essentiellement surjectif*. On se donne un groupe abélien de type fini sans p-torsion M. Alors, l'algèbre $k^{(M)}$ est une k-algèbre réduite de type fini qui correspond donc à une variété algébrique

$$G := \mathrm{Hom}_{k-alg}(k^{(M)}, k^*) \simeq \mathrm{Hom}_{Gr}(M, k^*).$$

Si on choisit une présentation $\mathbf{Z}^n \to M$, on en déduit une surjection

$$k[\underline{T}]_{\underline{T}} \simeq k^{(\mathbf{Z}^n)} \to k^{(M)} = A(G)$$

qui induit une immersion fermée $G \hookrightarrow \mathbf{G}_{m,k}^n$. Celle-ci correspond à l'application naturelle

$$G = \mathrm{Hom}_{Gr}(M, k^*) \to \mathrm{Hom}_{Gr}(\mathbf{Z}^n, k^*) \simeq \mathbf{G}_{m,k}^n,$$

ce qui montre que l'image de G est bien un sous-groupe fermé de $\mathbf{G}_{m,k}^n$. Et la structure d'algèbre de Hopf est bien celle attendue. Finalement, on a

$$M(G) = \mathrm{Hom}_{GrAlg}(G, \mathbf{G}_{m,k}) \simeq \mathrm{Hom}_{Hopf}(k[T]_T, A(G))$$

$$\simeq \{f \in A(G)^*, f \otimes f = \mu^*(f), 1 = \epsilon^*(f), f^{-1} = \sigma^*(f)\}.$$

La condition $f \in A(G)$ implique que $f = \lambda m$ avec $\lambda \in k$ et $m \in M$ et les autres conditions se résument donc à $\lambda = 1$. Cela signifie que $M(G) = M$. $\surd$

Comme première conséquence, le théorème de structure des modules de type fini sur les anneaux principaux nous dit que tout groupe abélien de type fini sans p-torsion est somme finie de copies de $\mathbf{Z}$ et de $\mathbf{Z}/l^n\mathbf{Z}$ avec $l \neq p$ premier. Il suit que tout groupe diagonalisable est produit fini de copies de $\mathbf{G}_{m,k}$ et de μ_{l^n} avec $l \neq p$ premier.

Définition 4.5.6 *Un groupe algébrique G est un* tore (algébrique) *s'il est isomorphe à $\mathbf{G}_{m,k}^n$.*

Proposition 4.5.7 *Soit G un groupe algébrique.*

1. *Les conditions suivantes sont équivalentes*
   (a) *G est diagonalisable*
   (b) *On a $G \simeq T \times H$ ou T est un tore et H un groupe abélien fini sans p-torsion.*

   De plus, T est la composante neutre de G et H est le groupe des composantes connexes.
2. *Si G est diagonalisable, les conditions suivantes sont équivalentes*
   (a) *G est un tore*
   (b) *G est connexe.*
   (c) *$M(G)$ est libre (ou sans torsion).*

Démonstration : Remarquons tout de suite qu'un tore est connexe et un groupe diagonalisable est un tore si et seulement si son groupe de caractère est libre.

Maintenant, comme un tore et un groupe abélien fini sans p-torsion sont tous deux diagonalisables, il en va de même de leur produit. Réciproquement, si G est diagonalisable, on a $M(G) \simeq \mathbf{Z}^n \oplus M$ ou M est un groupe abélien fini sans p-torsion. On en déduit que $G = T \times H$ ou T est un tore et H un groupe abélien fini sans p-torsion. Comme T est connexe d'indice fini, c'est la composante neutre de G et on en déduit un isomorphisme canonique entre H et le groupe des composantes connexes de G.

Finalement, si G est un groupe diagonalisable connexe, on a $G = T$ et G est donc un tore. $\surd$

5 Géométrie des groupes

5.1 Lissité

Si X est un espace topologique, la *fibre* en un point $x \in X$ d'un préfaisceau F est

$$F_x := \varinjlim_{x \in U} F(U)$$

ou U parcourt les ouverts de X contenant x. Si X est une variété algébrique, alors $\mathcal{O}_{X,x}$ est un anneau local dont l'idéal maximal se note $\mathfrak{m}_{X,x}$ et le corps résiduel est k. Si $f \in \mathcal{O}_{X,x}$, on notera $f(x)$ son image dans k. Dans le cas ou X est affine d'algèbre A et

$$\mathfrak{m}_x := \{f \in A, f(x) = 0\}$$

désigne l'idéal maximal de A associé à x, on a

$$\mathcal{O}_{X,x} = A_{\mathfrak{m}} \quad \text{et} \quad \mathfrak{m}_{X,x} = \mathfrak{m}_x A_{\mathfrak{m}}.$$

Notons aussi tout morphisme de variétés algébriques $\Phi : X \to Y$ induit un morphisme d'anneaux locaux $\Phi_x^* : \mathcal{O}_{Y,\Phi(x)} \to \mathcal{O}_{X,x}$.

On rappelle que si A est une k-algèbre et M un A-module, l'*espace des dérivations* de A dans M est

$$\mathrm{Der}_k(A,M) := \{D \in L(A,M), \forall f,g \in A, D(fg) = fD(g) + gD(f)\}.$$

Si X est une variété algébrique, l'*espace tangent en un point* x est

$$T_xX := \mathrm{Der}_k(\mathcal{O}_{X,x},k) = \{\xi \in A^\vee, \forall f,g \in A, \xi(fg) = f(x)\xi(g) + g(x)\xi(f)\}.$$

On voit aisément que l'on a un accouplement parfait

$$\begin{array}{ccc} T_xX \times \mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2 & \longrightarrow & k \\ (D,\overline{f}) & \longmapsto & \langle D,\overline{f}\rangle = D(f) \end{array} ,$$

et donc un isomorphisme $T_xX \simeq (\mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2)^\vee$. Si X est affine d'algèbre A, on vérifie aisément que

$$T_xX \simeq \mathrm{Der}_k(A,k) \simeq (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee.$$

On voit par exemple que $T_x\mathbf{A}_k^n \simeq k^n$ et, plus généralement, si E est un espace vectoriel de dimension finie, X un ouvert de E et $x \in X$, que l'on a un isomorphisme canonique

$$E \simeq \mathrm{Der}(S(\check{E}),k) = T_xE = T_xX.$$

Enfin, tout morphisme de variétés algébriques $\Phi : X \to Y$ induit une application linéaire

$$\begin{array}{ccc} T_xX & \xrightarrow{d\Phi_x} & T_{\Phi(x)}Y \\ \xi & \longmapsto & \xi \circ \Phi_x^* \end{array} .$$

En particulier, on voit que si $\xi \in T_xX$ et $f \in \mathfrak{m}_{Y,\Phi(x)}$, on a

$$\langle d\Phi_x(\xi),\overline{f}\rangle = \langle \xi, \overline{\Phi_x^*(f)}\rangle.$$

Par exemple, un morphisme $\phi : X \to \mathbf{A}_k^n$ va induire une application linéaire

$$\begin{array}{ccc} T_xX & \xrightarrow{d\Phi_x} & k^n \\ \xi & \longmapsto & (\xi(\Phi^*(T_1),\ldots,\xi(\Phi^*(T_n)) \end{array}$$

qui est injective si Φ est l'inclusion d'une sous variété.

Si X est irréductible, on a toujours $\dim_k T_xX \geq \dim X$ et on dit que X est *lisse en* x si l'égalité est satisfaite. En général, on dit que X est *lisse en* x s'il y a une unique composante irréductible en x et que celles-ci est lisse. Enfin, on dit que X est *lisse* s'il est lisse en tout point.

Par exemple, la courbe d'équation $y^2 = x^3 + x^2$ n'est pas lisse à l'origine car l'espace tangent en ce point est de dimension 2.

On dispose alors du théorème de lissité générique :

Théorème 5.1.1 *Toute variété algébrique sur k possède au moins un point lisse.*

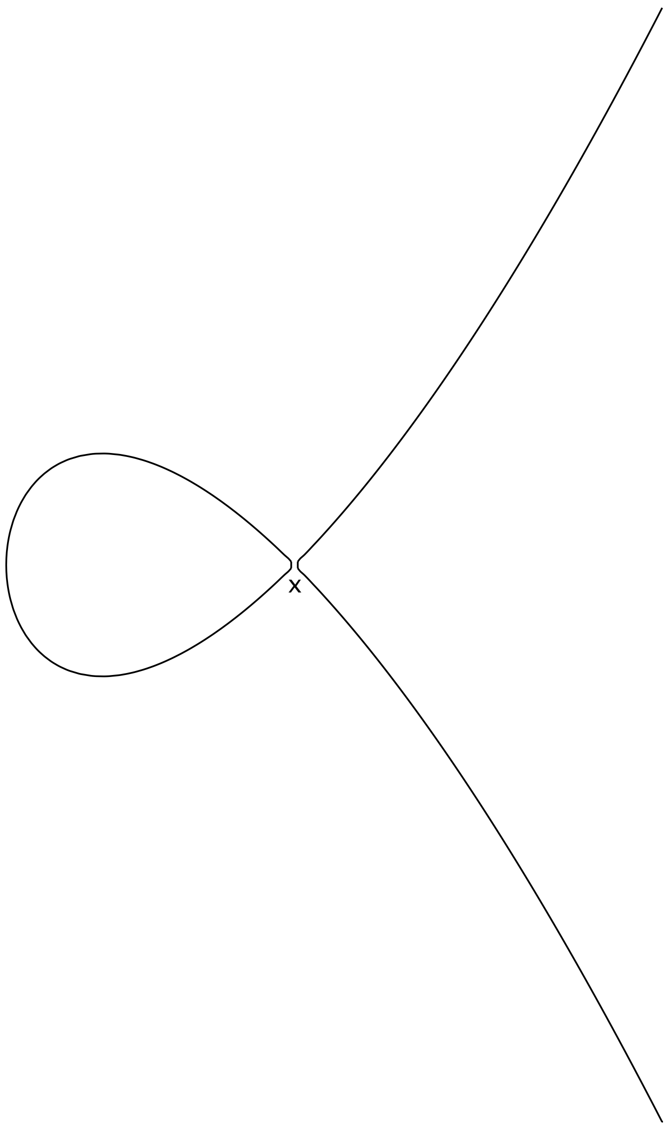

FIG. 2 – Un point double ordinaire

En fait, ceux-ci forment un ouvert dense.

On en déduit le résultat suivant :

Proposition 5.1.2 *Un groupe algébrique G est lisse. En fait, si X est une G-variété, ses orbites sont lisses. En particulier, si X est homogène, alors X est lisse.*

Démonstration : Remarquons tout d'abord que G est homogène sous l'action par translation (à droite par exemple) sur lui même et qu'une orbite est une variété homogène. Il suffit donc de montrer la seconde assertion. Grâce au théorème de lissité générique, X possède un point lisse x. Soit y un autre point. Comme X est homogène, il existe $g \in G$ tel que $y = gx$. On considère alors l'automorphisme de translation par g qui fournit un isomorphisme $Dg_x : T_xX \simeq T_yX$. $\surd$

5.2 Morphismes dominants

Si X est une variété algébrique irréductible, son *corps de fonctions* est son « anneau local au point générique » :

$$K(X) := \varinjlim_{U \subset X} \mathcal{O}_X(U).$$

On remarque tout de suite que $K(X)$ est un corps, que si U est un ouvert non vide de X, on a $K(X) = K(U)$ et que si X est affine d'algèbre A, on a $K(X) = \mathrm{Frac}(A)$.

Un morphisme $\Phi : X \to Y$ entre deux variétés algébriques est *dominant* si $\operatorname{im} \Phi$ est dense dans Y. Si X est irréductible, alors Y aussi et la condition est équivalente à dire que $\operatorname{im} \Phi$ contient un ouvert non-vide. Si X et Y sont affines d'algèbres A et B respectivement, on voit aisément que Φ est dominant si et seulement si $\Phi^* : B \to A$ est injective. Un morphisme dominant $\Phi : X \to Y$ entre variétés irréductibles induit une extension de corps $K(Y) \hookrightarrow K(X)$. On dit que Φ est *séparable* si cette extension est séparable (composée de transcendant et séparable algébrique). Par exemple, l'application de Frobenius

$$\begin{array}{ccc} \mathbf{A}^1_{\mathbf{F}_p} & \longrightarrow & \mathbf{A}^1_{\mathbf{F}_p} \\ T & \longmapsto & T^p \end{array}$$

n'est pas séparable. Mais tout morphisme dominant $X \to Y$ est séparable si $K(Y)$ est parfait, par exemple si $\operatorname{car} k = 0$.

On dispose alors du théorème suivant qui généralise le théorème de lissité générique :

Théorème 5.2.1 *Soit $\Phi : X \to Y$ un morphisme de variétés algébriques irréductibles. Alors, Φ est dominant séparable si et seulement si il existe un point lisse $x \in X$ tel que $\Phi(x)$ soit lisse et $d\Phi_x$ surjectif.*

On en déduit le résultat suivant :

Proposition 5.2.2 *Soit G un groupe algébrique connexe et $\Phi : Y \to X$ un G-morphisme de G-variétés homogènes. Alors, les conditions suivantes sont équivalentes :*

1. *Φ est séparable.*
2. *Il existe $x \in X$ tel que $d\Phi_x$ est surjectif.*
3. *Si $x \in X$, alors $d\Phi_x$ est surjectif.*

Remarquons que Φ est surjectif : en effet le morphisme composé

$$\begin{array}{ccccc} G & \longrightarrow & X & \xrightarrow{\Phi} & Y \, . \\ g & \longmapsto & gx & & \end{array}$$

est surjectif car Y est homogène et la seconde flèche l'est donc nécessairement aussi. Revenons à notre proposition.

Démonstration : On sait que les deux premières conditions sont équivalentes grâce au théorème de lissité générique relative. Et bien sûr, la dernière condition implique la seconde car $X \neq \emptyset$. Réciproquement si $d\Phi_x$ est surjectif tout autre point est de la forme gx. Si on note g_X et g_Y les morphismes d'actions par g sur X et Y respectivement, on a

$$g_Y \circ \Phi = \Phi \circ g_X$$

et il suit que

$$dg_{Y,\Phi(x)} \circ d\Phi_x = d\Phi_{gx} \circ dg_{X,x}.$$

Comme les trois autres applications sont surjectives (ou bijectives), il ne va de même de $d\Phi_{gx}$. $\surd$

Corollaire 5.2.3 *Soit $\Phi : G \to G'$ un morphisme de groupes algébriques connexes. Alors, les conditions suivantes sont équivalentes :*

1. *Φ est surjectif et séparable.*
2. *$d\Phi_1$ est surjectif.*
3. *Si $g \in G$, alors $d\Phi_g$ est surjectif.*

Remarquons qu'un morphisme dominant de groupes algébrique $\Phi : G \to G'$ est toujours surjectif car l'image est un sous-groupe fermé. Et alors, Φ fait de G' un espace homogène sous G pour lequel Φ est G-équivariant.

Démonstration : Les deux premières assertions sont donc équivalentes grâce au théorème. Et elles sont équivalentes à la troisième grace à la proposition. $\surd$

5.3 Platitude

Nous devons introduire différentes notions.

Rappelons tout d'abord que la *codimension* d'une sous variété X' d'une variété algébrique X est la différence $\dim X - \dim X'$.

Ensuite, un morphisme $\Phi : X \to Y$ est *universellement ouvert* si pour toute variété Z, le morphisme
$$\Phi \times \mathrm{Id}_Z : X \times Z \to Y \times Z$$
est ouvert. On définit de la même manière, *universellement fermé*, etc.

Enfin, on dit qu'un morphisme dominant $\Phi : X \to Y$ de variétés algébriques irréductibles est est *génériquement fini* si $[K(X) : K(Y)] < \infty$. On dit qu'il est *localement fini* en un point $x \in X$ s'il existe un voisinage ouvert affine d'algèbre A de x et un voisinage ouvert affine d'algèbre B de $\Phi(x)$ tel que Φ^* induise un morphisme fini $B \to A$. Un tel morphisme est génériquement fini.

On dispose alors du théorème de finitude générique dont nous aurons besoin plus loin :

Théorème 5.3.1 *Soit $\Phi : X \to Y$ un morphisme dominant de variétés algébriques irréductibles. S'il existe $x \in X$ tel que $|\Phi^{-1}(\Phi(x))| < \infty$ alors, Φ est localement fini en x.*

Le théorème de platitude générique est assez technique a exprimer ici :

Théorème 5.3.2 *Soit $\Phi : X \to Y$ un morphisme dominant de variétés algébriques irréductibles. Alors,* quitte à remplacer X par un ouvert non vide*, on a*

1. *Φ est universellement ouvert.*
2. *Si $Y' \subset Y$ est une sous-variété irréductible de codimension d, alors les composantes irréductibles X' de $\Phi^{-1}(Y')$ ont toutes codimension d.*
3. *Si Φ est génériquement fini, alors*
$$|\Phi^{-1}(\Phi(x))| = [K(X) : K(Y)]_s$$
pour tout $x \in X$.

Pour appliquer ça aux groupes, nous aurons besoin de la notion de *morphisme birationnel*. Cela se dit d'un morphisme dominant de variétés irréductibles $\Phi : X \to Y$ qui induit un isomorphisme $K(Y) \simeq K(X)$. Comme on le voit aisément, c'est un morphisme qui induit un isomorphisme entre un ouvert non vide de X et un ouvert non vide de Y.

Proposition 5.3.3 *Soit G un groupe algébrique et $\Phi : X \to Y$ un G-morphisme de G-variétés homogènes. Alors,*

1. *Φ est universellement ouvert.*
2. *Si $Y' \subset Y$ est une sous-variété irréductible de codimension d, alors les composantes irréductibles X' de $\Phi^{-1}(Y')$ ont toutes codimension d.*
3. *Φ est un isomorphisme si et seulement si Φ est bijectif et il existe $x \in X$ tel que $d\Phi_x$ est bijectif.*

Démonstration : Quitte à remplacer G par G° (et X et Y par des orbites sous G°), on peut supposer que G est connexe. Grace au théorème de platitude générique, on peut trouver un ouvert non vide U de X tel que les deux premières assertions soient vraies pour la restriction de Φ à U. Comme Φ est G-équivariant, elles sont aussi satisfaites sur tout gU avec $g \in G$. Comme X est homogène et que ces assertions sont de nature locale sur X, elles sont bien satisfaites.

Nous traitons maintenant la dernière assertion. La condition est bien sûr nécessaire. Réciproquement, comme Φ est bijective, c'est un morphisme génériquement fini et la dernière assertion du théorème de platitude générique implique que Φ est purement inséparable. Mais le fait que $d\Phi_x$ est surjectif implique que Φ est séparable. Donc Φ est birationnel. Il induit donc un isomorphisme entre deux ouverts. Comme Φ est G-équivariant, c'est nécessairement un isomorphisme : la condition est locale et Φ est surjectif. $\surd$

Corollaire 5.3.4 *Soit $\Phi : G \to G'$ un morphisme surjectif de groupes algébriques. Alors,*

1. *Φ est universellement ouvert.*
2. *On a $\dim G = \dim G' + \dim \ker \Phi$.*
3. *Φ est un isomorphisme si et seulement si Φ est bijectif et $d\Phi_1$ est bijectif.*

Démonstration : Résulte immédiatement de la proposition. $\surd$

6 Différentielles

6.1 Module des différentielles

Si A est une k-algèbre, le foncteur

$$M \mapsto \mathrm{Der}_k(A, M)$$

est représentable par un A-module Ω^1_A, appelé *module des différentielles* de A. Plus précisément, si on note I le noyau de la multiplication

$$\begin{array}{ccc} A \otimes_k A & \longrightarrow & A \\ f_1 \otimes f_2 & \longmapsto & f_1 f_2 \end{array} ,$$

on pose $\Omega^1_A = I/I^2$ vu comme A-module via l'action à gauche et on note

$$\begin{array}{ccc} A & \xrightarrow{d} & \Omega^1_A \\ f & \longmapsto & \overline{1 \otimes f - f \otimes 1} \end{array} .$$

Comme I est engendré comme idéal de $A \otimes_k A$ par les $1 \otimes f - f \otimes 1$, on voit que Ω^1_A est engendré comme A-module par les df. On a alors un isomorphisme

$$\begin{array}{ccc} \mathrm{Hom}_A(\Omega^1_A, M) & \xrightarrow{\simeq} & \mathrm{Der}_k(A, M) \\ u & \longmapsto & u \circ d \end{array} .$$

On écrira plus simplement $\mathrm{Der}_k(A) := \mathrm{Der}_k(A, A)$. On a alors une dualité parfaite à gauche

$$\begin{array}{rcl} \mathrm{Der}_k(A) \times \Omega^1_A & \longrightarrow & A \\ (D, df) & \longmapsto & \langle D, df\rangle := D(f) \end{array} .$$

Par exemple, si $A = k[T_1, \ldots, T_n]$, on a

$$\Omega^1_A = \oplus A dT_i \quad \text{et} \quad dF = \sum \frac{\partial F}{\partial T_i} dT_i.$$

Et si $A = k[T_1, \ldots, T_n]/(F_1, \cdots, F_r)$, alors

$$\Omega^1_A \simeq \oplus A d\overline{T_i}/(\overline{dF_j}).$$

Soit X une variété affine d'algèbre A et $x \in X$. On a alors un morphisme de suites exactes

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] \arrow[d] & A \otimes_k A \arrow[r] \arrow[d] & A \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \mathfrak{m}_x \arrow[r] & A \arrow[r] & k \arrow[r] & 0 \end{tikzcd}$$

ou la flèche du milieu est donnée par $f_1 \otimes f_2 \mapsto f_1(x) f_2$. On en déduit un morphisme

$$\begin{array}{rcl} \Omega^1_A & \longrightarrow & \mathfrak{m}_x/\mathfrak{m}_x^2 \\ \omega := f_1 df_2 & \longmapsto & \omega(x) := f_1(x)\overline{f_2 - f_2(x)} \end{array}$$

qui induit en fait un isomorphisme

$$k \otimes_A \Omega^1_A \simeq \mathfrak{m}_x/\mathfrak{m}_x^2.$$

D'autre part, on a aussi un morphisme naturel

$$\begin{array}{rcl} \mathrm{Der}_k(A) & \longrightarrow & T_x \\ D & \longmapsto & D_x \end{array}$$

défini comme suit : si $D \in \mathrm{Der}_k(A)$, l'application composée

$$\begin{array}{rcl} A & \longrightarrow & k \\ f & \longmapsto & D(f)(x) \end{array}$$

est une dérivation qui se prolonge de manière unique en une dérivation de $A_{\mathfrak{m}_x}$ par la formule

$$D_x\left(\frac{f_1}{f_2}\right) = \frac{D(f_1)(x) f_2(x) - f_1(x) D(f_2)(x)}{f_2(x)^2}.$$

On a alors un diagramme commutatif

$$\begin{tikzcd} \mathrm{Der}_k(A) \times \Omega^1_A \arrow[r] \arrow[d] & A \arrow[d] \\ T_x \times \mathfrak{m}_x/\mathfrak{m}_x^2 \arrow[r] & k \end{tikzcd} ,$$

c'est à dire que pour $D \in \mathrm{Der}_k(A)$ et $\omega \in \Omega^1_A$, on a

$$\langle D, \omega\rangle(x) = \langle D_x, \omega(x)\rangle.$$

6.2 Différentielles sur les groupes

Proposition 6.2.1 *Soit G un groupe affine d'algèbre A. Alors, l'isomorphisme*

$$\begin{array}{ccc} G \times G & \xrightarrow[\Phi]{\simeq} & G \times G \\ (g,h) & \longmapsto & (g,gh) \end{array}$$

induit un isomorphisme

$$\Phi^* : \Omega^1_A \simeq A \otimes_k \mathfrak{m}_1/\mathfrak{m}_1^2.$$

On pourra l'utiliser pour identifier $\mathfrak{m}_1/\mathfrak{m}_1^2$ à un sous-espace vectoriel de Ω^1_A via $\Phi^*(\omega) = 1 \otimes \omega$.

Démonstration : On a un diagramme commutatif

$$\begin{tikzcd} & G \arrow[dl, hook', "(\mathrm{Id}_G,1)"'] \arrow[dr, hook, "(\mathrm{Id}_G,\mathrm{Id}_G)"] & \\ G \times G \arrow[rr, "\simeq", "\Phi"'] & & G \times G \end{tikzcd}.$$

Si I est l'idéal de G dans $G \times G$, on a donc un diagramme commutatif

$$\begin{tikzcd} I \arrow[r, "\simeq"] \arrow[d, hook] & A \otimes_k \mathfrak{m}_1 \arrow[d, hook] \\ A \otimes_k A \arrow[r, "\simeq", "\Phi^*"'] & A \otimes_k A \end{tikzcd}.$$

On obtient donc comme annoncé,

$$\Omega^1_A = I/I^2 \simeq A \otimes_k \mathfrak{m}_1/\mathfrak{m}_1^2. \quad \surd$$

Corollaire 6.2.2 *On a un accouplement parfait de A-module libres*

$$\mathrm{Der}_k(A) \times \Omega^1_A \to A$$

et Φ induit un isomorphisme

$$A \otimes_k T_1 G \simeq \mathrm{Der}_k(A).$$

Ici encore, on pourra utiliser Φ pour identifier T_1G à un sous-espace vectoriel de $\mathrm{Der}_k(a)$ via $\Phi(1 \otimes D) = D$.

Démonstration : Il résulte de la proposition que Ω^1_A est libre et il suit que $\mathrm{Der}_k(A)$ qui est son dual est aussi libre et que la dualité est parfaite. La seconde assertion s'obtient alors par dualité. C'est formel. $\surd$

Proposition 6.2.3 *Soit G un groupe algébrique et X une G-variété d'algèbre A. Il existe alors une unique action de G sur Ω^1_A telle que*

$$g(f_1 df_2) = (gf_1)d(gf_2)$$

si $g \in G$ et $f_1, f_2 \in A$. Celle ci-est essentiellement finie.

Démonstration : L'action essentiellement finie de G sur A se prolonge naturellement en une action essentiellement finie sur $A \otimes_k A$. Et comme G agit par automorphismes d'anneau, la multiplication $A \otimes_k A \to A$ est G-équivariante. On a donc une action induite sur I qui préserve I^2 et qui induit donc une action essentiellement finie sur Ω^1_A. $\surd$

Par construction, cette action est semi-linéaire, c'est à dire que $g(f\omega) = (gf)(g\omega)$.

Proposition 6.2.4 *Soit G un groupe algébrique et X une G-variété d'algèbre A. Si $g \in G$ et $D \in \mathrm{Der}_k(A)$, alors*

$$gD := g \circ D \circ g^{-1} \in \mathrm{Der}_k(A)$$

et on obtient ainsi une action de G sur $\mathrm{Der}_k(A)$. De plus, si $\omega \in \Omega^1_A$, on a

$$\langle gD, g\omega\rangle = g\langle D, \omega\rangle$$

Démonstration : Il est clair que gD est k-linéaire et on a

$$\begin{aligned}(g \circ D \circ g^{-1})(f_1 f_2) &= g(D(g^{-1}(f_1 f_2))) = g(D((g^{-1}f_1)(g^{-1}f_2)))\\ = g(D(g^{-1}f_1)(g^{-1}f_2) + (g^{-1}f_1)D(g^{-1}f_2)) &= g(D(g^{-1}f_1))f_2 + f_1 g(D(g^{-1}f_2)))\\ &= (g \circ D \circ g^{-1})(f_1)f_2 + f_1(g \circ D \circ g^{-1})(f_2).\end{aligned}$$

Par dualité, pour s'assurer qu'on a bien une action, il suffit de montrer la dernière assertion. Par additivité, il suffit de traiter le cas $\omega = f_1 df_2$:

$$\begin{aligned}\langle g \circ D \circ g^{-1}, g(f_1 df_2)\rangle &= \langle g \circ D \circ g^{-1}, (gf_1)d(gf_2)\rangle\\ &= (gf_1)(g \circ D \circ g^{-1})(gf_2) = (gf_1)(g(D(f_2))\\ &= g(f_1)D(f_2) = g\langle D, f_1 df_2\rangle. \quad \surd\end{aligned}$$

Si G est un groupe algébrique, l'action par conjugaison de G sur lui même

$$\begin{aligned} G \times G &\longrightarrow G\\ (g, h) &\longmapsto \mathrm{int}_g(h) := ghg^{-1}\end{aligned}$$

induit une action linéaire Ad sur $T_1 G$. On a donc pour $g \in G$, $\mathrm{Ad}(g) = d\mathrm{int}_{g,1}$.

Nous aurons besoin dans la prochaine proposition de la notion de *contragrédient* : si $\varphi : E \simeq F$ est un isomorphisme d'espace vectoriels de dimension finie, son contragrédient est l'inverse du dual $\varphi^* = (\varphi^\vee)^{-1} : E^\vee \simeq F^\vee$. On a donc, pour $v \in E, w \in E^\vee$,

$$\langle \varphi(v), \varphi^*(w)\rangle = \langle v, w\rangle.$$

Proposition 6.2.5 *Soit G un groupe algébrique. Si on désigne par λ (resp. ρ) l'action par translation à gauche (resp. à droite), alors l'action induite sur Ω^1_A correspond via l'isomorphisme*

$$\Phi^* : \Omega^1_A \simeq A \otimes_k T_1 G^\vee.$$

à $\lambda \otimes \mathrm{Id}_{T_1 G^\vee}$ (resp. $\rho \otimes \mathrm{Ad}^*$).

Démonstration : On considère comme plus haut l'isomorphisme

$$\begin{tikzcd} G \times G \arrow[r, "\simeq", "\Phi"'] & G \times G \, . \\ (g,h) \arrow[r, mapsto] & (g,gh) \end{tikzcd}$$

Pour $g \in G$ fixé, on a alors un diagramme commutatif

$$\begin{tikzcd} (h,k) \arrow[d, mapsto] & G \times G \arrow[r, "\simeq", "\Phi"'] \arrow[d] & G \times G \arrow[d] & (h,k) \arrow[d, mapsto] \\ (gh,k) & G \times G \arrow[r, "\simeq", "\Phi"'] & G \times G & (gh,gk) \end{tikzcd}$$

dont l'assertion sur l'action par translation à gauche découle immédiatement. Pour l'action à par translation à droite, on utilise

$$\begin{tikzcd} (h,k) \arrow[d, mapsto] & G \times G \arrow[r, "\simeq", "\Phi"'] \arrow[d] & G \times G \arrow[d] & (h,k) \arrow[d, mapsto] \\ (hg^{-1},gkg^{-1}) & G \times G \arrow[r, "\simeq", "\Phi"'] & G \times G & (hg^{-1},kg^{-1}) \end{tikzcd} \, .$$

Il faut juste s'assurer que l'action induite par int_g sur $T_1G^\vee$ est bien celle annoncée. Par définition, l'action sur A est donnée par $\mathrm{int}_{g^{-1}}^*$ et c'est donc cet automorphisme qui induit l'action sur $\mathfrak{m}_1/\mathfrak{m}_1^2$. Son dual est donc bien $d\mathrm{int}_{g^{-1},1}$. Et son contragrédient est alors $d\mathrm{int}_{g,1}$. $\surd$

Corollaire 6.2.6 *L'action λ (resp. ρ) sur $\mathrm{Der}_k(A)$ correspond via l'isomorphisme*

$$\Phi : A \otimes_k T_1G \simeq \mathrm{Der}_k(A)$$

à $\lambda \otimes \mathrm{Id}_{T_1G}$ (resp. $\rho \otimes \mathrm{Ad}$).

Démonstration : C'est encore la dualité. Pour λ par exemple, on veut montrer que si $f_1 \in A$, $g \in G$ et $G \in T_1G$, on a

$$\Phi(\lambda(g)(f_1) \otimes D) = \lambda(g)(\Phi(f_1 \otimes D))$$

et il suffit de montrer que pout tout $\omega \in \Omega_A^1$, on a

$$\langle \Phi(\lambda(g)(f_1) \otimes D), \omega \rangle = \langle \lambda(g)(\Phi(f_1 \otimes D), \omega \rangle.$$

et par additivité, on peut supposer que $\Phi^*(\omega) = f_2 \otimes \eta$ avec $f_2 \in A$ et $\eta \in T_1G^\vee$. Le membre de gauche devient

$$\langle \lambda(g)(f_1) \otimes D, f_2 \otimes \eta \rangle = \lambda(g)(f_1) f_2 \langle D, \eta \rangle$$

Et le membre de droite devient

$$\lambda(g)(\langle \Phi(f_1 \otimes D), \lambda(g^{-1})(\omega) \rangle) = \lambda(g)(\langle (f_1 \otimes D)), \Phi^*(\lambda(g^{-1})(\omega)) \rangle)$$

$$= \lambda(g)(\langle f_1 \otimes D, \lambda(g^{-1})(f_2) \otimes \eta\rangle) = \lambda(g)(f_1\lambda(g^{-1})(f_2))\langle D, \eta\rangle.$$

Traitons maintenant le cas de ρ. Cette fois ci, on doit montrer que

$$\langle \Phi(\rho(g)(f_1) \otimes \mathrm{Ad}(g)(D)), \omega\rangle = \langle \rho(g)(\Phi(f_1 \otimes D)), \omega\rangle.$$

Le membre de gauche devient

$$\langle \rho(g)(f_1) \otimes \mathrm{Ad}(g)(D), f_2 \otimes \eta\rangle = \rho(g)(f_1)f_2\langle \mathrm{Ad}(g)(D), \eta\rangle$$

Et le membre de droite devient

$$\rho(g)(\langle \Phi(f_1 \otimes D), \rho(g^{-1})(\omega)\rangle) = \rho(g)(\langle (f_1 \otimes D)), \Phi^*(\rho(g^{-1})(\omega))\rangle)$$

$$= \rho(g)(\langle f_1 \otimes D, \rho(g^{-1})(f_2) \otimes \mathrm{Ad}^*(g^{-1})(\eta)\rangle) = \rho(g)(f_1\rho(g^{-1})(f_2))\langle D, \mathrm{Ad}^*(g^{-1})\rangle. \quad \surd$$

6.3 Algèbre de Lie

Une *algèbre de Lie* est un k-espace vectoriel (de dimension finie) $\mathfrak{g}$ muni d'une application bilinéaire

$$\begin{aligned} \mathfrak{g} \times \mathfrak{g} &\longrightarrow \mathfrak{g} \\ (x, y) &\longmapsto [x, y] \end{aligned}$$

satisfaisant

$$\forall x, y \in \mathfrak{g}, \quad [x, y] + [y, x] = 0$$

et l'identité de Jacobi

$$\forall x, y, z \in \mathfrak{g}, \quad [x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0.$$

C'est une *p-algèbre de Lie* si on se donne en plus un *endomorphisme de Frobenius*

$$\begin{aligned} \mathfrak{g} &\longrightarrow \mathfrak{g} \\ x &\longmapsto x^{[p]} \end{aligned}$$

qui est semi-linéaire par rapport au Frobenius de k :

$$\forall \lambda \in k, x \in \mathfrak{g}, \quad (\lambda x)^{[p]} = \lambda^p x^{[p]},$$

satisfait

$$\forall x, y \in \mathfrak{g}, \quad [x^{[p]}, y] = [x, [\cdots [x, y]] \cdots],$$

ou le produit à droite est itéré p fois, et

$$(x + y)^{[p]} = x^{[p]} + \cdots + y^{[p]}$$

avec des termes à préciser.

Par exemple, $\mathbf{M}_n(k)$ muni de

$$[M, N] := MN - NM \quad \text{et} \quad M^{[p]} := M^p$$

est une p-algèbre de Lie. Plus généralement, ces formules permettent de munir n'importe quelle k-algèbre associative d'un structure d'algèbre de Lie. De même, si A est une k-algèbre, alors $\mathrm{Der}_k(A)$ est une p-algèbre de Lie (de dimension infinie) pour

$$[D, D'] := D \circ D' - D' \circ D \quad \text{et} \quad D^{[p]} := D^p.$$

En fait, c'est une sous-algèbre de Lie de l'algèbre associative $L_k(A)$ (vérifier).

Un morphisme de p-algèbre de Lie est une application compatible avec les opérations et une sous p-algèbre de Lie est une partie stable par les opérations. Notons aussi que la somme directe de deux p-algèbres de Lie est de manière naturelle une p-algèbre de Lie.

Définition 6.3.1 *Soit G un groupe affine d'algèbre A. Alors,*

$$\mathfrak{g} := \mathrm{Lie}(G) := \{D \in \mathrm{Der}(A), \forall g \in G, \lambda(g) \circ D = D \circ \lambda(g)\}$$

est l'algèbre de Lie de G et l'application

$$\begin{array}{rcl} G & \xrightarrow{\quad\rho\quad} & \mathbf{GL}(\mathfrak{g}) \\ g & \longmapsto & (D \mapsto \rho(g) \circ D \circ \rho(g^{-1})) \end{array}$$

est la représentation adjointe.

Il faut bien sûr s'assurer que $\mathfrak{g}$ est bien une algèbre de Lie, que ρ est bien défini et que c'est une représentation. C'est l'objet du résultat suivant.

Proposition 6.3.2 *Soit G un groupe affine de dimension d et d'algèbre A. Alors, $\mathfrak{g} := \mathrm{Lie}(G)$ est une sous-p-algèbre de Lie de $\mathrm{Der}_k(A)$ de dimension d. De plus, l'isomorphisme*

$$A \otimes_k T_1G \simeq \mathrm{Der}_k(A).$$

induit un isomorphisme $T_1G \simeq \mathrm{Lie}(G)$ sous lequel ρ correspond à Ad.

Démonstration : On vérifie aisément que $\mathfrak{g}$ est une sous-p-algèbre de Lie. En fait, si $g \in G$, alors $\lambda(g)$ est un automorphisme de p-algèbre de Lie (compatible aux crochets et à Frobenius) et $\mathfrak{g}$ est la partie invariante par tous ces automorphismes.

Remarquons ensuite que l'espace des invariants de A sous l'action de ρ ou de λ est réduite aux constantes : si $f \in A$ satisfait $\rho(g)(f) = f$ pour tout $g \in G$, on a alors $f(g) = \rho(g)(f)(1) = f(1)$ (et idem pour λ).

On considère maintenant l'isomorphisme

$$A \otimes_k T_1G \simeq \mathrm{Der}_k(A).$$

Comme l'action λ (resp. ρ) sur $\mathrm{Der}_k(A)$ correspond à $\lambda \otimes \mathrm{Id}_{T_1G}$ (resp. $\rho \otimes \mathrm{Ad}$), on voit que l'on a un isomorphisme $T_1G \simeq \mathrm{Lie}(G)$ sous lequel ρ correspond à Ad. $\surd$

Il va être nécessaire de bien comprendre l'action des éléments de l'algèbre de Lie sur les fonctions.

Lemme 6.3.3 *Soit G un groupe affine d'algèbre A et*

$$\mu : G \times G \to G$$

la multiplication. Soit $f \in A$ et

$$\mu^*(f) =: \sum f_i \otimes \varphi_i.$$

Alors, pour $D \in \mathrm{Lie}(G)$, on a

$$D(f) = \sum D_1(\varphi_i) f_i.$$

Démonstration : Remarquons pour commencer que, par définition de l'unité, l'identité de G peut se décomposer en

$$G \xrightarrow{(\mathrm{Id},1)} G \times G \xrightarrow{\mu} G$$

Et on a donc $f = \sum \varphi_i(1) f_i$.

Maintenant, comme l'isomorphisme

$$\Phi^* : \Omega^1_A \simeq A \otimes_k \mathfrak{m}_1/\mathfrak{m}_1^2,$$

est induit par $\Phi := (p_1, \mu)$ ou p_1 est la première projection, on a

$$\Phi^*(1 \otimes f - f \otimes 1) = \mu^*(f) - f \otimes 1 = \sum f_i \otimes (\varphi_i - \varphi_i(1))$$

et donc

$$\Phi^*(df) = \sum f_i \otimes \overline{\varphi_i - \varphi_i(1)}.$$

Pour $D \in \mathrm{Lie} D$, on a $\Phi(D) = 1 \otimes D_1$ et donc

$$D(f) = \langle df, D\rangle = \langle \Phi^*(df), \Phi(D)\rangle = \langle \sum f_i \otimes \overline{\varphi_i - \varphi_i(1)}, 1 \otimes D_1\rangle$$

$$= \sum \langle \overline{\varphi_i - \varphi_i(1)}, D_1\rangle f_i = \sum D_1(\varphi_i) f_i. \quad \checkmark$$

Proposition 6.3.4 *Soit H un sous-groupe fermé d'idéal J d'un groupe affine G. On a alors*

$$\mathrm{Lie}(H) = \{D \in \mathrm{Lie}(G), \quad D(J) \subset J\}.$$

Démonstration : Tout d'abord, si A désigne l'algèbre de G, on voit que toute dérivation D de A telle que $D(J) \subset J$ induit une application linéaire de A/J dans lui même dont on voit de suite que c'est une dérivation. On voit aussi aisément que l'application canonique $T_1 H \to T_1 G$ est injective et par construction, on a donc le diagramme commutatif

$$\begin{tikzcd}
\{D \in \mathrm{Der}_k(A), D(J) \subset J\} \arrow[r] \arrow[d] & \mathrm{Der}_k(A/J) \arrow[dd] \\
\mathrm{Der}_k(A) \arrow[d] & \\
T_1 G & T_1 H \arrow[l, hook']
\end{tikzcd}.$$

Comme l'inclusion de H dan,s G commute avec les actions par translation, on en déduit le diagramme commutatif

$$\begin{tikzcd}
\{D \in \mathrm{Lie}(G), D(J) \subset J\} \arrow[r] \arrow[d, hook] & \mathrm{Lie}(H)\ . \arrow[dd, "\simeq"] \\
\mathrm{Lie}(G) \arrow[d, "\simeq"] & \\
T_1G & T_1H \arrow[l, hook']
\end{tikzcd}$$

Pour conclure, il suffit donc de montrer que la flèche du haut est surjective. On se donne donc $D \in \mathrm{Lie}(G)$ tel que D_1 tombe dans T_1H, c'est à dire $D_1(J) = 0$, et on veut montrer que $D(J) \subset J$. On se donne donc aussi $f \in J$ et on veut montrer que $D(f) \in J$. On a vu que si on désigne par μ la multiplication et qu'on écrit

$$\mu^*(f) =: \sum f_i \otimes \varphi_i,$$

on a alors

$$D(f) = \sum D(\varphi_i) f_i.$$

On remarque ensuite que

$$\mu^*(J) \subset J \otimes_k A + A \otimes_k J$$

car on a en fait un morphisme de suites exactes (traduisant le fait que H est un sous groupe de G) :

$$\begin{tikzcd}
0 \arrow[r] & J \arrow[r] \arrow[d] & A \arrow[r] \arrow[d, "\mu^*"] & A/J \arrow[r] \arrow[d, "\mu^*"] & 0\ . \\
0 \arrow[r] & J \otimes_k A + A \otimes_k J \arrow[r] & A \otimes_k A \arrow[r] & (A/J) \otimes_k (AJ) \arrow[r] & 0
\end{tikzcd}$$

On en déduit, que pour tout i, on a soit $f_i \in J$, et on a gagné, ou alors $\varphi_i \in J$ auquel cas $D_1(\varphi_i) = 0$ par hypothèse. $\surd$

Lemme 6.3.5 *Si G et H sont deux groupes affines, on a un isomorphisme canonique*

$$\mathrm{Lie}(G \times H) \simeq \mathrm{Lie}(G) \oplus \mathrm{Lie}(H).$$

Canonique signifie que c'est un isomorphisme de p-algèbres de Lie compatible avec les actions, avec les projections et avec les isomorphismes sur les espaces tangents.

Démonstration : Résulte par exemple des isomorphismes canoniques

$$\Omega^1_{A \otimes_k B} \simeq \Omega^1_A \otimes_k B \oplus A \otimes_k \Omega^1_B$$

si A et B sont deux k-algèbres et

$$T_{(x,y)}(X \times Y) \simeq T_xX \oplus T_yY$$

si X et Y sont deux variétés algébriques. Les détails sont laissés en exercice. $\surd$

Proposition 6.3.6 *Soit $\Phi : G \to G'$ un morphisme de groupes affines. Alors Φ induit un morphisme de p-algèbres de Lie*

$$\mathrm{Lie}(\Phi) : \mathrm{Lie}(G) \to \mathrm{Lie}(G')$$

compatible avec les actions (par translation à droite). Celui-ci correspond à $d\Phi_1$ via les isomorphismes $\mathrm{Lie}(G) \simeq T_1G$ et $\mathrm{Lie}(G') \simeq T_1G'$.

Démonstration : En général, on peut décomposer Φ en une suite de morphismes de groupes

$$\begin{array}{ccccc} G & \longrightarrow & G \times G' & \longrightarrow & G' \\ g & \longmapsto & (g, \Phi(g)) & & \\ & & (g,h) & \longmapsto & h \end{array}$$

ou le premier morphisme est l'inclusion d'un sous-groupe fermé et le second est la projection. Grace au lemme, on peut donc supposer que l'on a tout simplement une inclusion de sous-groupe $G \hookrightarrow G'$ et on peut appliquer la dernière proposition. Les détails sont à nouveau laissées au lecteur. $\surd$

6.4 Exemples

Tout d'abord, on a

$$\mathfrak{g}_{a,k} = \mathrm{Lie}(\mathbf{G}_{a,k}) \simeq k$$

avec $[x,y] = 0$ et $x^{[p]} = 0$: En effet, la « multiplication »sur $\mathbf{G}_{a,k}$ est donnée par

$$\mu^*(T) = 1 \otimes T + T \otimes 1$$

et donc la translation par $a \in k$ est donnée par

$$t_a^*(T) = T + a.$$

On a

$$\Omega^1_{k[T]} = k[T]dT \quad \text{et} \quad \mathrm{Der}_k(k[T]) = k[T]\partial_T.$$

Si $D = F(T)\partial_T$, on a d'une part

$$(D \circ t_a^*)(T) = D(t_a^*(T)) = D(T+a) = F(T)\partial_T(T+a) = F(T),$$

et d'autre part,

$$(t_a^* \circ D)(T) = t_a^*(D(T)) = t_a^*(F(T)\partial_T(T)) = t_a^*(F(T)) = F(T+a).$$

On voit donc que D est invariant si et seulement si pour tout $a \in k$,

$$F(T) = F(T+a).$$

Cela signifie que $F = c \in k$ et donc $D = c\partial_T$. On voit immédiatement que

$$[\partial_T, \partial_T] = 0 \quad \text{et} \quad \partial_T^p = 0.$$

Il n'est pas difficile de voir que

$$\mathfrak{g}_{m,k} = \mathrm{Lie}(\mathbf{G}_{m,k}) \simeq k$$

avec $[x, y] = 0$ et $x^{[p]} = x^p$. En effet, la multiplication ainsi que la translation par $a \in k^*$ sont données par

$$\mu^*(T) = T \otimes T \quad \text{et} \quad t_a^*(T) = aT.$$

On a

$$\Omega^1_{k[T]_T} = k[T]_T dT \quad \text{et} \quad \mathrm{Der}_k(k[T]_T) = k[T]_T \partial_T.$$

Si $D = F(T)\partial_T$, on a d'une part

$$(D \circ t_a^*)(T) = D(t_a^*(T)) = D(aT) = F(T)\partial_T(aT) = aF(T),$$

et d'autre part,

$$(t_a^* \circ D)(T) = t_a^*(D(T)) = t_a^*(F(T)\partial_T(T)) = t_a^*(F(T)) = F(aT).$$

On voit donc que D est invariant si et seulement si pour tout $a \in k^*$,

$$F(aT) = aF(T).$$

Cela signifie que $F = cT$ et donc $D = cT\partial_T$. On a alors

$$[T\partial_T, T\partial_T] = 0 \quad \text{et} \quad (T\partial_T)^p = T\partial_T.$$

Nous allons voir que, plus généralement, on a

$$\mathfrak{gl}_{n,k} = \mathrm{Lie}(\mathbf{GL}_{n,k}) \simeq M_n(k)$$

avec $[M, N] = MN - NM$ et $M^{[p]} = M^p$.

La multiplication ainsi que la translation à gauche par $M := [m_{ij}] \in \mathbf{GL}_n(k)$ sont données par

$$\mu^*(T_{ij}) = \sum T_{ik} \otimes T_{kj} \quad \text{et} \quad t_M^*(T_{ij}) = \sum m_{ik} T_{kj}.$$

On définit alors un morphisme (vérifier)

$$\begin{aligned} M_n(k) &\longrightarrow \mathrm{Der}_k(A) \\ M &\longmapsto D_M \end{aligned}$$

en posant $D_M(T_{ij}) := \sum T_{ik} m_{kj}$. Celui-ci est clairement injectif et à valeur dans $\mathrm{Lie}(\mathbf{GL}_{n,k})$. Pour des raisons de dimensions, c'est donc un isomorphisme de p-d'algèbres de Lie. On peut aussi voir que l'application induite $M_n(k) \simeq T_I \mathbf{GL}_{n,k}$ envoie M sur la dérivation $\xi_M : T_{ij} \mapsto m_{ij}$.

Comme on sait caractériser les algèbres de Lie des sous-groupes fermés, on montre alors que

$$\mathfrak{sl}_{n,k} = \mathrm{Lie}(\mathbf{SL}_{n,k}) \simeq \{M \in M_n(k), \mathrm{tr}M = 0\}.$$

En effet, comme $\mathbf{SL}_{n,k}$ est le sous-groupe fermé de $\mathbf{GL}_{n,k}$ défini par $\det -1$, on voit que $\mathfrak{sl}_{n,k}$ est la sous-algèbre de Lie de $\mathfrak{gl}_{n,k}$ des D_M tels que $\xi_M(\det -1) = 0$ et on a

$$\xi_M(\det -1) = \xi_M(\sum_\sigma \epsilon(\sigma) \prod_i T_{i\sigma(i)}) = \sum_\sigma \epsilon(\sigma) \xi_M(\prod_i T_{i\sigma(i)})$$
$$= \sum_\sigma \epsilon(\sigma) \sum_i (\prod_{j \neq i} \delta_{j\sigma(j)}) m_{i\sigma(i)} = \sum_i m_{ii} = \mathrm{tr} M.$$

On montre de même que

$$\mathfrak{t}_{n,k} = \mathrm{Lie}(\mathbf{T}_{n,k})$$

correspond à $\mathbf{T}_{n,k}$, que

$$\mathfrak{u}_{n,k} = \mathrm{Lie}(\mathbf{U}_{n,k})$$

correspond à la p-algèbre de Lie des matrices triangulaires supérieures à diagonale nulle, et que

$$\mathfrak{d}_{n,k} = \mathrm{Lie}(\mathbf{D}_{n,k})$$

correspond aux matrices diagonales.

Enfin,

$$\mathfrak{o}_{n,k} = \mathrm{Lie}(\mathbf{O}_{n,k})$$

correspond aux matrices antisymétriques M avec ${}^tM + M = 0$ et

$$\mathfrak{sp}_{2n,k} = \mathrm{Lie}(\mathbf{Sp}_{2n,k})$$

correspond aux matrices M qui satisfont ${}^tMJ + JM = 0$.

On finit par une remarque bien utile : si $\Phi : G \to \mathbf{GL}_{n,k}$ est un morphisme de groupes algébriques et qu'on identifie $\mathfrak{gl}_{n,k}$ avec $\mathbf{M}_{n,k}$, on a pour $D \in \mathfrak{g} := \mathrm{Lie}(G)$,

$$\mathrm{Lie}(\Phi)(D) = [D_1(\Phi^*(T_{ij}))].$$

7 Quotients et applications

7.1 Sous-groupes et représentations

En général, si E est un espace vectoriel sur k, on notera $\mathfrak{gl}(E)$ l'algèbre de Lie du groupe algébrique $\mathbf{GL}(E)$. Bien sûr, si on choisit une base de E, on déduit de l' isomorphisme $\mathfrak{gl}_{n,k} \simeq \mathbf{M}_n(k)$ un isomorphisme $\mathfrak{gl}(E) \simeq \mathbf{L}(E)$. Celui-ci est naturel dans la mesure ou on a un isomorphisme canonique

$$\mathbf{L}(E) \simeq T_1 L(E) = T_1 \mathbf{G}L(E) = \mathfrak{gl}(E).$$

Si on désigne comme d'habitude par $T(E)$, $S(E)$ et $\Lambda(E)$, l'algèbre tensorielle, respectivement symétrique ou extérieure de E, on a un morphisme de groupes algébriques évident

$$\begin{array}{ccc} \mathbf{GL}(E) & \xrightarrow{T^r} & \mathbf{GL}(T^r(E)) \\ g & \longmapsto & T^r(g) \end{array}$$

où
$$T^r(g)(v_1 \otimes \cdots \otimes v_r) = g(v_1) \otimes \cdots \otimes g(v_r)$$
et de même avec S^r et Λ^r.

Lemme 7.1.1 *Soit E un espace vectoriel de dimension finie sur k. Si $D \in \mathfrak{g}l(E)$ et $v_1, \ldots, v_r \in E$, on a*

$$\mathrm{Lie}(T^r)(D)(v_1 \otimes \cdots \otimes v_r) = \sum_i v_1 \otimes \cdots \otimes D(v_i) \otimes \cdots \otimes v_r$$

et de même avec S^r et Λ^r.

Démonstration On traite le cas de T^r, les autres étant analogues. Il suffit bien sûr de montrer que si on considère le morphisme de variétés affines

$$\begin{array}{rcl} \mathbf{L}(E) & \xrightarrow{T^r} & \mathbf{L}(T^r(E)) \\ g & \longmapsto & T^r(g) \end{array}$$

et si $\xi \in T_1L(E) = L(E)$ et $v_1, \ldots, v_r \in E$, on a

$$dT^r_{\mathrm{Id}}(\xi)(v_1 \otimes \cdots \otimes v_r) = \sum_i v_1 \otimes \cdots \otimes \xi(v_i) \otimes \cdots \otimes v_r.$$

Cela se vérifie aisément. $\surd$

Lemme 7.1.2 *Soit E un espace vectoriel de dimension finie sur k et F un sous-espace vectoriel de dimension d et $L := \Lambda^d F$. Alors,*

1. $\forall g \in \mathbf{GL}(E), \quad gF \subset F \Leftrightarrow \Lambda^d(g)L \subset L$
2. $\forall D \in \mathfrak{gl}(E), DF \subset F \Leftrightarrow \mathrm{Lie}(\Lambda^d)(D)L \subset L$

Démonstration : La première assertion est claire car, si $g \in \mathbf{GL}(E)$, on a

$$\Lambda^d(F \cap gF) = (\Lambda^d F) \cap (\Lambda^d gF) = L \cap \Lambda^d L.$$

La condition signifie que le membre de droite est non nul car ce sont deux droites. Et le membre de gauche est non nul si et seulement si $F \cap gF$ est de dimension d, c'est à dire $F = gF$.

La seconde assertion se démontre de la même façon. En fait, la condition est clairement nécessaire et on montre qu'elle est suffisante. On choisit une base base $v_1, \ldots, v_d$ de F que l'on complète en une base $v_1, \ldots, v_n$ de E. On écrit pour $i = 1, \ldots, d$, $D(v_i) = \sum_{j=1}^n a_{ij} v_j$ si bien que

$$\mathrm{Lie}(\Lambda^d)(D)(v_1 \wedge \cdots \wedge v_d) = \sum_{i=1}^d v_1 \wedge \cdots \wedge D(v_i) \wedge \cdots \wedge v_d =$$

$$= \sum_{i=1}^{d} \sum_{j>d}^{t} a_{ij}\, v_1 \wedge \cdots \wedge v_j \wedge \cdots \wedge v_d + (\sum_{i=1}^{d} a_{ii}) v_1 \wedge \cdots \wedge v_d$$

car $v_1 \wedge \cdots \wedge v_j \wedge \cdots \wedge v_d = 0$ si $j \leq d$ et $j \neq i$. Tous les vecteurs apparaissant dans la somme sont linéairement indépendants car v_j apparaît à la i-ème place. La condition implique donc que $a_{ij} = 0$ pour $j > d$. $\surd$

Proposition 7.1.3 (Chevalley) *Soit G un groupe affine d'algèbre de Lie $\mathfrak{g}$ et H un sous-groupe fermé de G d'algèbre de Lie $\mathfrak{h}$. Il existe alors une représentation linéaire algébrique $\Phi : G \to GL(E)$ et $v \in E$ tel que*

1. $H = \{g \in G, \quad \exists \lambda \in k, \quad \Phi(g)(v) = \lambda v\}$
2. $\mathfrak{h} = \{D \in \mathfrak{g}, \quad \exists \lambda \in k, \quad \mathrm{Lie}\Phi(D)(v) = \lambda v\}$

Démonstration : On montre d'abord le lemme suivant :

Lemme 7.1.4 *Soit A et l'algèbre G et J l'idéal de H. Alors, il existe un sous-espace de dimension finie E de A invariant sous l'action de G par translation à droite et un sous-espace F de E tel que*

1. $H = \{g \in G, \quad gF \subset F\}$
2. $\mathfrak{h} = \{D \in \mathfrak{g}, \quad D(F) \subset F\}$

Démonstration : Grace à la proposition 3.2.4, on peut trouver E satisfaisant la première condition et contenant des générateurs de l'idéal J. On pose alors $F := E \cap J$. On a vu que dans la proposition 3.3.4 que $g \in H$ si et seulement si $g(J) \subset J$ et dans la proposition 6.3.4 que $D \in \mathfrak{h}$ si et seulement si $D(J) \subset J$. $\surd$

Grace au lemme précédent, il suffit alors de remplacer E par $\Lambda^d(E)$ ou d est la dimension de F, pour obtenir le résultat de la proposition. $\surd$

7.2 Quotients

Nous allons voir que le quotient d'un groupe affine par un sous-groupe a une structure naturelle de variété quasi-projective. Considérons le sous-groupe $\mathbf{T}_{2,k}$ de $\mathbf{GL}_{2,k}$. On peut considérer l'action naturelle de $\mathbf{GL}_{2,k}$ sur $\mathbf{P}^1_k$:

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, x \right) \mapsto \frac{ax+b}{cx+d}.$$

C'est une action algébrique et simplement transitive et le stabilisateur de l'infini est $\mathbf{T}_{2,k}$. on a donc une bijection

$$\mathbf{GL}_{2,k}/\mathbf{T}_{2,k} \simeq \mathbf{P}^1_k$$

qui permet de munir le quotient d'une structure de droite projective par transport de structure. Ça se généralise très bien.

Proposition 7.2.1 *Soit G un groupe affine d'algèbre de lie $\mathfrak{g}$ et H un sous-groupe fermé de G d'algèbre de Lie $\mathfrak{h}$. Il existe alors une variété algébrique (quasi-projective) X homogène sous G et $x \in X$ telle que l'application*

$$\begin{array}{ccc} G & \xrightarrow{\Psi} & X \\ g & \longmapsto & gx \end{array}$$

induise des bijections

$$G/H \simeq X \quad \textit{et} \quad \mathfrak{g}/\mathfrak{h} \simeq T_xX.$$

En particulier, Ψ est séparable.

Démonstration : On peut supposer $H \neq G$. La proposition précédente nous dit qu'il existe une représentation linéaire algébrique $\Phi : G \to GL(E)$ et une droite vectorielle x dans E telle que

$$H = \{g \in G, \quad \Phi(g)(x) = x\} \quad \text{et} \quad \mathfrak{h} = \{D \in \mathfrak{g},\ \mathrm{Lie}\Phi(D)(x) \subset x\}$$

Bien sûr, on a noté x la droite dirigée par le vecteur v. On en déduit une action de G sur l'espace projectif $\mathbf{P}(E)$ et on note X l'orbite de x qui est une variété quasi-projective. C'est bien sûr une variété homogène sous l'action de G et on a $G_x = H$ si bien que Ψ induit bien une bijection $G/H \simeq X$. Il reste donc à montrer que Ψ est séparable. On considère alors la décomposition suivante de $\iota \circ \Psi$, ou $\iota : X \hookrightarrow \mathbf{P}(E)$ désigne l'inclusion,

$$\begin{array}{ccccccc} g & \longmapsto & & & & & gx \\ g & \longrightarrow & & & gv & & \\ G & \xrightarrow{\Phi} & \mathbf{GL}(E) & \longrightarrow & E \setminus 0 & \twoheadrightarrow & \mathbf{P}(E) \end{array}$$

et la décomposition correspondante sur les espaces tangents

$$\begin{tikzcd} T_1G \arrow[r] \arrow[d, equal] & T_I\mathbf{GL}(E) \arrow[r] \arrow[d, equal] & T_v(E\setminus 0) \arrow[r, two heads] \arrow[d, equal] & T_x\mathbf{P}(E) \arrow[d, equal] \\ \mathfrak{g} \arrow[r] & \mathbf{L}(E) \arrow[r] & E \arrow[r, two heads] & E/x \end{tikzcd}.$$

On a donc $D \in \mathfrak{h}$ si et seulement si $\mathrm{Lie}\Phi(D)(x) \subset x$, c'est à dire si $d(\iota\circ\Psi)_1(D) = 0$. Et comme ι est une inclusion, on en déduit que $\mathfrak{h} = \ker d\Psi_1$. On a donc une suite exacte à gauche

$$0 \longrightarrow \mathfrak{h} \longrightarrow \mathfrak{g} \longrightarrow T_xX$$

Or, en appliquant la proposition 5.3.3 à Ψ, on voit que $\dim T_xX = \dim\mathfrak{g} - \dim\mathfrak{h}$ et il suit que la suite est exacte à droite aussi. En particulier, $d_{\Psi 1} : T_1G \to T_1X$ est surjective et Ψ est donc bien séparable. $\surd$

On peut donc munir G/H d'une structure de variété algébrique (par transport de structure) mais nous devons nous assurer que ça ne dépend pas des choix. C'est l'objet du théorème suivant.

Théorème 7.2.2 *Si H est un sous-groupe fermé d'un groupe affine G, il existe un couple (X, x) universel parmi tous les couples (Y, y) formé d'une G-variété Y et d'un point y tel que $H \subset G_y$. On a en fait $G_x = H$.*

Cela signifie tout simplement que X est une G-variété munie d'un point x tel que $G_x = H$ et que si Y est une G-variété munie d'un point y tel que $H \subset G_y$, alors, il existe un unique morphisme de G-variétés $X \to Y$ qui envoie x sur y. En particulier, si X' est une autre G-variété munie d'un point x' qui a la même propriété, il existe un unique isomorphisme $X \simeq X'$ qui échange x et x'.

Démonstration : On munit G/H de la topologie quotient et on note $\pi : G \to G/H$ l'application quotient. On considère alors le faisceau des fonctions *constantes sur les classes* :

$$U \mapsto \mathcal{O}(U) = \{f \in \mathcal{O}_G(\pi^{-1}(U)), \forall g \in G, f_{|gH} \in k\}$$

(on vérifie aisément que c'est un faisceau).

On ne sait pas encore que G/H est une variété algébrique mais si on se donne Y et y comme dans l'énoncé (avec $H \subset G_y$), on peut considérer l'application

$$\begin{array}{ccc} G/H & \longrightarrow & Y \\ \overline{g} & \longmapsto & gy \end{array}.$$

Celle ci est bien sûr continue compatible avec les faisceaux d'algèbres et avec l'action de G. Et c'est la seule.

En particulier, avec X comme dans la proposition, on a une bijection continue $G/H \simeq X$ et c'est même un homéomorphisme car l'application

$$\begin{array}{ccc} G & \xrightarrow{\Psi} & X \\ g & \longmapsto & gx \end{array}$$

est ouverte. Il reste à montrer que cette application induit un isomorphisme sur les faisceaux d'algèbres, c'est à dire le lemme suivant :

Lemme 7.2.3 *Soit U un ouvert de X. Si $F \in \mathcal{O}(\Psi^{-1}(U))$ satisfait*

$$\forall g \in \Psi^{-1}(U), \forall h \in H, F(gh) = F(g),$$

il existe une unique $f \in \mathcal{O}_X(U)$ tel que

$$\forall g \in \Psi^{-1}(U), f(\Psi(g)) = F(g).$$

Démonstration : On considère le graphe

$$\Gamma \subset \Psi^{-1}(U) \times \mathbf{A}_{1,k}$$

de F et son image γ par le morphisme induit par $\Psi \times Id$:

$$\Phi : \Psi^{-1}(U) \times \mathbf{A}_{1,k} \to U \times \mathbf{A}_{1,k}.$$

Comme Ψ est universellement ouvert, Φ est ouverte. D'autre part, notre hypothèse nous dit que $\Phi^{-1}(\gamma) = \Gamma$. Il suit que γ est une sous-variété fermée de $U \times \mathbf{A}_{1,k}$.

Par construction, le morphisme composé

$$\gamma \hookrightarrow U \times \mathbf{A}_{1,k} \overset{p_1}{\twoheadrightarrow} U$$

est bijectif. C'est donc un morphisme génériquement fini et la dernière assertion du théorème de platitude générique implique que ce morphisme est purement inséparable. Il est aussi séparable car Ψ est séparable. C'est donc un morphisme birationnel, et il résulte du théorème de Zariski ci-dessous que c'est un isomorphisme. On définit alors f comme le composé :

$$U \xrightarrow{\simeq} \gamma \hookrightarrow U \times \mathbf{A}_{1,k} \overset{p_2}{\twoheadrightarrow} \mathbf{A}_{1,k} \ .$$

$\surd$

$\surd$

On a utilisé ci-dessus le théorème « principal »de Zariski :

Théorème 7.2.4 (Zariski) *Si Y est une variété lisse (ou plus généralement normale), alors tout morphisme bijectif et birationnel $X \to Y$ est un isomorphisme.*

C'est faut si Y n'est pas lisse : considérer par exemple, l'application $t \mapsto (t^2, t^3)$ de la droite vers la courbe d'équation $Y^2 = X^3$.

Théorème 7.2.5 *Si H est un sous-groupe fermé distingué d'un groupe affine G, alors G/H est un groupe affine.*

Avant de démontrer ce théorème, remarquons que, grâce à la propriété universelle, si H est un sous-groupe fermé d'un groupe affine G, l'inversion dans G induit un isomorphisme de variétés algébriques $G/H \simeq H\backslash G$. Pour voir ça, on peut utiliser le fait que l'inversion est un isomorphisme de groupes algébriques $G^{op} \simeq G$ et que $G^{op}/H^{op} = H\backslash G$.

Démonstration : Comme on suppose H distingué dans G, on a $G/H = H\backslash G$ et il suit que l'inversion dans G/H est un un isomorphisme de variétés algébriques. On considère maintenant l'action de $G \times G$ sur G par translation bilatère : $(g, h)k = gkh^{-1}$. Comme H est distingué dans G, on en déduit une action de $G \times G$ sur G/H qui est algébrique grace à la propriété universelle et le sous-groupe d'isotropie de H contient $H \times H$. La propriété universelle encore nous donne l'existence d'un morphisme de variétés algébriques

$$G/H \times G/H \simeq (G \times G)/(H \times H) \to G/H$$

qui se trouve être la multiplication tordue. Il suit que G/H est bien un groupe algébrique.

Il faut montrer que G/H est une variété affine. On note $\mathfrak{g}$ et $\mathfrak{h}$ les algèbres de Lie de G et H respectivement. Le théorème de Chevalley nous garantit l'existence d'une représentation linéaire algébrique $\Phi : G \to GL(E)$ et d'une droite $L \subset E$ telle que

$$H = \{g \in G, \quad \Phi(g)(L) \subset L\} \quad \text{et} \quad \mathfrak{h} = \{D \in \mathfrak{g}, \quad \mathrm{Lie}\Phi(D)(L) \subset L\}.$$

En particulier, on a une action du groupe algébrique sur la droite L qui correspond à un caractère

$$H \to \mathbf{GL}(L) = \mathbf{G}_{m,k}.$$

En général, si $\chi : H \to \mathbf{G}_{m,k}$ est un caractère de H, on pose

$$E_\chi := \{v \in E, \forall h \in H, \Phi(h)(v) = \chi(h)v\}.$$

Il résulte du théorème d'indépendance des caractères que l'application canonique $E' := \oplus E_\chi \to E$ est injective (et presque tous les E_χ sont donc nuls). En effet, si $v_i \in E_{\chi_i}$ pour $i = 1, \ldots, n$ satisfont $\sum v_i = 0$ et si ψ est une forme linéaire sur E, on aura pour tout $h \in H$,

$$(\sum \psi(v_i)\chi_i)(h) = \sum \psi(v_i)\chi_i(h) = \psi(\sum \chi_i(h)v_i)$$

$$= \psi(\sum \Phi(h)(v_i)) = \psi(\Phi(\sum v_i) = \psi(0) = 0.$$

Il suit que pour tout i, on a $\psi(v_i) = 0$. Et ceci étant vrai pour tout ψ, on a bien $v_i = 0$. D'autre part, comme H est distingué, E' est stable sous l'action de G. Plus précisément, on a $\Phi(g)(E_\chi) = E_{^g\chi}$ avec ${}^g\chi(h) = \chi(ghg^{-1})$. Comme, par construction $L \subset E'$, on peut supposer que $E = E'$.

On considère maintenant

$$F = \oplus L(E_\chi) \simeq \{f \in L(E), \quad \forall \chi \in M(H), f(E_\chi) \subset E_\chi\}$$

et l'action du groupe algébrique G sur F induite par la représentation adjointe

$$(g, f) \mapsto \Psi(g)(f) := \Phi(g) \circ f \circ \Phi(g)^{-1}.$$

Si $g \in \ker \Psi$, alors $\Phi(g)$ commute avec tous les $f \in F$. En particulier, $\Phi(g)$ commute avec les projecteurs sur les E_χ et laisse donc ces sous-espaces stables. Il commute alors avec tous les endormorphismes de E_χ et doit donc être la multiplication par un scalaire. En particulier, $\Phi(g)(L) \subset L$ et il suit que $g \in H$. On voit donc que Ψ fournit un homomorphisme de groupes abstraits

$$\overline{\Psi} : G/H \to \mathbf{GL}(F)$$

qui est en fait un morphisme de groupes algébriques grace à la propriété universelle du quotient.

Il suffit pour conclure de montrer que à montrer que c'est un isomorphisme sur son image qui est un sous-groupe fermé de $\mathbf{GL}(F)$ et donc un groupe affine. Grace au corollaire 5.3.4, il suffit de montrer que $d\overline{\Psi}_1$ est injectif. Comme on sait que $T(G/H)_1 \simeq \mathfrak{g}/\mathfrak{h}$, il faut donc montrer que si $D \in \mathfrak{g}$ satisfait $\mathrm{Lie}(\Psi)(D) = 0$, alors

$D \in \mathfrak{h}$. Comme Ψ est induit par la représentation adjointe, il n'est pas difficile de voir que

$$\mathrm{Lie}(\Psi)(D)(f) = [\mathrm{Lie}(\Phi)(D), f]$$

Notre condition implique donc que $\mathrm{Lie}(\Phi)(D)$ commute avec tous les $f \in F$, c'est à dire agit par multiplication par une constante sur chaque E_χ et en particulier, laisse L invariant. On a donc bien $D \in \mathfrak{h}$. $\surd$

7.3 Variétés complètes

Une variété algébrique X est *complète* (ou *propre*) si le morphisme structural $X \to 0$ est universellement fermé (pour toute variété (affine) Y, la projection $X \times Y \to Y$ est fermée).

On peut voir par exemple que $\mathbf{A}^1_k$ n'est pas complète car les projections $\mathbf{A}^2_k \to \mathbf{A}^1_k$ envoient l'hyperbole d'équation $xy = 1$ qui est fermée sur le complémentaire de 0 dans la droite qui est un ouvert (et pas fermé).

On montre que
- Si X est complète, toute sous-variété fermée de X est aussi complète.
- Si $\varphi : X \to Y$ est un morphisme de variétés algébriques avec X complète, alors $\mathrm{im}\,\varphi$ est une sous variété fermée complète de Y.
- Si X est une variété complète connexe, alors $\mathcal{O}_X(X) = k$.
- Une variété affine est complète si et seulement si elle est finie.

En fait, les seules variétés complètes que l'on rencontrera sont les variétés projectives. En effet, on a

Théorème 7.3.1 *Toute variété projective est complète.*

Nous allons démontrer le résultat suivant :

Théorème 7.3.2 *Un groupe algébrique connexe propre est nécessairement commutatif.*

Définition 7.3.3 *On appelle ça une* variété abélienne. *En dimension 1, on dit* courbe elliptique.

Remarquons aussi avant de commencer la démonstration que ça implique que tout groupe algébrique connexe de dimension 1 est commutatif. En effet, une courbe est soit affine, soit projective.

Démonstration : On considère l'image X du morphisme

$$\begin{array}{ccc} G \times G & \xrightarrow{\Phi} & G \times G \\ (h, g) & \longmapsto & (h, ghg^{-1}) \end{array}$$

qui est une sous-variété irréductible fermée. Le morphisme composé

$$\pi : X \hookrightarrow G \times G \xrightarrow{p_1} G$$

est surjectif car $p_1 \circ \Phi$ l'est et on a $\pi^{-1}(\pi(1,1)) = (1,1)$. Le théorème de platitude générique implique que $\dim X = \dim G$.

Si on fixe $g \in G$, le même raisonnement s'applique à l'image X_g du morphisme composé

$$\begin{array}{l} G \xrightarrow{(Id,g)} G \times G \xrightarrow{\Phi} G \times G \\ h \longmapsto (h, ghg^{-1}). \end{array}$$

Comme $X_g \subset X$ et que ce sont des fermés irréductibles de même dimension, on a $X_g = X$. Il suit que pour tout $g \in G$, $X_g = X_1$, ce qui nous dit que pour tout $h \in G$, on a $ghg^{-1} = h$. Le groupe G est donc bien commutatif. $\surd$

7.4 Sous-groupes paraboliques

Lemme 7.4.1 *Soit G un groupe algébrique affine et $\varphi : X \to Y$ un G-morphisme bijectif de G-variétés homogènes. Alors, X est complète si et seulement si Y l'est.*

Démonstration : Le morphisme $X \to Y$ est universellement ouvert et bijectif c'est donc un homéomorphisme universel. Il suit que si l'un des morphismes structuraux est universellement fermé, l'autre aussi. $\surd$

Définition 7.4.2 *Un sous-groupe fermé P d'un groupe affine G est* parabolique *si G/P est propre (c'est à dire projectif).*

Proposition 7.4.3 *Si P est un sous-groupe parabolique d'un groupe affine G et Q un sous-groupe parabolique de P, alors Q est un sous-groupe parabolique de G.*

Démonstration : On fixe une variété X et on considère le diagramme commutatif

$$\begin{tikzcd}
P \times G \times X \arrow[r, "\mu"] \arrow[d, "\pi"] & G \times X \arrow[d, "\pi_Q"] \\
P/Q \times G \times X \arrow[r, "\overline{\mu}"] \arrow[d, "p_2"] & G/Q \times X \arrow[ddd, "p_Q"] \\
G \times X \arrow[d, "\pi_P"] & \\
G/P \times X \arrow[r, "p_P"] & X
\end{tikzcd}$$

dans lequel toutes les flèches sont surjectives et μ est l'action par translation à droite de P sur G. On veut montrer que p_Q est fermée.

Si Y est un fermé de $G/Q \times X$, alors $\overline{\mu}^{-1}(Y)$ est un fermé de $P/Q \times G \times X$ et comme Q est parabolique dans P, on voit que $p_2(\overline{\mu}^{-1}(Y))$ est fermé. On note Z son image dans $G/P \times X$. Comme le diagramme est commutatif et que toutes les flèches sont surjectives, on a $p_Q(Y) = p_P(Z)$. Comme P est parabolique dans G, p_P est fermée et il suffit donc pour conclure de montrer que Z est fermé.

Il résulte du théorème de platitude générique que le morphisme quotient $G \to G/P$ est universellement ouvert et il suit que π_P est ouvert. Comme il est surjectif, on voit que Z est fermé si et seulement si $\pi_P^{-1}(Z)$ est fermé et il suffit donc pour conclure de montrer que $\pi_P^{-1}(Z) = p_2(\overline{\mu}^{-1}(Y))$.

On se donne donc $(g, x) \in G \times X$ et on suppose qu'il existe $p \in P$ tel que $(gp, x) \in p_2(\overline{\mu}^{-1}(Y))$ et il faut montrer que $(g, x) \in p_2(\overline{\mu}^{-1}(Y))$. Notre hypothèse implique qu'il existe $p' \in P$ tel que $(\overline{gpp'}, x) \in Y$ et on écrit alors $(g, x) = p_2(\overline{pp'}, g, x)$. $\surd$

Proposition 7.4.4 *Soit G un groupe affine. Alors,*

1. *Si $P \subset Q \subset G$ est une suite de sous-groupes fermés de G avec P parabolique, alors Q est aussi parabolique.*
2. *Un sous-groupe fermé P de G est parabolique si et seulement si P° est un sous-groupe parabolique de G°.*

Démonstration : Dans le premier cas, on a un morphisme surjectif $G/P \to G/Q$. Comme G/P est complète, il en va de même de G/Q.

On montre maintenant la seconde assertion. Tout d'abord, on remarque que G° est parabolique dans G car G/G° est le groupe des composantes connexes qui est fini et donc propre.

Pour la même raison, P° est parabolique dans P et on voit donc que si P est parabolique dans G, alors P° aussi grace à la proposition précédente. Comme l'inclusion $G^\circ/P^\circ \hookrightarrow G/P^\circ$ est une immersion fermée, on voit que P° est bien parabolique dans G°.

Réciproquement, si P° est parabolique dans G°, alors, grace à la proposition précédente, on voit que P° est parabolique dans G et par la première partie, il en va de même de P. $\surd$

7.5 Théorème du point fixe

Théorème 7.5.1 *Soit G un groupe affine connexe. Alors, G est résoluble si et seulement si G ne contient aucun sous-groupe parabolique strict ($\neq G$).*

On démontrera ça plus tard mais on peut déjà mentionner le corollaire suivant :

Corollaire 7.5.2 (Borel) *Soit G un groupe affine connexe résoluble et X une G-variété complète. Alors, X possède au moins un point fixe sous l'action de G.*

Et on a aussi la proposition suivante :

Proposition 7.5.3 (Lie-Kolchin) *Si* $\rho : G \to \mathbf{G}L(E)$ *est une représentation d'un groupe affine connexe résoluble, il existe une base de* E *telle que* $\operatorname{im}\rho \subset \mathbf{T}_{n,k}$.

On démontre le corollaire et la proposition en faisant l'hypothèse que G n'a pas de parabolique strict.

Démonstration : (du corollaire lorsque G n'a pas de parabolique strict)

Quitte à remplacer X par une orbite fermée, on peut suppose que X est homogène. Si $x \in X$, on a un morphisme bijectif $G/G_x \to X$ de variétés homogènes sous G. Comme X est complète, il en va de même de G/G_x et G_x est parabolique. Il suit que $G_x = G$ et x est un point fixe. $\surd$

Démonstration : (de la proposition lorsque G n'a pas de parabolique strict)

On procède par récurrence sur la dimension de E. On considère l'action induite sur $\mathbf{P}(E)$ qui a un point fixe $L \subset E$. C'est un droite de E stable sous l'action de G et on peut considérer la suite exacte

$$0 \longrightarrow L \longrightarrow E \longrightarrow E/L \longrightarrow 0$$

On relève une base de E/L telle que la représentation soit à valeurs dans $\mathbf{T}_{n-1,k}$ et on prolonge par un vecteur de L. $\surd$

Démonstration : (du théorème)

Si G ne possède pas de parabolique strict, la proposition que nous avons démontrée nous permet de plonger G comme sous-groupe fermé de $\mathbf{T}_{n,k}$ qui est résoluble. Et un sous-groupe d'un groupe résoluble est résoluble.

Pour la réciproque, on procède par l'absurde. On suppose donc que G est un groupe affine connexe résoluble et que $P \subset G$ est un sous-groupe parabolique connexe maximal strict. On sait que le groupe dérivé $D := D(G)$ est un sous-groupe fermé connexe, donc aussi affine résoluble et strict. On va montrer que $D \subset P$

On considère la projection $\pi : G \to G^{\mathrm{ab}} := G/D$ et on note $Q := \pi^{-1}(\pi(P))$ qui est un sous groupe fermé de G. Comme P est connexe, on a $P \subset Q^\circ \subset G$.

Si $Q^\circ = P$, comme $D \subset Q$ et que D est connexe, on a $D \subset Q^\circ = P$. Sinon, comme P est un parabolique connexe maximal, on a nécessairement $Q = G$, ce qui signifie que l'application induite $P \to G^{\mathrm{ab}}$ est surjective. On peut donc considérer le morphisme de suites exactes :

$$\begin{tikzcd}
1 \arrow[r] & D \arrow[r] & G \arrow[r] & G^{\mathrm{ab}} \arrow[r] & 0 \\
1 \arrow[r] & D \cap P \arrow[r] \arrow[u, hook] & P \arrow[r] \arrow[u, hook] & G^{\mathrm{ab}} \arrow[r] \arrow[u, equal] & 0
\end{tikzcd}$$

qui fournit un morphisme bijectif $D/(D \cap P) \simeq G/P$ de D-variétés homogènes. On voit donc que $D \cap P$ est un parabolique dans D. Par récurrence sur la dimension de G, il suite que $D \cap P = D$ et donc que $D \subset P$.

Comme P contient le groupe dérivé, c'est un sous-groupe distingué et il suit que G/P est affine. Étant une variété complète, il est fini. Comme G est connexe, il n'y a pas de sous-groupe strict d'indice fini. Contradiction. $\surd$

Notre théorème permet de comparer les sous-groupes résolubles et les sous-groupes paraboliques dans un groupe quelconque.

Corollaire 7.5.4 *Soit G un groupe affine, B un sous-groupe fermé connexe résoluble de G et P un sous-groupe parabolique de G. Alors, B est conjugué à un sous-groupe de P :*

$$\exists g \in G, \quad gBg^{-1} \subset P$$

Démonstration : On fait agir B par translation à gauche sur G/P qui est une variété complète. Grace au théorème du point fixe de Borel, il existe $g \in G$ tel que pour tout $b \in B$, on ait $bgP = gP$ et donc $g^{-1}bg \subset P$. $\surd$

Définition 7.5.5 *Un sous-groupe de* Borel *d'un groupe affine G est un sous-groupe fermé connexe résoluble maximal.*

Proposition 7.5.6 *Soit G un groupe affine. Alors,*

1. *Un sous-groupe fermé de G est parabolique si et seulement si il contient un Borel de G.*
2. *Un Borel est un sous-groupe fermé résoluble connexe parabolique.*
3. *Deux Borel sont conjugués.*

Démonstration : Soit B un Borel de G. Grâce au corollaire, si P est un parabolique, il contient un conjugué de B qui est bien sûr aussi un Borel. Comme on sait que tout groupe qui contient un parabolique est lui même parabolique, il suffit donc pour obtenir les deux premières assertions de s'assurer que B est parabolique. On peut supposer que G est connexe. Si G est résoluble, alors $G = B$ et on n'a rien à faire. Sinon, il existe un sous-groupe parabolique strict P dans G, et quitte à conjuguer, on peut grace au corollaire, supposer que $B \subset P$. Alors, B est un Borel de P et par récurrence, c'est un parabolique de P. Par composition, c'est un parabolique de G.

Maintenant, si B' est un autre Borel, c'est un parabolique et, quitte à conjuguer, on peut supposer grace au corollaire que $B \subset B'$. Par maximalité, on a $B = B'$ $\surd$

Corollaire 7.5.7 *Soit $\Phi : G \to G'$ un morphisme surjectif de groupes affines. Alors,*

1. *Si B est un Borel de G, alors, $\Phi(B)$ est un Borel de G'.*
2. *Si P est un parabolique de G, alors, $\Phi(P)$ est un parabolique de G'.*

Démonstration : Il suffit bien sûr de traiter le premier cas. L'image B' de B est un sous-groupe fermé connexe résoluble (un quotient de résoluble est résoluble). On considère alors le morphisme surjectif $G/B \to G'/B'$. Comme B est un Borel, il est parabolique et G/B est donc complète. Il suit que G'/B' est aussi complète et donc que B' est un parabolique. C'est donc bien un Borel. $\surd$

Réciproquement, si P' est un parabolique de G', alors, $P := \Phi^{-1}(P')$ est un parabolique de G' car on a alors un morphisme bijectif $G/P \simeq G'/P'$.

On peut montrer par exemple que $\mathbf{T}_{n,k}$ est un Borel de $\mathbf{GL}_{n,k}$. On sait qu'il est résoluble et connexe. Il suffit donc de montrer qu'il est parabolique. On fait agir $G := \mathbf{GL}_{n,k}$ naturellement sur $\mathbf{P}^n_k$ et on note G_1 le stabilisateur du point de coordonnées homogènes $(1, 0, \ldots, 0)$. On a donc

$$G_1 := \left\{ \begin{pmatrix} \star & \star & \cdots & \star \\ 0 & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & \star & \cdots & \star \end{pmatrix} \right\}$$

Comme $\mathbf{P}^n_k$ est homogène sous G, on a $G/G_1 \simeq \mathbf{P}^n_k$ et G_1 est donc parabolique dans G. Si on écrit $k^n = k \oplus k^{n-1}$, on voit que k^{n-1} est stable sous l'action de G_1 et on peut considérer le morphisme induit

$$\begin{array}{rcl} G_1 & \xrightarrow{\Phi} & \mathbf{GL}_{n-1,k} \\ g & \longmapsto & g_{|k^{n-1}} \end{array}$$

Par récurrence, on voit que $\Phi^{-1}(\mathbf{T}_{n-1,k}) = \mathbf{T}_{n,k}$ est parabolique dans G_1, et donc aussi dans G.

8 Exercices

Exercice 1 *Montrer que les matrices ayant une unique entrée non nulle sur chaque ligne et chaque colonne forment un sous-groupe fermé G de $\mathbf{GL}_n$. Déterminer sa dimension, sa composante neutre et son groupe de composante connexes.*

Exercice 2 *Les éléments unipotents d'un groupe algébrique G forment ils un sous-groupe ? Une partie fermée de G ? Une partie ouverte de G ? Mêmes questions avec les éléments semi-simples.*

Exercice 3 *Un groupe algébrique nilpotent est-il unipotent ? Quels sont les groupes diagonalisables unipotents ?*

Exercice 4 *Soit G un groupe affine.*

1. *Montrer que si $p \neq 0$, les éléments unipotents de G sont* les *éléments dont l'ordre est une puissance de p.*
2. *Montrer que si $p = 0$, alors* 1 *est le seul élément unipotent de G d'ordre fini.*

Exercice 5 *Soit $\pi : G \to H$ un morphisme de groupes affines de noyau N.*

1. *Montrer que le morphisme canonique $G/N \to H$ est un isomorphisme de groupes algébriques si et seulement si π et $\mathrm{Lie}(\pi)$ sont surjectifs.*
2. *Montrer que l'hypothése "$\mathrm{Lie}(\pi)$ surjectif" est nécessaire.*

Exercice 6 *Soit $\pi : G \to H$ un morphisme de groupes affines de noyau N qui est une rétraction sur un sous-groupe H de G.*

1. *Montrer que $\mathrm{Lie}(\pi)$ est surjectif.*
2. *Montrer que l'application naturelle $N \times H \to G$ est un isomorphisme de variétés algébriques.*

Exercice 7 *Montrer qu'on a un isomorphisme de groupes algébriques $\mathbf{U}_n \simeq \mathbf{G}_a^{n-1} \rtimes \mathbf{U}_{n-1}$*

Exercice 8

1. *Montrer que si G est un groupe connexe unipotent non trivial, il existe un homomorphisme de groupes algébriques $\varphi : G \to \mathbf{G}_a$ avec $\mathrm{Lie}(\varphi)$ non trivial.*
2. *Montrer qu'un groupe algébrique connexe non trivial est unipotent si et seulement si $G \simeq H \rtimes \mathbf{G}_a$ avec H unipotent connexe.*

Exercice 9 *Expliciter dans chacun des cas suivants un sous-groupe de Borel de G :*

1. $G := \mathbf{GL}_{n,k}$
2. $G := \mathbf{SL}_{n,k}$
3. $G := \mathbf{O}_{n,k}$
4. $G := \mathbf{S}p_{n,k}$.

Références

[1] Armand Borel. *Linear algebraic groups.* Mathematics Lecture Notes. W.A. Benjamin, inc., New York, New York, 1969.

[2] Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[3] J.-E Humphreys. *Linear algebraic groups.* Springer, 1975.

[4] Nathan Jacobson. *Basic Algebra*, volume I. Springer-Verlag, second edition, 1989.

[5] T. A Springer. *Linear algebraic groups.* Perspectives in mathematics, Birkhäuser, Basel, 1984.

[6] Jan R Strooker. *Introduction to categories, homological algebra and sheaf cohomology.* Cambridge University Press, Cambridge-New York-Melbourne, 1978.

[7] William C. Waterhouse. *Introduction to affine group schemes.* Springer, 1979.