CHAPITRE 3

DÉCOMPOSITION DE JORDAN, GROUPES DIAGONALISABLES, UNIPOTENTS, RÉSOLUBLES

Version du 6 décembre 2005

7. Décomposition de Jordan

7.1. Décomposition de Jordan dans End(V) et GL(V). — Commençons par rappeler quelques notions et résultats d'algèbre linéaire. On rappelle que k est algébriquement clos. Soient V un k-espace vectoriel, et $a \in \operatorname{End}(V)$.

Définition 7.1. — On dit que a est :
1) localement fini si, pour tout $v \in V$, le sous-espace engendré par les $a^i v$, $i \geq 0$, est de dimension finie.
2) semi-simple si V admet une base formée de vecteurs propres de a. Si $\dim_k V < \infty$, ceci équivaut à : a est racine d'un polynôme $P \in k[T]$ sans racines multiples.
3) nilpotent (resp. unipotent) s'il existe $n > 0$ tel que $a^n = 0$ (resp. $(a-1)^n = 0$).
4) localement nilpotent (resp. unipotent) si pour tout $v \in V$ il existe $n > 0$ tel que $a^n v = 0$ (resp. $(a-1)^n v = 0$).

Lemme 7.2. — *Supposons que $a, b \in \operatorname{End}(V)$ commutent.*
1) *Si a, b sont semi-simples, alors $a+b$ et ab le sont aussi.*
2) *Si a, b sont nilpotents, alors $a+b$ et ab le sont aussi.*
3) *Si a, b sont unipotents, alors ab l'est aussi.*

Démonstration. — 1) On voit facilement que b laisse stables les espaces propres de a, et donc V admet une base formée de vecteurs propres communs à a et b. L'assertion en découle.

2) Il existe n tel que $a^n = 0 = b^n$. Alors $(ab)^n = 0 = (a+b)^{2n}$.

3) Il existe n tel que $(a-1)^n = 0 = (b-1)^n$. Alors, comme $ab - 1 = (a-1)b + b - 1$, on a $(ab-1)^{2n} = 0$. □

***Proposition 7.3* (Décomposition de Jordan additive).** — *On suppose* $\dim_k V < \infty$. *Soit* $a \in \mathrm{End}(V)$.

(1) *Il existe* a_s *semi-simple et* a_n *nilpotent, tels que* $a_s a_n = a_n a_s$ *et* $a = a_s + a_n$. *Ces propriétés déterminent uniquement* a_s *et* a_n. *L'écriture* $a = a_s + a_n$ *s'appelle la décomposition de Jordan* (*additive*) *de* a.

(2) *Il existe des polynômes* P, Q *sans termes constants tels que* $a_s = P(a)$ *et* $a_n = Q(a)$.

(3) *Si* $b \in \mathrm{End}(V)$ *commute à* a *il commute aussi à* a_s *et* a_n.

(4) *Soient* E *un sous-espace de* V *stable par* a, *et* $W = V/E$. *Alors* E *est stable par* a_s *et* a_n, *et* $a_{|E} = a_{s|E} + a_{n|E}$ *et* $a_{|W} = a_{s|W} + a_{n|W}$ *sont les décomposition de Jordan de* $a_{|E}$ *et* $a_{|W}$.

Démonstration. — L'existence de a_s et a_n, donnés par des polynômes P et Q est bien connue, et (3) ainsi que la première assertion de (4) en découlent aussitôt. On obtient aussi l'unicité : si a'_s, a'_n vérifient les même conditions alors ils commutent à a et donc à a_s, a_n et par conséquent $a_s - a'_s = a'_n - a_n$ est à la fois semi-simple et nilpotent, donc nul.

Enfin, si E est a-stable et si $W = V/E$, il est clair que $a_{n|E}$ et $a_{n|W}$ sont nilpotents, et $a_{s|E}$ et $a_{s|W}$ sont semi-simples car annulés par le polynôme minimal de a, qui est sans racines multiples. Évidemment, $a_{s|E}$ et $a_{n|E}$ commutent, de même que $a_{s|W}$ et $a_{n|W}$. Donc, par unicité, $a_{|E} = a_{s|E} + a_{n|E}$ et $a_{|W} = a_{s|W} + a_{n|W}$ sont les décomposition de Jordan de $a_{|E}$ et $a_{|W}$. □

***Corollaire 7.4* (Décomposition de Jordan multiplicative).** — *On suppose* $\dim_k V$ *finie. Soit* $a \in \mathrm{GL}(V)$.

(1′) *Il existe* a_s *semi-simple et* a_u *unipotent, tels que* $a = a_s a_u = a_u a_s$. *Ces propriétés déterminent uniquement* a_s *et* a_u ; a_s *est la partie semi-simple de* a *définie plus haut, et* $a_u = \mathrm{id} + a_s^{-1} a_n$. *L'écriture* $a = a_s a_u$ *s'appelle la décomposition de Jordan multiplicative de* a.

(3′) *Si* $b \in \mathrm{End}(V)$ *commute à* a *il commute aussi à* a_s *et* a_u.

(4′) *Soient* E *un sous-espace de* V *stable par* a *et* $W = V/E$. *Alors* E *est stable par* a_s *et* a_u, *et* $a_{|E} = a_{s|E} a_{u|E}$ *et* $a_{|W} = a_{s|W} a_{u|W}$ *sont les décompositions de Jordan de* $a_{|E}$ *et* $a_{|W}$.

Démonstration. — Soient $a \in \mathrm{GL}(V)$ et $a = a_s + a_n$ sa décomposition de Jordan additive dans $\mathrm{End}(V)$. Comme a_s et a ont les mêmes valeurs propres, alors $a_s \in \mathrm{GL}(V)$. On pose alors $a_u = \mathrm{id} + a_s^{-1} a_n$. Le reste de la démonstration est analogue à celle de la proposition. □

***Proposition 7.5* (Décompositions pour un endomorphisme localement fini)**

Soient V *un* k*-espace vectoriel arbitraire et* a *un endomorphisme localement fini de* V.

(1) *Il existe* a_s *semi-simple et* a_n *localement nilpotent tels que* $a_s a_n = a_n a_s$ *et* $a = a_s + a_n$*, et ces propriétés déterminent uniquement* a_s *et* a_n*. L'écriture* $a = a_s + a_n$ *s'appelle la décomposition de Jordan* (*additive*) *de* a*.*

(3) *Si* $b \in \mathrm{End}(V)$ *commute à* a *il commute aussi à* a_s *et* a_n*.*

(4) *Soient* E *un sous-espace de* V *stable par* a *et* $W = V/E$*. Alors* E *est stable par* a_s *et* a_n*, et* $a_{|E} = a_{s|E} + a_{n|E}$ *et* $a_{|W} = a_{s|W} + a_{n|W}$ *sont les décomposition de Jordan de* $a_{|E}$ *et* $a_{|W}$*.*

De plus, si a *est* **inversible**, *on a aussi* $(1')$, $(3')$, *et* $(4')$*.*

Démonstration. — Cela se déduit facilement du cas de la dimension finie. □

7.2. Décomposition de Jordan pour les groupes algébriques affines. — Soient G un groupe algébrique affine et $\mathfrak{g} = \mathrm{Lie}(G)$. On note ρ la structure de G-module rationnel sur $k[G]$ définie par $(\rho(g)\phi)(h) = \phi(hg)$, et $\mathrm{d}\rho : \mathfrak{g} \to \mathrm{End}(k[G])$ sa dérivée.

Lemme 7.6. — *Les représentations* ρ *et* $\mathrm{d}\rho$ *sont fidèles.*

Démonstration. — Soit $g \in G$, $g \neq e$. Les idéaux maximaux $\mathfrak{m}_e$ et $\mathfrak{m}_g$ sont distincts, et donc il existe $\phi \in \mathfrak{m}_g$ telle que $\phi(e) \neq 0$. Comme $(\rho(g)\phi)(e) = \phi(g) = 0$, alors $\rho(g)\phi \neq \phi$. Ceci montre que $\rho(g) \neq \mathrm{id}$.

D'autre part, on a vu dans la remarque 6.23 que $\mathrm{d}\rho$ est fidèle. □

Théorème 7.7 **(Décomposition de Jordan dans** G **et** $\mathfrak{g}$**)**. —

a) *Pour tout* $g \in G$*, il existe un couple unique* $(g_s, g_u) \in G \times G$ *tel que :* $g = g_s g_u = g_u g_s$ *et* $\rho(g) = \rho(g_s)\rho(g_u)$ *est la décomposition de Jordan multiplicative de* $\rho(g)$*.*

a′) *Pour tout* $X \in \mathfrak{g}$*, il existe un couple unique* $(X_s, X_n) \in \mathfrak{g} \times \mathfrak{g}$ *tel que :* $X = X_s + X_n$*,* $[X_s, X_n] = 0$*, et* $\mathrm{d}\rho(X) = \mathrm{d}\rho(X_s) + \mathrm{d}\rho(X_n)$ *est la décomposition de Jordan de* $\mathrm{d}\rho(X)$*.*

b) *Si* $G = \mathrm{GL}(V)$ *et donc* $\mathfrak{g} = \mathfrak{gl}(V)$*, alors les décompositions précédentes coïncident avec les décompositions usuelles.*

c) *Si* $\pi : G \to H$ *est un morphisme de groupes algébriques, alors* π *et* $\mathrm{d}\pi$ *préservent les décompositions de* a) *et* a′)*.*

c′) *Si* π *est une représentation rationnelle arbitraire de* G*, alors* π *et* $\mathrm{d}\pi$ *préservent les décompositions de* a) *et* a′)*.*

Pour la démonstration, commençons par remarquer que, comme ρ et $\mathrm{d}\rho$ sont fidèles, l'unicité de la décomposition de Jordan pour $\rho(g)$ ou $\mathrm{d}\rho(X)$, entraîne l'unicité de (g_s, g_u) et de (X_s, X_n).

La suite de la démonstration nécessite plusieurs résultats intermédiaires. Dans la suite, on écrira parfois unipotent ou nilpotent au lieu de : localement unipotent ou nilpotent.

7.2.1. Démonstration de a), a′) et b) pour $\mathrm{GL}(V)$. — Le lemme suivant est laissé au lecteur. Soient V un k-espace vectoriel de dimension finie, $r \geq 1$ et $E = V \oplus \cdots \oplus V$ (r copies).

Lemme 7.8. — *Soient $g \in \mathrm{GL}(V)$ et $X \in \mathfrak{gl}(V)$. Si g ou X est semi-simple, il en est de même de l'application induite sur E, puis sur chaque $T^n(E)$ et donc sur chaque $S^n(E)$. On a un énoncé analogue si g est unipotent ou X nilpotent.*

Proposition 7.9. — *Soient $g \in \mathrm{GL}(V)$ et $X \in \mathfrak{gl}(V)$.*

1) *Si g est semi-simple, resp. unipotent, il en est de même de $\rho(g)$.*

2) *Si X est semi-simple, resp. nilpotent, il en est de même de $\mathrm{d}\rho(X)$.*

Par conséquent, si $g = g_s g_u$, resp. $X = X_s + X_n$, est la décomposition de Jordan de g dans $\mathrm{GL}(V)$, resp. de X dans $\mathfrak{gl}(V)$, alors $\rho(g_s) = \rho(g_s)\rho(g_u)$ est la décomposition de Jordan de $\rho(g)$, et $\mathrm{d}\rho(X) = \mathrm{d}\rho(X_s) + \mathrm{d}\rho(X_n)$ celle de $\mathrm{d}\rho(X)$.

Démonstration. — Posons $G = \mathrm{GL}(V)$. Alors $\mathrm{End}(V) \cong V \otimes V^*$, comme $(G \times G)$-module, et donc

$$k[\mathrm{End}(V)] \cong k[V \otimes V^*] \cong S(V^* \otimes V).$$

On en déduit que, comme $\rho(G)$-module, $k[\mathrm{End}(V)] \cong S(E)$, où E est la somme directe de $\dim_k V$ copies de V.

On a $k[G] = k[\mathrm{End}(V)]_D$, où D est le déterminant. De $D(hg) = D(h)D(g)$, on déduit évidemment que $\rho(g)D = D(g)D$, mais aussi que $\Delta(D) = D \otimes D$. On a vu en 6.19 que $X(D) = \mathrm{Tr}(X)$, pour $X \in \mathrm{Lie}(G)$. Il en résulte que $\mathrm{d}\rho(X)(D) = (1 \otimes X)\Delta(D) = \mathrm{Tr}(X)D$. Comme, d'après la remarque 6.23, $\mathrm{d}\rho(X)$ est une dérivation de $k[G]$, on en déduit que $\mathrm{d}\rho(X)(D^n) = n\,\mathrm{Tr}(X)D^n$ pour tout $n \in \mathbb{Z}$.

Supposons g ou X semi-simple. Alors, d'après le lemme, l'application induite sur $k[\mathrm{End}(V)]$ l'est aussi. De plus, si ϕ est un vecteur propre pour g ou X, de valeur propre $\xi \in k$, alors

$$\rho(g)(\phi D^{-n}) = \xi D(g)^{-n}\phi D^{-n}, \qquad \mathrm{d}\rho(X)(\phi D^{-n}) = (\xi - n\,\mathrm{Tr}(X))\phi D^{-n}.$$

Dans les deux cas, ϕD^{-n} est un vecteur propre. On en déduit que $\rho(g)$, resp. $\mathrm{d}\rho(X)$, est semi-simple.

Si g est unipotent et X nilpotent, alors $D(g) = 1$ et $\mathrm{Tr}(X) = 0$ et donc $(\rho(g) - \mathrm{id})(\phi D^{-n}) = (\rho(g) - \mathrm{id})(\phi)D^{-n}$ et $\mathrm{d}\rho(X)(\phi D^{-n}) = \mathrm{d}\rho(X)(\phi)D^{-n}$. On en déduit que $\rho(g)$, resp. $\mathrm{d}\rho(X)$, est localement unipotent, resp. nilpotent.

Ceci prouve les assertions 1) et 2), et la dernière assertion en découle par unicité de la décomposition de Jordan de $\rho(g)$ et $\mathrm{d}\rho(X)$. □

7.2.2. Fin de la démonstration du théorème 7.7. — Soient G un groupe algébrique affine et $\mathfrak{g} = \mathrm{Lie}(G)$. D'après le théorème 2.14, G est un sous-groupe fermé d'un certain $\mathrm{GL}(V)$, d'où aussi $\mathfrak{g} \subseteq \mathfrak{gl}(V)$. Posons $A = k[\mathrm{GL}(V)]$ et $B = k[G] = A/I$, où I est l'idéal de G dans A.

Soient $g \in G$, $X \in \mathfrak{g}$ et soient $g = g_s g_u$ la décomposition de Jordan de g dans $\mathrm{GL}(V)$, et $X = X_s + X_n$ celle de X dans $\mathfrak{gl}(V)$. D'après le lemme 6.24 et la remarque 6.23, $\rho(g)$ et $\mathrm{d}\rho(X)$ préservent I. Donc, d'après la proposition 7.5 (4), I est stable par $\rho(g_s), \rho(g_u)$ et $\mathrm{d}\rho(X_s), \mathrm{d}\rho(X_n)$. D'après le lemme 6.24, à nouveau, ceci entraîne que g_s, g_u appartiennent à G, et X_s, X_n à $\mathfrak{g}$. De plus, d'après 7.5 (4),

$$\rho(g)_{|B} = \rho(g_s)_{|B}\rho(g_u)_{|B}, \qquad \mathrm{d}\rho(X)_{|B} = \mathrm{d}\rho(X_s)_{|B} + \mathrm{d}\rho(X_s)_{|B}$$

sont les décompositions de Jordan de $\rho(g)_{|B}$ et $\mathrm{d}\rho(X)_{|B}$. Les assertions a), a$'$) et b) du théorème 7.7 en découlent. Reste à voir c) et c$'$).

Si $\pi : G \to H$ est une immersion fermée, l'assertion découle de la construction qui précède, en plongeant H dans un $\mathrm{GL}(V)$. Reste donc à voir le cas où π est surjectif. Dans ce cas, le comorphisme $\pi^{\#}$ identifie $k[H]$ à une sous-algèbre de $k[G]$, et c'est un sous-$\rho(G)$-module : pour tout $\phi \in k[H]$, $g \in G$ et $h \in H$, on a :

$$(\rho(g)\phi)(h) = \phi(h\pi(g)); \tag{1}$$

de façon équivalente, la structure de $k[G]$-comodule sur $k[H]$ est donnée par

$$\Delta_{k[H]} = (\mathrm{id} \otimes \pi^{\#})\Delta_H, \tag{2}$$

où Δ_H est la comultiplication de $k[H]$. Avec des notations évidentes, (1) montre que la restriction $\rho(g)|_{k[H]}$ coïncide avec $\rho_H(\pi(g))$, pour tout $g \in G$.

De plus, pour $\xi \in \mathrm{Lie}(G)$, on a $\xi \circ \pi^{\#} = d\pi(\xi)$ et donc (2) montre que la restriction de $\mathrm{d}\rho(\xi)$ à $k[H]$ est $\mathrm{d}\rho_H(\mathrm{d}\pi(\xi))$.

Appliquant ce qui précède à g, g_s, g_u et X, X_s, X_n, on déduit de la proposition 7.5 (4) que

$$\begin{cases} \rho_H(\pi(g)) & = & \rho_H(\pi(g_s))\rho_H(\pi(g_u)), \\ \mathrm{d}\rho_H(\mathrm{d}\pi(X)) & = & \mathrm{d}\rho_H(\mathrm{d}\pi(X_s)) + \mathrm{d}\rho_H(\mathrm{d}\pi(X_n)) \end{cases}$$

sont les décompositions de Jordan de $\rho_H(\pi(g))$ et de $\mathrm{d}\rho_H(\mathrm{d}\pi(X))$. Par conséquent, $\pi(g_s) = \pi(g)_s$, $\pi(g_u) = \pi(g)_u$, etc. Ceci prouve l'assertion c). Enfin, comme toute représentation rationnelle est réunion de représentations de dimension finie, l'assertion c$'$) en découle aussitôt, en utilisant encore 7.5 (4).

7.3. Éléments semi-simples, unipotents, nilpotents. —

Définition 7.10. — Soit $g \in G$. On dit que g est **semi-simple**, resp. **unipotent**, si $g = g_s$, resp. $g = g_u$. On note G_s et G_u l'ensemble des éléments semi-simples, resp. unipotents. On définit de façon analogue les éléments **semi-simples** ou **nilpotents** dans $\mathfrak{g} = \mathrm{Lie}(G)$, et les ensembles $\mathfrak{g}_s$ et $\mathfrak{g}_n$.

Remarque 7.11. — Il résulte des définitions que si $g \in G$ est à la fois semi-simple et unipotent, alors $g = e$. De même, si $X \in \mathfrak{g}$ est à la fois semi-simple et nilpotent, alors $X = 0$.

Proposition 7.12. — *G_u, resp. $\mathfrak{g}_n$, est une sous-variété fermée de G, resp. $\mathfrak{g}$.*

Démonstration. — Plongeant G dans un $\mathrm{GL}(V)$, on se ramène au cas où $G = \mathrm{GL}_n$. Alors

$$\{g \in \mathrm{GL}_n \mid g \text{ est unipotent}\} = \{g \in \mathrm{GL}_n \mid (g-1)^n = 0\},$$

$$\{X \in \mathfrak{gl}_n \mid X \text{ est nilpotent}\} = \{X \in \mathfrak{gl}_n \mid X^n = 0\},$$

et la proposition en découle. □

7.4. Groupes unipotents ou diagonalisables, groupes commutatifs. —

Définition 7.13. — Soit G un groupe algébrique affine. On dit que :

1) G est **unipotent** si tous ses éléments le sont.

2) G est **diagonalisable** s'il admet une représentation fidèle V de dimension finie n, ayant une base de vecteurs propres communs aux éléments de G. Ceci équivaut à dire que G est isomorphe à un sous-groupe de $(\mathbb{G}_m)^n$. De plus, d'après le lemme ci-dessous, ceci équivaut à dire que G est commutatif et que tous ses éléments sont semi-simples.

Lemme 7.14. — *Soient V un espace vectoriel de dimension finie, $\mathcal{C}$ une famille commutative d'endomorphismes de V. Alors*

a) *$\mathcal{C}$ est trigonalisable.*

b) *Soit $\mathcal{D}$ une sous-famille formée d'éléments semi-simples. Alors il existe une base de V où $\mathcal{D}$ est diagonale et $\mathcal{C}$ triangulaire.*

Démonstration. — On procède par récurrence sur $\dim_k V$. Si $\mathcal{C}$ est formé d'homothéties, les assertions sont vérifiées. On peut donc supposer qu'il existe $f \in \mathcal{C}$ et $a \in k$ tels que $W := \mathrm{Ker}(f - a\,\mathrm{id})$ soit non-nul et distinct de V. Alors W est stable par $\mathcal{C}$. Par hypothèse de récurrence, il existe $e_1 \in W$, vecteur propre pour $\mathcal{C}$, et une base triangulaire pour $\mathcal{C}$ dans V/ke_1. En relevant cette base dans V, on obtient une base triangulaire pour $\mathcal{C}$, d'où a).

Voyons b). Si $\mathcal{D}$ est formée d'homothéties, le résultat découle de a). Sinon, soit $f \in \mathcal{D}$ n'étant pas une homothétie. Alors $V = V_1 \oplus \cdots V_r$ (espaces propres de f), et les V_i sont $\mathcal{C}$-stables, distincts de V, et on conclut par récurrence. □

***Théorème 7.15* (Structure des groupes commutatifs)**. — *Soient G un groupe linéaire* **commutatif** *et* $\mathfrak{g} = \mathrm{Lie}(G)$. *Alors G_s et G_u sont des sous-groupes fermés, connexes si G l'est, et l'application $\phi : G_s \times G_u \to G$, $(g,h) \mapsto gh$, est un isomorphisme, dont l'inverse est donné par la décomposition de Jordan. De plus,* $\mathrm{Lie}(G_s) = \mathfrak{g}_s$, $\mathrm{Lie}(G_u) = \mathfrak{g}_n$, *et* $\mathfrak{g} = \mathfrak{g}_s \oplus \mathfrak{g}_n$.

Démonstration. — Comme G est commutatif, alors G_s et G_u sont des sous-groupes. De plus, d'après le théorème 6.26, $\mathfrak{g}$ est commutative, et on en déduit que $\mathfrak{g}_s$ et $\mathfrak{g}_n$ sont des sous-espaces vectoriels de $\mathfrak{g}$. D'après la remarque 7.11, on a $G_s \cap G_u = \{e\}$ et $\mathfrak{g}_s \cap \mathfrak{g}_n = \{0\}$.

D'après le lemme précédent, on peut plonger G dans le groupe $B_n(k)$ des matrices triangulaires, de sorte que G_s soit contenu dans le sous-groupe fermé $D_n(k)$ des matrices diagonales. Alors on a $G_s = D_n(k) \cap G$, car tout $g \in D_n(k) \cap G$ est semi-simple dans GL_n et donc dans G. Ceci montre que G_s est un sous-groupe fermé. Alors, il est clair que ϕ est un morphisme de variétés, et l'unicité de la décomposition de Jordan montre que ϕ est un isomorphisme de groupes.

Montrons que l'application $G \to G_s$, $g \mapsto g_s$ est un morphisme. Soient $g \in G \subseteq B_n(k)$ et $g = g_s g_u$ sa décomposition de Jordan. Comme g_s est diagonale et g_u triangulaire unipotente, alors g_s est la partie diagonale de g. Donc l'application $g \mapsto g_s$ n'est autre que la restriction à G de la projection $B_n(k) \to D_n(k)$, qui est clairement un morphisme de groupes. Comme $g_u = g_s^{-1}g$, on en déduit que l'application $g \mapsto (g_s, g_u)$ est un morphisme, inverse de ϕ. En particulier, G_s et G_u sont connexes si G l'est.

Enfin, soient $\mathfrak{h} = \mathrm{Lie}(D_n) = \{\text{matrices diagonales}\}$ et $\mathfrak{n} = \mathrm{Lie}(U_n) = \{\text{matrices triangulaires strictes}\}$. Alors les éléments de $\mathfrak{h}$ sont semi-simples, et ceux de $\mathfrak{n}$ nilpotents. Comme $\mathrm{Lie}(G_s) \subseteq \mathfrak{h}$ et $\mathrm{Lie}(G_u) \subseteq \mathfrak{n}$, il en résulte que $\mathrm{Lie}(G_s) \subseteq \mathfrak{g}_s$ et $\mathrm{Lie}(G_u) \subseteq \mathfrak{g}_n$. Comme $\dim G_s + \dim G_u = \dim G$ (puisque $G_s \times G_u \cong G$) et $\mathfrak{g}_s \cap \mathfrak{g}_n = \{0\}$, on en déduit que les deux inclusions sont des égalités et que $\mathfrak{g} = \mathfrak{g}_s \oplus \mathfrak{g}_n$. □

8. Caractères et groupes diagonalisables

8.1. Caractères, lemme de Dedekind. —

***Définition 8.1* (Caractères)**. — Soit G un groupe algébrique affine. Un **caractère** de G est un morphisme de groupes algébriques $G \to \mathbb{G}_m$. On note $X(G)$ l'ensemble des caractères. C'est un groupe abélien, la multiplication étant définie par $(\chi\chi')(g) = \chi(g)\chi'(g)$.

***Définition 8.2* (Espaces de poids)**. — Si V est un G-module de dimension 1, alors G agit dans V via un caractère $\chi : G \to \mathrm{GL}(V) = \mathbb{G}_m$. Ce G-module de dimension 1 sera noté k_χ. Plus généralement, si V est un G-module, on note, pour tout $\chi \in X(G)$,

$$V_\chi = \{v \in V \mid \forall g \in G,\ gv = \chi(g)v\}.$$

***Proposition 8.3* (Lemme de Dedekind)**. — *Soit G un groupe quelconque.*

a) $\Theta(G) := \mathrm{Hom}_{gpes}(G, k^*)$ *est une partie libre de* k^G *(fonctions* $G \to k$*).*

b) *pour tout G-module V, la somme $\sum_{\chi\in\Theta(G)} V_\chi$ est directe.*

Démonstration. — a) Supposons que ce ne soit pas le cas. Alors il existe une relation de dépendance linéaire $0 = a_1\chi_1 + \cdots + a_n\chi_n$, avec n minimal et donc les a_i tous non nuls (et $n \geq 2$). Soient $g, h \in G$. Alors

$$\sum_i a_i\chi_i(g)\chi_i(h) = \sum_i a_i\chi_i(gh) = 0 = \chi_1(g)\sum_i a_i\chi_i(h).$$

Soustrayant le dernier terme du premier, on obtient une relation de dépendance ayant au plus $n-1$ termes : $\sum_{i=2}^n a_i(\chi_i(g) - \chi_1(g))\chi_i = 0$. De plus, comme $\chi_1 \neq \chi_2$, il existe $g \in G$ tel que $\chi_1(g) \neq \chi_2(g)$ et donc cette relation est non triviale. Ceci contredit la minimalité de n.

b) Sinon, il existerait une relation de dépendance non triviale $0 = v_{\chi_1} + \cdots + v_{\chi_n}$ avec n minimal et chaque v_{χ_i} dans $V_{\chi_i} \setminus \{0\}$. Alors, pour tout g,

$$\sum_i \chi_i(g)v_{\chi_i} = g(\sum_i v_{\chi_i}) = 0 = \chi_1(g)(\sum_i v_{\chi_i}).$$

Soit g tel que $\chi_1(g) \neq \chi_2(g)$. On obtient une relation non triviale $0 = \sum_{i=2}^n (\chi_i(g) - \chi_1(g))v_{\chi_i}$, ce qui contredit la minimalité de n. La proposition est démontrée. $\square$

Corollaire 8.4. — *$X(G)$ est une partie libre de $k[G]$.*

Le lemme suivant sera utile plus tard. Soit H un second groupe algébrique affine.

Lemme 8.5. — a) *On a un isomorphisme de groupes $X(G \times H) \cong X(G) \times X(H)$, via $\chi \mapsto (\chi_{|G}, \chi_{|H})$.*

b) *Si G est connexe, alors $X(G)$ est sans torsion.*

Démonstration. — a) Un inverse est donné par $(\chi_1, \chi_2) \mapsto \chi_1\chi_2$ (le vérifier).

b) Si $\chi^n = 1$ alors $\chi(G)$ est contenu dans le groupe μ_n des racines n-ièmes de l'unité. Or μ_n est fini, et comme G est supposé connexe ceci entraîne $\chi(G) = \{1\}$, d'où $\chi = 1$. $\square$

8.2. Groupes diagonalisables et d-groupes. — On rappelle qu'un groupe algébrique isomorphe à $(\mathbb{G}_m)^n$ est appelé un tore (de dimension n). Pour tout $n \geq 1$, on note D_n le sous-groupe de GL_n formé des matrices diagonales ; c'est un tore de dimension n.

Proposition 8.6. — *Pour tout $n \geq 1$, $X(D_n)$ est isomorphe à $\mathbb{Z}^n$ et forme une base de $k[D_n]$.*

Démonstration. — Voyons d'abord le cas $n = 1$. Soit χ un caractère de k^*. Alors son comorphisme, $\chi^\#$, est un endomorphisme de l'algèbre $k[\mathbb{G}_m] = k[T, T^{-1}]$, et pour tout $t \in k^*$ on a $\chi(t) = \varphi(t)$, où $\varphi = \chi^\#(T)$. Comme T est inversible, il en est de même de φ. Donc φ ne s'annule pas sur k^* et on en déduit que $\varphi = aT^i$, avec $a \in k \setminus \{0\}$, $i \in \mathbb{Z}$. Puis, $\chi(st) = \chi(s)\chi(t)$ donne $a = 1$. On en déduit que $X(k^*)$ est formé des T^i, $i \in \mathbb{Z}$. Il est donc isomorphe à $\mathbb{Z}$ et forme une base de $k[\mathbb{G}_m]$.

Pour n arbitraire, on choisit un isomorphisme $D_n \cong (k^*)^n$, d'où un isomorphisme $k[D_n] \cong k[T_1^\pm, \ldots, T_n^\pm]$. Alors, il résulte du lemme 8.5.a) et de ce qui précède que $X(D_n)$ est formé des fonctions $\{T_1^{i_1} \cdots T_n^{i_n} \mid (i_1, \ldots, i_n) \in \mathbb{Z}^n\}$. Il est isomorphe à $\mathbb{Z}^n$ et forme une base de $k[D_n]$. $\square$

Définition 8.7. — Soit G un groupe algébrique affine. On dira (provisoirement) que G est un **d-groupe** si $X(G)$ engendre $k[G]$ (et donc en forme une base, d'après le lemme de Dedekind).

D'après ce qui précède, D_n est un d-groupe.

Proposition 8.8. — *Soit G un d-groupe.*

a) *$X(G)$ est de type fini et G est diagonalisable.*

b) *Soit H un sous-groupe fermé de G . Alors H est un d-groupe, et l'application de restriction $X(G) \to X(H)$ est surjective. De plus, H est égal à l'intersection des* $\operatorname{Ker} \chi$*, pour les $\chi \in X(G)$ tels que $\chi_{|H} = 1$.*

Démonstration. — a) Soient $x_1, \ldots, x_r$ des générateurs de l'algèbre $k[G]$. Ils s'écrivent comme combinaisons linéaires d'un nombre fini de caractères $\chi_1, \ldots, \chi_n$. Alors les χ_i engendrent $k[G]$ comme algèbre, d'où $k[G] = \bigoplus_{(i_1,\ldots,i_n)\in\mathbb{N}^n} k\chi_1^{i_1} \ldots \chi_n^{i_n}$. Le lemme de Dedekind entraîne alors que tout $\chi \in X(G)$ est une somme à coefficients dans $\mathbb{N}$ des χ_i, d'où la 1ère assertion de a).

Enfin, l'application $\phi : G \to (k^*)^n$, $g \mapsto (\chi_1(g), \ldots, \chi_n(g))$ est clairement un morphisme de groupes algébriques. C'est une immersion fermée car son comorphisme $\phi^\# : k[T_1^\pm, \ldots, T_n^\pm] \to k[G]$ est surjectif, puisque $\phi^\#(T_i) = \chi_i$.

b) Comme l'application de restriction $k[G] \to k[H]$ est surjective, et $k[G]$ engendré par $X(G)$, alors $k[H]$ est engendré par les $\chi_{|H}$, pour $\chi \in X(G)$. Or les $\chi_{|H}$ sont des caractères de H, et ceci montre que H est un d-groupe. En particulier, si $\theta \in X(H)$ alors θ est la restriction d'un élément $\sum_i a_i\chi_i$ de $k[G]$, et donc dans $X(H)$ on a l'égalité $\theta = \sum_i a_i\chi_{i|H}$. D'après le lemme de Dedekind, ceci entraîne $\theta = \chi_{i|H}$, pour un i.

Enfin, soit I l'idéal de H dans $k[G]$. Il faut montrer que I est engendré par les éléments $\chi - 1$, pour $\chi \in X(G)$ tel que $\chi_{|H} = 1$. Soit $f \in I$. Ecrivons $f = \sum_{i=1}^n a_i\chi_i$. D'après le lemme de Dedekind, à nouveau, on se ramène au cas où les χ_i ont tous la même restriction à H. Alors chaque $\chi_i\chi_1^{-1}$ est trivial sur H et, comme $\sum_i a_i = f(e) = 0$, on obtient que $f = \sum_{i=1}^n a_i\chi_1(\chi_i\chi_1^{-1} - 1)$, d'où l'assertion cherchée. □

Remarque 8.9. — Avec d'autres méthodes, on peut montrer que $X(G)$ est de type fini pour tout groupe algébrique G. Ceci découle de la Prop. 1.3, p. 79, dans [**KSS**].

Théorème 8.10 **(Caractérisation des groupes diagonalisables)**
Soit G un groupe algébrique affine. Les conditions suivantes sont équivalentes :
a) *G est commutatif et $G = G_s$*
b) *G est diagonalisable*
c) $k[G] = kX(G)$
d) *Tout G-module rationnel V est somme directe de modules k_χ, $\chi \in X(G)$.*

Démonstration. — On a déjà vu que a) $\Leftrightarrow$ b), et l'équivalence b) $\Leftrightarrow$ c) résulte des propositions 8.6 et 8.8. D'autre part, il est clair que d) $\Rightarrow$ b).

Prouvons que a) $\Rightarrow$ d). Soit V un G-module rationnel. D'après la proposition 8.3, les V_χ, $\chi \in X(G)$, sont en somme directe. Montrons que $V = \sum_{\chi\in X(G)} V_\chi$. Il suffit de voir cela quand V est de dimension finie. Dans ce cas, d'après le lemme 7.14, V admet une base $\{e_1, \dots, e_n\}$ où G agit sur chaque e_i par un caractère χ_i. Le théorème est démontré. □

8.3. Tores. — Soient G un groupe diagonalisable et $\chi_1, \dots, \chi_r \in X(G)$. On considère le morphisme $\phi : G \to (k^*)^r$, $g \mapsto (\chi_1(g), \dots, \chi_r(g))$.

Proposition 8.11. — a) *ϕ est une immersion fermée $\Leftrightarrow$ les χ_i engendrent $X(G)$.*
b) *ϕ est surjectif $\Leftrightarrow$ les χ_i sont linéairement indépendants.*

Démonstration. — Supposons que les χ_i engendrent $X(G)$. Comme $k[G] = kX(G)$, alors $k[G]$ est engendré comme algèbre par les $\chi_i^{\pm}$. Il en résulte que le comorphisme $\phi^\#$ est surjectif, puisque $\phi^\#(T_i^{\pm}) = \chi_i^{\pm}$. Donc ϕ est une immersion fermée. Réciproquement, si ϕ est une immersion fermée alors, d'après la proposition 8.8.b, $\phi^\#$ induit une surjection $X((k^*)^r) \to X(G)$. Comme les T_i engendrent $X((k^*)^r)$, alors les $\phi^\#(T_i) = \chi_i$ engendrent $X(G)$.

Prouvons b). Si $\phi(G)$ est un sous-groupe propre, il est contenu, d'après la dernière assertion de 8.8.b, dans le noyau d'un caractère non trivial $T_1^{a_1} \cdots T_r^{a_r}$.

Alors on la relation $\sum_i a_i \chi_i = 0$. Réciproquement, si ϕ est surjectif alors $\phi^\#$ induit une injection $X((k^*)^r) \hookrightarrow X(G)$, $T_i \mapsto \chi_i$. Il en résulte que les χ_i sont linéairement indépendants dans $X(G)$, puisque les T_i le sont dans $X((k^*)^r)$. $\square$

Corollaire 8.12. — *Soit G diagonalisable. Les conditions suivantes sont équivalentes : a) G est connexe, b) $X(G)$ est sans-torsion, c) G est un tore.*

Démonstration. — c) $\Rightarrow$ a) est clair, et on a vu que a) $\Rightarrow$ b) dans le lemme 8.5.b). Enfin, b) $\Rightarrow$ c) résulte de la proposition précédente. En effet, $X(G)$ est de type fini et sans torsion donc libre, et il suffit de prendre pour $\chi_1, \dots, \chi_r$ une base de $X(G)$. $\square$

Le corollaire admet la généralisation suivante.

Théorème 8.13. — *Soit G un groupe diagonalisable. Alors G^0 est un tore et $G \cong F \times G^0$, où $F \cong G/G^0$, et* car(k) *ne divise pas l'ordre de F.*

Démonstration. — On plonge G dans un D_n. Alors l'application de restriction $\pi : X(D_n) \to X(G^0)$ est surjective. Comme $X(G^0)$ est libre, π est scindée. Donc il existe une base $\{\chi_1, \dots, \chi_n\}$ de $X(D_n)$ et $r \leq n$ tels que $\{\chi_{1|G^0}, \dots, \chi_{r|G^0}\}$ soit une base de $X(G^0)$, et $\chi_{i|G^0} = 1$ pour $i > r$. D'après la proposition 8.11, le morphisme $g \mapsto (\chi_1(g), \dots, \chi_n(g))$ induit un automorphisme de D_n, qui envoie G^0 sur $(k^*)^r \times \{1\}^{n-r}$.

On en déduit que $G = G^0 \times F$, où $F = G \cap \big(\{1\}^r \times (k^*)^{n-r}\big)$. Alors $F \cong G/G^0$. De plus, si $\mathrm{car}(k) = p$ alors F est sans p-torsion car si $(t_1^p, \dots, t_{n-r}^p) = (1, \dots, 1)$ alors $t_i = 1$ pour tout i. $\square$

8.4. Rigidité des groupes diagonalisables. —

Proposition 8.14. — *Soient V une variété connexe, H, H' des groupes algébriques, et $\alpha : V \times H \to H'$ un morphisme de variétés tel que*

$$\alpha(v, gh) = \alpha(v, g)\alpha(v, h), \qquad \forall v \in V,\ g, h \in H.$$

On suppose que les éléments d'ordre fini sont denses dans H, et que, pour tout n, l'ensemble des éléments d'ordre n dans H' est fini. Alors $\alpha(x, h) = \alpha(y, h)$, pour tout $x, y \in V$, $h \in H$.

Démonstration. — Pour $h \in H$, notons β_h le morphisme $V \to H'$, $v \mapsto \alpha(v, h)$. Supposons $h^n = 1$. Alors $\beta_h(v)^n = 1$, car $\beta_h(v)^n = \alpha(v, h)^n = \alpha(v, h^n)$. Comme l'ensemble $\{x \in H' \mid x^n = 1\}$ est fini, et V connexe, on en déduit que β_h est constant. Par conséquent, pour x, y fixés dans V, le morphisme $\theta_{x,y} : h \mapsto \alpha(x, h)\alpha(y, h)^{-1} = \beta_h(x)\beta_h(y)^{-1}$ prend la valeur e sur l'ensemble dense des éléments de H d'ordre fini, et est donc constant. La proposition est démontrée. $\square$

Lemme 8.15. — *Soient X, Y deux variétés et $D \subseteq X$, $E \subseteq Y$ des parties denses. Alors $D \times E$ est dense dans $X \times Y$.*

Démonstration. — Laissée au lecteur. □

Soit H un groupe diagonalisable. D'après le théorème 8.13, on a $H \cong (k^*)^r \times F$, où F est un groupe fini. On voit aussitôt que, pour tout n, l'ensemble des éléments d'ordre n est fini. D'autre part, dans k^* les éléments d'ordre fini sont denses (car en nombre infini) et on en déduit qu'il en est de même dans H, grâce au lemme ci-dessus. On en déduit le

***Théorème 8.16* (Rigidité des groupes diagonalisables)**. —
Soient G un groupe algébrique et H un sous-groupe fermé diagonalisable. Alors $N_G(H)^0 = C_G(H)^0$. Par conséquent, $W_G(H) := N_G(H)/C_G(H)$ est un groupe fini.

Démonstration. — Appliquant la proposition au triplet $(N_G(H)^0, H, H)$, avec $\alpha(g, h) = ghg^{-1}$, on obtient que $N_G(H)^0$ est contenu dans $C_G(H)$, d'où l'égalité $C_G(H)^0 = N_G(H)^0$.

Montrons la 2ème assertion. D'abord, $C_G(H)$ est normal dans $N_G(H)$. En effet, si $g \in N_G(H)$, $x \in C_G(H)$ et $h \in H$, alors

$$(gxg^{-1})\, h = g\, x\, (g^{-1}hg)\, g^{-1} = g\, (g^{-1}hg)\, x\, g^{-1} = h\, (gxg^{-1}).$$

Enfin, le quotient $N_G(H)/C_G(H)$ est fini car $C_G(H)$ contient $N_G(H)^0$. Ceci prouve le théorème. □

8.5. Centralisateurs de tores : un lemme. — Le lemme suivant sera utile plus loin.

Lemme 8.17. — *Soit T un tore de G. Il existe $t \in T$ tel que $C_G(t) = C_G(T)$ et $\mathfrak{g}^t = \mathfrak{g}^T$.*

Démonstration. — Plongeant G dans un $\mathrm{GL}(V)$, on se ramène au cas où $G = \mathrm{GL}(V)$ (car $C_G(T) = G \cap C_{\mathrm{GL}(V)}(T)$, etc.). On a $V = V_{\chi_1} \oplus \cdots \oplus V_{\chi_r}$ pour certains $\chi_i \in X(T)$, deux à deux distincts, et, pour $i \neq j$, $\mathrm{Ker}(\chi_i\chi_j^{-1})$ est un sous-groupe propre, donc de dimension $< \dim T$ (car T connexe). Donc la réunion des $\mathrm{Ker}(\chi_i\chi_j^{-1})$ est une sous-variété fermée propre, et il existe $t \in T$ tel que $\chi_i(t) \neq \chi_j(t)$ pour $i \neq j$. On a alors

$$C_G(t) = \prod_{i=1}^{r} \mathrm{GL}(V_{\chi_i}) \subseteq C_G(T) \subseteq C_G(t),$$

$$\mathfrak{gl}(V)^t = \prod_{i=1}^{r} \mathfrak{gl}(V_{\chi_i}) \subseteq \mathfrak{gl}(V)^T \subseteq \mathfrak{gl}(V)^t,$$

d'où les égalités voulues. $\square$

Remarque 8.18. — L'énoncé est en défaut si T n'est pas connexe ; par exemple si $T = \{\pm 1\}^3 \subseteq \mathrm{GL}(3)$.

9. Le couplage $X(T) \times X^{\vee}(T) \to \mathbb{Z}$

Définition 9.1. — Soit T un tore de dimension r. On note $X^{\vee}(T)$ l'ensemble des morphismes de groupes algébriques de $\mathbb{G}_m$ vers T. Il est muni d'une structure de groupe abélien : si $\gamma, \gamma' \in X^{\vee}(T)$, on définit $\gamma+\gamma'$ par $(\gamma+\gamma')(t) = \gamma(t)\gamma'(t)$, pour $t \in \mathbb{G}_m$.

Ce qui suit est repris d'un problème donné en 1997-1998, qui apporte des compléments sur le couplage $X(T) \times X^{\vee}(T) \to \mathbb{Z}$ et sur les isomorphismes

$$X(T) \otimes_{\mathbb{Z}} k \cong \mathrm{Lie}(T)^*, \qquad X^{\vee}(T) \otimes_{\mathbb{Z}} k \cong \mathrm{Lie}(T).$$

Pour tout sous-groupe M de $X(T)$, on pose $\mathrm{Ker}(M) = \bigcap_{\chi \in M} \mathrm{Ker}\, \chi$.

9.1. Le couplage $X(T) \times X^{\vee}(T) \to \mathbb{Z}$. —

1.1) Montrer que $\gamma + \gamma'$ est bien un élément de $X^{\vee}(T)$.

1.2) Montrer que $X^{\vee}(T)$ et $X(T)$ sont isomorphes à $\mathbb{Z}^r$. Pour cela, identifier T à $(k^*)^r$, et montrer qu'alors tout élément de $X^{\vee}(T)$ (resp. $X(T)$) est donné par $t \mapsto (t^{n_1}, \dots, t^{n_r})$, (resp. $(t_1, \dots, t_n) \mapsto t_1^{m_1} \cdots t_r^{m_r}$), avec les n_i et m_i dans $\mathbb{Z}$, et que ceci fournit les isomorphismes voulus.

1.3) Soient $\chi \in X(T)$ et $\gamma \in X^{\vee}(T)$. Alors $\chi \circ \gamma$ est un endomorphisme de $\mathbb{G}_m = k^*$. En déduire qu'il existe un entier n tel que $(\chi \circ \gamma)(t) = t^n$, quel que soit $t \in k^*$. On notera $\langle \chi, \gamma \rangle$ cet entier. Montrer que $\langle\ ,\ \rangle : X(T) \times X^{\vee}(T) \to \mathbb{Z}$ est bilinéaire.

1.4) Montrer que le couplage $\langle\ ,\ \rangle : X(T) \times X^{\vee}(T) \to \mathbb{Z}$ est *parfait*, c.à.d. que les applications induites $X^{\vee}(T) \to \mathrm{Hom}_{\mathbb{Z}}(X(T), \mathbb{Z})$ et $X(T) \to \mathrm{Hom}_{\mathbb{Z}}(X(T)^{\vee}, \mathbb{Z})$ sont des isomorphismes. (Utiliser la question 1.2).

1.5) Soit $\{\gamma_1, \dots, \gamma_r\}$ une base du $\mathbb{Z}$-module $X(T)$. Montrer qu'il existe une base $\{y_1, \dots, y_r\}$ de $X^{\vee}(T)$ telle que l'application $\phi : (k^*)^r \to T$, $(t_1, \dots, t_r) \mapsto \prod_{i=1}^r y_i(t_i)$ soit un isomorphisme et vérifie $\gamma_i \circ \phi = pr_i$ pour tout i.

1.6) Soit M un sous-groupe de $X(T)$. On veut montrer que $\mathrm{Ker}(M)$ est fini si et seulement si M est d'indice fini dans $X(T)$. Soit s le rang de M. D'après le théorème de structure des $\mathbb{Z}$-modules de type fini, il existe une base $\{\gamma_1, \dots, \gamma_r\}$ de $X(T)$ et des entiers $m_1, \dots, m_s \geq 1$ tels que $\{m_1\gamma_1, \dots, m_s\gamma_s\}$ soit une base de M. (On ne demande pas de redémontrer ce résultat).

Déduire alors de la question précédente qu'il existe un isomorphisme ψ : $T \xrightarrow{\sim} (k^*)^r$ tel que

$$\psi(\mathrm{Ker}(M)) = (k^*)^{r-s} \times \{(t_1, \dots, t_s) \in (k^*)^s \mid t_i^{m_i} = 1, \text{ pour } i = 1, \dots, s\}.$$

En tirer l'équivalence cherchée.

9.2. Lien avec $\mathrm{Lie}(T)$**.** —

2.1) Si y est un élément de $X^\vee(T)$, alors $\mathrm{d}y$ est une application linéaire $k \to \mathrm{Lie}(T)$, et à y on peut donc associer l'élément $\mathrm{d}y(1)$ de $\mathrm{Lie}(T)$, qu'on notera $\delta(y)$. Montrer que $\delta(y + y') = \delta(y) + \delta(y')$, pour $y, y' \in X^\vee(T)$, puis que δ induit une application k-linéaire $\delta_k : X^\vee(T) \otimes_{\mathbb{Z}} k \to \mathrm{Lie}(T)$.

medskip2.2) On choisit une identification $T \cong (k^*)^r$, d'où aussi une identification $\mathrm{Lie}(T) \cong k^r$. Pour $i = 1, \dots, r$, soit y_i l'élément de $X^\vee(T)$ défini par $y_i(t) = (1, \dots, t, \dots, 1)$ (c.-à-d., t à la i-ème place). Montrer que $\mathrm{d}y_i(1) = e_i$, le i-ème vecteur de la base canonique de k^r. En déduire que δ_k est un isomorphisme.

2.3) D'autre part, si χ est un élément de $X(T)$, alors sa différentielle $\mathrm{d}\chi$ est une application linéaire $\mathrm{Lie}(T) \to k$, c.-à-d., un élément de $\mathrm{Lie}(T)^*$. Montrer que $\mathrm{d}(\chi\chi') = \mathrm{d}\chi + \mathrm{d}\chi'$, pour $\chi, \chi' \in X(T)$, c.-à-d., puis que d induit une application k-linéaire $X(T) \otimes_{\mathbb{Z}} k \to \mathrm{Lie}(T)^*$, qu'on notera ϕ.

2.4) Soient $\chi \in X(T)$ et $y \in X^\vee(T)$. Montrer que $\mathrm{d}\chi(\mathrm{d}y(1)) = \langle \chi, y \rangle$. En déduire que ϕ est un isomorphisme et, plus précisément, que ϕ est la transposée de δ_k^{-1}.

2.5) On suppose k de caractéristique nulle. Un sous-groupe L d'un k-espace vectoriel V de dimension finie est appelé un *réseau* s'il est engendré par une base de V. Montrer que δ et d sont injectives et identifient $X^\vee(T)$, resp. $X(T)$, à un réseau de $\mathrm{Lie}(T)$, resp. $\mathrm{Lie}(T)^*$.

2.6) On suppose $\mathrm{car}(k) = 0$. On rappelle que, dans ce cas, le groupe des racines n-ièmes de l'unité dans k est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, pour tout $n \geq 1$. (Pourquoi ?) Soit Q un sous-groupe d'indice fini dans $X(T)$. Déduire de la question 1.6 que $\mathrm{Ker}(Q)$ est isomorphe à $X(T)/Q$.

9.3. Une application. — Les questions suivantes pourront être traitées après avoir vu la structure des groupes linéaires résolubles connexes (voir plus loin). On suppose $\mathrm{car}(k) = 0$.

3.1) Soient B un groupe algébrique affine résoluble connexe, et $\mathfrak{b} = \mathrm{Lie}(B)$. Montrer que $\mathfrak{b}$ admet une base $\{e_1, \dots, e_n\}$ telle que les valeurs propres de chaque $\mathrm{ad}\, e_i$ soient des entiers. (Utiliser les décompositions $B = TU$, $\mathfrak{b} = \mathfrak{t} \oplus \mathfrak{u}$, et ce qui précède).

3.2) Donner un exemple d'une algèbre de Lie résoluble qui n'est pas l'algèbre de Lie d'un groupe algébrique affine résoluble. On pourra utiliser la question précédente et chercher un exemple de dimension 3.

10. Résolubilité et nilpotence

10.1. Sous-groupe engendré par des parties irréductibles. — La proposition suivante est d'une grande utilité. On note ι le morphisme $g \mapsto g^{-1}$.

Proposition 10.1. — *Soient G un groupe algébrique, et $(f_i)_{i\in I}$ une famille de morphismes $f_i : X_i \to G$, avec X_i une variété irréductible. On suppose que chaque $Y_i := f_i(X_i)$ contient e. Alors le sous-groupe engendré par les Y_i est fermé, irréductible, et égal à un produit fini $Y_{i_1}^{\pm} \cdots Y_{i_m}^{\pm}$, où $Y_i^+ = Y_i$ et $Y_i^- = \iota(Y_i)$.*

Corollaire 10.2. — *Soient $(H_i)_{i\in I}$ des sous-groupes fermés connexes de G. Le sous-groupe qu'ils engendrent est fermé et connexe.*

Démonstration. — Quitte à agrandir I, on peut supposer que les morphismes $\iota \circ f_i$ font partie de la famille $(f_i)_{i\in I}$. Alors la famille $(Y_i)_{i\in I}$ est stable par ι. Notons H le sous-groupe qu'elle engendre.

Pour toute suite finie $\mathbf{i} = (i_1, \dots, i_n)$, on pose $Y_{\mathbf{i}} = Y_{i_1} \cdots Y_{i_n}$. Alors $\overline{Y_{\mathbf{i}}}$ est une sous-variété fermée irréductible de G. Soit $\mathbf{j}$ tel que $\overline{Y_{\mathbf{j}}} := Y$ soit de dimension maximale. Pour tout $i \in I$, on a $Y_{\mathbf{j}} \subseteq Y_i Y_{\mathbf{j}}$ (car $e \in Y_i$) et donc, par maximalité, $Y = \overline{Y_{\mathbf{j}}} = \overline{Y_i Y_{\mathbf{j}}} \supseteq Y_i Y_{\mathbf{j}} = Y_i Y$.

Il en résulte que $\overline{Y_{\mathbf{i}}}\, Y \subseteq Y$, pour tout $\mathbf{i}$. On en déduit que Y est un sous-groupe fermé de G, contenant H. Comme $Y_{\mathbf{j}}$ contient un ouvert dense de Y, d'après le corollaire 4.19, il résulte du lemme 4.22 que $Y = Y_{\mathbf{j}} Y_{\mathbf{j}}$. Ceci montre que $Y \subseteq H$, d'où $Y = H$. □

10.2. Groupes résolubles et nilpotents. —

Définition 10.3. — Soit G un groupe arbitraire.

1) Si A, B sont deux sous-groupes de G, on note (A, B) le sous-groupe engendré par les commutateurs $(a, b) := aba^{-1}b^{-1}$. On a $(A, B) = (B, A)$ puisque $(b, a) = (a, b)^{-1}$.

2) On note $\mathcal{D}(G) = (G, G)$, le sous-groupe dérivé de G. On définit la **série dérivée** $\mathcal{D}^i(G)$ et la **série centrale descendante** $\mathcal{C}^i(G)$ par $\mathcal{D}^1(G) = \mathcal{D}(G) = \mathcal{C}^1(G)$ et

$$\mathcal{D}^{i+1}(G) = (\mathcal{D}^i(G), \mathcal{D}^i(G)), \qquad \mathcal{C}^{i+1}(G) = (G, \mathcal{C}^i(G)).$$

Il est clair que les $\mathcal{D}^i(G)$ et $\mathcal{C}^i(G)$ sont des sous-groupes normaux ; ils sont même *caractéristiques*, c.à.d. stables par tout automorphisme de G.

3) On dit que G est **résoluble**, resp. **nilpotent**, s'il existe $n \geq 1$ tel que $\mathcal{D}^n(G) = \{e\}$, resp. $\mathcal{C}^n(G) = \{e\}$. Comme $\mathcal{D}^i(G) \subseteq \mathcal{C}^i(G)$ pour tout i, on voit que tout groupe nilpotent est résoluble.

Lemme 10.4. — *Considérons une suite exacte $1 \to K \to G \to H \to 1$ de groupes. Si G est résoluble ou nilpotent, K et H le sont. De plus, si H, K sont résolubles, alors G l'est aussi.*

Démonstration. — Laissée au lecteur. □

Proposition 10.5. — *Soient G un groupe algébrique affine, et A, B deux sous-groupes fermés.*

a) *Si A est connexe, alors (A, B) est fermé et connexe.*

b) *Si A et B sont normaux, alors (A, B) est fermé et normal.*

Par conséquent, les sous-groupes $\mathcal{D}^i(G)$ et $\mathcal{C}^i(G)$ sont fermés.

Démonstration. — a) Pour tout $b \in B$, considérons le morphisme $f_b : A \to G$, $a \mapsto aba^{-1}b^{-1}$. Alors (A, B) est le sous-groupe engendré par les $f_b(A)$, et l'assertion découle de la proposition 10.1.

b) Soient A^0 et B^0 les composantes connexes de A et B. D'après a), les sous-groupes (A^0, B) et (A, B^0) sont fermés et connexes, et il en est de même du sous-groupe C qu'ils engendrent, d'après la proposition 10.1 à nouveau. Or on peut montrer (voir [**Hu2**, 17.2]) que C est d'indice fini dans (A, B). Par conséquent, (A, B) est réunion d'un nombre fini de translatés de C et est donc un sous-groupe fermé. □

Définition 10.6. — Les suites $(\mathcal{D}^i(G))_{i \geq 1}$ et $(\mathcal{C}^i(G))_{i \geq 1}$ sont des suites décroissantes de fermés ; elles sont donc stationnaires. On pose $\mathcal{D}^\infty(G) = \bigcap_i \mathcal{D}^i(G)$ et $\mathcal{C}^\infty(G) = \bigcap_i \mathcal{C}^i(G)$.

10.3. Algèbres de Lie résolubles et nilpotentes. —

Définition 10.7. — Soit $\mathfrak{g}$ une algèbre de Lie.

1) Si $\mathfrak{h}$ est un sous-espace de $\mathfrak{g}$, on dit que $\mathfrak{h}$ est un **idéal** de $\mathfrak{g}$ si l'on a $\mathrm{ad}(X)(\mathfrak{h}) \subseteq \mathfrak{h}$, pour tout $X \in \mathfrak{g}$. Dans ce cas, $\mathfrak{g}/\mathfrak{h}$ est muni d'une structure d'algèbre de Lie (le vérifier !).

2) Si $\mathfrak{h}, \mathfrak{k}$ sont des idéaux de $\mathfrak{g}$, on note $[\mathfrak{h}, \mathfrak{k}]$ le sous-espace engendré par les $[X, Y]$, pour $X \in \mathfrak{h}$, $Y \in \mathfrak{k}$; c'est un idéal de $\mathfrak{g}$.

3) On note $\mathcal{D}(\mathfrak{g}) = [\mathfrak{g}, \mathfrak{g}]$ l'idéal dérivé de $\mathfrak{g}$, et on définit la **série dérivée** $\mathcal{D}^i(\mathfrak{g})$ et la **série centrale descendante** $\mathcal{C}^i(\mathfrak{g})$ par $\mathcal{D}^1(\mathfrak{g}) = \mathcal{D}(\mathfrak{g}) = \mathcal{C}^1(\mathfrak{g})$ et

$$\mathcal{D}^{i+1}(\mathfrak{g}) = [\mathcal{D}^i(\mathfrak{g}), \mathcal{D}^i(\mathfrak{g})], \qquad \mathcal{C}^{i+1}(\mathfrak{g}) = [\mathfrak{g}, \mathcal{D}^i(\mathfrak{g})].$$

4) On dit que $\mathfrak{g}$ est **résoluble**, resp. **nilpotente**, s'il existe n tel que $\mathcal{D}^n(\mathfrak{g}) = 0$, resp. $\mathcal{C}^n(\mathfrak{g}) = 0$.

Lemme 10.8. — *Soient $\mathfrak{g}$ une algèbre de Lie et $\mathfrak{h}$ un idéal. Si $\mathfrak{g}$ est résoluble ou nilpotente, $\mathfrak{h}$ et $\mathfrak{g}/\mathfrak{h}$ le sont. De plus, si $\mathfrak{h}$ et $\mathfrak{g}/\mathfrak{h}$ sont résolubles, alors $\mathfrak{g}$ est résoluble.*

Démonstration. — Laissée au lecteur. □

Proposition 10.9. — *Soit G un groupe algébrique. Si G est commutatif, nilpotent, ou résoluble, il en est de même de $\mathfrak{g} := \mathrm{Lie}(G)$. Plus précisément, si $\mathcal{D}^r(G) = \{1\}$, resp. $\mathcal{C}^r(G) = \{1\}$, alors $\mathcal{D}^r(\mathfrak{g}) = \{0\}$, resp. $\mathcal{C}^r(\mathfrak{g}) = \{0\}$.*

On voit facilement que la proposition découle du lemme ci-dessous.

Lemme 10.10. — *Soient G un groupe algébrique, H un sous-groupe fermé normal, et $\mathfrak{g}, \mathfrak{h}$ leurs algèbres de Lie. Alors $[\mathfrak{g}, \mathfrak{h}] \subseteq \mathrm{Lie}\big((G, H)\big)$.*

Démonstration. — Posons $H' = (G, H)$ et $\mathfrak{h}' = \mathrm{Lie}(H')$. Soient $X \in \mathfrak{g}$ et $Y \in \mathfrak{h}$. On note θ_Y le morphisme $G \to \mathfrak{g}$, $g \mapsto \mathrm{Ad}(g)(Y)$. Alors $\mathrm{d}\theta_Y(X) = [X, Y]$, d'après la preuve de la proposition 6.10.b). Or, pour tout $g \in G$, on a $\mathrm{Int}(g)(H) = H$, et donc $\mathrm{Ad}(g)(Y) \in \mathfrak{h}$. Il en résulte que $\mathrm{d}\theta_Y$ applique $\mathfrak{g}$ dans $\mathfrak{h}$, d'où le lemme. □

10.4. Exemple fondamental : les matrices triangulaires. — On note B_n le groupe des matrices triangulaires, U_n le sous-groupe des matrices triangulaires unipotentes, et $\mathfrak{b}_n$, $\mathfrak{u}_n$ leurs algèbres de Lie. On voit facilement que $\mathcal{D}(B_n) \subseteq U_n$ et $\mathcal{D}(\mathfrak{b}_n) \subseteq \mathfrak{u}_n$; en particulier U_n est normal dans B_n et $\mathfrak{u}_n$ est un idéal de $\mathfrak{b}_n$.

Proposition 10.11. — a) *U_n et B_n sont connexes.*

b) *U_n est nilpotent et B_n résoluble, et de même pour $\mathfrak{u}_n$ et $\mathfrak{b}_n$.*

Démonstration. — Comme variétés, U_n est isomorphe à $k^{n(n-1)/2}$, et B_n à $U_n \times (k^*)^n$, d'où a).

Montrons que U_n est nilpotent. Soit A la sous-algèbre de $M_n(k)$ formée des matrices triangulaires. On note V_i le sous-espace engendré par $v_1, \ldots, v_i$, où $\{v_1, \ldots, v_n\}$ est la base standard de k^n. Pour $r = 0, 1, \ldots, n-1$, soit $I_r = \{a \in A \mid aV_i \subseteq V_{i-r},\ \forall i = 1, \ldots, n\}$. Alors chaque I_r est un idéal de A, et l'on a $I_r I_s \subseteq I_{r+s}$ et $I_n = 0$. Il en résulte, au passage, que $\mathfrak{u}_n$ est nilpotente puisque $\mathcal{C}^r(\mathfrak{u}_n) \subseteq I_{r+1}$ pour tout r.

D'après le lemme suivant, U_n est nilpotent. Comme $\mathcal{D}(B_n) \subseteq U_n$ et $\mathcal{D}(\mathfrak{b}_n) \subseteq \mathfrak{u}_n$, on conclut que B_n et $\mathfrak{b}_n$ sont résolubles. La proposition est démontrée, modulo le lemme qui suit. □

Posons $H_r = \{g \in \mathrm{GL}_n \mid g - 1 \in I_{r+1}\}$. Alors $H_0 = U_n$, $H_{n-1} = \{1\}$, et donc la nilpotence de U_n résulte du lemme ci-dessous.

Lemme 10.12. — *On a $\mathcal{C}^r(U_n) \subseteq H_r$, pour $r = 0, 1, \ldots, n-1$.*

Démonstration. — Récurrence sur r, vrai pour $r = 0$. Soit $r \geq 1$ et supposons avoir montré $\mathcal{C}^{r-1}(U_n) \subseteq H_{r-1}$, et soient $g \in U_n$, $h \in \mathcal{C}^{r-1}(U_n)$. Posons $X = g - 1$ et $Y = h - 1$. Alors $X \in I_1$ et $Y \in I_r$. Puisque X est nilpotent, alors l'inverse de g est donné par la formule $g^{-1} = 1 - X + u$, où $u = \sum_{i=2}^{n} (-X)^i$. De même, $h^{-1} = 1 - Y + v$, où $v = \sum_{i=2}^{n} (-Y)^i$. Notons que $u \in I_2$ et $v \in I_{2r} \subseteq I_{r+1}$. Un calcul facile montre alors que

$$ghg^{-1}h^{-1} - 1 = (1 + X)(1 + Y)(1 - X + u)(1 - Y + v) - 1$$

appartient à I_{r+1}. Ceci prouve le lemme. $\square$

11. Théorèmes de Lie-Kolchin

11.1. Théorème de Burnside et Wedderburn. — On rappelle que k est supposé algébriquement clos.

***Lemme 11.1* (Lemme de Schur).** — *Soient A une k-algèbre et V un A-module simple de dimension finie sur k. Alors tout A-endomorphisme de V est scalaire, c.-à-d.,* $\mathrm{End}_A(V) = k$.

Démonstration. — Posons $D = \mathrm{End}_A(V)$. C'est un corps (éventuellement non-commutatif). En effet, soit $\phi \in D \setminus \{0\}$. Comme V est un A-module simple, on a nécessairement $\mathrm{Ker}(\phi) = 0$ et $\mathrm{Im}(\phi) = V$, donc ϕ est un isomorphisme.

De plus, $\dim_k D < \infty$, puisque D est une sous-k-algèbre de $\mathrm{End}_k(V)$. Maintenant, soit $\alpha \in D$ et soit $f : k[X] \to D$ le morphisme de k-algèbres défini par $f(X) = \alpha$; son image est la sous-algèbre $k[\alpha]$ de D engendrée par α, qui est intègre. Par conséquent $\mathrm{Ker}(f)$ est un idéal premier de $k[X]$, non nul puisque $\dim_k k[\alpha] < \infty$. Donc $\mathrm{Ker}(f) = (P)$, où P est un polynôme irréductible unitaire. Comme k est algébriquement clos, P est de degré 1 et donc $\alpha \in k$. Ceci montre que $D = k$. Le lemme est démontré. $\square$

***Théorème 11.2* (Burnside-Wedderburn).** — *Soit A une sous-algèbre de* $\mathrm{End}_k(V)$*, où* $\dim_k V < \infty$*. Si V est un A-module simple, alors* $A = \mathrm{End}_k(V)$.

Démonstration. — Commençons par démontrer le lemme suivant.

***Lemme 11.3*.** — *Soit W un sous-espace de V et $v \in V \setminus W$. Alors il existe $a \in A$ tel que $aW = 0$ et $av \neq 0$.*

Démonstration. — Par récurrence sur $\dim_k W$. Si $W = 0$, on peut prendre $a = 1$. Donc on peut supposer $\dim_k W = m \geq 1$ et le lemme démontré pour $m - 1$. Écrivons $W = W' \oplus kw$ et soient $I = \mathrm{Ann}_A(W')$ et $J = \mathrm{Ann}_A(W)$; ce sont des idéaux à gauche de A. On veut montrer que $Jw \neq 0$ pour tout $v \in V \setminus W$. Supposons au contraire qu'il existe $v \in V \setminus W$ tel que $Jv = 0$ et montrons que l'on aboutit à une contradiction.

Par hypothèse de récurrence, Iw est un sous-module non nul de V, donc égale V puisque V est simple. Donc tout $x \in V$ s'écrit $x = aw$, avec $a \in I$ (non nécessairement unique). On pose alors

$$\phi(x) = av.$$

Ceci est bien défini, car si $x = a'w$ pour un autre $a' \in I$, alors $a' - a$ appartient à I et annule w, donc appartient à J, donc annule v par hypothèse. Ceci montre que ϕ est bien défini. C'est un A-endomorphisme de V car si $b \in A$ et $x = aw$, $x' = a'w$, avec $a, a' \in I$, alors $ba + a' \in I$, d'où

$$\phi(bx + x') = \phi((ba + a')w) = (ba + a')v = b\phi(x) + \phi(x').$$

Donc, d'après le lemme de Schur, il existe $\lambda \in k$ tel que $\phi = \lambda \mathrm{id}_V$. Mais alors, pour tout $a \in I$, on a :

$$0 = \phi(aw) - \lambda aw = a(v - \lambda w).$$

Par conséquent, d'après l'hypothèse de récurrence appliquée à W' et $I = \mathrm{Ann}_A(W')$, on a $v - \lambda w \in W'$, d'où $v \in W$, une contradiction. Ceci prouve le lemme. $\square$

Démontrons maintenant le théorème. Choisissant une base $(e_1, \dots, e_n)$ de V, on identifie $\mathrm{End}_k(V)$ à $M_n(k)$. Il suffit donc de montrer que chaque matrice élémentaire $E_{\ell j}$ appartient à A.

Fixons j et notons V^j le sous-espace de V engendré par les e_i, pour $i \neq j$. D'après le lemme précédent appliqué à $W = V^j$ et $v = e_j$, il existe $a \in A$ tel que $ae_i = 0$ pour $i \neq j$ et $ae_j \neq 0$. Alors, comme V est un A-simple, $Aae_j = V$, et donc il existe $b \in A$ tel que $bae_j = e_\ell$, et de plus $bae_i = 0$ pour $i \neq j$. Donc $ba = E_{\ell j}$. Ceci prouve le théorème. $\square$

11.2. Groupes unipotents. — Le premier théorème est un résultat d'algèbre abstraite.

Théorème 11.4 **(Lie-Kolchin pour les groupes de matrices unipotentes)**
Soient $V = k^n$ et G un sous-groupe de $GL(V)$ formé de matrices unipotentes. Alors il existe une base de V dans laquelle G est triangulaire.

Démonstration. — Procédant par récurrence sur $\dim V$, il suffit de montrer l'existence d'un vecteur non-nul fixé par G. Pour cela, on peut supposer que V est un G-module simple. Alors, d'après le théorème de Burnside-Wedderburn, appliqué à la sous-algèbre kG, on obtient $kG = \mathrm{End}(V)$.

Comme tout élément de G est unipotent, alors, pour $g, h \in G$, on a $\mathrm{Tr}(g) = \dim(V) = \mathrm{Tr}(gh)$, et donc $\mathrm{Tr}((g-1)h) = 0$. Comme $kG = \mathrm{End}(V)$, il vient $\mathrm{Tr}((g-1)Y) = 0$, pour tout $Y \in \mathrm{End}(V)$. Or, on a $\mathrm{Tr}((g-1)E_{ij}) = (g-1)_{ji}$. Il en résulte que $g = 1$, pour tout $g \in G$. Donc V est de dimension 1, avec action triviale de G, et le théorème est démontré. $\square$

Corollaire 11.5 **(Lie-Kolchin pour les groupes unipotents)**
Soient G un groupe algébrique affine unipotent et $\rho : G \to \mathrm{GL}_n$ une représentation. Alors $\rho(G)$ est conjugué à un sous-groupe de U_n. Par conséquent, G est nilpotent, ainsi que $\mathrm{Lie}(G)$.

Démonstration. — La décomposition de Jordan et le théorème entraînent la première assertion. La seconde en découle, d'après le théorème 2.14, la proposition 10.11, et le lemme 10.4. □

11.3. Groupes résolubles connexes. — Pour les groupes algébriques résolubles *connexes*, on a le

Théorème 11.6 **(Lie-Kolchin pour les groupes résolubles connexes)**
Soit G un groupe algébrique affine résoluble connexe, et $\rho : G \to \mathrm{GL}_n$ une représentation. Alors $\rho(G)$ est conjugué à un sous-groupe de B_n.

Démonstration. — On procède par récurrence sur $\dim V + \dim G$. Il suffit de montrer l'existence d'une droite stable par G. Pour cela, on peut supposer que V est un G-module simple. Comme $H := \mathcal{D}(G)$ est résoluble, connexe, et de dimension $< \dim G$, il stabilise une droite de V, i.e. il existe $\chi_0 \in X(H)$ tel que V_{χ_0} soit non-nul.

Observons que G agit morphiquement dans $k[H]$ et $X(H)$. En effet, considérons le morphisme $G \times H \to H$, $(g, h) \mapsto g^{-1}hg$. Son comorphisme $k[H] \to k[H] \otimes k[G]$ fait de $k[H]$ un G-module rationnel, où l'action est donnée par $(g\phi)(h) = \phi(ghg^{-1})$, pour $\phi \in k[H]$, $g \in G$, $h \in H$, et le sous-espace $kX(H) \subseteq k[H]$ est clairement stable. On a donc une représentation rationnelle de G dans $k[H]$ et dans $kX(H)$. En particulier, pour tout $\phi \in k[H]$, le stabilisateur G_ϕ est un sous-groupe fermé.

D'autre part, d'après la proposition 8.3, les sous-espaces $V_{g\chi_0}$ sont en somme directe. Comme V est de dimension finie, ceci entraîne que l'orbite $G\chi_0$ est finie. Il en résulte que G_{χ_0} est fermé, d'indice fini, et donc égal à G puisque G est connexe. Alors, pour $v \in V_{\chi_0}$, $g \in G$ et $h \in H$, on a

$$hgv = g\, g^{-1}hgv = \chi_0(g^{-1}hg)gv = (g\chi_0)(h)gv = \chi_0(h)gv.$$

Ceci montre que V_{χ_0} est un sous-G-module. Puisque V est simple, il vient $V = V_{\chi_0}$. Donc tout $h \in H$ agit sur V par une homothétie $\rho(h)$ de rapport $\chi_0(h)$. Or, comme h est un commutateur, on a $\det(\rho(h)) = 1$. Donc $\chi_0(H)$ est contenu dans le groupe des racines n-ièmes de l'unité, où $n = \dim V$, et comme H est connexe il vient $H \subseteq \operatorname{Ker} \rho$. Par conséquent, $\rho(G)$ est un sous-groupe commutatif de $\mathrm{GL}(V)$; d'après le lemme 7.14 il stabilise donc une droite de V (d'où $\dim V = 1$ puisque V est simple). Le théorème est démontré. □

On déduit du théorème le corollaire suivant. (On obtiendra plus loin des résultats plus précis sur la structure des groupes résolubles connexes.)

Corollaire 11.7. — *Soit G résoluble connexe. Alors :* a) $\mathcal{D}(G)$ *est connexe et unipotent,* b) G_u *est un sous-groupe fermé normal.*

Démonstration. — D'après le théorème, on peut plonger G dans un B_n. Alors $\mathcal{D}(G) \subseteq \mathcal{D}(B_n) \subseteq U_n$, et donc $\mathcal{D}(G)$ est unipotent. D'autre part, on a $G_u = G \cap U_n$ et donc G_u est un sous-groupe fermé normal, puisque U_n est normal dans B_n. Enfin, on a $\mathrm{Lie}(G_u) \subseteq \mathrm{Lie}(G) \cap \mathfrak{u}_n \subseteq \mathfrak{g}_n$. □

Remarque 11.8. — L'hypothèse de connexité dans le théorème est essentielle. Par exemple, soit N le normalisateur de D_2 dans GL_2. Montrer que N est résoluble, mais pas conjugué à un sous-groupe de B_2.

11.4. Algèbres de Lie résolubles complexes. — De façon similaire (*cf.* [**Hu1**, Chap. 4]) on peut établir le

Théorème 11.9. — *On suppose* $\mathrm{car}(k) = 0$. *Soit* $\mathfrak{g}$ *une algèbre de Lie résoluble, et* $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ *une représentation de dimension finie. Alors il existe une base de V où* $\rho(\mathfrak{g})$ *est triangulaire.*

12. Structure des groupes résolubles connexes

12.1. Variétés homogènes et groupes quotients : un aperçu. —

Définition 12.1. — Soient G un groupe algébrique et X une G-variété. On dit que X est une G-variété **homogène** si l'action de G est transitive (c.à.d., si l'on a $X = Gx$ pour un, et donc tout, $x \in X$).

Lemme 12.2. — *Soit X une G-variété homogène.*

a) *Les composantes irréductibles de X coïncident avec les composantes connexes, et chacune est une variété homogène sous G^0. Elles sont translatées l'une de l'autre, et sont toutes de dimension* $\dim G - \dim G_x$ (*pour x arbitraire*).

b) *Si X et G_x sont irréductibles, alors G aussi. En particulier, si l'on a une suite exacte* $1 \to K \to G \to H \to 1$ *avec H, K connexes, alors G l'est aussi.*

Démonstration. — Soient $e = g_1, \ldots, g_n$ un système de représentants de G/G^0, et $x \in X$. Alors $G = G^0 g_1 \sqcup \cdots \sqcup G^0 g_n$ et, comme les $G^0 g_i x$ sont deux à deux disjoints ou égaux, on peut supposer que $X = G^0 x \sqcup \cdots \sqcup G^0 g_m x$, pour un $m \leq n$. L'une au moins de ces G^0-orbites est fermée, d'après le corollaire 4.28. Or, pour $i, j = 1, \ldots, m$, on a $G^0 g_j x = g_j g_i^{-1} G^0 g_i x$. Il en résulte que les $G^0 g_i x$, $1 \leq i \leq m$, sont toutes fermées et ouvertes. Ce sont donc les composantes connexes de X. Enfin, notons ϕ le morphisme $G \to X$, $g \mapsto gx$. Pour tout g, on a $\phi^{-1}(gx) = gG_x$. D'après le théorème 4.18, on en déduit que chaque composante de X est de dimension $\dim G - \dim G_x$. Ceci prouve a).

Voyons b). D'après a), on a $X = G^0 x$. Soit $g \in G$. Alors, $gx = hx$ pour un $h \in G^0$, et donc $h^{-1}g \in G_x$. Or $G_x \subseteq G^0$, puisque G_x est connexe, et donc $g \in G^0$. Ceci prouve le lemme. $\square$

Remarque 12.3. — On peut avoir G et X irréductibles sans que G_x le soit. Par exemple, considérons l'action adjointe de $G = \mathrm{SL}_2$ dans $\mathfrak{sl}_2$. Soit $x = E_{11}$. Alors G et Gx sont irréductibles, mais pas G_x.

Pour établir le théorème de structure des groupes résolubles connexes, on a besoin du théorème suivant, qui sera démontré dans le chapitre suivant.

Théorème 12.4. — *Soient G un groupe algébrique affine et H un sous-groupe fermé. Alors, l'ensemble G/H des classes à gauche gH, pour $g \in G$, est muni d'une structure de variété algébrique telle que la projection $\pi : G \to G/H$ soit un morphisme de variétés algébriques et vérifie la propriété universelle suivante :*

$(*)$ *pour tout morphisme de variétés $\alpha : G \to Z$ constant sur les classes gH, il existe un unique morphisme $\beta : G/H \to Z$ tel que $\beta \circ \pi = \alpha$.*

De plus, si H est un sous-groupe distingué, G/H est un groupe algébrique affine. Enfin, tout morphisme de groupes algébriques affines $\phi : G \to G'$ induit un morphisme bijectif de groupes algébriques $G/\operatorname{Ker}(\phi) \to \operatorname{Im}(\phi)$.

Remarque 12.5. — **Attention !** En caractéristique $p > 0$, l'exemple du morphisme bijectif $\mathrm{SL}_p \to \mathrm{PGL}_p$, qui n'est pas un isomorphisme (*cf.* 4.25), montre que le morphisme bijectif $G/\operatorname{Ker}(\phi) \to \operatorname{Im}(\phi)$ n'est pas nécessairement un isomorphisme.

Afin d'étudier à quelle condition c'est un isomorphisme, on a besoin d'introduire et d'étudier la notion de séparabilité.

***Définition 12.6* (Extensions algébriques séparables)**. — Soit L/K une extension algébrique de corps. Pour tout $\alpha \in L$, la sous-algèbre $K[\alpha]$ est isomorphe à $K[X]/(P_\alpha)$, où P_α est un polynôme irréductible unitaire, appelé le **polynôme minimal de α sur K**. Son degré se note $\deg_K(\alpha)$.

On dit que α est **séparable** sur K si P_α a $\deg_K(\alpha)$ racines distinctes dans un clôture algébrique $\overline{K}$ de K. Enfin, on dit que l'extension L/K est **séparable** si tout $\alpha \in L$ est séparable sur K.

***Définition 12.7* (Extensions séparables)**. — Soit L/K une extension de corps de type fini. On dit qu'elle est **séparablement engendrée** s'il existe une base de transcendance $x_1, \dots, x_r$ de L/K telle que l'extension algébrique $L/K(x_1, \dots, x_r)$ soit séparable. Dans ce cas, on dira simplement (par un abus de language qui sera justifié plus tard) que l'extension L/K est **séparable**.

Remarque 12.8. — Si $\operatorname{car}(K) = 0$, tout polynôme irréductible $P \in K[X]$, de degré d, a d racines simples dans $\overline{K}$ (car le polynôme dérivé P' est non nul et de degré $d-1$, donc premier avec P). Par conséquent, en caractéristique 0, toute extension L/K de type fini est séparable.

***Définition 12.9* (Morphismes séparables)**. — Soit $f : X \to Y$ un morphisme dominant de variétés algébriques irréductibles. Le comorphisme $f^* : k[Y] \hookrightarrow k[X]$ est injectif donc induit une extension de corps $k(Y) \subseteq k(X)$. On dit que f est **séparable** si cette extension est séparable. (Par conséquent, en caractéristique 0, tout morphisme dominant est séparable, mais ce n'est pas le cas en caractéristique positive).

Un intérêt de la notion de séparabilité est fourni par la proposition ci-dessous.

Proposition 12.10. — *Soient X, Y des variétés irréductibles et $f : X \to Y$ un morphisme bijectif séparable. Alors f est* **birationnel***, c.-à-d., il existe un ouvert non vide V de Y tel que f induise un isomorphisme de $f^{-1}(V)$ sur V.*

D'autre part, la séparabilité peut se vérifier comme suit.

Théorème 12.11. — *Soit $f : X \to Y$ un morphisme de variétés irréductibles. S'il existe un ouvert non vide U de X tel que $\mathrm{d}_x f$ soit surjective, pour tout $x \in X$, alors f est séparable.*

Dans le cas d'un morphisme G-équivariant entre variétés homogènes, il suffit que cette condition soit vérifiée en un seul point pour que le morphisme soit séparable ; s'il est de plus bijectif il est alors birationnel, d'après la proposition 12.10, et par homogénéité on en déduit que c'est un isomorphisme. C'est-à-dire, on a la proposition suivante. (Les démonstrations seront données dans le prochain chapitre).

Proposition 12.12. — *Soient G un groupe algébrique, X, Y deux G-variétés homogènes et $\phi : X \to Y$ un morphisme* **G-équivariant bijectif**. *S'il existe $x \in X$ tel que la différentielle $\mathrm{d}_x\phi$ soit surjective, alors ϕ est un isomorphisme.*

Cette proposition est utilisée dans démonstration du théorème 12.4, ainsi que du supplément donné plus bas, et nous en aurons également besoin pour l'étude des groupes résolubles connexes.

Théorème 12.13. — *Soit $\phi : G \to G'$ un morphisme de groupes algébriques affines et soit*

$$\overline{\phi} : G/\operatorname{Ker}(\phi) \to \operatorname{Im}(\phi)$$

le morphisme induit. Si $\overline{\phi}$ est **séparable**, *c.-à-d., si sa différentielle en l'identité est surjective, alors c'est un isomorphisme de groupes algébriques.*

12.2. Le théorème de structure. — On va démontrer le

Théorème 12.14 **(Structure des groupes résolubles connexes)**
Soient G résoluble connexe, et $\mathfrak{g} = \mathrm{Lie}(G)$.

1) *G_u est connexe.*

2) *Si T est un tore maximal de G, l'application $T \times G_u \to G$, $(t,u) \mapsto tu$ est un isomorphisme de variétés. En particulier, $T \cong G/G_u$. De plus, on a $\mathrm{Lie}(G_u) = \mathfrak{g}_n$, et $\mathfrak{g} = \mathrm{Lie}(T) \oplus \mathfrak{g}_n$.*

3) *Tous les tores maximaux de G sont conjugués par $\mathcal{C}^\infty(G)$. De plus, tout sous-groupe formé d'éléments semi-simples est contenu dans un tore de G.*

4) *Pour toute famille S d'éléments semi-simples qui commutent, on a $N_G(S) = C_G(S) = C_G(S)^0$.*

Démonstration. — Voyons 1). Soit $G' = G/\mathcal{D}(G)$. Alors G' est commutatif, donc $G' \cong G'_s \times G'_u$. Comme G est connexe, G' et G'_u le sont aussi. Soit π le morphisme $G \to G'$. Montrons que $G_u = \pi^{-1}(G'_u)$. L'inclusion $\subseteq$ est claire. Réciproquement, soient $g \in \pi^{-1}(G'_u)$ et $g = g_s g_u$ sa décomposition de Jordan. Alors $\pi(g_s)\pi(g_u)$ est la décomposition de Jordan de $\pi(g) \in G_u$, d'où $\pi(g_s) = 1$. Donc $g_s \in \mathcal{D}(G)$, et comme $\mathcal{D}(G) \subseteq G_u$ il vient $g_s = 1$. Donc $G_u = \pi^{-1}(G'_u)$. D'après le lemme 12.2.b), on en déduit que G_u est connexe. Ceci prouve le point 1).

Le reste de la démonstration se fait en plusieurs étapes. On a suivi la démonstration, assez élémentaire, de [**Do88**]. Pour d'autres démonstrations, voir [**Bo**], [**Hu2**] ou [**Sp**].

On aura besoin du lemme suivant, qui résulte des propriétés de la décomposition de Jordan.

Lemme 12.15. — *Si T est diagonalisable alors* $\mathrm{Lie}(T) = \mathrm{Lie}(T)_s$. *Si U est unipotent, alors* $\mathrm{Lie}(U) = \mathrm{Lie}(U)_n$.

Démonstration. — T se plonge dans un D_n ; alors $\mathrm{Lie}(T) \subseteq \mathrm{Lie}(D_n)$ est formé d'éléments semi-simples. D'après le théorème de Lie-Kolchin 11.4, U se plonge dans un U_n ; alors $\mathrm{Lie}(T) \subseteq \mathrm{Lie}(U_n)$ est formé d'éléments nilpotents. □

12.3. Groupes nilpotents connexes. — La proposition ci-dessous est une étape dans la démonstration du théorème 12.14.

Proposition 12.16. — *Soient G résoluble connexe, $\mathfrak{g} = \mathrm{Lie}(G)$. Alors : G est nilpotent $\Leftrightarrow$ $G_s \subseteq Z(G)$. Dans ce cas, G_s est un sous-groupe fermé connexe central et la multiplication induit un isomorphisme $G_s \times G_u \cong G$, dont l'inverse* *est donné par la décomposition de Jordan. De plus,* $\mathrm{Lie}(G_s) = \mathfrak{g}_s$, $\mathrm{Lie}(G_u) = \mathfrak{g}_n$, *et* $\mathfrak{g} = \mathfrak{g}_s \oplus \mathfrak{g}_n$.

Démonstration. — Supposons G nilpotent et montrons par récurrence sur $\dim G$ que $G_s \subseteq Z(G)$. C'est vrai si G est abélien. Sinon, soient $N = \mathcal{C}^n(G)$ (avec $n \geq 1$ et $\mathcal{C}^{n+1}(G) = \{1\}$) et $\pi : G \to G/N := G'$. Soient $s \in G_s$ et $g \in G$. Par hypothèse de récurrence, $\pi(s) \in Z(G')$ et donc $z := gsg^{-1}s^{-1} \in N$. Or $N \subseteq Z(G)$ (car $(G, N) = \{1\}$) et donc $sz = zs = gsg^{-1}$, avec s et gsg^{-1} semi-simples, et z unipotent (car $N \subseteq \mathcal{D}(G)$). On en déduit que $z = 1$. Ceci prouve que s est central.

Supposons $G_s \subseteq Z(G)$. Alors G_s est un sous-groupe. Plongeons G dans un $\mathrm{GL}(V) = \mathrm{GL}_n$. D'après le lemme 7.14, on peut supposer que $G_s \subseteq G \cap D_n$. Alors, d'une part, on a $G_s = G \cap D_n$ et donc G_s est fermé. D'autre part, on a $V = V_{\chi_1} \oplus \cdots \oplus V_{\chi_r}$ pour certains $\chi_i \in X(G_s)$, et chaque V_{χ_i} est G-stable (car G_s est central). D'après le théorème de Lie-Kolchin 11.4, chaque V_{χ_i} admet une base où G_u est triangulaire unipotent ; dans cette base tout $g \in G$ est représenté par une matrice triangulaire dont chaque terme diagonal est $\chi_i(g) = \chi_i(g_s)$.

On conclut alors, comme dans la démonstration du théorème 7.15, que le morphisme $G_s \times G_u \to G$ est un isomorphisme, dont l'inverse est donné par la décomposition de Jordan. Par conséquent, G_s est connexe, et G est nilpotent (car G_s et G_u le sont). De plus, on a $\mathfrak{g} = \mathrm{Lie}(G_s) \oplus \mathrm{Lie}(G_u)$. Or, $\mathrm{Lie}(G_s) \subseteq \mathfrak{g}_s$ et $\mathrm{Lie}(G_u) \subseteq \mathfrak{g}_n$, d'après le lemme 12.15. La dernière assertion en découle, puisque $\mathfrak{g}_s \cap \mathfrak{g}_n = \{0\}$. La proposition est démontrée. □

Au passage, consignons ici la propriété suivante des groupes nilpotents connexes :

Lemme 12.17. — *Soit G nilpotent connexe $\neq \{1\}$. Alors $Z(G)^0$ est non-trivial.*

Démonstration. — C'est clair si G est abélien. Sinon, soit $n \geq 1$ tel que $\mathcal{C}^n(G) \neq \{1\}$ et $\mathcal{C}^{n+1}(G) = \{1\}$. Alors $\mathcal{C}^n(G)$ est fermé, connexe, central et non trivial. □

12.4. Un lemme-clé. — On aura besoin du

Lemme 12.18. — *Soit N un sous-groupe commutatif de G_u, fermé, connexe, et normal dans G, et soit $s \in G_s$. Alors l'application $f : N \to N$, $x \mapsto sxs^{-1}x^{-1}$ est un morphisme de groupes algébriques, et donc $f(N) := M$ est un sous-groupe fermé connexe de N. De plus, le morphisme $C_N(s) \times M \to N$, $(v, u) \mapsto vu$ est bijectif, et $C_N(s) = \mathrm{Ker}\, f$ est connexe.*

Démonstration. — f est évidemment un morphisme de variétés ; montrons que c'est un morphisme de groupes. Soient $x, y \in N$. Alors

$$f(xy) = s\,x\,y\,s^{-1}\,y^{-1}\,x^{-1} = (sxs^{-1})\ (sys^{-1})\ y^{-1}\ x^{-1}.$$

Mais sxs^{-1}, $sys^{-1} \in N$, puisque N est normal dans G, et comme N est abélien il vient $f(xy) = f(x)f(y)$, d'où la 1ère assertion. Il est clair que $\operatorname{Ker} f = C_N(s)$, d'où $\dim N = \dim M + \dim C_N(s)$. Montrons que $C_N(s) \cap M = \{1\}$. Soit $x \in N$ tel que $g := f(x) \in C_N(s)$. Alors

$$xs^{-1}x^{-1} = s^{-1}g = gs^{-1}$$

et ceci est la décomposition de Jordan de $xs^{-1}x^{-1}$, puisque $g \in N \subseteq G_u$ est unipotent. Mais $xs^{-1}x^{-1}$ est semi-simple, car s^{-1} l'est, et donc $g = 1$.

Il en résulte que le morphisme $\mu : C_N(s) \times M \to N$, $(x, y) \mapsto xy$ est injectif. Son image est donc un sous-groupe fermé de N, de dimension $\dim C_N(s) + \dim M = \dim N$. Comme N est connexe, on conclut que μ est bijectif. On en déduit que $C_N(s) := C$ est connexe. En effet, écrivons $C = C^0 g_1 \sqcup \cdots \sqcup C^0 g_n$ (avec $g_1 = 1$). Comme μ est bijectif, alors $N = CM$ est réunion disjointe des $C^0 g_i M$. L'une au moins de ces orbites sous $C^0 \times M$ est fermée ; or $C^0 g_i M = g_i C^0 M$ donc ces orbites sont toutes fermées et ouvertes. Comme N est connexe, il vient $n = 1$, et donc C est connexe. □

Corollaire 12.19. — *Soient G résoluble connexe, $s \in G_s$. Alors $C_G(s)$ est connexe, et on a $G = C_G(s)G_u$.*

Démonstration. — On procède par récurrence sur $\dim G$. Les assertions sont vraies si s est central, donc en particulier si G est abélien. Sinon, soit $n \geq 1$ tel que $\mathcal{D}^n(G) \neq \{1\}$ et $\mathcal{D}^{n+1}(G) = \{1\}$. Posons $N = \mathcal{D}^n(G)$. Alors N est abélien, fermé, connexe, normal et unipotent (car $N \subseteq \mathcal{D}(G) \subseteq G_u$). Soient $G' = G/N$ et $\pi : G \to G'$. On a $\dim G' = \dim G - \dim N < \dim G$.

Montrons que $\pi(C_G(s)) = C_{G'}(\pi(s))$. L'inclusion $\subseteq$ est claire. Soit $z \in G$ tel que $\pi(z) \in C_{G'}(\pi(s))$. Alors $szs^{-1}z^{-1} \in N$ et donc, d'après le lemme, il existe $u \in N$ et $v \in C_N(s)$ tels que $szs^{-1}z^{-1} = vf(u) = vsus^{-1}u^{-1}$. Or, v commute à s, et à u (car N est abélien), donc aussi à $us^{-1}u^{-1}$. Donc, on a

$$zs^{-1}z^{-1} = v\ us^{-1}u^{-1} = us^{-1}u^{-1}\ v.$$

Comme v est unipotent et $us^{-1}u^{-1}$ semi-simple, ceci est la décomposition de Jordan de $zs^{-1}z^{-1}$. Or ce dernier est semi-simple, d'où $v = 1$ et $zs^{-1}z^{-1} = us^{-1}u^{-1}$. Donc $u^{-1}z \in C_G(s)$, et $\pi(u^{-1}z) = \pi(z)$ (car $u \in N$). Ceci prouve que $\pi(C_G(s)) = C_{G'}(\pi(s))$. On en déduit que $C_G(s)$ est connexe. En effet, comme $C_G(s) \cap N = C_N(s)$, on a une suite exacte

$$1 \longrightarrow C_N(s) \longrightarrow C_G(s) \longrightarrow C_{G'}(\pi(s)) \longrightarrow 1.$$

Or $C_N(s)$ est connexe, d'après le lemme, et $C_{G'}(\pi(s))$ l'est, par hypothèse de récurrence. Donc $C_G(s)$ l'est aussi, d'après le lemme 12.2.b).

Enfin, par hypothèse de récurrence, on a $G' = C_{G'}(\pi(s))G'_u$, et comme $C_{G'}(\pi(s)) = \pi(C_G(s))$ il vient $G = C_G(s)\pi^{-1}(G'_u)$. Or $\pi^{-1}(G'_u) \subseteq G_u$. En effet, si $\pi(g) \in G'_u$ alors $\pi(g_s) = 1$ et donc $g_s \in \operatorname{Ker}\pi = N$, d'où $g_s = 1$ puisque $N \subseteq G_u$. Le corollaire est démontré. $\square$

12.5. Sections de $G \to G/G_u$. — On déduit des paragraphes précédents le corollaire suivant.

Corollaire 12.20. — *Soit G résoluble connexe. Il existe un tore T tel que la multiplication induise un isomorphisme $T \times G_u \cong G$. Alors, $T \cong G/G_u$. De plus, on a* $\operatorname{Lie}(G) = \operatorname{Lie}(T) \oplus \operatorname{Lie}(G_u)$, *et* $\operatorname{Lie}(G_u) = \operatorname{Lie}(G)_n$.

Démonstration. — On procède par récurrence sur $\dim G$. D'après la proposition 12.16 , les assertions sont vraies si G est nilpotent. Sinon, il existe $s \in G_s$ non central, et $C_G(s)$ est un sous-groupe propre, donc de dimension $< \dim G$. D'après le corollaire 12.19, $C_G(s)$ est connexe. Donc, par hypothèse de récurrence, il existe un tore T tel que $C_G(s) = TC_G(s)_u$. D'après le corollaire 12.19, à nouveau, il vient $G = C_G(s)G_u = TG_u$.

Par conséquent, G est un espace homogène sous $T \times G_u$. Le morphisme $\phi : T \times G_u \to G$, $(t, u) \mapsto tu$ est surjectif d'après ce qui précède, injectif car $T \cap G_u = \{1\}$. Il est de plus séparable. En effet, $\mathrm{d}\phi(X, Y) = X + Y$, et comme $\operatorname{Lie}(T) \cap \operatorname{Lie}(G_u) = \{0\}$, d'après le lemme 12.15, on en déduit que $\mathrm{d}\phi$ est injective, et donc surjective puisque $\dim(T \times G_u) = \dim G$.

Donc ϕ est un isomorphisme, d'après la proposition 12.12, et $\mathfrak{g} = \operatorname{Lie}(T) \oplus \operatorname{Lie}(G_u)$. Ceci entraîne que $\mathfrak{g}_n = \operatorname{Lie}(G_u)$. Enfin, soient $\pi : G \to G/G_u$ et $\varphi = \pi_{|T}$. Alors φ est T-équivariant et bijectif. De plus, $\mathrm{d}\varphi$ est injective (car $\operatorname{Ker}\mathrm{d}\pi = \operatorname{Lie}(G_u)$ et $\operatorname{Lie}(T) \cap \operatorname{Lie}(G_u) = \{0\}$), donc bijective puisque $\dim T = \dim G/G_u$. Donc φ est un isomorphisme $T \cong G/G_u$. $\square$

12.6. Conjugaison des tores maximaux. —

Proposition 12.21. — *Soient G résoluble connexe, T un tore tel que $G = TG_u$, et $s \in G_s$. Alors il existe $g \in \mathcal{C}^\infty(G)$ tel que $gsg^{-1} \in T$.*

Démonstration. — A nouveau, on procède par récurrence sur $\dim G$. Si G est nilpotent, l'hypothèse $G = TG_u$ entraîne, par décomposition de Jordan, que $T = G_s$. L'assertion est donc vraie dans ce cas. Supposons G non nilpotent. Alors $H := \mathcal{C}^\infty(G)$ est fermé, connexe, non-trivial et nilpotent (car inclus dans $\mathcal{C}(G) \subseteq G_u$). Soit $n \geq 0$ tel que $\mathcal{C}^n(H) \neq \{1\}$ et $\mathcal{C}^{n+1}(H) = \{1\}$, et soient $N = \mathcal{C}^n(H)$ et $\pi : G \to G/N := G'$. Alors $G' = \pi(T)G'_u$ et, par hypothèse de récurrence, il existe $g \in \mathcal{C}^\infty(G)$ tel que $\pi(g)\pi(s)\pi(g^{-1}) \in \pi(T)$. (Ici, on a utilisé le lemme suivant, qui se voit facilement par récurrence sur m).

Lemme 12.22. — *Soit $\pi : G \to G'$ un morphisme surjectif de groupes. Alors, pour tout $m \geq 0$, $\mathcal{C}^m(G') = \pi(\mathcal{C}^m(G))$. De même, $\mathcal{D}^m(G') = \pi(\mathcal{D}^m(G))$.*

Donc, on a $gsg^{-1} \in \pi^{-1}(T) = TN$. Ecrivons $gsg^{-1} = tv$, avec $t \in T, v \in N$. Or N est un sous-groupe commutatif de G_u, fermé, connexe, et normal dans G (car G normalise H et donc aussi N). D'après le lemme 12.18, il existe $u \in N$ et $z \in C_N(t)$ tels que $v = t^{-1}\, u\, t\, u^{-1}\, z$. Or z commute à t, et aussi à u (car N est abélien), donc

$$gsg^{-1} = tv = u\, t\, u^{-1}\, z = z\, u\, t\, u^{-1}.$$

Comme gsg^{-1} et utu^{-1} sont semi-simples, et z unipotent (car $z \in N$), il vient $z = 1$ et $(u^{-1}g)\, s\, (u^{-1}g)^{-1} = t \in T$. Or $u^{-1}g \in \mathcal{C}^\infty(G)$, puisque $g, u \in \mathcal{C}^\infty(G)$. La proposition est démontrée. □

Théorème 12.23. — **(Connexité des centralisateurs et conjugaison des tores maximaux)**
Soient T un tore tel que $G = TG_u$, et S un sous-groupe, non nécessairement fermé, formé d'éléments semi-simples. Alors S est commutatif et

a) *$C_G(S)$ est connexe et il existe $g \in \mathcal{C}^\infty(G)$ tel que $gSg^{-1} \subseteq T$. En particulier, tous les tores maximaux de G sont conjugués par $\mathcal{C}^\infty(G)$.*

b) *De plus, $C_G(S) = N_G(S)$.*

Démonstration. — On observe d'abord que S est commutatif, car G/G_u l'est (par exemple car $\mathcal{D}(G) \subseteq G_u$) et la restriction à S du morphisme $\pi : G \to G/G_u$ est injective. En effet, si $\pi(s) = \pi(t)$ alors $st^{-1} \in G_u$, d'où $s = t$ d'après la décomposition de Jordan.

On procède par récurrence sur $\dim G$. Si S est central, alors $C_G(S) = G$ est connexe, et le sous-groupe H de G engendré par S et T est formé d'éléments semi-simples. Donc, à nouveau, $\pi_{|H}$ est injective. Mais comme $G/G_u = \pi(T)$, par hypothèse, il vient $H = T$ d'où $S \subseteq T$.

Sinon, il existe $s \in S$ non central. D'après la proposition 12.21, quitte à remplacer S par un conjugué sous $\mathcal{C}^\infty(G)$, on peut supposer $s \in T$. Alors $C_G(s)$ contient T et S (car S est abélien), et est un sous-groupe propre, connexe d'après le corollaire 12.19. Par hypothèse de récurrence, $C_{C_G(s)}(S)$ est connexe, et il existe $g \in \mathcal{C}^\infty(C_G(s))$ tel que $gSg^{-1} \subseteq T$. Or $C_{C_G(s)}(S) = C_G(S)$ et $\mathcal{C}^\infty(C_G(s)) \subseteq \mathcal{C}^\infty(G)$. Ceci prouve a).

Enfin, soient $g \in N_G(S)$ et $s \in S$. Comme G/G_u est abélien, alors $\pi(gsg^{-1}s^{-1}) = 1$. Donc $(gsg^{-1})\, s^{-1} \in G_u \cap S$, d'où $gs = sg$ et $g \in C_G(S)$. □

En combinant le théorème précédent et le corollaire 12.20, on obtient le théorème 12.14. □

TABLE DES MATIÈRES

BIBLIOGRAPHIE

[Abe] E. Abe, Hopf algebras, Cambridge Univ. Press, 1977.

[AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison Wesley, 1969.

[Bo] A. Borel, Linear algebraic groups, Second enlarged edition, Springer Verlag, 1991.

[BA] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dix] J. Dixmier, Algèbres enveloppantes, Gauthier-Villars, 1974.

[Do88] D. Z. Doković, An elementary proof of the structure theorem for connected solvable affine algebraic groups, Enseign. Math. (2) 34 (1988), 269-273.

[Eis] D. Eisenbud, Commutative algebra with a view towards algebraic geometry, Springer, 1995.

[Ho] G. P. Hochschild, Basic theory of algebriac groups and Lie algebras, Springer-Verlag, 1981.

[Hu1] J. E. Humphreys, Introduction to Lie algebras and representation theory, Springer-Verlag, 1972, third printing, revised, 1980.

[Hu2] J. E. Humphreys, Linear algebraic groups, Springer-Verlag, 1975, corrected 2nd printing 1981.

[Ja] J. C. Jantzen, Representation of algebraic groups, Academic Press, 1987, second edition, Amer. Math. Soc., 2003.

[Ku] E. Kunz, Introduction to commutative algebra and algebraic geometry, Birkäuser, 1985.

[KSS] H. Kraft, P. Slodowy, T. A. Springer (Ed.), Algebraische Transformationsgruppen und Invariantentheorie - Algebraic Transformation Groupes and Invariant Theory, Birkäuser, 1989.

[Laf] J.-P. Lafon, Algèbre commutative (Langages géométrique et algébrique), Hermann, 1977.

[Las] Y. Laszlo, Introduction à la géométrie algébrique, cours de Master 2, 2004-2005.

[Ma1] H. Matsumura, Commutative algebra (2nd edition), The Benjamin Cummings publishing company, 1980.

[Ma2] H. Matsumura, Commutative ring theory, Cambridge Univ. Press, 1986, paperback edition with corrections, 1989.

[Sp] T. A. Springer, Linear algebraic groups, Birkäuser, 1981, 2nd edition 1998.