Introduction aux groupes algébriques

Alexis TCHOUDJEM

Institut Camille Jordan

Université Claude Bernard Lyon I

Boulevard du Onze Novembre 1918

69622 Villeurbanne

FRANCE

Villeurbanne, le 7 janvier 2013

Résumé :

Table des matières

Index

DORÉNAVANT, ON SUPPOSE k ALGÉBRIQUEMENT CLOS.

Chapitre 1

Rappel sur les variétés algébriques affines

1.1 Définition

Une *variété algébrique affine* est la donnée d'une paire

$$(X, k[X])$$

où X est un ensemble et $k[X]$ une sous-$k-$algèbre de type fini de l'algèbre des fonctions $X \to k$ tels que

$$X \to \mathrm{Hom}_{k-\mathrm{alg}}(k[X], k),\ x \mapsto \mathrm{ev}_x$$

est bijective.

On dit que $k[X]$ est *l'algèbre des fonctions régulières* sur X.

Remarque : en particulier, si $x \neq x'$, il existe $f \in k[X]$ tel que $f(x) \neq f(x')$.

Si I est un idéal de $k[X]$, on note $Z(I)$ l'ensemble des $x \in X$ tels que $f(x) = 0$ pour tout $f \in I$. Il existe une topologie, la *topologie de Zariski*, dont les fermés sont précisément les sous-ensembles $Z(I)$ de X.

Remarque : la paire $(X, k[X])$ est entièrement déterminée par $k[X]$.

Exemples :

i) tout ensemble fini X avec $k[X] = k^X$;

ii) on notera $\mathbb{A}^n$, la variété algébrique affine $(k^n, k[T_1, ..., T_n])$;

iii) on notera $\mathbb{G}_m$ la variété algébrique affine $(k^\times, k[T, T^{-1}])$.

1.2 Morphismes

Un *morphisme de variétés algébriques* $f : (X, k[X]) \to (Y, k[Y])$ est une application $f : X \to Y$ telle que pour tout $h \in k[Y]$, $h \circ f \in k[X]$.

Remarque : Si X est fini, alors toute application vers une variété algébrique Y : $f : X \to Y$ est un morphisme.

Exercice 1 *Vérifier que si X est une variété algébrique affine, $k[X]$ est aussi l'ensemble des morphismes de variétés algébriques $X \to \mathbb{A}^1$.*

Exemple : soient X un fermé algébrique de $\mathbb{A}^m$, Y un fermé algébrique de $\mathbb{A}^n$, alors si $f_1, ..., f_n \in k[X]$ et si pour tout $x \in X$, $(f_1(x), ..., f_n(x)) \in Y$, alors l'application :

$$X \to Y,\ x \mapsto (f_1(x), ..., f_n(x))$$

est un morphisme de variétés algébriques. De plus tous les morphismes de variétés : $X \to Y$ sont de cette forme.

Si $f : X \to Y$ est un morphisme de variétés algébriques, on notera $f^* : k[Y] \to k[X]$ le morphisme de $k-$algèbres associé.

Remarque : soient X, Y deux variétés algébriques affines. Pour tout morphisme de $k-$algèbres : $\phi : k[Y] \to k[X]$, il existe un unique morphisme de de variétés algébriques $f : X \to Y$ tel que $f^* = \phi$.

Exercice 2 *Toute variété algébrique affine est isomorphe à un sous-ensemble algébrique d'un certain k^n.*

Exercice 3 *Soit $f : X \to Y$ un morphisme de variétés algébriques. Alors f est un isomorphisme si et seulement si $f^* : k[Y] \to k[X]$ est un isomorphisme d'algèbres. Contre-exemple : le morphisme $f : \mathbb{A}^1 \to Z(X^2 - Y^3) \subseteq \mathbb{A}^2$, $t \mapsto (t^3, t^2)$ est bijectif mais n'est pas un isomorphisme.*

Soit X une variété algébrique affine.

Si Y est un fermé de X, alors Y a une structure canonique de variété algébrique affine avec pour $k-$algèbre $k[Y]$ l'algèbre des restrictions à X des fonctions régulières sur X. On dit que Y est une sous-variété fermée de Y.

On notera $I(Y)$ l'idéal $\{f \in k[X] \ : \ f|_Y = 0\}$. On a : $k[Y] \simeq k[X]/I(Y)$.

Soit $0 \neq f \in k[X]$. L'ouvert $D(f) := \{x \in X \ : \ f(x) \neq 0\}$ de X a une structure canonique de variété algébrique affine avec pour $k-$algèbre $k[D(f)] = k[X]_f \simeq k[X][T]/(1 - fT)$. Tout ouvert de X est une réunion finie de certains $D(f)$. On dit que $D(f)$ est un *ouvert principal* de X.

Exemple : $\mathrm{GL}_n(k)$ est un ouvert principal de $\mathbb{A}^{n^2}$.

Exercice 4 *Vérifier que l'on a un isomorphisme de variétés : $k^\times \simeq Z(1 - XY) \subseteq \mathbb{A}^2$.*

Exercice 5 *Soit X une variété algébrique affine. Soit $f \in k[X]$ tel que $\forall x \in X$, $f(x) \neq 0$. Montrer que $\frac{1}{f} \in k[X]$ (indication : considérer l'idéal de $k[X]$: $\{h \in k[X] \ : \ h/f \in k[X]\}$ et utiliser le théorème des zéros de Hilbert).*

Produit

Soient X, Y deux variétés algébriques affines, on munit le produit $X \times Y$ d'une structure de variétés en posant :

$$k[X \times Y] = k[X] \otimes_k k[Y] \ .$$

Remarque : on peut identifier $k[X] \otimes k[Y]$ avec la sous-algèbre des fonctions $X \times Y \to k$ de la forme :

$$(x, y) \mapsto \sum_i f_i(x) g_i(y)$$

pour certains $f_i \in k[X]$, $g_i \in k[Y]$.

Exercice 6 *i) Vérifier que* $\mathbb{A}^m \times \mathbb{A}^n \simeq \mathbb{A}^{m+n}$.

ii) Vérifier que $p_X : X \times Y \to X$ *et* $p_Y : X \times Y \to Y$ *sont des morphismes et que pour tous morphismes de variétés :* $f_1 : Z \to X$, $f_2 : Z \to Y$, *il existe un unique morphisme* $f : Z \to X \times Y$ *tel que* $\pi_X f = f_1$ *et* $\pi_Y f = f_2$.

Exercice 7 *Vérifier que la topologie de Zariski de* $\mathbb{A}^2$ *est plus fine que la topologie produit de* $\mathbb{A}^1 \times \mathbb{A}^1$.

Exercice 8 *Vérifier que si* X *est une variété algébrique le morphisme diagonal :*

$$X \to X \times X, \, x \mapsto (x, x)$$

est bien un morphisme de variétés et que Δ^* *est le morphisme de multiplication* $m : k[X] \otimes_k k[X] \to k[X]$.

1.2.1 Propriétés topologiques

Soit X une variété algèbrique affine. Comme espace topologique, X est *nœthérien i.e.* toute famille de fermés contient un élément minimal.

On dit qu'un espace topologique non vide X est *irréductible* si X n'est pas la réunion de deux fermés propres ; autrement dit tous les ouverts non vides sont denses.

Propriétés :

i) si $Y \subseteq X$ est une partie d'un espace topologique, alors Y est irréductible si et seulement si $\overline{Y}$ l'est ;

ii) l'image continue d'un irréductible est aussi irréductible.

Proposition 1.2.1 *Une variété algébrique affine est irréductible si et seulement si* $k[X]$ *est intègre.*

Corollaire 1.2.1.1 *Si X est une variété algébrique, alors un fermé $Z \subseteq X$ est irréductible si et seulement si $I(Z)$ est un idéal premier de $k[X]$.*

Par exemple, $\mathbb{A}^n$ est irréductible.

Soit $f \in k[X_1, ..., X_n]$ un polynôme non nul. Alors le fermé $Z(f)$ de $\mathbb{A}^n$ est irréductible si et seulement si f est irréductible. Si

$$f = f_1^{a_1} ... f_r^{a_r}$$

est la décomposition de f en produit d'irréductibles distincts, alors on a une décomposition en union de fermés irréductibles :

$$Z(f) = \cup_i Z(f_i)$$

Proposition 1.2.2 *Une variété algèbrique affine est une réunion finie de fermés irréductibles maximaux : ce sont les composantes irréductibles de X.*

Proposition 1.2.3 *Si X, Y sont irréductibles, alors $X \times Y$ aussi.*

Contre-exemple : vérifier que $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ n'est pas intègre.

Exercice 9 *Montrer que sur $\mathbb{C}$, $V_{\mathbb{C}^2}(x^2 + y^2 - 1) \simeq V_{\mathbb{C}^2}(xy = 1)$.*

Proposition 1.2.4 *$(X \times Y, k[X \times Y])$ est une variété algébrique et les projections $\pi_X : X \times Y \to X$* et *$\pi_Y : X \times Y \to Y$ sont des morphismes.*

Chapitre 2

Groupes algébriques affines

2.1 Définition, groupes classiques

Soit G un groupe. On dit que G est un *groupe algébrique affine* si G est aussi une variété algébrique affine telle que :

i) la multiplication : $\mu : G \times G \to G$, $(g, g') \mapsto gg'$;

ii) l'inversion : $i : G \to G,\ g \mapsto g^{-1}$;

sont des morphismes de variétés.

Autrement dit, pour tout $f \in k[G]$,

$$(g, h) \mapsto f(gh) \in k[G] \otimes_k k[G]$$

$$g \mapsto f(g^{-1}) \in k[G] \ .$$

Exemples :

i) Tout groupe fini est un groupe algébrique ;

ii) on note $\mathbb{G}_a$ le groupe algébrique k muni de l'addition :

$$k[\mathbb{G}_a] = k[T] \text{ et } \mu^* T = T \otimes 1 + 1 \otimes T,\ i^* T = -T \ .$$

iii) GL_n avec $k[\mathrm{GL}_n] = k[T_{i,j}, \det^{-1}]$. On notera $\mathbb{G}_m := \mathrm{GL}_1 : k[\mathbb{G}_m] = k[T, T^{-1}]$.

Soient $I : G \to G$ et $\mu : G \times G \to G$ l'inversion et la multiplication. On a :

$$T_{i,j} \circ I = \frac{(-1)^{i+j} \det_{j,i}}{\det} \in k[G]$$

$$\overset{-1}{\det} \circ I = \det \in k[G]$$

$$T_{i,j} \circ \mu = \sum_{k=1}^{n} T_{i,k} \otimes T_{k,j} \in k[G \times G] = k[G] \otimes k[G]$$

$$\overset{-1}{\det} \circ \mu = \overset{-1}{\det} \otimes \overset{-1}{\det} \in k[G \times G] \ .$$

iv) Si G_1, G_2 sont des groupes algébriques, alors $G_1 \times G_2$ aussi.

Proposition 2.1.1 *Tout sous-groupe fermé d'un groupe algébrique linéaire (en particulier de* GL_n*) est un groupe algébrique linéaire.*

Un *morphisme* de groupes algébriques est un morphisme de groupes qui est en même temps un morphisme de variétés.

Exemple : nous verrons que si k est un corps de caractéristique 2, alors $\mathrm{SL}_2(k)$ est isomorphe à $\mathrm{PSL}_2(k)$ comme groupe abstrait mais non comme groupe algébrique.

2.1.1 Les groupes classiques

Exemples :

i) le groupe $B_n(k)$ (resp. $D_n(k)$ (resp. $U_n(k)$)) des matrices inversibles triangulaires supérieures (resp. diagonales (resp. triangulaires supérieures avec seulement des 1 sur la diagonale)) ;

ii) SL_n avec $k[\mathrm{SL}_n] = k[T_{i,j}]/(\det -1)$;

iii) Soit $S \in \mathrm{GL}_n$, le sous-groupe des $M \in \mathrm{GL}_n$ tels que

$$MS({}^tM) = S$$

forme un groupe algébrique linéaire. On obtient ainsi les groupes classiques :

iv) si $n = 2m$ est pair, si :

$$S = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$$

on obtient le groupe symplectique Sp_{2m}.

v) si k est de caractéristique $\neq 2$, si $S = I_n$, on obtient le groupe orthogonal O_n. Le groupe spécial orthogonal SO_n est l'intersection $O_n \cap SL_n$.

Un *(iso)morphisme* de groupes algébriques est un (iso)morphisme de groupes qui est en même temps un (iso)morphisme de variétés.

exo : $SO_2 \simeq \mathbb{G}_m$ si k est de caractéristique $\neq 2$.

On appelle groupes classiques les groupes algébriques suivants :

:

— type A_{n-1} : $SL_n(k)$, k quelconque,

— type B_n : $SO_{2n+1}(k)$, k de caractéristique $\neq 2$,

— type C_n : $Sp_{2n}(k) := \{g \in \mathrm{GL}_n(k) \ : \ tgJg = J\}$, k quelconque, où J est une matrice antisymétrique inversible.

— type D_n : $SO_{2n}(k)$, k de caractéristique $\neq 2$.

Exercice 10 *Soit* $A := k[\mathrm{SL}_2] = k[T_1, T_2, T_3, T_4]/(T_1T_4 - T_2T_3 - 1)$*. Posons* t_i *l'image de* T_i *dans* A*. Soit* B *la sous-*$k-$*algèbre de* A *engendrée par les* t_it_j*,* $1 \leq i, j \leq 4$*.*

i) Montrer que $\mu^*B \subseteq B \otimes B$ *et* $i^*B \subseteq B$*. En déduire qu'il existe un groupe algébrique dont l'algèbre des fonctions régulières est* B*.*

On notera PSL_2 *ce groupe.*

ii) Montrer que l'inclusion $B \subseteq A$ *induit un morphisme de groupes :*

$$\phi : \mathrm{SL}_2 \to \mathrm{PSL}_2$$

dont le noyau est d'ordre au plus 2*.*

iii) si k *est de caractéristique* $\neq 2$*, montrer que* B *est l'algèbre des fonctions* $f \in A$ *telle que* $f(M) = f(-M)$ *pour tout* $M \in \mathrm{SL}_2$ *;*

iv) si k *est de caractéristique* 2*, montrer que* ϕ *est un isomorphisme de groupes mais n'est pas un isomorphisme de groupes algébriques.*

2.2 Schémas en groupes

Soit G un groupe algébrique linéaire. Notons e le neutre de G.

La multiplication, l'inversion et le neutre induisent des morphismes de $k-$algèbres :

$$\mu^* : k[G] \to k[G] \otimes k[G]$$

$$i^* : k[G] \to k[G]$$

$$e^* : k[G] \to k,\ f \mapsto f(e)\ .$$

Si on note $A := k[G]$ et $m : A \otimes A \to A$ la multiplication, alors les axiomes de définition d'un groupe se traduisent par les diagrammes commutatifs suivants :

associativité :

$$\begin{tikzcd}
A \otimes A \arrow[r, "\mathrm{Id}\otimes\mu^*"] & A \otimes A \otimes A \\
A \arrow[u, "\mu^*"] \arrow[r, "\mu^*"] & A \otimes A \arrow[u, "\mu^*\otimes\mathrm{Id}"']
\end{tikzcd}$$

définition du neutre :

$$\begin{tikzcd}
A & A \otimes A \arrow[l, "\mathrm{Id}\otimes e^*"'] \\
A \otimes A \arrow[u, "e^*\otimes\mathrm{Id}"] & A \arrow[l, "\mu^*"] \arrow[u, "\mu^*"'] \arrow[ul, "\mathrm{Id}"]
\end{tikzcd}$$

définition de l'inverse :

$$\begin{tikzcd}
 & A \otimes A \arrow[dl, "m"'] & A \otimes A \arrow[l, "i^* \otimes \mathrm{Id}"'] & \\
A & & & A \arrow[lll, "e^*"] \arrow[ul, "\mu^*"'] \arrow[dl, "\mu^*"] \\
 & A \otimes A \arrow[ul, "m"] & A \otimes A \arrow[l, "\mathrm{Id} \otimes i^*"] &
\end{tikzcd}$$

Soit R un anneau commutatif (avec 1). Soit A une $R-$algèbre. On suppose qu'il existe des morphismes de $R-$algèbres :

$$\mu^* : A \to A \otimes_R A$$

$$i^* : A \to A$$

$$e^* : A \to R$$

qui vérifient les diagrammes commutatifs ci-dessus. On dit alors que A définit un *schéma en groupes affine* sur R.

Supposons que G est un groupe algébrique linéaire sur k et que k est une $R-$algèbre. On dit que G possède une $R-$*structure* s'il existe un schéma en groupes affine A tel que

$$k[G] = A \otimes_R k$$

et tel que les opérations de groupes sont associées aux morphismes :

$$\mu^* \otimes \mathrm{Id}, i^* \otimes \mathrm{Id}, e^* \otimes \mathrm{Id} \ .$$

Dans cette situation, on note $G(R)$ les morphismes $A \to R$. Alors μ^* induit un produit :

$$G(R) \times G(R) \to G(R)$$

qui définit une structure de groupes sur $G(R)$. C'est le groupe des $R-$*points* de G.

Exemples :

i) les groupes GL_n, SO_n, Sp_{2m}, SL_n ont tous une $\mathbb{Z}-$structure.

ii) Si $n \geq 1$, soit $A := \mathbb{Z}[T]/[T^n - 1]$. Les morphismes tels que $\mu^* t = t \otimes t$, $i^* t = t^{n-1}$, $e^* t = 1$ où $t := T \bmod T^n - 1$ définissent un schéma en groupes affine noté $\boldsymbol{\mu}_n$. C'est le schéma en groupes des racines $n-$ièmes de l'unité. Si k est de caractéristique première à n ou zéro, $A \otimes_{\mathbb{Z}} k$ définit le groupe algébrique linéaire fini des racines $n-$ièmes de l'unité. Si k est de caractéristique n, $A \otimes_{\mathbb{Z}} k = k[T]/(T^n - 1)$ n'est pas réduite donc ce n'est pas l'algèbre des fonctions régulières sur un groupe algébrique.

2.3 Premières propriétés des sous-groupes

Soit G un groupe algébrique affine.

Lemme 2.3.1 *Soient U, V des parties de G. On suppose que U est dense et que V est un ouvert non vide de G. Alors $UV = G$.*

Démonstration : Soit $g \in G$. Comme l'inversion et la multiplication par g sont des homéomorphismes : $G \to G$, $U^{-1}g$ est dense dans G.Donc rencontre V : il existe $v \in V \cap U^{-1}g$ *i.e.* : il existe $u, v \in U \times V$ tel que : $g = uv$. **Q.e.d.**

Lemme 2.3.2 *Soit $H \leq G$ un sous-groupe. Alors, $\overline{H}$ est un sous-groupe de G et si H contient un ouvert non vide de $\overline{H}$, alors, H est fermé.*

Démonstration : Comme $^{-1}$ est un homéomorphisme, $\overline{H}^{-1} = \overline{H^{-1}}$.

Soit $h \in H$. La multiplication à gauche par h est un homéomorphisme. Donc $h\overline{H} = \overline{hH} = \overline{H}$.

Soit $g \in \overline{H}$. La multiplication à droite par g est un homéomorphisme donc $\overline{H}g = \overline{Hg} \subseteq \overline{H}$. D'où la stabilité par passage à l'inverse et par multiplication.

Soit V un ouvert de $\overline{H}$ contenu dans H. On applique le lemme précédent à V et H. **Q.e.d.**

Exemples : soit S une partie d'un groupe algébrique G. Les sous-groupes suivants sont fermés :

— le normalisateur $N_G(S) := \{g \in G \ : \ gSg^{-1} = S\}$;

— le centralisateur : $C_G(S) := \{g \in G \ : \ \forall\, s \in S,\ gsg^{-1} = s\}$.

2.4 Composante neutre

Théorème 2.4.1 *Soit G un groupe algébrique linéaire.*

Il existe une unique composante irréductible de G contenant 1, notée G°. De plus, on a :

— G° est la composante connexe de 1 ;

— G° est un sous-groupe distingué et d'indice fini dans G ;

— tout sous-groupe fermé d'indice fini contient G°.

Remarque : en particulier, pour un groupe algébrique, connexe $\Leftrightarrow$ irréductible. *Contre-exemple :* $Z(xy) = Z(x) \cup Z(y)$ est réductible dans $\mathbb{A}^2$ mais connexe.

Démonstration : Unicité : Soit X une autre composante irréductible de G contenant 1. Alors $\overline{X.G^\circ} = \overline{\mu(X \times G^\circ)}$ est irréductible, contient G° et X et donc est égal à $G^\circ = X$.

On a de plus $G^\circ.G^\circ = G^\circ$. Donc G° est bien un sous-groupe car l'inversion étant un isomorphisme, elle préserve G°.

Si $x \in G$, $xG^\circ x^{-1}$ est une composante irréductible contenant 1 c'est donc G°. Donc G° est distingué.

Les classes à gauche de G° sont des composantes irréductibles car si $x \in G$, $\lambda_x : G \to G, y \mapsto xy$ est un isomorphisme. Comme G n'a qu'un nombre fini de composantes irréductibles, G° n'a qu'un nombre fini de classes à gauche donc est d'indice fini.

En particulier, les composantes irréductibles sont disjointes donc ce sont aussi les composantes connexes.

Enfin, si H est fermé et d'indice fini dans G, la composante connexe G° est contenue dans une classe à gauche de H. C'est forcément la classe de 1. Donc $G^\circ \subseteq H$.

Q.e.d.

Exercice 11 *Montrer que* $O(2,k)^\circ = SO(2,k)$.

Exercice 12 G_a, $\mathbb{G}_m$, GL_m, D_n, B_n, U_n, SL_n *sont connexes*

Puisque l'on est dans des rappels de nature topologiques, voici une digression sur la notion importante de *dimension*

2.5 Rappels sur la dimension

Soit X une variété algébrique affine non vide. On définit la dimension de X comme $\partial_k k[X] := \sup\{m : \exists,\ a_1, .., a_m \in k[X] \text{ algébriquements indépendants}\}$.

Exemples :

i) $\dim X = 0 \Leftrightarrow X$ fini et dans ce cas, $|X| = \dim_k k[X]$;

ii) dim(cercle)= 1 ;

iii) $\dim(SL(2; k)) = 3$;

iv) $\dim(\text{sous} - \text{espace vectoriel de } k^n) =$dimension usuelle ;

v) si X est irréductible et si $X_f \neq \emptyset$, alors, $\dim X_f = \dim X$;

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

Proposition 2.5.1 *Soit X une variété affine non vide. Soient $X_1, ..., X_n$ ses composantes irréductibles. Alors* $\dim X = \max_i \dim X_i$.

Démonstration : X_i est fermé dans X donc $k[X_i]$ est une image de $k[X]$. En particulier $\partial_k k[X_i] \leq \partial_k k[X]$. Donc le max est plus petit que $\dim X$.

Dans l'autre sens : Soient $m > \max_i \dim X_i$. Soient $a_1, ..., a_m \in k[X]$. Pour tout i, $a_1|_{X_i}, ..., a_m|_{X_i}$ sont forcément algébriquement dépendants sur k. Donc pour tout i, il existe un $f_i \in k[T_1, ..., T_m]$ non nul tel que $f_i(a_1, ..., a_m)|_{X_i} =$

0. Mais alors si $f = \prod_i f_i$. On a $f \neq 0$ et $f(a_1, ..., a_m) = 0$ sur $\cup_i X_i = X$ et donc les a_j ne sauraient être algébriquement indépendants sur k. On a donc $\dim X < m$.

Q.e.d.

Proposition 2.5.2 (IMPORTANTE) *Soit* Y *un fermé de* X*, une variété affine* **irréductible**.

Si $Y \underset{\neq}{\subset} X$*, alors :* $\dim Y < \dim X$.

Démonstration : Soient $f_1, ..., f_y \in k[X]$ tels que $f_1|_Y, ..., f_y|_Y$ soient algébriquement indépendants dans $k[Y]$ et $y = \dim Y$. Soit $f \in k[X]$ non nul tel que $f|_Y = 0$. Alors, $(f_1, ..., f_y, f)$ sont algébriquement indépendants dans $k[X]$.

En effet, si $a_0, ..., a_N \in k[T_1, ..., T_y]$ vérivient :

$$a_0(f_1, ..., f_y)f^N + ... + a_N(f_1, ..., f_y) = 0$$

dans $k[X]$. En restreignant à Y, on trouve : $a_N(f_1|_Y, ..., f_y|_Y) = 0$ dans $k[Y]$. Donc $a_N(T_1, ..., T_y) = 0$. Comme $k[X]$ est intègre et f non nul, on peut simplifier par f et on trouve que $a_{N-1}(T_1, ..., T_y) = 0$, *etc.* **Q.e.d.**

2.6 Quelques propriétés des morphismes

2.6.1 Morphismes dominants et immersions fermées

Soit $\phi : Z \to X$. Si $\overline{\phi(Z)} = X$, on dit que ϕ est *dominant*.

On dit que ϕ est une immersion fermée si $\phi(Z)$ est fermé dans X et $\phi : Z \to \phi(Z)$ est un isomorphisme.

Proposition 2.6.1 *Soit* $\phi : Z \to X$ *un morphisme.*

i) ϕ *est dominant* $\Leftrightarrow$ ϕ^* *injective ;*

ii) ϕ *est une immersion fermée* $\Leftrightarrow$ ϕ^* *est surjective (on n'en a peut-être pas besoin !).*

iii) Si Z *est irréductible, alors* $\overline{\phi(Z)}$ *aussi et* $\dim \overline{\phi(Z)} \leq \dim Z$.

Démonstration :

i) $\Rightarrow$: Si $f \in \ker \phi^*$, alors $f \circ \phi = 0$ *i.e.* $f$est nulle sur $\phi(Z)$; par densité, f est nulle sur tout X.

$\Leftarrow$: Si $\overline{\phi(Z)} \underset{\neq}{\subset} X$, alors il existe $f \in k[X]$ non nulle mais nulle sur $\phi(Z)$. Mézalor : $\phi^*(f) = 0 \Rightarrow f = 0$ impossible !

ii) $\Rightarrow$: exo $\Leftarrow$: $\phi(Z) = V_X(\ker \phi^*)$.

En effet, $\phi(Z) \subseteq V_X(\ker \phi^*)$ (facile) et réciproquement, si $y \in V_X(\ker \phi^*)$, alors le morphisme :

$$e_y : k[X] \to k$$

passe au quotient :

$$k[X]/\ker \phi^* \simeq k[Z] \to k \ .$$

Ce morphisme est de la forme e_z pour un certain $z \in Z$. Et on a : $e_z \circ \phi^* = e_y$ *i.e.* $e_{\phi(z)} = e_y$ *i.e.* $y = \phi(z)$.

Pour montrer que $Z \simeq \phi(Z)$, on va supposer $\phi(Z) = X$ *i.e.* ϕ^* est un isomorphisme d'après i).

On utilise alors la caractérisation des isomorphismes ci-dessus. **Q.e.d.**

2.6.2 Constructibilité de l'image

Théorème 2.6.2 *Soit $\phi : X \to Y$ un morphisme de variétés. Alors $\phi(X)$ contient un ouvert non vide de $\overline{\phi(X)}$.*

Exemple : soit $\phi : \mathbb{A}^2 \to \mathbb{A}^2$, $(x,y) \mapsto (x, xy)$. On a :

$$k^\times \times k \subset \phi(\mathbb{A}^2) = k^\times \times k \cup \{(0,0)\} \subset \mathbb{A}^2 = \overline{\phi(\mathbb{A}^2)} \ .$$

Démonstration :

Théorème 2.6.3 *Soient $A \subseteq B$ deux anneaux intègres tels que B est de type fini sur A. Soit K un corps algébriquement clos et soit $0 \neq b \in B$. Alors il existe $0 \neq a \in A$ tel que tout morphisme d'anneaux $\phi : A \to K$ tel que $\phi(a) \neq 0$ se prolonge en un morphisme $\widetilde{\phi} : B \to K$ tel que $\phi(b) \neq 0$.*

Remarque : comme corollaire on retrouve la forme faible du théorème des zéros : Si L/K est une $K-$algèbre de type fini qui est un corps, alors L/K est une extension algébrique.

1er cas : X irréductible. On suppose $Y = \overline{\phi(X)}$. Donc : $k[Y] \subseteq k[X]$. Il existe $a \neq 0 \in k[Y]$ tel que si $t : k[Y] \to k$ est un morphisme d'algèbres tel que $t(a) \neq 0$, t se prolonge à $k[X]$. Alors $\phi(X) \supseteq Y_a$.

2e cas : $X = X_1 \cup ... \cup X_n$ décomposition en union d'irréductibles. Soient U_i ouverts de $\overline{\phi(X_i)}$ contenus dans $\phi(X_i)$. Soient Ω_i ouverts de $\overline{\phi(X)}$ tels que $\Omega_i \cap \overline{\phi(X_i)} = U_i$. Soit k maximal pour qu'il existe $i_1, ..., i_k$ tels que : $\Omega := \bigcap_{1 \leq j \leq k} \Omega_{i_j} \neq \emptyset$. Alors Ω convient. **Q.e.d.**

Démonstration : du théorème 2.6.3

Supposons que $B = A[x]$ pour un certain $x \in B$. On considère le noyau I du morphisme $A[T] \to B$, $P(T) \mapsto P(x)$.

— si $I = 0$: exo ;

— sinon, soit $f = cT^n + ... \in I \setminus \{0\}$ de degré minimal $n > 0$.

Comme B est intègre, f est irréductible sur le corps des fractions de A, noté L.

Remarque : En utilisant l'algorithme d'Euclide on trouve que :

$$g \in I \Rightarrow \exists\, m \geq 0, f | c^m g \text{ dans } A \ . \tag{2.1}$$

Soit $h \in A[T]$ tel que $b = h(x)$. Puisque $b \neq 0$, $h \notin I$. On en déduit que h et f sont premiers entre eux sur L. Il existe donc $\alpha, \beta, \gamma \in A$ tels que :

$$\alpha f + \beta h = \gamma \neq 0 \ .$$

On pose alors : $a := c\gamma$.

Soit $\phi : A \to K$ un morphisme d'anneaux tel que $\phi(a) \neq 0$. Alors, $\phi(c) \neq 0$ et $\phi(\gamma) \neq 0$. Posons pour tout $P = p_0 + p_1 T + ... \in A[T]$, $P^\phi := \phi(p_0) + \phi(p_1)T + ... \in K[T]$.

Comme $\phi(c) \neq 0$, le polynôme $f^\phi \in K[T]$ est non constant et admet donc une racine $z \in K$.

On pose alors

$$\widetilde{\phi} : A[T] \to K \ , \ P \mapsto P^\phi(z) \ .$$

Remarquons que $\widetilde{\phi}(h) \neq 0$ car $\widetilde{\phi}(f) = 0$ et $\phi(\gamma) \neq 0$.

D'après (2.1), et comme $\phi(c) \neq 0$, $\widetilde{\phi}$ passe au quotient par I et on obtient ainsi un prolongement de ϕ à $B \simeq A[T]/I$ tel que $\widetilde{\phi}(b) \neq 0$.

Q.e.d.

2.7 Sous-groupes engendrés

Corollaire 2.7.0.1 *Si $\phi : G \to G'$ est un morphisme de groupes algébriques, alors $\phi(G)$ est fermé. On a aussi $\phi(G^\circ) = \phi(G)^\circ$.*

Démonstration : Le sous-groupe $\phi(G)$ contient un ouvert de son adhérence d'après le théorème 2.6.2. C'est donc un sous-groupe fermé de G' d'après le lemme 2.3.2.

On a $\phi(G^\circ) \subseteq \phi(G)^\circ$ car $\phi(G^\circ)$ est connexe et contient 1. Le morphisme de groupes $G/G^\circ \to \phi(G)/\phi(G^\circ)$ auquel on pense est surjectif. Donc $\phi(G^\circ)$ est d'indice fini dans $\phi(G)$. On a donc $\phi(G^\circ) = \phi(G)^\circ$. **Q.e.d.**

Proposition 2.7.1 *Soient $(X_i, \phi_i)_{i \in I}$ une famille de morphismes $\phi_i : X_i \to G$ où G est un groupe algébrique linéaire, les X_i sont des variétés irréductibles. On suppose que $1 \in \phi_i(X_i)$ pour tout i.*

Soit H le plus petit sous-groupe de G contenant les $\phi_i(X_i)$. Alors :

i) H est fermé connexe ;

ii) $\exists\, i_1, ..., i_n \in I, \epsilon_1, ..., \epsilon_n \in \{\pm 1\}, H = (\phi_{i_1} X_{i_1})^{\epsilon_1} ... (\phi_{i_n} X_{i_n})^{\epsilon_n}$.

Démonstration : Posons pour tout $i \in I$, $Y_i := \phi_i(X_i)$. Quitte à les ajouter, on peut supposer que les ensemble Y_i^{-1} figurent dans la liste des Y_j, $j \in I$.

Pour toute suite finie $a = (a_1, ..., a_n)$ d'éléments de I, on pose $Y_a := Y_{a_1}...Y_{a_n}$; c'est l'image de $Y_{a_1} \times ... \times Y_{a_n}$ dans G par la multiplication : $G^n \to G$. Cette multiplication est un morphisme de variétés algébriques et le produit $Y_{a_1} \times ... \times Y_{a_n}$ est irréductible, donc pour toute suite finie a, Y_a est une partie irréductible de G. Il en est de même pour les $\overline{Y_a}$. Si a, b sont des suites finies on note (a, b) leur mise bout à bout. On a :

$$Y_a.Y_b = Y_{a,b} \ .$$

On a donc : $\overline{Y_a}.\overline{Y_b} \subseteq \overline{Y_{a,b}}$. Soit a une suite finie telle que la partie $\overline{Y_a}$ de G soit de dimension maximale.

Pour toute suite finie b, $\overline{Y_a} \subseteq \overline{Y_a}.\overline{Y_b} \subseteq \overline{Y_{a,b}}$, puisque $1 \in Y_a$. Comme la dimension de $\overline{Y_a}$ est maximale et comme $Y_{a,b}$ est irréductible, $\overline{Y_a} = \overline{Y_{a,b}}$. En particulier, $\overline{Y_a} = \overline{Y_a}.\overline{Y_b}$. Et donc $\overline{Y_b} \subseteq \overline{Y_a}$ pour toute suite finie b. En particulier, $\overline{Y_a}$ est stable par passage à l'inverse et $\overline{Y_a} = \overline{Y_a}.\overline{Y_a}$; d'où : $\overline{Y_a}$ est un sous-groupe fermé de G. Puisque Y_a contient un ouvert non vide de $\overline{Y_a}$ (*cf.* le théorème 2.6.2), $\overline{Y_a} = Y_a.Y_a = Y_{a,a}$. **Q.e.d.**

Corollaire 2.7.1.1 *Soient G_i une famille de sous-groupes fermés connexes de G. Alors les G_i engendrent un sous-groupe H de G fermé connexe ; de plus, $H = G_{i_1}...G_{i_n}$ pour certains indices i_j.*

Exercice 13 *SL_n, SO_n et Sp_{2n} sont connexes (indication pour le groupe orthogonal : montrer que* SO_n *est engendré par les $s_x : y \mapsto y - 2\langle x, y\rangle x$, avec $x \in k^n$, $\langle x, x\rangle = 1$).*

Soient $H, K \leq G$. On pose $(H, K) := \langle xyx^{-1}y^{-1} \ : \ x \in H, y \in K\rangle$.

Corollaire 2.7.1.2 *Soient H, K deux sous-groupes fermés de G dont l'un est connexe. Alors (H, K) est un sous-groupe fermé connexe de G.*

Démonstration : Si par exemple, H est connexe, le groupe (H, K) est engendré par les sous-groupes connexes kHk^{-1}. **Q.e.d.**

Par exemple, si G est connexe, les groupes dérivé $D(G) = (G, G)$, $D^n(G) = (D^{n-1}(G), D^{n-1}(G))$, sont connexes.

2.8 Linéarisation des groupes algébriques affines

Définition 1 *Soit G un groupe algébrique affine. pour tout $x \in G$, on pose :*
$\delta(x) : k[G] \to k[G], f \mapsto f(\cdot x)$ *et* $\gamma(x) : k[G] \to k[G], f \mapsto f(x^{-1}\cdot)$.

Proposition 2.8.1 *Soit G un groupe algébrique affine et $\mu : G \times G \to G$ sa multiplication.*

i) Soit V un sous-espace de $k[G]$ de dimension finie alors il existe W un sous-espace de $k[G]$ de dimension finie contenant V et stable par $\delta(x)$ (resp. $\gamma(x)$)pour tout $x \in G$.

ii) Si V est un sous-espace vectoriel de $k[G]$, alors V est stable pour tous les $\delta(x)$ (resp. tous les $\gamma(x)$), $x \in G$, $\Leftrightarrow$ $\mu^*(V) \subseteq V \otimes k[G]$ (resp. $\mu^*(V) \subseteq k[G] \otimes V$).

Démonstration : i) Il suffit de traiter le cas où $V = k.f$ pour un certain $f \in k[G]$.

Soit $\mu : G \times G \to G$ la multiplication. On a :

$$f \circ \mu = \sum_{i=1}^{n} p_i \otimes q_i \in k[G] \otimes k[G]$$

pour certains $p_i, q_i \in k[G]$. On a alors pour tout $g, x \in G$:

$$f(gx) = p_1(g)q_1(x) + ... + p_n(g)q_n(x)$$

donc $\delta(x)(f) \in \langle p_1, ..., p_n \rangle$ pour tout $x \in G$. L'espace vectoriel $W := \langle \delta(x)(f) \ : \ x \in G \rangle$ est donc de dimension finie.

ii) $\Leftarrow$: facile !

$\Rightarrow$: Soit $(f_i)_{i \in I}$ une base de V. On la complète en une base $(f_i)_{i \in I} \sqcup (f_j)_{j \in J}$ de $k[G]$. Pour tout $\alpha \in I$, on a :

$$\mu^*(f_\alpha) = \sum_{i \in I} f_i \otimes a_i + \sum_{j \in J} f_j \otimes a_j$$

pour certains $a_i, a_j \in k[G]$. Mais alors pour tout $x \in G$:

$$\delta(x)(f_\alpha) = \sum_{i \in I} a_i(x) f_i + \sum_{j \in J} a_j(x) f_j \in V = \sum_{i \in I} k f_i \ .$$

Comme les f_i, $i \in I \sqcup J$, sont linéairement indépendants, $a_j(x) = 0$ pour tout $j \in J$ et tout $x \in G$. Donc les a_j sont nuls dans $k[G]$, pour tout $j \in J$. Ainsi, $\mu^*(f_\alpha) \in V \otimes k[G]$, pour tous $\alpha \in I$ et $\mu^*(V) \subseteq V \otimes k[G]$. **Q.e.d.**

Proposition 2.8.2 (Linéarisation des groupes algébriques) *Soit G un groupe algébrique affine. Alors G est un groupe algébrique linéaire* i.e. *isomorphe à un sous-groupe fermé de $GL_n(k)$ pour un certain $n > 0$ et un certain corps k.*

Démonstration : Comme $k[G]$ est de type fini, il existe $f_1, ..., f_n \in k[G]$ tels que $k[f_1, ...f_n] = k[G]$. Quitte à ajouter des f_i, on peut supposer, d'après la proposition 2.8.1, que $kf_1 + ... + kf_n$ est stable par $\delta(x)$ pour tout $x \in G$.

On peut aussi supposer que les f_i sont linéairement indépendants. D'après la proposition 2.8.1 ii), on a pour tout $x \in G$:

$$\delta(x) f_j = \sum_{i=1}^{n} a_{i,j}(x) f_i$$

où les $a_{i,j}$ sont des éléments de $k[G]$.

On a alors une application : $G \to GL_n(k)$, $g \mapsto (a_{i,j}(g))_{1 \le i,j \le n}$ qui est un morphisme de groupes algébriques (exo).

Ce morphisme est injectif car si g est dans le noyau, $\delta(g) f_j = f_j$ pour tout j. Donc $\delta(g)(f) = f$ pour tout $f \in k[G]$ *i.e.* : $f(xg) = f(x)$ pour tout $x \in G$. En conséquence comme $k[G]$ sépare les points de G :

$$\forall\, x \in G, xg = x \Rightarrow g = 1 \ .$$

Q.e.d.

Chapitre 3

Décomposition de Jordan

3.1 Décomposition de Jordan dans $\boldsymbol{GL_n}$

Soit V un $k-$ev de dimension finie. Si $g \in GL(V)$, on dit que g est *semi-simple* s'il existe une base de V formée de vecteurs propres de g et que g est *unipotent* si $g-1$ est nilpotent.

Autrement dit g semi-simple $\Leftrightarrow$ g diagonalisable et g unipotent $\Leftrightarrow$ g conjugué à une matrice de la forme

$$\begin{pmatrix} 1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & 1 \end{pmatrix}.$$

Remarques :

— g semi-simple ET unipotent $\Leftrightarrow g = 1$.

— en caractéristique p, g unipotent $\Leftrightarrow \exists\, s,\ g^{p^s} = 1$.

Théorème 3.1.1 *Soit $g \in GL(V)$. Il existe un unique couple $(g_s, g_u) \in$* $\mathrm{GL}(V) \times \mathrm{GL}(V)$ *tel que :*

i) g_s *semi-simple ;*

ii) g_u *unipotent ;*

iii) $g = g_s g_u = g_u g_s$.

De plus, on a :

— $g_s = P(g)$ *avec* $P(T) \in Tk[T]$ *;*

— g_u *est un polynôme en* g *;*

— *si* $W \leq V$ *est stable par* g*, alors* W *est stable par* g_s *et* g_u *et :* $(g|_W)_s = g_s|_W$, $(g|_W)_u = g_u|_W$.

Démonstration : Soit $\chi_g(T)$ le polynôme caractéristique de g. On le factorise :

$$\chi_g(T) = \prod_{i=1}^{r} (T - \lambda_i)^{\alpha_i}$$

où les λ_i sont les valeurs propres de g, deux à deux distinctes (et non nulles). On choisit $P_s(T)$ un polynôme tel que :

$$P_s(T) = \begin{cases} \lambda_i \bmod (T - \lambda_i)^{\alpha_i} & (\forall\, 1 \leq i \leq r) \\ T \bmod T \end{cases}$$

On pose $g_s := P_s(g)$ et $g_u = P_s(g)^{-1}g$. On a : $g_s = \lambda_i$ et $(g_u - Id)^{\alpha_i} = 0$ sur $\ker(g - \lambda_i)^{\alpha_i}$. **Q.e.d.**

Exercice 14 *Soient V_1 et V_2 deux $k-$espaces vectoriels et ϕ_i un endomorphisme de V_i ($i = 1$ ou 2). Alors : $(\phi_1 \otimes \phi_2)_s = (\phi_{1s} \otimes \phi_{2s})$ (resp. $(\phi_1 \otimes \phi_2)_u = (\phi_{1u} \otimes \phi_{2u})$).*

3.2 Décomposition de Jordan dans un groupe algébrique

3.2.1 Endomorphismes localement finis

Soit V un $k-$ev éventuellement de dimension infinie.

On dit qu'un endomorphisme $g \in \mathrm{End}_k(V)$ est *localement fini* si V est une réunion de sous-$k-$espaces vectoriels stables par g et de dimension finie.

Exemples : les semi-simples ; ou $f(T) \mapsto f(T + a)$ dans $k[T]$.

Contre-exemple : $f(T) \mapsto f(T + a)$ dans $k(T)$.

On dit que $g \in \mathrm{End}_k(V)$ est *localement nilpotent* si V est une réunion finie de sous-espaces de dimension finie stables par g où g est nilpotent.

On dit que g est *unipotent* si $g - 1$ est localement nilpotent.

Exemple : la dérivation sur $k[T]$ localement nilpotente mais non nilpotente.

Définition 2 *Soit g un endomorphisme localement fini d'un $k-$espace vectoriel V. On définit g_s (resp. g_u) comme l'endomorphisme de V tel que pour tout sous-espace stable W de dimension finie, $g_s|_W = (g|_W)_s$ (resp. $g_u|_W = (g|_W)_u$.*

Remarque : C'est bien défini sans ambiguïté d'après le théorème 3.1.1.

3.2.2 Parties semi-simple et unipotente

Soit G un groupe algébrique linéaire. Soit $A = k[G]$ On pose $\delta : G \to GL(A)$, $f \mapsto f(\cdot g)$.

Théorème 3.2.1 (Décomposition de Jordan dans G) *Soit $g \in G$.*

i) $\exists\,!(g_s, g_u) \in G$, $g = g_s g_u = g_u g_s$, $\delta(g)_s = \delta(g_s), \delta(g)_u = \delta(g_u)$;

ii) Pour tout morphisme de groupes algébriques : $\phi : G \to G'$, on a :

$$\phi(g)_s = \phi(g_s), \phi(g_u) = \phi(g)_u \ .$$

iii) Si $G \subseteq \mathrm{GL}_n(k)$, alors g_s et g_u sont les composantes semi-simples et unipotentes traditionnelles !

On dira que g_s et g_u sont les *composantes semi-simple et unipotente* de g.

Définition 3 *g est semi-simple (resp. unipotent) si $g = g_s$ (resp. $g = g_u$).*

Corollaire 3.2.1.1 *Soit $g \in G$. Alors g est semisimple (respectivement unipotent) si et seulement si pour un isomorphisme quelconque ϕ de G vers un sous-groupe fermé de GL_n, $\phi(g)$ est semi-simple (respectivement unipotent) au sens traditionnel.*

Démonstration :

i)

L'unicité est donnée par l'injectivité de δ ; montrons l'existence.

On remarque que $\delta(g) : A \to A$ est en fait un automorphisme d'algèbre (pour tout $g \in G$). Cela signifie que :

$$\delta(g) \circ p = p \circ (\delta(g) \otimes \delta(g))$$

où $p : k[G] \otimes k[G] \to k[G]$, $a \otimes b \mapsto a.b$ est la multiplication.

Mais alors :

$$\delta(g)_s \circ p = p \circ (\delta(g)_s \otimes \delta(g)_s) \ ,$$

$$\delta(g)_u \circ p = p \circ (\delta(g)_u \otimes \delta(g)_u) \ ,$$

car sur chaque sous-espace de dimension finie de $k[G]$ stable par $\delta(g)$, $\delta(g)_s, \delta(g)_u$ sont des polynômes en $\delta(g)$ (exo).

On en déduit que $\delta(g)_s$ et $\delta(g)_u$ sont aussi des automorphismes de l'algèbre $A = k[G]$.

On a donc un morphisme de $k-$algèbres :

$$k[G] \to k \ , f \mapsto (\delta(g)_s(f))(1)(\text{resp. } f \mapsto (\delta(g)_u(f))(1) \ .$$

Il existe donc $g_s \in G$ (resp. $g_u \in G$) tel que $f(g_s) = (\delta(g)_s(f))(1)$ (resp. $f(g_u) = (\delta(g)_u(f))(1)$) pour tout $f \in k[G]$.

Or $\delta(g)$ commute à $\gamma(g')$ (la représentation par multiplication à gauche) pour tous $g, g' \in G$. Donc :

$$\forall\, g, g' \in G, \delta(g)_s \circ \gamma(g') = \gamma(g') \circ \delta(g)_s \ .$$

D'où les équivalences :

$$\delta(g_s) = \delta(g)_s \Leftrightarrow \forall\, f \in k[G], \delta(g_s)(f) = \delta(g)_s(f)$$
$$\Leftrightarrow \forall\, f \in k[G], \forall\, g' \in G, \delta(g_s)(f)(g') = \delta(g)_s(f)(g')$$
$$\Leftrightarrow \forall\, f \in k[G], \forall\, g' \in G, [(\gamma(g'^{-1}) \circ \delta(g_s))(f)](1) = [(\gamma(g'^{-1}) \circ \delta(g)_s(f))](1)$$
$$\Leftrightarrow \delta(g_s) \circ \gamma(g'^{-1})(f)(1) = \delta(g)_s \circ \gamma(g'^{-1})(f)(1)$$

ce qui est vérifié !

ii) Pour tout $g \in G$:

$$\delta(g) \circ \phi^* = \phi^* \circ \delta(\phi(g)) \ .$$

Donc :

$$\delta(g)_s \circ \phi^* = \phi^* \circ \delta(\phi(g))_s$$
$$\Rightarrow \delta(g_s) \circ \phi^* = \phi^* \circ \delta(\phi(g)_s)$$
$$\Rightarrow \forall\, f \in k[G'],\ f(\phi(g_s)) = f(\phi(g)_s)$$
$$\Rightarrow \phi(g_s) = \phi(g)_s \ ;$$

de même : $\phi(g_u) = \phi(g)_u$.

Q.e.d.

Exercice 15 *Soit $\chi : G \to \mathbb{G}_m$ un morphisme de groupes algébriques. Montrer que χ est trivial sur les unipotents ($g \in \mathbb{G}_m$ est unipotent ssi $g = 1$).*

Contre-exemple : soit $K = \mathbb{F}_2(T)$. Soit

$$x := \begin{pmatrix} 0 & 1 \\ T & 0 \end{pmatrix} \in \mathrm{GL}_2(K) \ .$$

Alors $x_s, x_u \notin \mathrm{GL}_2(K)$.

On notera G_s l'ensemble des éléments semi-simples de G et G_u l'ensemble des éléments unipotents de G.

Corollaire 3.2.1.2 *G_u est fermé.*

Démonstration : D'après le iii) du théorème 3.2.1, il suffit de le vérifier pour $G = GL_n(k)$. **Q.e.d.**

Remarques :

i) Vérifier que pour tout $g \in G$, $\gamma(g_s) = \gamma(g)_s$ et $\gamma(g_u) = \gamma(g)_u$.

ii) G_s n'est pas forcément fermé ni ouvert (ex : $B_n(k)$).

iii) ATTENTION : en général, G_s, G_u ne sont pas des sous-groupes de G (trouver des contre-exemples dans $\mathrm{GL}_2(k)$).

3.2.3 Groupes unipotents

Définition 4 *Un groupe algébrique linéaire est unipotent si tous ses éléments le sont.*

Remarque : Un groupe semi-simple **n'est pas** un groupe dont tous les éléments sont semi-simples (ex : $\mathrm{SL}_n(k)$ est semi-simple).

Proposition 3.2.2 *Soit G sous-groupe de GL_n formé de matrices unipotentes. Alors il existe $x \in GL_n(k)$ tel que $xGx^{-1} \subseteq U_n$.*

Démonstration :

On raisonne par récurrence sur $n > 0$. C'est évident si $n = 1$.

On peut supposer que G est un sous-groupe fermé de $\mathrm{GL}_n(k)$. Soit V un sous-espace non nul de k^n, stable par G et de dimension minimale. Le groupe G agit irréductiblement sur V. Notons pour tout $g \in G$, $\rho(g)$ la restriction de g à V. Posons $A := \sum_{g \in G} k.\rho(g) \subseteq \mathrm{End}_k(V)$. D'après la fiche de td III (ou bien *« Maths en tête » de X. Gourdon, chapitre IV, pb. 7*), on a :

$$A = \mathrm{End}(V) \ . \tag{3.1}$$

Or toute matrice unipotente de $GL(V)$ est de trace $\dim V$.

Donc :

$$\forall\, g, h \in G, \mathrm{Tr}((1 - \rho(g))\rho(h)) = \mathrm{Tr}(\rho(g)) - \mathrm{Tr}(\rho(g)\rho(h)) = 0 \ .$$

Mais alors d'après (3.1), on a :

$$\forall\, a \in \mathrm{End}(V),\ \mathrm{Tr}((1 - \rho(g))a) = 0$$

et donc $\rho(g) = 1$, dans $\mathrm{End}(V)$, pour tout $g \in G$.

Donc il existe $0 \neq v \in k^n$ tel que $g.v = v$ pour tout $g \in G$. On applique l'hypothèse de récurrence à $k^n/k.v$. **Q.e.d.**

Suite centrale et suite dérivée

Soit G un groupe quelconque (non forcément algébrique). On définit par récurrence : — la *suite centrale* :

$$\mathcal{C}^0(G) := G,\ \mathcal{C}^i(G) := (G, \mathcal{C}^{i-1}(G)\ (\forall\, i > 0) \ ;$$

— la *suite dérivée* :

$$\mathcal{D}^0(G) := G,\ \mathcal{D}^i(G) := (\mathcal{D}^{i-1}(G), \mathcal{D}^{i-1}(G))\ (\forall\, i > 0) \ .$$

On a bien entendu :

$$... \supseteq \mathcal{C}^i(G) \supseteq \mathcal{C}^{i-1}(G) \supseteq ...$$

$$... \supseteq \mathcal{D}^i(G) \supseteq \mathcal{D}^{i-1}(G) \supseteq ...$$

On dit que G est *nilpotent* (resp. *résoluble*) si $\mathcal{C}^i(G) = 1$ (resp. $\mathcal{D}^i(G) = 1$) pour i assez grand.

Exemple : le groupe U_n est nilpotent et le groupe B_n est résoluble (mais non nilpotent).

Corollaire 3.2.2.1 *Tout groupe algébrique unipotent est est un groupe nilpotent.*

Exercice 16 *Soit G un sous-groupe fermé de GL_n qui agit irréductiblement sur k^n. Alors le groupe trivial est le seul sous-groupe unipotent et distingué de G.*

3.3 Groupes commutatifs

Théorème 3.3.1 *Soit G un groupe algébrique commutatif. Alors :*
i) G_s et G_u sont fermés ;
ii) $G_s \times G_u \simeq G$.

Démonstration : On suppose que G est un sous-groupe fermé de $\mathrm{GL}_n(k)$.

i) Comme G est commutatif, on peut diagonaliser simultanément les éléments de G_s. On a donc une décomposition :

$$k^n = \oplus_\lambda V_\lambda$$

où pour toute famille de scalaires $\lambda = (\lambda_g)_{g \in G_s}$, on a noté : $V_\lambda := \cap_{g \in G_s}(\ker g - \lambda_g I_n)$.

Puis que G est commutatif, les sous-espaces V_λ, sont $G-$stables et on peut donc triangulariser simultanémént les $g|_{V_\lambda}$, $g \in G$.

Il existe donc une base de k^n formée de vecteurs propres des $g \in G_s$ où toutes les matrices $g \in G$ sont triangulaires supérieures.

On peut donc supposer que $G \subseteq B_n(k)$, le groupe des matrices triangulaires supérieures inversibles et que $G_s \subseteq D_n(k)$, le sous-groupe des matrices diagonales inversibles.

On a alors : $G_s = G \cap D_n(k)$ et $G_u = G \cap U_n(k)$: G_s et G_u sont donc bien des sous-groupes fermés de G.

ii) L'application $G_s \times G_u \to G$, $(g_s, g_u) \mapsto g_s.g_u$ est bien sûr un morphisme de groupes algébriques. La réciproque est :

$$G \to G_s \times G_u, \; g \mapsto (g_s, g_s^{-1} g)$$

qui est bien un morphisme de variétés car (en se ramenant, comme dans i) au cas où $G \subseteq B_n(k)$ et $G_s \subseteq D_n(k)$, $g \mapsto g_s$ est simplement la « prise des coefficients diagonaux de g ».

Q.e.d.

Corollaire 3.3.1.1 *Si G est un groupe algébrique commutatif connexe, alors G_s et G_u sont aussi des groupes algébriques commutatifs connexes.*

3.3.1 Groupes connexes de dimension 1

Proposition 3.3.2 *Soit G un groupe connexe de dimension* 1*. Alors :*
i) G commutatif;
ii) $G = G_s$ ou G_u.

Démonstration : On suppose que G est un sous-groupe fermé de $\mathrm{GL}_n(k)$.

i) Soit $g \in G$. On considère $\phi : G \to G$, $x \mapsto xgx^{-1}$.

Comme G est connexe de dimension 1, $\overline{\phi(G)}$ est irréductible de dimension ≤ 1. Donc $\overline{\phi(G)} = \{g\}$ ou G. Dans le premier cas, g est dans le centre de G. Dans le second, puisque $\phi(G)$ contient un ouvert non vide de $\overline{\phi(G)}$, $G \setminus \phi(G)$ est fini. En particulier, l'ensemble des polynômes $\chi_h(T) \in k[T]$, $h \in G$ est fini. Comme G est connexe, tous les éléments de G ont le même polynôme caractéristique : celui de I_n *i.e.* : $(T-1)^n$. En particulier, G est un sous-groupe unipotent de $GL_n(k)$ donc G est nilpotent. *Mézalor* : $(G, G) \underset{\neq}{\subset} G$. Comme G est connexe et de dimension 1, (G, G) est aussi connexe et $(G, G) = 1$ *i.e.* G est commutatif.

Dans tous les cas, g commute à tous les éléments de G. On en déduit que G est commutatif.

ii) Comme G est commutatif et connexe, G_s et G_u sont des sous-groupes fermés connexes de G et $G \simeq G_s \times G_u$. Puisque G est de dimension 1, $G = G_s$ ou G_u.

Q.e.d.

Nous verrons plus tard que G est isomorphe à $\mathbb{G}_m$ ou $\mathbb{G}_a$.

Chapitre 4

$G-$variétés

4.1 Cas des variétés algébriques affines

Une *$G-$variété* est une variété X munie d'une action (à gauche) de G telle que $G \times X \to X$ est un morphisme de variétés.

Exercice 17 *Si G est un groupe algébrique linéaire, si X est une variété affine, un morphisme $\sigma : G \times X \to X$ définit une action de G sur X si et seulement si :*

i) $(\mu^* \otimes \mathrm{id}) \circ \sigma^* = (\mathrm{id} \otimes \sigma^*) \circ \sigma^* : k[X] \to k[G] \otimes k[G] \otimes k[X]$ *;*

ii) $e^* \otimes \mathrm{id} \circ \sigma^* = \mathrm{id} : k[X] \to k[X]$ *;*

où $\mu : G \times G \to G$ est la loi de groupes et $e : \{1\} \to G$ est le neutre.

4.1.1 Exemples

i) soit V un $k-$espace vectoriel de dimension finie. Un morphisme de groupes algébriques $\phi : G \to \mathrm{GL}(V)$ est aussi appelé une *représentation rationnelle* de G dans V. Dans ce cas, la variété V est une $G-$variété et on dit que l'action est *linéaire* .

ii) Soit $G = \mathbb{G}_m$. Soit X une variété affine. Se donner une $G-$action sur X équivaut à donner une $\mathbb{Z}-$graduation sur l'algèbre $k[X]$ *i.e.* une décomposition :
$$k[X] = \oplus_{n \in \mathbb{Z}} k[X]_n$$
en somme directe de sous-espaces telle que :
$$k[X]_m k[X]_n \subseteq k[X]_{m+n}$$
pour tous m, n.
En effet si on a une telle graduation, alors le morphisme d'algèbres :
$$\sigma^* : k[X] \to k[G] \otimes k[X], \, \oplus_m f_m \mapsto \sum_m T^m \otimes f_m$$

correspond à une action $\sigma : G \times X \to X$.
Réciproquement si on a une action $\sigma : G \times X \to X$, alors on pose pour tout m entier :

$$k[X]_m := \{f \in k[X] \;:\; \sigma^*(f) = T^m \otimes f\} \;.$$

Comme σ^* est un morphisme d'algèbres, on a bien

$$k[X]_m k[X]_n \subseteq k[X]_{m+n}$$

pour tous m, n.
De plus, si $f \in k[X]$, alors $\sigma^*(f) = \sum_m T^m \otimes f_m$ pour certains $f_m \in k[X]$ et les f_m sont uniques (*exo*). De plus, on a :

$$\forall\, t_1, t_2 \in G, \forall\, x \in G,\; f(t_1.(t_2.x)) = f((t_1t_2).x)$$

$$equi \forall\, t_1, t_2 \in G,\; \sum_m \sum_n t_1^m t_2^n f_{m,n} = \sum_m (t_1t_2)^m f_m$$

$$\Leftrightarrow \forall\, m \neq n,\; f_{m,n} = 0$$

i.e. $f_m \in k[X]_m$ pour tout m et on en déduit que :

$$k[X] = \oplus_{n\in\mathbb{Z}} k[X]_n \;.$$

iii) Si $G = \mathbb{G}_a$, si k est de caractéristique 0, se donner une action de G sur une variété X revient à se donner une $k-$dérivation D sur $k[X]$ tellle que tout élément de $k[X]$ est annulé par une puissance de D. Le lien entre l'action et la dérivation est donné par la relation :

$$\sigma^* f = \sum_{m\geq 0} T^m \otimes \frac{D^m(f)}{m!} \;.$$

4.1.2 Actions induites sur l'algèbre des fonctions régulières

Soient G un groupe algébrique linéaire et X une variété affine. Soit $G \times X \to X$ une action algébrique. Pour tout $g \in G$, pour toute $f \in k[X]$, on peut définir une nouvelle fonction régulière :

$$\rho(g)(f) : x \mapsto f(g^{-1}.x) \;\in k[X] \;.$$

Le morphisme ρ définit une représentation du groupe abstrait g dans le $k-$espace vectoriel (en général de dimension infinie) $k[X]$.

Proposition 4.1.1 *Il existe une suite croissante E_n de sous-$k-$espaces vectoriels de $k[X]$ tels que :*

i) $\cup_n E_n = k[X]$ *;*

ii) $\forall\, g \in G$, $\rho(g)E_n \subseteq E_n$ *;*

iii) *les morphismes induits par* $\rho : G \to \mathrm{GL}(E_n)$ *sont des représentations rationnelles de* G *dans* E_n *pour tout* n*.*

Si ρ est une représentation de G dans un $k-$espace vectoriel E, s'il existe une suite croissante de sous-$k-$espaces vectoriels E_n de E qui vérifient i),ii),iii) de la proposition (avec E à la place de $k[X]$), on dit que ρ est une *représentation rationnelle* de G dans E.
Exemple : soit G un groupe algébrique linéaire. Les translations à gauche et à droite $G \times G \to G$, $g, x \mapsto gx$, $g, x \mapsto xg^{-1}$ définissent des représentations rationnelles de G dans $k[G]$ qui « commutent » :

$$\forall\, g \in G, \forall\, f \in k[X], \forall\, x \in X,\ \gamma(g)(f)(x) := f(g^{-1}x) \text{ et } \delta(g)(f)(x) = f(xg)\ .$$

On a : $\gamma(g)\delta(h) = \delta(h)\gamma(g)$ pour tous $g, h \in G$.

Théorème 4.1.2 (Kostant-Rosenlicht) *Soient* G *un groupe algébrique unipotent et* X *une variété algébrique affine. Soit une action algébrique de* G *sur* X*. Alors toutes les orbites de* G *sont fermées.*

Démonstration : Soit $x \in X$. Posons $Y := \overline{G.x}$. Alors, l'orbite $G.x$ est ouverte dans Y. En effet, il existe un ouvert non vide U de Y contenu dans $G.x$ et on a :

$$G.x = \cup_{g \in G} gU$$

qui est ouvert dans Y. Soient $Z := Y \setminus G.x$ et $I(Z)$ l'idéal des fonctions régulières sur Y nulles sur Z. Comme G est unipotent et comme l'action de G sur $I(Z)$ est une représentation rationnelle de G, il existe un élément $f \in I(Z)$ non nul et $G-$invariant. Forcément, $f(x) \neq 0$ (sinon f serait nulle sur $G.x$ et donc sur $Y = \overline{G.x}$). On a alors :

$$\forall\, g \in G,\ f(gx) = f(x) \neq 0$$

d'où f est constante égale à $f(x)$ sur $G.x$ et donc sur Y. Mais alors f est inversible et $I(Z) = (1)$. Donc $Z = \emptyset$ *i.e.* $\overline{G.x} = G.x$ est une orbite fermée.
Q.e.d.

4.2 Variétés algébriques

Un *espace à fonctions* est un couple $(X, \mathcal{O}_X)$ où X est un espace topologique et pour tout ouvert U de X, $\mathcal{O}_X(U)$ est une sous-$k-$algèbre des fonctions $U \to k$ tel que :

i) pour tout recouvrement ouvert : $U = \cup_\alpha U_\alpha$, $f \in \mathcal{O}(U) \Leftrightarrow \forall\, \alpha, f|_{U_\alpha} \in \mathcal{O}(U_\alpha)$;

ii) Si $f \in \mathcal{O}_X(U)$, alors : $D(f) = \{x \in U \ : \ f(x) \neq 0\}$ est ouvert et $f^{-1} \in \mathcal{O}(D(f))$;

Si $f \in \mathcal{O}_X(U)$, on dit que f *est régulière sur* U.

Soient $(X, \mathcal{O}_X)$, $(Y, \mathcal{O}_Y)$ deux espaces à fonctions Un morphisme de $(X, \mathcal{O}_X)$ vers $(Y, \mathcal{O}_Y)$ est une application continue $f : X \to Y$ telle que pour tout $a \in \mathcal{O}_Y(U)$, $a \circ f \in \mathcal{O}_X(f^{-1}U)$.

Exercice 18 *La composée de morphismes est encore un morphisme.*

Exemples :

— $X = \mathbb{R}$ ou $\mathbb{C}$ muni de la topologie usuelle et pour tout ouvert U de X $\mathcal{O}_X(U) =$ les fonctions continues (resp. analytiques) sur U.

— $X = \mathbb{A}^1$ muni de la topologie de Zariski et pour tout ouvert $U = X \setminus \{x_1, ..., x_n\}$, $x_1, ..., x_n \in k$,

$$\mathcal{O}_X(U) := \left\{ \frac{p(t)}{q(t)} \ : \ p, q \in k[t], \forall\, i,\ q(x_i) \neq 0 \right\} \ ;$$

— $X = \mathbb{P}^1$ muni de la topologie dont les ouverts non vides sont les complémentaires d'ensembles finis et pour tout ouvert $U = X \setminus \{z_1, ..., z_n\}$, $z_1, ..., z_n \in \mathbb{P}^1$,

$$\mathcal{O}_X(U) := \left\{ \frac{p(X,Y)}{q(X,Y)} \ : \ p, q \in k[X,Y] \text{ homogènes de même degré et } \forall\, z_i,\ q(z_i) \neq 0 \right\}.$$

Remarque : si Y est localement fermé dans un espace à fonctions X,si U est un ouvert de Y, on dira qu'une fonction $f : U \to k$ est régulière sur U s'il existe un recouvrement ouvert $U = \cup_\alpha U_\alpha$ et pour tout α, un ouvert Ω_α de X, une fonction $g_\alpha \in \mathcal{O}_X(\Omega_\alpha)$ qui vérifient $U_\alpha = U \cap \Omega_\alpha$, $f_\alpha = g_\alpha|_{U_\alpha}$. Soit $\mathcal{O}_Y(U)$ l'algèbre des fonctions régulières sur U.

On obtient ainsi $(Y, \mathcal{O}_Y)$ la seule structure d'espaces à fonctions sur Y telle que l'inclusion $Y \subseteq X$ est un morphisme.

Exercice 19 *Si $f : X \to Y$ est un morphisme d'espaces à fonctions, si Z est un sous-espace localement fermé de Y tel que $f(X) \subseteq Z$, alors la restriction :$f : X \to Z$ est encore un morphisme.*

Notation : . Si $f : X \to Y$ est un morphisme d'espaces à fonctions, on note f^* la famille des morphismes de $k-$algèbres :

$$\mathcal{O}_Y(U) \to \mathcal{O}_X(f^{-1}U),\ \ h \mapsto hf\,,$$

U ouvert de Y.

4.2.1 Variétés affines

Soit $(X, k[X])$ une variété affine. Soit $x \in X$; on dit que f est régulière au voisinage de x s'il existe $g, h \in k[X]$, U un ouvert de X qui contient x tel que :

$$\forall\, t \in U, h(t) \neq 0 \text{ et } f(t) = \frac{g(t)}{h(t)} \ .$$

On pose $\mathcal{O}_X(U) :=$ les fonctions $U \to k$ régulières au voisinage de tout $x \in U$.

Exercice 20 *Vérifier que $\mathcal{O}_X(X) = k[X]$ et que si $f \in k[X]$, si $X_f := \{x \in X \ : \ f(x) \neq 0\}$, alors $\mathcal{O}_X(X_f) = k[X]_f$.*

Notation : Si $X, \mathcal{O}_X$ est un espace à fonctions, on pose $k[X] := \mathcal{O}_X(X)$.

Nouvelle définition des variétés affines :

On dit qu'un espace à fonctions $(Y, \mathcal{O}_Y)$ est affine si $(Y, k[Y])$ est affine *i.e.* si $k[Y]$ est de type fini comme $k-$algèbre et si $Y \to \mathrm{Hom}_{k-\mathrm{alg}}(k[Y], k)$ est bijective.

Vérifier

Proposition 4.2.1 *Un espace à fonctions $(X, \mathcal{O}_X)$ est affine si et seulement si $k[X]$ est une $k-$algèbre de type fini et pour tout espace à fonctions $(Y, \mathcal{O}_Y)$, on a une bijection :*

$$\mathrm{Mor}(X, Y) \to \mathrm{Hom}_{k-\mathrm{alg}}(k[Y], k[X])\,,\ f \mapsto f^* \ .$$

Exercice 21 *Un fermé d'une variété affine est encore une variété affine.*

4.2.2 Produit

Soient X, Y deux espaces à fonctions on définit l'espace à fonctions $(X \times Y, \mathcal{O}_{X\times Y})$:

(topologie) : les ouverts sont les réunions d'ensemble de la forme $O_f = \{(u, v) \in U \times V : f(u, v) \neq 0\}$ où U est un ouvert de X, V un ouvert de Y et f une fonction sur $U \times V$ de la forme : $(u, v) \in U \times V \mapsto f(u, v) = \sum_i f_i(u) g_i(v)$ pour certaines fonctions f_i régulières sur U et certaines fonctions g_i régulières sur V ;

(fonctions) : si Ω est un ouvert de $X \times Y$, on dira que $f : \Omega \to k$ est régulière sur Ω si :

$$\Omega = \cup_i O_{f_i}$$

où les O_{f_i} sont des ouverts comme ci-dessus et si pour tout i, $f\Big|_{O_{f_i}}$ est de la forme $(u, v) \mapsto \sum_k a_k(u) b_k(v) / f_i(u, v)^{n_k}$ pour certains $a_k \in \mathcal{O}(U)$, $b_k \in \mathcal{O}(V)$, $n_k \geq 0$.

Remarques :

— les applications $p_X : X \times Y \to X$, $p_Y : X \times Y \to Y$ sont des morphismes.

— Pour X, Y affines, on retrouve la définition usuelle.

Définition 5 *Un espace à fonctions X est une prévariété algébrique si X admet un recouvrement ouvert FINI $X = \cup_i X_i$ où les X_i sont affines. Une variété algébrique est une prévariété X telle que la digonale de X, Δ_X, est fermée dans $X \times X$.*

Remarque : une partie localement fermée d'une variété algébrique est encore une variété algébrique et un produit de variétés est encore une variété.

Exercice 22 *Vérifier que $k[\mathbb{A}^2 \setminus \{0\}] = k[\mathbb{A}^2]$ et en déduire que la variété $\mathbb{A}^2 \setminus \{0\}$ n'est pas affine.*

4.2.3 Variétés projectives

L'espace projectif $\mathbb{P}^n := k^{n+1} \setminus \{0\}/k^\times$ a une structure d'espace à fonctions. En effet, soit $\pi : k^{n+1} \setminus \{0\} \to \mathbb{P}^n$ la projection canonique.

(topologie) : on dira que $U \subseteq \mathbb{P}^n$ est ouvert si $\pi^{-1}(U)$ est ouvert dans $\mathbb{A}^{n+1}$;

(fonctions) : pour tout ouvert U de $\mathbb{P}^n$, on dira qu'une fonction $f : U \to k$ est régulière si $f \circ \pi$ est régulière sur $\pi^{-1}U$.

On obtient ainsi un espace à fonctions $(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n})$ (*exo*).

Exercice 23 *Soit F une partie de $\mathbb{P}^n$. Montrer que F est fermée si et seulement si F est de la forme*

$$F = \{[x] \in \mathbb{P}^n \ : \ f_0(x) = ... = f_l(x) = 0\}$$

où les f_i sont des polynômes homogènes en $n+1$ variables.

Proposition 4.2.2 *L'espace $(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n})$ est une variété algébrique.*

Démonstration : Posons $U_i := \{[x_0 : ... : x_n] \in \mathbb{P}^n \ : \ x_i \neq 0\}$. Les U_i sont des ouverts qui recouvrent $\mathbb{P}^n$ et pour tout i, $(U_i, \mathscr{U}) \simeq {}^n : [x] \mapsto (x_k/x_i)_{\substack{1 \leq k \leq n \\ k \neq i}}$. De plus, il est facile de voir que $\Delta_{\mathbb{P}^n}$ est fermé dans $\mathbb{P}^n \times \mathbb{P}^n$: en effet, si $[x], [y] \in \mathbb{P}^n$, alors :

$$[x] = [y] \Leftrightarrow \forall\, 1 \leq i < j \leq n,\ x_i y_j - x_j y_i = 0\ .$$

<u>**Q.e.d.**</u>

Exercice 24 *$k[\mathbb{P}^n] = k$. En déduire que si $n \geq 1$, $\mathbb{P}^n$ n'est pas affine.*

En particulier, tout sous-espace localement fermé d'un $\mathbb{P}^n$ est une variété algébrique. On dit qu'une variété est *projective* (resp. *quasi projective*) si elle est isomorphe à un fermé (resp. un localement fermé) d'un $\mathbb{P}^n$.

Exemple : une variété affine est quasiprojective.

Proposition 4.2.3 *Soit $f_0, ..., f_n \in k[T_0, ..., T_m]$ des polynômes homogènes de même degré. Soit U l'ouvert de $\mathbb{P}^m$ des points où au moins un des f_i n'est pas nul. Alors l'application :*

$$f : U \to \mathbb{P}^n,\ [x] \mapsto [f_0(x) : ... : f_n(x)]$$

est un morphisme.

Exercice 25 *Soient $k, l, m > 0$ des entiers. Soient $f_0, ..., f_m \in k[U_0, ..., U_k, V_0, ..., V_l]$ des polynômes homogènes de même degré en les variables V_i. Soit Ω l'ensemble des $(u, [v]) \in \mathbb{A}^k \times \mathbb{P}^l$ tels que :*

$$\exists\, i,\ f_i(u, v) \neq 0\ .$$

Alors Ω est un ouvert de $\mathbb{A}^k \times \mathbb{P}^l$ et l'application :

$$\Omega \to \mathbb{P}^m,\ (u, [v]) \mapsto [f_0(u, v) : ... : f_m(u, v)]$$

est un morphisme.

4.2.4 Composantes irréductibles, dimension

Toute variété est quasicompacte donc est un espace nœthérien. On peut définir comme dans le cas affine les composantes irréductibles. Si X est une variété irréductible, alors tous les ouverts affines non vides U de X ont la même dimension (comme variété affine *i.e.* $\mathrm{degtr}_k(k[U])$). On dit que cette dimension commune est la *dimension de X*. Pour une variété X quelconque, on définit sa dimension comme le maximum des dimensions de ses composantes irréductibles.

4.2.5 Germes de fonctions

Soit X une variété algébrique.

Définition 6 *Si $x \in X$, on note $\mathcal{O}_{X,x}$ ou $\mathcal{O}_x$ l'anneau des germes de fonctions en x* i.e. *:*

$$\mathcal{O}_x = \varinjlim_{\substack{U \\ x \in U}} \mathcal{O}_X(U) = \{(f, U)\ :\ U \text{ ouvert tel que } x \in U \text{ et } f \in \mathcal{O}_X(U)\} / \sim$$

où $(f, U) \sim (g, V)$ s'il existe un ouvert $x \in W \subseteq U \cap V$ tel que $f|_W = g|_W$

Remarque : Si U est un ouvert de X contenant x, alors les restrictions de V à $V \cap U$, V ouvert de X contenant x, induisent un isomorphisme : $\mathcal{O}_{X,x} \simeq \mathcal{O}_{U,x}$.

Exercice 26 *Soit X une variété. Si $x \in X$, si U est un ouvert affine de X qui contient x, alors $k[U] \to \mathcal{O}_x$, $f \mapsto (f, U) \bmod \sim$ induit un isomorphisme d'algèbres :*

$$k[U]_{M_x} \to \mathcal{O}_x$$

où M_x est l'idéal maximal de $k[U]$ des fonctions qui s'annulent en x.

On note $\mathfrak{m}_x$ l'idéal des fonctions nulles en x.

Proposition 4.2.4 *L'anneau $\mathcal{O}_x$ est un local d'idéal maximal $\mathfrak{m}_x$ et $\mathcal{O}_x/\mathfrak{m}_x \simeq k$, $f \mapsto f(x)$.*

4.2.6 Orbites

Soit G un groupe algébrique. Soit X une *$G-$variété i.e.* une variété algébrique X avec une action (à gauche) de G telle que l'action :

$$G \times X \to X$$

est un morphisme. Si $x \in X$, l'orbite de X est l'ensemble :

$$G.x := \{gx \ : \ g \in G\}$$

le groupe d'isotropie de x est le sous-groupe fermé :

$$G_x := \{g \in G \ : \ gx = x\} \ .$$

Si $G_x = G$, on dit que x est un point fixe de G. L'ensemble des points fixes de G est un fermé de X, noté X^G.

Exercice 27 *Vérifier que G_x est fermé dans G et que X^G est fermé dans X.*

Un morphisme de $G-$variétés $\phi : X \to Y$ est *$G-$équivariant* si :

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

Proposition 4.2.5 *Une orbite est toujours localement fermée* i.e. *ouverte dans son adhérence.*

On utilise cette propriété des morphismes :

Lemme 4.2.6 *Soit $f : X \to Y$ un morphisme de variétés, alors il existe un ouvert non vide de $\overline{f(X)}$ contenu dans $f(X)$.*

Démonstration : Il suffit de le démontrer dans le cas affine. **Q.e.d.**

On dit que X est un *espace homogène* si G agit transitivement sur X.
Exemple : la droite projective $\mathbb{P}^1$ est une $G-$variété homogène avec $G = \mathrm{SL}_2$ pour :

$$G \times \mathbb{P}^1 \to \mathbb{P}^1$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, [x : y] \mapsto [ax + by : cx + dy] \ .$$

L'action induite du sous-groupe B des matrices triangulaires supérieures a deux orbites :

$$U := \mathbb{P}^1 \setminus \{[1:0]\}, \, F := \{[1:0]\} \ .$$

Exercice 28 *Déterminer les orbites de GL_n et D_n dans $\mathbb{A}^n$, et dans $\mathbb{P}^n$.*

4.3 Espaces homogènes

Soit G un groupe algébrique linéaire.
On dit qu'une $G-$variété

Lemme 4.3.1 *i) Les composantes irréductibles de X sont homogènes pour l'action de G°.*
ii) Les composantes de X sont ouvetes et fermées et X est leur union disjointe.

Théorème 4.3.2 *Soit $\phi : X \to Y$ un morphisme $G-$équivariant d'espaces homogènes pour G. Soit $r := \dim X - \dim Y$. ϕ est dominant et :*
i) pour toute variété Z, $\phi \times \mathrm{Id} : X \times Z \to Y \times Z$ est ouvert ;
ii) Si Y' est une sous-variété fermée irréductible de Y et X' une composante irréductible de $\phi^{-1}Y'$, alors :
$\dim X' = \dim Y' + r$. *En particulier, toutes les composantes irréductibles des fibres sont de dimension r ;*
iii) ϕ est un isomorphisme $\Leftrightarrow$ ϕ est bijective et pour un certain $x \in X$, la différentielle : $d\phi|_x : T_x X \to T_{\phi x} Y$ est un isomorphisme.

Corollaire 4.3.2.1 *Soit $\phi : G \to H$ un morphisme surjectif de groupes algébriques. Alors :*
i) $\dim G = \dim H + \dim \ker \phi$ *;*
ii) ϕ est un isomorphisme ssi $d\phi|_e$ est bijective.

exo : Les composantes d'un espace homogène sont lisses.

4.3.1 Quotients

Soient G un groupe algébrique linéaire et H un sous-groupe fermé de G.

Définition 7 *On munit G/H d'une structure d'espace à fonctions :*
— *topologie : $U \subseteq G/H$ ouvert si $\pi^{-1}U$ ouvert de G ;*
— *fonctions : $f : U \to k$ régulière si $f \circ \pi$ régulière sur $\pi^{-1}U$.*

Théorème 4.3.3 *G/H est isomorphe à une variété quasi-projective (c'est donc une variété algébrique. De plus, si Y est une $G-$variété, et $y \in Y$ est un point dont le groupe d'isotropie contient H alors il existe un unique morphisme $G-$équivariant : $G/H \to Y$ qui envoie H/H sur y.*

Propriété universelle : exo !
Quasi-projectivité :
Nous le démontrerons plus tard !

Proposition 4.3.4 *Soit H un sous-groupe fermé distingué de G, alors G/H est un groupe algébrique.*

Chapitre 5

Espace tangent, algèbre de Lie

5.1 Espace tangent

5.1.1 Dérivations

Soient A une $R-$algèbre. et M un $A-$module. Une $R-$*dérivation* de A dans M est un morphisme $R-$linéaire : $d : A \to M$ tel que :

$$d(ab) = ad(b) + bd(a)$$

pour tous $a, b \in A$.

D'après cette définition, une $R-$dérivation d vérifie toujours : $d(a) = 0$ pour tout $a \in A$. De plus, l'ensemble des $R-$dérivations de A dans M, $\mathrm{Der}_R(A, M)$, forme un $A-$module.

Exercice 29 *Si* $A = k(T_1, ..., T_n)$, *déterminer* $\mathrm{Der}_k(A, A)$.

5.1.2 Tangentes

Soit X un fermé de $\mathbb{A}^n$ défini par des équations $f_1, ..., f_n \in k[T_1, ..., T_n]$.

Soient $v \in k^n \setminus \{0\}$ et $L_v := \{x + tv \ : \ t \in k\}$ la droite passant par x dirigée par v. On a :

$$L_v \cap X = \{x + tv \ : \ \forall\, i, \ f_i(x + tv)\} \ .$$

D'un autre côté, si $v = (v_1, ..., v_n)$, alors

$$f_i(x + tv) = t(\sum_j \partial_j f_i(x) v_j) \bmod t^2$$

On dira que L_v est tangente à X en x si 0 est une racine (commune) double des équations :

$$\forall\, i, f_i(x + tv) = 0$$

i.e. si
$$\forall\, i, \sum_j \partial_j f_i(x) v_j = 0 \ .$$

Notons k_x le corps k vu comme $k[X]-$module via : $f.z := f(x)z$. Autrement dit : $k[X]/M_x \simeq k_x$.

On a alors une bijection :

$$\begin{array}{ccc} \{0 \neq v \in k^n \ : \ L_v \text{ est tangente à } X \text{ en } x\} \cup \{0\} & \xleftrightarrow{1:1} & Der_k(k[X], k_x) \ . \\ v & \longmapsto & \sum_j v_j \partial_j \\ (d(T_1), ..., d(T_n)) & \longleftarrow\!\shortmid & d \end{array}$$

5.1.3 Espace tangent de Zariski

Soit X une variété algébrique, si $x \in X$, on définit *l'espace tangent* de X en x comme le $k-$espace vectoriel :

$$T_x X := Der_k(\mathcal{O}_x, k_x) \ .$$

Remarque : si X est affine, alors le morphisme $k[X] \to \mathcal{O}_x$ induit un insomorphisme (de $k-$espaces vectoriels) :

$$Der_k(\mathcal{O}_x, k_x) \to \mathrm{Der}_k(k[X], k) \ .$$

Exercice 30 *Montrer que pour tout $x \in \mathbb{A}^n$, $T_x\mathbb{A}^n \simeq k^n$ puis déterminer $T_x X$ dans les cas suivants : X est un point, $X = \{(u,v) \in \mathbb{A}^2 \ : \ uv = 0\}$ et $x = (0,0)$, $X = \{(u,v) \in \mathbb{A}^2 \ : \ u^2 = v^3\}$ et $x = (0,0)$.*

Si $D \in T_x X$, alors $D(\mathfrak{m}_x^2) = 0$. On en déduit donc une forme linéaire :

$$\lambda(D) : \mathfrak{m}_x/\mathfrak{m}_x^2 \to k \ .$$

Lemme 5.1.1 *On a un isomorphisme :*

$$\lambda : T_x X \to \left(\mathfrak{m}_x/\mathfrak{m}_x^2\right)^* \ .$$

Différentielles

Si $f : X \to Y$ est un morphisme de variétés algébriques, alors f induit un morphisme local : $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ et donc une application linéaire :

$$df|_x : T_x X \to T_{f(x)} Y$$

qu'on appelle la *diférentielle* de f en x.

Remarque : Si $f : X \to Y$, $g : Y \to Z$ sont des morphismes de variétés, alors pour tout $x \in X$, $d(g \circ f)|_x = dg\Big|_{f(x)} \circ df|_x$.

Remarques :

i) si $f : X \to Y$ est un isomorphisme sur un ouvert de Y, alors $df|_x : T_xX \to T_{f(x)}Y$ est un isomorphisme linéaire ;

ii) si $Z = Z(f_1, ..., f_r)$ est un fermé d'une variété affine X, alors pour tout $x \in Z$, T_xZ s'identifie au sous-espace des $D \in T_xX$ tels que :

$$D(f_i) = 0$$

pour tout i. En particulier, pour toute variété algébrique X et tout $x \in X$, l'espace vectoriel T_xX est de dimension finie.

Exercice 31 *Déterminer T_xX dans les cas suivants :*

a) $X = \{(x, y) \in \mathbb{A}^2 \,:\, xy = 0\}$, $x = (0, 0)$ *;*

b) $X = \{(x, y) \in \mathbb{A}^2 \,:\, y^2 = x^3\}$, $x = (0, 0)$.

Exercice 32 *Soient X, Y des variétés, $x \in X$, $y \in Y$. Alors $T_{(x,y)}X \times Y \simeq T_xX \oplus T_yY$.*

Exercice 33 *Soit X une variété affine. On pose $k[\epsilon] := k[T]/(T^2)$ avec $\epsilon = T \bmod T^2$. Soit $x \in X$. Montrer T_xX est en bijection avec l'ensemble des morphismes de $k-$algèbres $\phi : k[X] \to k[\epsilon]$ tels que pour toute $f \in k[X]$, $\phi(f) - f(x) \in k\epsilon$ (c'est l'ensemble des « $k[\epsilon]-$points de X au-dessus de x »).*

5.2 Algèbre de Lie d'un groupe algébrique

Soit G un groupe algébrique.

5.2.1 Définition avec les nombres duaux

Rappelons que pour toute $k-$algèbre A, on note $G(A) := \mathrm{Hom}_{k-alg}(k[G], A)$. Cet ensemble a une structure de groupe induite par le comorphisme $\mu^* : k[G] \to k[G] \otimes k[G]$:

$$\forall\, \phi, \phi' \in G(A),\ \phi\phi' := m \circ (\phi \otimes \phi') \circ \mu^*$$

où $m : A \otimes_k A \to A$ est la multiplication de A.

On considère $k[\epsilon] := k[T]/(T^2)$ avec $\epsilon = T \bmod T^2$.

Soit G un groupe algébrique linéaire sur k. Le morphisme $\pi : k[\epsilon] \to k$, $a + b\epsilon \mapsto a$ induit un morphisme de groupes (abstraits) : $G(k[\epsilon]) \to G(k)$.

On pose :

$$\mathrm{Lie}(G) := \ker\left(G(k[\epsilon]) \to G(k)\right)$$

Exemple : si $G = \mathrm{GL}_n$, alors $\mathrm{Lie}(G) = \{I_n + \epsilon A \ : \ A \in \mathscr{M}_n(k)\}$.

On en déduit que si G est un sous-groupe fermé de GL_n, et si $\phi \in \mathrm{Lie}(G)$, alors dans l'algèbre $\mathscr{M}_n(k[\epsilon])$, on a :

$$(\phi(T_{i,j}))_{1\le i,j\le n} = I_n \bmod \epsilon \ .$$

Structure de $k-$espace vectoriel

Si $t \in k$, on note $\theta_t : k[\epsilon] \to k[\epsilon]$, $a + b\epsilon \mapsto a + tb\epsilon$.

On pose alors pour tous $\phi, \phi' \in \mathrm{Lie}(G)$, $t \in k$:

$$\phi + \phi' := \phi\phi'$$

$$t\phi := \theta_t \circ \phi \ .$$

Exercice 34 *Vérifier que pour ces opérations,* $\mathrm{Lie}(G)$ *est bien un espace vectoriel (en particulier que $\phi\phi' = phi'\phi$ dans* $\mathrm{Lie}(G)$*)(indication : il suffit de le vérifier pour un sous-groupe fermé de* GL_n*).*

Remarques :

i) on a un isomorphisme $T_eG \to \mathrm{Lie}(G)$, $d \mapsto (f \mapsto f(e) + d(f)\epsilon)$ et en particulier, $\mathrm{Lie}(G^\circ) = \mathrm{Lie}(G)$. En particulier, si G est fini, $\mathrm{Lie}(G)$ est nul (comme espace vectoriel).

ii) tout morphisme de groupes $\phi : G \to K$ induit un morphisme $k-$linéaire : $d\phi : \mathrm{Lie}(G) \to \mathrm{Lie}(K)$. En particulier, si H est un sous-groupe fermé de g, on peut identifier $\mathrm{Lie}(H)$ et le sous-espace des $A \in \mathrm{Lie}(G)$ tels que $A \in H(k[\epsilon]) \subseteq G(k[\epsilon])$.

Si G est un sous-groupe fermé de GL_n, on pourra donc identifier G et l'espace $\mathfrak{g}$ des matrices $M \in \mathfrak{gl}_n$ telles que $I_n + \epsilon M \in G(k[\epsilon])$.

5.2.2 Exemples

i) $\mathrm{Lie}(\mathrm{SL}_n) \simeq$ espace des matrices de traces nulles ;

ii) $\mathrm{Lie}(D_n) \simeq$ espace des matrices diagonales ;

iii) $\mathrm{Lie}(B_n) \simeq$ espace des matrices triangulaires supérieures ;

iv) $\mathrm{Lie}(U_n) \simeq$ espace des matrices triangulaires supérieures de diagonale nulle ;

v) $\mathrm{Lie}(SO_n) \simeq$ espace des matrices antisymétriques.

On trouve à chaque fois des sous-algèbres de Lie de $\mathfrak{gl}_n$.

Si G est un sous-groupe fermé de GL_n, nous verrons que pour tous $M, M' \in \mathfrak{gl}_n$, si $I_n + \epsilon M, I_n + \epsilon M' \in \mathrm{Lie}(G)$, alors $I_n + \epsilon(MM' - M'M) \in \mathrm{Lie}(G)$.

5.2.3 Dérivations invariantes

L'espace $T := \mathrm{Der}_k(k[G], k[G])$ est une algèbre de Lie pour le crochet :

$$[d, d'] := d \circ d' - d' \circ d \ .$$

De plus, si k est de caractéristique p, pour tout $d \in T$, $d^p \in T$ (on dit que T est une *$p-$algèbre de Lie* ou algèbre de Lie *restreinte.*

Pour tout $g \in G$, on note $\gamma(g) : k[G] \to k[G]$, $f \mapsto f(g^{-1} \cdot)$.

On note $L(G)$ l'espace des dérivations $d \in \mathrm{Der}_k(k[G], k[G])$ qui commutent à tous les $\gamma(g)$, $g \in G$.

Remarque : l'algèbre $\mathrm{Lie}(G)$ est une sous-algèbre de Lie de T (et même une sous-algèbre de Lie restreinte).

Exercice 35 *Notons $\mu^* : k[G] \to k[G] \otimes_k k[G]$ le morphisme induit par la multiplication de G. Vérifier que si $d \in T$, alors*

$$d \in L(G) \Leftrightarrow \Delta \circ d = \mathrm{Id} \otimes d \circ \Delta \ .$$

Proposition 5.2.1 *On a un isomorphisme :*

$$\begin{tikzcd}
L(G) \arrow[r, "\sim"] & T_e G \\
d \arrow[r, mapsto] & \epsilon \circ d \\
(1 \otimes \delta) \circ \mu^* & \delta \arrow[l, mapsto]
\end{tikzcd}$$

où $\mu^* : k[G] \to k[G] \to k[G]$ est le morphisme induit par la multiplication μ de G.

En particulier, $L(G)$ est de dimension finie.

5.2.4 Adjoint

Si $g \in G$, on note

$$\mathrm{Ad}(g) : \mathfrak{g} \to \mathfrak{g}$$

l'isomorphisme linéaire induit par l'automorphisme intérieur $G \to G$, $x \mapsto gxg^{-1}$.

Exemple : si $G = \mathrm{GL}_n$, si on identifie $\mathrm{Lie}(GL_n)$ et $\mathfrak{gl}_n$, on a $\mathrm{Ad}(g)(M) = gMg^{-1}$ pour tout $M \in \mathfrak{gl}_n$.

Vérifier que $G \to \mathrm{GL}(\mathfrak{g})$, $g \mapsto \mathrm{Ad}(g)$ est un morphisme de groupes.

On en déduit en différentiant une application :

$$\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g}) \ .$$

On pose alors : $[A,B] := \mathrm{ad}(A)(B)$ pour tous $A, B \in \mathrm{Lie}(G)$.

Exemple : si $G = GL_n$, vérifier que $[A,B] = AB - BA$ (en identifiant $I_n + \epsilon M \in \mathrm{Lie}(G)$ et $M \in \mathscr{M}_n$.

Proposition 5.2.2 *i)* $[\cdot,\cdot] : \mathrm{Lie}(G) \times \mathrm{Lie}(G) \to \mathrm{Lie}(G)$ *est un crochet de Lie ;*

ii) on a un isomorphisme d'algèbres de Lie (restreinte) : $\mathrm{Lie}(G) \simeq T_e(G) \to L(G)$ *;*

iii) si $\phi : G \to G'$ *est un morphisme de groupes algébriques, alors* $d\phi : \mathrm{Lie}(G) \to \mathrm{Lie}(G')$ *est un morphisme d'algèbres de Lie.*

Démonstration : Si on suppose que G est un sous-groupe fermé de GL_n, tout est clair. **Q.e.d.**

5.2.5 Distributions

Soit G un groupe algébrique linéaire. On va voir ici une autre manière (plus directe) de définir une structure d'algèbre de Lie sur T_eG : Notons $\mu : G \times G \to G$ le produit de G.

On pose $\mathrm{Dist}_n(G,e) := \{\delta \in k[G]^* \ : \ \delta\Big|_{M_e^{n+1}} = 0\}$, $Dist(G,1) := \cup_{n\geq 0} Dist_n(G,1)$ et $Dist_n^+(G,1) := \{left\delta \in Dist_n(G,1) \ : \ \delta(1) = 0\}$.

On munit $Dist(G,1)$ du produit suivant :

$$\forall\ \delta, \delta',\ \delta\delta' := \delta \otimes \delta' \circ \mu^* : k[G] \stackrel{\mu^*}{\to} k[G] \otimes k[G] \stackrel{\delta\otimes\delta'}{\to} k \otimes k \simeq k$$

i.e. :

$$\forall\ f \in k[G], \delta.\delta'(f) := \sum_i \delta(f_i)\delta(g_i)$$

où $f(gg') = \sum f_i(g)g_i(g')$.

Exercice 36 *Pour le produit défini ci-dessus,* $Dist(G,1)$ *est une algèbre associative et* $Dist_m(G,1).Dist_n(G,1) \subseteq Dist_{m+n}(G,1)$.

On a $T_eG = Dist_e^+(G,e)$. Pour tout $\delta, \delta' \in T_eG$, on pose : $[\delta,\delta'] := \delta\delta' - \delta'\delta$.

Le produit se fait dans $Dist(G,e)$ et le résultat tombe dans $Dist_e^+(G,1) = T_eG$.

Soit $G \subseteq GL_n(k)$ un sous-groupe fermé. L'algèbre $k[G]$ est une image de $k[\mathrm{GL}_n]$ donc une dérivation $d \in T_eG$ est entièrement déterminé par les

$$d(T_{i,j})_{1\leq i,j\leq n} \ .$$

On vérifie facilement que :

$$T_eG \to \mathfrak{gl}_n,\ d \mapsto (d(T_{i,j}))_{1\leq i,j\leq n}$$

est un morphisme injectif d'algèbres de Lie.

Plus génééralement :

Proposition 5.2.3 *Si $\phi : G \to H$ est un morhisme de groupes algébriques, alors $d\phi|_e : T_eG \to T_eH$ est un morphisme d'algèbres de Lie.*

5.3 Dérivations abstraites

5.3.1 Séparabilité

Définition 8 *Soit E/F une extension de corps. On dit que E/F est séparable si F est de caractéristique nulle ou si F est de caractéristique p et si pour tous $x_1, ..., x_n \in E$ $F-$linéairement indépendants, $x_1^p, ..., x_n^p$ sont aussi $F-$linéairement indépendants.*

On dit que x est séparable algébrique sur F si $F(x)/F$ est algébrique et séparable

Exercice 37 *Vérifier que l'on retrouve la définition bien connue pour les éléments algébriques* i.e. *x séparable si et seulement si x est racine d'un polynôme à racines simples.*

Exemples : toutes les extensions des corps finis, des corps algébriquement clos sont séparables (pas évident), si K est un corps, $K(T)/K$ est séparable.

Contre-exemple : l'extension $\mathbb{F}_p(T)/\mathbb{F}_p(T^p)$ n'est pas séparable.

Lemme 5.3.1 *Soit E/F une extension de corps de type fini. Alors E/F est séparable si et seulement s'il existe une base de transcendance $x_1, ..., x_m$ de E sur F telle que $E/F(x_1, ..., x_m)$ soit algébrique séparable (on dit que $x_1, ..., x_m$ forment une base de transcendance séparante de E/F).*

Théorème 5.3.2 *Soit E/F une extension de corps de type fini. Alors on a :*

$$\dim_E \mathrm{Der}_F(E, E) \geq \mathrm{degtr}(E/F)$$

et E/F est séparable si et seulement si $\dim_E Der_F(E, E) = \mathrm{degtr}E/F$.

Exemple : Si $K = k(X_1, ..., X_n)$, alors K/k est séparable car : $Der_k(K, K) = K\partial_{X_1} \oplus ... \oplus K\partial_{X_n}$.

Démonstration : Soit E/F une extension finie. Supposons que $E \subseteq \Omega$ est une extension de corps. Soit $x \in \Omega$. On a un isomorphisme :

$$E(x) \otimes_E \mathrm{Der}_F(E, E) \to \mathrm{Der}_F(E, E(x)),\ r(x) \otimes d \mapsto r(x)d$$

(pour la surjectivité, on vérifie que si $d \in \mathrm{Der}_F(E, E(x))$, alors comme E/F est de type fini, il existe $0 \neq q(x) \in E(x)$ tel que $q(x)d \in \mathrm{Der}_F(E, E[x])$; on a alors pour tout $e \in E$, $q(x)d(e) = \sum_n d_n(e)X^n$ avec des $d_n \in \mathrm{Der}_F(E, E)$).

Donc $\dim_E \mathrm{Der}_F(E,E) = \dim_{E(x)} \mathrm{Der}_F(E,E(x))$. Soit $D \in \mathrm{Der}_F(E,E(x))$. Si x est transcendant sur E, alors on peut prolonger D à $E[x]$, en posant :

$$\widetilde{D}(r(x)) := r^D(x)$$

où r^D est le polynôme obtenu en appliquant D aux coefficients de r. On obtient une dérivation sur $E[x]$ que l'on peut alors prolonger à $E(x)$.

Si x est algébrique séparable sur E, de polynôme minimal $P \in E[T]$, on peut prolonger D à $E(x) = E[x]$ en posant :

$$\widetilde{D}(x) := -P^D(x)/P'(x)$$

et :

$$\widetilde{D}(r(x)) := r^D(x) + r'(x)\widetilde{D}(x) \ .$$

Si $x^p \in E$ et $x \notin E$, alors on peut prolonger D à $E(x)$ seulemnt si $D(x^p) = 0$. Dans ce cas, il suffit de poser :

$$\widetilde{D}(r(x)) := r^D(x)$$

pour tout $r(x) \in E(x)$. Remarquons que

$$\{D \in \mathrm{Der}_F(E,E(x)) \ : \ D(x^p) = 0\}$$

est un hyperplan de $\mathrm{Der}_F(E,E(x))$ (sauf si $\mathrm{Der}_F(E,E(x)) = 0$.

Or l'application $E(x)-$linéaire :

$$\mathrm{Der}_F(E(x),E(x)) \to \mathrm{Der}_F(E,E(x)),\ D \mapsto D|_E$$

est de noyau :

$$\mathrm{Der}_E(E(x),E(x)) \ .$$

On vérifie que :

$$\dim_{E(x)} \mathrm{Der}_E(E(x),E(x)) = \begin{cases} 1 & \text{si } x \text{ est transcendant sur } E \text{ ou si } x^p \in E\,; \\ 0 & \text{si } x \text{ est algébrique séparable sur } E. \end{cases}$$

On en déduit donc que :

$$\dim_{E(x)} \mathrm{Der}_F(E(x),E(x)) \geq \dim_E \mathrm{Der}_F(E,E) + \mathrm{degtr}(E(x)/E)$$

si (1) x est transcendant sur E, (2) x est algébrique séparable sur E, (3) $x^p \in E$. Dans les cas (1), (2), (3), on a égalité sauf dans le cas (3) si $\mathrm{Der}_F(E,E(x)) = 0$.

On en déduit que :

$$\dim_E \mathrm{Der}_F(E,E) \geq \mathrm{degtr}(E/F) \ .$$

Vérifions que $\mathrm{Der}_F(E,E)=0 \Leftrightarrow E/F$ algébrique séparable.

D'après ce qui précède, on a bien : $\Leftarrow$. Supposons que $\mathrm{Der}_F(E,E)=0$. Alors, on peut trouver des éléments $y_1,...,y_N$ dans E tels que :

$$E = F(y_1,...,y_N)$$

et pour tout k :

(I) y_k est transcendant sur $F(y_1,...,y_{k-1})$ ou

(II) y_k est algébrique séparable sur $F(y_1,...,y_{k-1})$ ou

(III) $y_k^p \in F(y_1,...,y_{k-1})$ et $y_k \notin \$F(y_1,...,y_{k-1})$.

Considérons le plus grand entier $k \leq N$ tel que l'on ait (II) ou (III). Il est clair que l'on peut trouver une dérivation $0 \neq D \in \mathrm{Der}_{F(y_1,...,y_{k-1})}(F(y_1,...,y_k),F(y_1,...,y_k))$ et que l'on peut prolonger cette dérivation à E : *absurde !* Donc E/F est bien algébrique séparable.

Soient $x_1,...,x_n \in E$ tels que $E=F(x_1,...,x_n)$. Il est clair que l'application $E-$linéaire :

$$\mathrm{Der}_F(E,E) \to E^n,\ D \mapsto (D(x_1),...,D(x_n))$$

est injective. Donc $\mathrm{Der}_F(E,E)$ est de dimension finie $r \leq n$. Soit $D_1,...,D_r$ une base de $\mathrm{Der}_F(E,E)$. La matrice $(D_i(x_j))_{1\leq i,j\leq r}$ est de rang r. Supposons par exemple (quitte à renuméroter les x_j) que la matrice extraite :

$$(D_i(x_j))_{1\leq i,j\leq r}$$

est inversible. On a alors pour tout $D \in Der_F(E,E)$:

$$\forall\, 1\leq k\leq r,\ D(x_k)=0 \Rightarrow \forall\, 1\leq j\leq n,\ D(x_j)=0 \Rightarrow D=0$$

donc $\mathrm{Der}_{F(x_1,...,x_r)}(E,E)=0$ et l'extension $E/F(x_1,...,x_r)$ est algébrique séparable. Si $r=\dim_E \mathrm{Der}_F(E,E)=\mathrm{degtr}(E/F)$, alors les x_k, $1\leq k\leq r$ forme une base de transcendance de E/F qui est séparante.

Réciproquement, s'il existe une base de transcendance séparante : $y_1,...,y_d$ de E/F, alors :

$$\dim_E(E/F)=\dim_{F(y_1,...,y_d)} \mathrm{Der}_F(F(y_1,...,y_d),F(y_1,...,y_d))=d=\mathrm{degtr}E/F).$$

Q.e.d.

5.4 Points lisses

Soit X une variété algébrique. Si $x\in X$, on note $\dim_x X$ la dimension maximale d'une composante irréductible de X passant par x.

Exemple : Soit $I := (X,Y)(X^2+Y^2+Z^2-1) \leq \mathbb{C}[X,Y,Z]$. Alors $\dim_P Z(I) = 2$ si $P = (0,0,1)$.

On dit qu'un point x sur une variété X est *lisse* si $\dim_x X = \dim T_x X$. Sinon, on dit que x est singulier.

On dit que la variété X est lisse si tous ses points le sont.

Nous verrons que l'ensemble des points lisses d'une variété forme un ouvert non vide.

Exemple : $\mathbb{A}^n$ est lisse.

Exercice 38 *Déterminer les points lisses de* $X_1 = \{(x,y) \in \mathbb{A}^2 \ : \ xy = 0\}$ *et* $X_2 := \{(x,y) \in \mathbb{A}^2 \ : \ y^2 = x^3\}$.

Soit X une sous-variété fermée irréductible de $\mathbb{A}^n$ définie par des équations $f_1, ..., f_m \in k[T_1, ..., T_n]$. On pose $A := (\partial_{T_j} f_i)_{\substack{1\leq i\leq m \\ 1\leq j\leq n}} \in \mathscr{M}_{m\times n}(k(X))$ (où $k(X)$ est le corps des fractions de $k[X]$).

Lemme 5.4.1 *i)* $n - \mathrm{rg}(A) = \dim X$ *;*

ii) $n - \mathrm{rg}(A(x)) = \dim T_x X$ *;*

iii) Pour tout $x \in X$, $\dim T_x X \geq \dim X$ *;*

iv) pour tout d, $\{x \ : \ \dim T_x X \leq d\}$ *est un ouvert de* X *et* $\{x \ : \ \dim T_x X = \dim X\}$ *est un ouvert non vide de* X.

Démonstration : Pour le i), on remarque que l'on a un isomorphisme de $k(X)-$espace vectoriel :

$$\mathrm{Der}_k(k(X), k(X)) \to \ker_{k(X)} A, \ \ d \mapsto d(T_j)_{1\leq j\leq n} \ .$$

Q.e.d.

Théorème 5.4.2 *Soit* X *une variété algébrique. Alors l'ensembmle des points lisses de* X *est un ouvert non vide.*

Démonstration : Il suffit de vérifier que l'ensemble X^{reg} des points lisses est un ouvert. Soit $x \in X$ un point lisse. Notons $C_1, ..., C_k$ les composantes irréductible qui ne contiennent pas x, $C_{k+1}, ..., C_N$ celles qui contiennent x. On a : $\dim_x X = \max_{i=1}^k \dim C_i =: d$ et l'ensemble

$$\{x \in X \ \setminus \ C_1 \cup ... \cup C_k \ : \ \dim T_x X \leq d\}$$

est un voisinage ouvert de x formé de points lisses. **Q.e.d.**

Proposition 5.4.3 *Soit* G *un groupe algébrique linéaire. Alors* G *est lisse et* $\dim G = \dim T_e G = \dim \mathrm{Lie}(G) = \dim L(G)$.

Exercice 39 *En calculant la dimension de leur algèbre de Lie, retrouver les dimensions des groupes* $Sp_{2n}, SO_n, \mathrm{SL}_n$: $2n^2+n$, $n(n-1)/2$ *et* n^2-1.

Lemme 5.4.4 *Soit* $M \in \mathscr{M}_{m,n}(k[X])$ *une matrice. Soit* r *le rang de* M *vue comme matrice à coefficients dans* $k(X)$.

i) Il existe $B \in \mathrm{GL}_m(k(X))$, $C \in \mathrm{GL}_n(k(X))$ *tels que :*

$$BMC = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$$

ii) si $M(x)$ *est de razng* r, *on peut choisir* B, C *à coefficients dans* $k[U]$ *où* U *est un voisinage ouvert affine de* x.

Démonstration :

Démonstration : Supposons que $\mathrm{rg} M(x) = r$. Quitte à permuter les lignes et les colonnes de M (ce qui revient à multiplier à gauche et à droite par des matrices de permutations), on peut supposer que le mineur

$$f := \det(M_{i,j})_{1 \le i,j \le r}$$

est non nul en x.

On a $M = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$ où $A \in \mathscr{M}_r(k[X])$, $f = \det A \neq 0$, $B \in \mathscr{M}_{r,q-r}(k[X])$, $C \in \mathscr{M}_{p-r,r}(k[X])$, $D \in \mathscr{M}_{p-r,q-r}(k[X])$.

Soient $P := \left(\begin{array}{c|c} I_r & 0 \\ \hline -CA^{-1} & I_{p-r} \end{array}\right) \in \mathrm{GL}_p(k[X]_f)$ et $Q := \left(\begin{array}{c|c} A^{-1} & -A^{-1}B \\ \hline 0 & I_{q-r} \end{array}\right) \in \mathrm{GL}_q(k[X]_f)$. On a :

$$PMQ = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & ? \end{array}\right) .$$

Comme M est de rang r, PMQ aussi et donc $? = 0$.

Q.e.d.

Q.e.d.

Chapitre 6

Le théorème de Chevalley

6.1 Propriétés des morphismes

Théorème 6.1.1 *Soit $\phi : X \to Y$ un morphisme de variétés irréductibles.*

*i) Si $x \in X$ et $\phi(x) \in Y$ sont lisses et si $d\phi|_x : T_xX \to T_{\phi(x)}Y$ est surjectif alors ϕ est dominant et séparable (*i.e. *l'extension $\phi^*(k(Y)) \subseteq k(X)$ est séparable).*

ii) Si ϕ est dominant et séparable, alors les x qui satisfont aux hypothèses de i) forment un ouvert non vide de X.

Démonstration : On commence par *i*).

Il suffit de traiter le cas où X, Y sont des variétés affines. Supposons que X est un fermé de $\mathbb{A}^m$ de dimension t et Y un fermé de $\mathbb{A}^n$ de dimension u. Quitte à remplacer Y par un voisinage ouvert de de $y = \phi(x)$ et X par un voisinage ouvert de x, on peut supposer que X, Y sont lisses.

Soient $F_1, ..., F_p \in k[X_1, ..., X_m]$ des générateurs de l'idéal $I(X)$. Soient $G_1, ..., G_q \in k[Y_1, ..., Y_n]$ des générateurs de l'idéal $I(Y)$. On pose :

$$M_X := (\partial_{X_j} F_i)_{\substack{1\leq i\leq p\\ 1\leq j\leq m}} \in \mathscr{M}_{p,m}(k[X])$$

$$M_Y := (\partial_{Y_j} G_i)_{\substack{1\leq i\leq q\\ 1\leq j\leq n}} \in \mathscr{M}_{q,n}(k[Y])$$

Quitte à remplacer X par un voisinage ouvert affine de x, on peut supposer qu'il existe $B \in \mathrm{GL}_p(k[X])$, $C \in \mathrm{GL}_m(k[X])$ tels que :

$$BM_XC = \left(\begin{array}{c|c} I_d & 0 \\ \hline 0 & 0 \end{array}\right)$$

où $d = \mathrm{rang} M_X = m - \dim X$.

Pour tout $z \in X$, tout $z' \in Y$, on identifiera T_zX au noyau de $M_X(z)$ et $T_{z'}Y$ au noyau de $M_Y(z')$.

Notons $\phi_1, ..., \phi_n \in k[X_1, ..., X_m]$ les fonctions coordonnées du morphisme ϕ.

On pose :

$$J_\phi := (\partial_{X_j}\phi_i)_{\substack{1\leq i\leq n \\ 1\leq j\leq m}} \in \mathscr{M}_{n,m}(k[X]) \ .$$

On vérifie facilement que pour tout $z \in X$, la matrice $J_\phi(z)(T_zX) = d\phi_z(T_zX)$.

Il existe des vecteurs colonnes $C_1, ..., C_t \in k[X]^m$ tels que pour tout $z \in X$, T_zX est engendré par les vecteurs $C_1(z), ..., C_t(z)$. Il suffit de prendre les t dernières colonnes de la matrice C ci-dessus.

Donc pour tout $z \in X$, $d\phi_z : T_zX \to T_{\phi(z)}Y$ est surjective si et seulement si la matrice $B(z)$ de colonnes $J_\phi(z)C_1(z), ..., J_\phi(z)C_t(z)$ est de rang $\geq \dim T_{\phi(z)}Y = \dim Y$. En particulier, l'ensemble S des $z \in X$ tels que $d\phi|_z$ est surjective est un voisinage ouvert de x dans X. Soit V l'ouvert (non vide) des points lisses de $\overline{\phi(X)}$. Comme X est irréductible, $S \cap \phi^{-1}(V)$ est non vide. Il existe donc $z \in X$ tel que $d\phi(z)(T_zX) = T_{\phi(z)}Y$ et $\dim T_{\phi(z)}\overline{\phi(X)} = \dim \overline{\phi(X)}$. Comme $d\phi(z)(T_zX) \subseteq T_{\phi(z)}\overline{\phi(X)}$, on a : $T_{\phi(z)}\overline{\phi(X)} = T_{\phi(z)}Y \Rightarrow \dim \overline{\phi(X)} = \dim Y \Rightarrow Y = \overline{\phi(X)}$

Donc ϕ est dominant. D'où un morphisme injectif de corps : $\phi^* : k(Y) \to k(X)$.

Les colonnes $C_1, ..., C_t$ forment une base de $\ker M_X$. Or, on a :

$$\ker M_X = \left\{ \begin{pmatrix} D(X_1) \\ \vdots \\ D(X_m) \end{pmatrix} : D \in \mathrm{Der}_k(k(X), k(X)) \right\} \ .$$

De plus, si $D \in \mathrm{Der}_k(k(X), k(X))$, alors :

$$\begin{aligned} D \in \mathrm{Der}_{\phi^*(k(Y))}(k(X), k(X)) &\Leftrightarrow \forall\, 1 \leq i \leq n,\ D(\phi^* Y_i) = 0 \\ &\Leftrightarrow \forall\, i,\ D(\phi_i) = 0 \\ &\Leftrightarrow \forall\, i,\ \sum_j \partial_{X_j}\phi_i D(X_j) = 0 \\ &\Leftrightarrow \begin{pmatrix} D(X_1) \\ \vdots \\ D(X_m) \end{pmatrix} \in \ker J_\phi \ . \end{aligned}$$

Donc :

$$\begin{aligned} \dim_k \mathrm{Der}_{\phi^*(k(Y))}(k(X), k(X)) = \dim \ker J_\phi|_{\ker M_X} &= \dim \ker M_X - \dim J_\phi(\ker M_X) \\ &= \dim X - \dim_k \mathrm{vect}_k\{J_\phi C_1, ..., J_\phi C_t\} \end{aligned}$$

$$\leq \dim X - \dim_k \mathrm{vect}_k\{J_\phi(x)C_1(x), ..., J_\phi(x)C_t(x)\}$$

$$\leq \dim X - \dim_k J_\phi(x)(T_xX)$$

$$\leq \dim X - \dim Y \ .$$

Donc l'extension $k(X)/\phi^* k(Y)$ est séparable.

ii)

Il suffit de montrer qu'il existe un $x \in X$ tel que $d\phi|_x : T_xX \to T_{\phi(x)}Y$ est surjective.

Supposons que X et Y sont lisses. Comme dans la démonstration de ii), on peut trouver des colonnes $C_1, ..., C_t \in k[X]^m$ qui forment une base de $\ker M_X$. On a alors :

$$\dim_k \mathrm{Der}_{\phi^*(k(Y))}(k(X), k(X)) = \dim \ker J_\phi|_{\ker M_X} = \dim \ker M_X - \dim J_\phi(\ker M_X)$$

$$= \dim X - \dim_k \mathrm{vect}_k\{J_\phi C_1, ..., J_\phi C_t\}$$

$$= \dim X - \dim Y \ .$$

Comme $d\phi|_x(T_xX) = \mathrm{vect}_k\{J_\phi(x)C_1(x), ..., J_\phi(x)C_t(x)\}$, $d\phi|_x$ est surjective si et seulement si $\dim_k \mathrm{vect}_k\{J_\phi C_1, ..., J_\phi C_t\} = \dim T_{\phi(x)}Y = \dim Y$ car Y est lisse. L'ensemble des x qui vérifient cette égalité est bien un ouvert de X. **Q.e.d.**

Théorème 6.1.2 *Soient X, Y deux variétés irréductibles. Soit $\phi : X \to Y$ un morphisme dominant ; on pose $r := \dim X - \dim Y$. Alors il existe un ouvert non vide U de X tel que :*

i) pour toute variété Z, la restriction $\phi \times \mathrm{Id} : U \times Z \to Y \times Z$ est ouverte ;

ii) pour toute sous-variété fermée irréductible Y' de Y et toute composante irréductible X' de $\phi^{-1}Y'$ telle que $X' \cap U \neq \emptyset$, on a : $\dim X' = \dim Y' + r$ (en particulier les composantes irréductibles des fibres qui rencontrent U sont de dimension r ;

iii) Si $r = 0$, alors $\phi^{-1}\phi U \subseteq U$ et pour tout $x \in U$, $\phi^{-1}\phi(x)$ est de cardinal $|\phi^{-1}\phi x| = [k(X) : k(Y)]_s$ (où $[k(X) : k(Y)]_s := [k(X)_s : k(Y)]$ avec $k(X)_s =$ le sous-corps des éléments de $k(X)$ séparables sur $k(Y)$).

Remarque : dans iii), pour tout $x \in U$, on a $\phi^{-1}\phi x = \phi|_U{}^{-1}\phi|_U x$.

Démonstration :

Pour une variété affine V et une fonction $h \neq 0$, régulière sur V, on notera V_h l'ouvert affine :

$$V_h = \{v \in V \ : \ h(v) \neq 0\} \ .$$

Il suffit de traiter le cas où X, Y, Z sont affines. Dans i), il suffit de traiter le cas où Z est un espace affine $\mathbb{A}^N$.

Remarquons que si $\phi_1 : X_1 \to X_2$ et $\phi_2 : X_2 \to X_3$ sont deux morphismes dominants qui vérifient $i), ii), iii)$, alors $\phi_2 \circ \phi_1 : X_1 \to X_3$ aussi (*exo*).

Soit $\phi : X \to Y$ un morphisme dominant. Comme $k[X]$ est une $\phi^*k[Y]-$algèbre de type fini, en utilisant la remarque précédente, il suffit de traiter un des cas suivants :

$$k[X] = \phi^*k[Y][h]$$

où $h \in k[X]$ et :

(I) h est transcendant sur $\phi^*k(Y)$;

(II) h est algébrique séparable sur $\phi^*k(Y)$;

(III) k est de caractéristique p, $h \notin \phi^*k(Y)$ et $h^p \in \phi^*k(Y)$.

Lemme 6.1.3 *Le théorème est vrai dans le cas (I).*

Démonstration : Le diagramme suivant commute :

$$x \longmapsto (\phi(x), h(x))$$

$$\begin{tikzcd} X \arrow[r, "\simeq"] \arrow[dr, "\phi"'] & Y \times \mathbb{A}^1 \arrow[d, "p_Y"] \\ & Y \end{tikzcd}$$

Il suffit donc de traiter le cas où $X = Y \times \mathbb{A}^1$ et où $\phi = p_Y : Y \times \mathbb{A}^1$: *facile !* **Q.e.d.**

Lemme 6.1.4 *Le théorème est vrai dans le cas (II).*

Démonstration : Soit $F \in \phi^*k(Y)[T]$ le polynôme minimal unitaire de h sur $\phi^*k(Y)$. Soit $f \in k[Y]$ tel que $F \in \phi^*k[Y]_f[T]$. Quitte à remplacer X parl'ouvert affine $\phi^{-1}(Y_f) = X_{\phi^*f}$, on peut supposer que $F \in \phi^*k[Y][T]$. Soit n le degré de F en T :

$$F = \phi^*a_0 + ... + \phi^*a_{n-1}T^{n-1} + T^n$$

pour certains $a_i \in k[Y]$. Le discriminant de F est un élément $\Delta \in \phi^*k[Y]$ non nul car h est séparable. Quitte à remplacer X par l'ouvert affine X_Δ, on peut supposer que pour tout $x \in X$, le polynôme $F(\phi(x), T) \in k[T]$ est de discriminant $\Delta(x) \neq 0$.

Soit X_1 le fermé de $Y \times \mathbb{A}^1$ défini par le polynôme $\sum_i a_i T^i \in k[Y][T]$:

$$X_1 := \{(y, t) \in Y \times \mathbb{A}^1 \ : \ a_0(y) + ... + t^n = 0\} \ .$$

On a $k[X_1] \simeq k[X]$ d'où un isomorphisme $X_1 \simeq X$. De plus le diagramme suivant commute :

$$x \longmapsto (\phi(x), h(x)) \quad .$$

$$\begin{tikzcd} X \arrow[r, "\simeq"] \arrow[dr, "\phi"'] & X_1 \subseteq Y \times \mathbb{A}^1 \arrow[d, "p_Y"] \\ & Y \end{tikzcd}$$

Il suffit donc de traiter le cas où $X = X_1$ et où $\phi = p_Y : X_1 \to Y$. Posons $F(y,t) := a_0(y)+...+a_{n-1}t^{n-1}+t^n$. i) Dans ce cas, $\phi\times\mathrm{Id} : X\times\mathbb{A}^N \to Y\times\mathbb{A}^N$ est ouverte. En effet, soit $G \in k[Y \times \mathbb{A}^N][T]$, alors :

$$\phi\times\mathrm{Id}(G \neq 0) = \{(y,z) \in Y \times \mathbb{A}^N \ : \exists t \in \mathbb{A}^1,\ F(y,t) = 0 \text{ et } G(y,z,t) \neq 0\} \ .$$

On a : $G = \sum_i g_i T^i$ pour certains $g_i \in k[Y\times\mathbb{A}^N]$. En faisant une division euclidienne par F, on peut supposer que G est de degré $< n$ en T. Mais alors :

$$\phi \times \mathrm{Id}(G \neq 0) = \cup_{i=0}^{n-1} (Y \times \mathbb{A}^N)_{g_i} \ .$$

En effet, si $g_j(y,z) \neq 0$, pour un certain j, alors le polynôme :

$$\sum_{i=0}^{n-1} g_i(y,z)T^i$$

est non nul de degré $< n$ et a donc au plus $n-1$ racines dans $\mathbb{A}^1$. Or, $F(y,T)$ est un polynôme de degré n avec n racines distinctes dans $\mathbb{A}^1$ (son discriminant est non nul). Donc il y a au moins une racine t de $F(y,T)$ qui n'est pas une racine de $G(y,z,T)$.

ii) Soit Y' un fermé irréductible de Y. On a :

$$\phi^{-1}Y' = \{(y,t) \in Y' \times \mathbb{A}^1 \ : \ F(y,t) = 0\} \ .$$

Notons $\overline{F} \in k[Y'][T]$ le polynôme $a_0|_{Y'} + ... + T^n$.

Soient $P_1, ..., P_r$ des idéaux premiers de $k[Y'][T]$ tels que : $\sqrt{(\overline{F})} = \cap_{i=1}^r P_i$. On peut supposer qu'il n'y a pas d'inclusion entre les P_i. On a $\sqrt{(\overline{F})} = I(\phi^{-1}Y')$. Les composantes irréductibles de $\phi^{-1}Y'$ sont définies par les P_i. Pour tout i, $P_i \cap k[Y'] = \{0\}$. En effet, si par exemple $P_1 \cap k[Y'] \neq 0$, soit $0 \neq a_1 \in P_1 \cap k[Y']$. Si $r = 1$, alors $P_1 = \sqrt{(\overline{F})}$ et dans $k[Y'][T]$,

$$F | a_1^q$$

pour un certain q : impossible vu que $k[Y']$ est intègre et F est de degré $n > 0$. Si $r > 1$, soient $a_2 \in P_2 \setminus P_1, ..., a_r \in P_r \setminus P_1$. On a :

$$a_1 ... a_r \in \sqrt{(\overline{F})}$$

$$\Rightarrow \overline{F}|(a_1...a_r)^q$$

pour un certain $q > 0$. Or, $(a_2...a_r)^q = \mu_1 + ... + \mu_{n-1}T^{n-1} \bmod \overline{F}$ (car $\overline{F}$ est unitaire de degré n). Donc $a_1^q(a_2...a_r)^q = a_1^q\mu_1 + ... + a_1^q\mu_{n-1}T^{n-1} \bmod \overline{F} = 0 \bmod \overline{F}$. Pour des raisons de degré on a alors $a_1^q\mu_i = 0$ dans $k[Y']$ pour tout i et donc $\mu_i = 0$ dans $k[Y']$ pour tout i d'où :

$$(a_2...a_r)^q \in \overline{F} \subseteq P_1$$

$$\Rightarrow a_2...a_r \in P_1$$

absurde !

On a donc :

$$k[Y'] \subseteq k[Y'][T]/P_i$$

pour tout i et les extensions de corps :

$$k(Y') \subseteq \mathrm{Frac}(k[Y'][T]/P_i)$$

sont algébriques. Donc : $\mathrm{degtr}(\mathrm{Frac}(k[Y'][T]/P_i)/k) = \mathrm{degtr}(k(Y')/k)$ pur tout i.

iii) Soit $x = (y_0, t_0) \in X_1$, on a : $\phi^{-1}\phi(x) = \{(y_0, t) \in Y \times \mathbb{A}^1 : F(y_0, t) = 0\}$ qui est bien de cardinal n car $F(y_0, T) \in k[T]$ est un polynôme de degré n avec n racines distinctes dans k.

Remarquons que l'on a en fait montrer qu'il existe un ouvert non vide U de X tel que ${\phi|_U}^{-1}\phi|_U(x)$ est de cardinal n pour tout $x \in U$. Mais a priori, ${\phi|_U}^{-1}\phi|_U(x) = \phi^{-1}\phi(x) \cap U \neq \phi^{-1}\phi(x)$.

Il suffit alors de remplacer U par l'ouvert non vide :

$$U' := U \cap \phi^{-1}(Y \setminus \overline{\phi(X \setminus U)}$$

(comme $\dim X = \dim Y$, comme X est irréductible, $\dim(\overline{\phi(X \setminus U)}) < \dim X = \dim Y$ donc l'ouvert $Y \setminus \overline{\phi(X \setminus U)}$ est non vide et rencontre $\phi(X)$).

On a : $\phi^{-1}\phi(U') \subseteq U'$. **Q.e.d.**

Lemme 6.1.5 *Le théorème est vrai dans le cas (III) :*

Démonstration : Le polynôme $T^p - h^p \in \phi^*k(Y)[T]$ est le polynôme minimal de h sur $\phi^*k(Y)$. Comme précédemment, quitte à remplacer X par un ouvert afinne non vide, on peut supposer que $h^p = \phi^*a \in \phi^*k[Y]$ *, que $X = \{(y, t) \in Y \times \mathbb{A}^1 : t^p = a\}$ et que $\phi = p_Y : X \to Y$.

i) Soit $f = f_0 + ... + f_mT^m \in k[Y \times A^N][T]$. On a :

$$\phi \times \mathrm{Id}(f \neq 0) = \{(y, z) \in Y \times A^N : \exists t,\ t^p = a(y) \text{ et } f_0(y, z) + ... + f_m(y, z)t^m \neq 0\}$$

*. pour un $a \in k[Y] \notin k(Y)^p$.

$$= \{(y,z) \in Y \times A^N \ : \ \exists\, t,\, t^p = a(y) \text{ et } (f_0(y,z) + ... + f_m(y,z)t^m)^p \neq 0\}$$
$$= \{(y,z) \in Y \times A^N \ : \ f_0(y,z)^p + ... + f_m(y,z)^p a(y)^m \neq 0\}$$

qui est bien un ouvert de Y.

De plus, ϕ est bijective (en caractéristique p, tout élément de k a une seule racine $p-$ième) d'où iii).

ii) Soit Y' un fermé irréductible de Y. On a :

$$\phi^{-1}(Y') = \{(y,t) \in Y' \times \mathbb{A}^1 \ : \ t^p = a(y)\} \ .$$

Posons $a' := a|_{Y'}$. Si le polynôme $T^p - a' \in k[Y'][T]$ est irréductible sur $k(Y')$, alors $T^p - a'$ est le polynôme minimal sur $k(Y')$ de son unique racine (dans une extension algébrique de $k(Y')$). L'idéal $(T^p - a')$ est donc premier dans $k[Y'][T]$ et $k[\phi^{-1}Y'] = k[Y'][T]/(T^p - a')$ est intègre et son corps des fractions est une extension algébrique de $k(Y')$ donc : $\phi^{-1}Y'$ est irréductible et $\dim \phi^{-1}Y' = \dim Y'$.

Si $T^p - a'$ est réductible sur $k(Y')$, alors il existe $\alpha \in k(Y')$ tel que $\alpha^p = a'$. Soit P le noyau du morphisme :

$$k[Y'][T] \to k(Y'),\ r \mapsto r(\alpha) \ .$$

L'idéal P est un idéal premier. De plus, $r(\alpha) = 0 \Leftrightarrow r(\alpha)^p = 0 \Leftrightarrow r^p = 0 \bmod T^p - a'$. Donc $P = \sqrt{(T^p - a')}$. On a alors :

$$k[\phi^{-1}Y'] = k[Y'][T]/P$$
$$P \cap k[Y'] = 0$$

et comme précédemment, $\phi^{-1}Y'$ est irréductible de dimension $\dim \phi^{-1}Y' = \dim Y'$.

Q.e.d.

Q.e.d.

6.2 Application : G/H

Soit G un groupe algébrique affine. Soit H un sous-groupe fermé de G ; Soient $\mathfrak{g}$ (resp. $\mathfrak{h}$) l'algèbre de Lie de G (resp. de H). On identifiera $\mathfrak{h}$ avec le sous-espace $di|_e(\mathfrak{h})$ de $\mathfrak{g}$ (où i est l'inclusion $H \to G$.

Si $f \in k[G]$, $\xi \in \mathfrak{g}$, on pose $\xi.f \in k[G] : g \mapsto \xi(\delta(g)(f))$.

Remarque : si $\mu^*(f) = \sum_i a_i \otimes b_i \in k[G \times G]$, alors $\xi.f = \sum_i \xi(a_i) b_i$ pour tout $\xi \in \mathfrak{g}$.

Exercice 40 *Notons $I(H)$ l'idéal des fonctions régulières sur G nulles sur H ;*

Vérifier que $\xi \in \mathfrak{h} \Leftrightarrow \forall\, f \in I(H), \xi.f \in I(H)$.

Lemme 6.2.1 *Il existe $V \subseteq k[G]$ de dim finie, $W \subseteq V$ tels que :*
i) V est stable par $\delta(x), \forall\, x \in G$;
ii)

$$H = \{x \in G \,:\, \delta(x)W = W\}$$

$$\mathfrak{h} = \{\xi \in \mathfrak{g} \,:\, \xi.W \subseteq W\} \ .$$

Démonstration : Soient $f_1, ..., f_r \in k[G]$ des générateurs de l'idéal $I(H)$. Soit $V \subseteq k[G]$ un sous-espace de $k[G]$ de dimension finie stable par tous les $\delta(x)$, $x \in G$. il suffit de poser $W := V \cap I(H)$. **Q.e.d.**

Lemme 6.2.2 *Il existe V $k-$espace vectoriel de dim finie et $v \in V$ non nul et $\phi : G \to GL(V)$ un morphisme de groupes algébriques tels que :*

$$H = \{x \in G \,:\, \phi(x)v \in kv\}$$

$$\mathfrak{h} = \{X \in \mathfrak{g} \,:\, (d\phi X)v \in kv\} \ .$$

Démonstration : Soient V_0, W_0 comme dans le lemme précédent. Soit $w_1, ..., w_d$ une base de W_0. On pose :
$V := \Lambda^d V_0$, $v := w_1 \wedge ... \wedge w_d$ et ϕ :

$$G \to \mathrm{GL}(V),\ x \mapsto \Lambda^d \delta(x) \ .$$

Q.e.d.

On pose $X :=$ la $G-$orbite de $[v]$ dans $\mathbb{P}(V)$. Soit $x := [v]$ on a :

Proposition 6.2.3 *i) $G_x = H$; ii) $\phi : g \mapsto g.x$ définit un morphisme séparable : $G^\circ \to \phi G^\circ$; iii) Les fibres de ϕ sont les gH, $g \in G$.*

Démonstration : Pour le *ii*), il suffit de remarquer que $T_{[v]}V$ s'identifie *naturellement* à V/kv. **Q.e.d.**

On peut définir une structure d'espace à fonctions sur G/H : soit $p : g \to G/H$, $g \mapsto gH$;
topologie : si $U \subseteq G/H$, on dit que U est ouvert si $p^{-1}U$ est ouvert dans G ;
fonctions : si $U \subseteq G/H$ est ouvert, on dit qu'une fonction $f : U \to k$ est régulière si $f \circ p$ l'est sur $p^{-1}U$.

Proposition 6.2.4 *L'orbite $X := G.[v]$ est ouverte dans son adhérence (dans $\mathbb{P}(V)$). L'application $gH \mapsto g.[v]$ est induit un isomorphisme d'espace à fonctions :*

$$(G/H, \mathscr{O}_{G/H}) \to (X, \mathscr{O}_X)$$

en particulier, $(G/H, \mathcal{O}_{G/H})$ est une variété algébrique.

Remarque : on a la propriété universelle suivante : si Y est une $G-$variété avec un point y_0 $H-$stable alors $gH \mapsto g.y_0$ est un morphisme de variétés.

Démonstration : Soit $x := [v]$. Il s'agit de montrer que $\phi : G/H \to X$, $gH \mapsto g.x$ est un isomorphisme. Les G^0-orbites de X : $X_1, ..., X_q$ sont les composantes irréductibles de X et elles sont donc ouvertes et fermées. En particulier, il suffit de montrer que $\phi : \phi^{-1}X_i \to X_i$ est un isomorphisme pour tout i. Il suffit donc de traiter le cas où G est connexe.

Posons $\psi : G \to X$, $g \mapsto g.x$. L'application ψ est ouverte. On en déduit que ϕ aussi est ouverte. Donc ϕ est un homéomorphisme. Il reste à montrer que pour un ouvert U de X, $\phi^* : \mathcal{O}_X(U) \to \mathcal{O}_{G/H}(\phi^{-1}U)$ est un isomorphisme. Seule la surjectivité pose problème. Soit $f \in \mathcal{O}_G(p^{-1}\phi^{-1}U)$ une fonction telle que $f(gh) = f(g)$ pour tout $g \in V := p^{-1}\phi^{-1}U$ et btout $h \in H$. Soit $\Gamma := \{(g, f(g)) \ : \ g \in V\} \subseteq V \times \mathbb{A}^1$ le graphe de f. C'est un fermé de $V \times \mathbb{A}^1$. Or l'application $\psi \times \mathrm{Id}$ est ouverte donc $\Gamma' := \psi \times \mathrm{Id}\Gamma$ est fermé dans $U \times \mathbb{A}^1$. Soit q la restriction à Γ' de la projection sur le premier facteur : $U \times \mathbb{A}^1 \to U$. Il est clair que q est bijective. De plus, q est séparable car on peut trouver un morphisme χ tel que $q \circ \chi = \psi : \psi^{-1}U \to U$ qui est séparable. Donc q est un isomorphisme birationnel. D'après le théorème principal de Zariski (*cf.* ci-dessous), q est un isomorphisme. Il existe donc une fonction F régulière sur U telle que $\Gamma' = \{(u, Fu) \ : \ u \in U\}$. il est clair que $f \circ \phi \circ p = f$ sur $p^{-1}U$.

Q.e.d.

Corollaire 6.2.4.1 *i) G/H est une variété quasi projective de dimension* $\dim G - \dim H$ *;*

ii) si G est connexe, $G \to G/H$, $g \mapsto gH$ est séparable.

6.2.1 Théorème principal de Zariski

On dit qu'une variété irréductible X est *normale* si pour tout $x \in X$, l'anneau $\mathcal{O}_{X,x}$ est intégralement clos.

Remarque : si X est affine, alors X est normale $\Leftrightarrow$ $k[X]$ est intégralement clos.

Proposition 6.2.5 (*cf.* **Matsumura,** *Commutative algebra, th. 34, th. 35, th.36*) *Si x est un point lisse d'une variété irréductible X, alors $\mathcal{O}_{X,x}$ est intégralement clos.*

Soient X, Y deux variétés affines. On dit qu'un morphisme $f : X \to Y$ est *fini* si $k[X]$ est une $f^*k[Y]-$algèbre finie. Par exemple, $\mathbb{A}^1 \to \mathbb{A}^1$, $t \mapsto t^2$.

Proposition 6.2.6 *Si $f : X \to Y$ est un morphisme fini, alors les fibres $f^{-1}f(x)$, $x \in X$ sont toutes finies. De plus, f est une application fermée.*

Démonstration : Notons $x_1, ..., x_m$ des fonctions coordonnées pour X. Chaque x_i est entier sur $f^*k[Y]$:

$$\forall\, i,\; x_i^d + f^*a_1 x_i^{d-1} + ... + f^*a_d = 0$$

pour certains $a_j \in k[Y]$. Le scalaire x_i est une coordonnée d'un point de $f^{-1}f(x)$ seulement si :

$$x_i^d + a_1(f(x))x_i^{d-1} + ... + a_d(f(x)) = 0$$

ce qui ne laisse qu'un nombre fini de possibilités.

Soit F un fermé de X. Il est clair que $f|_F : F \to Y$ est fini. Il suffit donc de montrer que $f(X)$ est fermé. Soit $y \in \overline{f(X)}$ *i.e.* $\forall\, h \in \ker f^*,\ h(y) = 0$. Alors $f^*\mathfrak{m}_y$ est un idéal maximal de $f^*k[Y]$. Il existe donc un idéal maximal $\mathfrak{m}$ de $k[X]$ tel que $\mathfrak{m} \cap f^*k[Y] = f^*\mathfrak{m}_y$ (car $k[X]$ est entier sur $f^*k[Y]$). Soit $x \in X$ tel que $\mathfrak{m}_x = \mathfrak{m}$. On a : $y = f(x)$. **Q.e.d.**

Lemme 6.2.7 *Soit $f : X \to Y$ un morphisme dominant de variétés irréductibles affines. Soit $x \in X$ tel que $f^{-1}f(x)$ est fini. Alors, f est localement fini en x* i.e. *: il existe un ouvert affine V de Y tel que $f^{-1}V$ soit un ouvert affine et le morphisme restreint :*

$$f^{-1}V \to V$$

soit un morphisme fini.

Démonstration : posons $A := f^*k[Y]$, $B := k[X]$. Soient $b_1, ..., b_h \in B$ tels que $B = A[b_1, ..., b_h]$. On raisonne par récurrence sur h.

Si $h = 1$:

soit I le noyau de $A[T] \to A$, $P(T) \mapsto P(b_1)$. Soit $\epsilon : A[T] \to k[T]$, $a_0 + ... + a_dT^d \mapsto a_0(x) + ... + a_d(x)T^d$. Si $\epsilon I = 0$, alors :

$$f^{-1}f(x) \simeq \mathbb{A}^1 \qquad (6.1)$$

absurde ! Il existe donc $r \in I$ non constant tel que $\epsilon r \neq 0$. On a :

$$r = r_nT^n + ... + r_0$$

avec des $r_j \in A$ tels que $r_n(x) = ... = r_{m+1}(x) = 0, r_m(x) \neq 0$ pour un certain $m > 0$. Si on pose $s := r_nb_1^{n-m} + ... + r_m \in B$, on a :

$$s(x) \neq 0 \text{ et } sb_1^m + r_{m-1}b_1^{m-1} ... + r_0 = 0\ .$$

Donc b_1 est entier sur $A[s^{-1}]$. Comme $s \in A[b_1]$, s est entier sur $A[s^{-1}]$ et donc s est entier sur A. Donc on a des relations :

$$s^d + c_1s^{d-1} + ... + c_d = 0$$

pour certains $c_i \in A$. En particulier, $s^{-1} \in A[s]_{c_d}$. Soit $h \in k[Y]$ tel que $f^*h = c_d$. On a $f^{-1}Y_h = X_{c_d} \subseteq X_s$. De plus, $k[X_{c_d}] = k[X]_{c_d} = A[b_1]_{c_d}$ est entier sur $A[s]_{c_d}$ donc sur $f^*k[Y_h] = A_{c_d}$. On peut donc prendre $V = Y_h$.

Si $h > 1$. On peut trouver X' une variété affine, $g : X \to X'$, $f' : X' \to Y$ des morphismes tels que $k[X'] = A[b_1]$ et g^*, f'^* correspondent aux inclusions d'algèbres $k[X'] \subseteq B$, $A \subseteq k[X']$. on a : $f = f'g$. Comme $f^{-1}f(x) = g^{-1}f'^{-1}f'g(x) \supseteq g^{-1}g(x)$, $g^{-1}g(x)$ est fini et par hypothèse de récurrence, g est localement fini en x : on peut trouver un voisinage ouvert affine U' de $g(x)$ dans X' tel que $g^{-1}U'$ est affine et la restriction $g : g^{-1}U' \to U'$ est un morphisme fini. En particulier, $g : g^{-1}U' \to U'$ est un morphisme surjectif. Donc $f'^{-1}f'g(x) \cap U'$ est fini. D'après (6.1), $f'^{-1}f'g(x)$ est fini ou isomorphe à $\mathbb{A}^1$. En particulier, comme $f'^{-1}f'g(x) \cap U'$ est fini, $f'^{-1}f'g(x)$ est forcément fini. Il existe donc un voisinage ouvert affine de $f(x) = f'g(x)$ dans Y tel que l'ouvert $f'^{-1}V$ est affine et le morphisme $f'^{-1}V \to V$ est fini. Soit $t \in k[X']$ tel que $g(x) \in X'_t \subseteq U'$. Comme $k[f'^{-1}V]$ est entier sur $f'^*k[V]$, on a une relation :

$$t^d + f'^*a_1t^{d-1} + ... + f'^*a_d = 0$$

pour certains $a_i \in k[V]$. On alors $f'^{-1}V_{a_d} \subseteq X'_t$ et le morphisme :

$$f = f'g : f^{-1}V_{a_d} \to f'^{-1}V_{a_d} \to V_{a_d}$$

est fini comme composé de morphismes finis. **Q.e.d.**

Théorème 6.2.8 (principal de Zariski) *Soient X, Y deux variétés irréductibles. Soit $\phi : X \to Y$ un morphisme bijectif, birationnel. Si Y est normale, alors ϕ est un isomorphisme ;*

Remarque : en particulier, si Y est lisse, le théorème est vrai.

Démonstration : Soit $x \in X$, d'après le lemme 6.2.7, il existe un voisinage ouvert affine V de $\phi(x)$ dans Y, un voisinage ouvert affine U de x dans X tel que $\Omega := \phi_U^{-1}V := \phi^{-1}V \cap U$ est affine et $\phi : \omega \to V$ est un morphisme fini. Mais comme ϕ est birationnel, on a :

$$\phi^*k[V] \subseteq k[\Omega] \subseteq k(\Omega) = \phi^*k(V) \ .$$

Or, $k[V]$ est intégralement clos dans son corps des fractions donc :

$$\phi^*k[V] = k[\Omega]$$

et $\phi : \Omega \to V$ est un isomorphisme. en particulier, l'application $\phi^{-1} : Y \to X$ restreinte à V est un morphisme. C'est vrai pour tout $y = \phi(x) \in Y$ donc ϕ^{-1} est un morphisme sur Y. **Q.e.d.**

Récapitulons : i) G/H est quasiprojective de dimension $\dim G - \dim H$;
ii) si G est connexe, alors $G \to G/H$ est séparable.

Exercice. Si $H \leq G$ est un sous-groupe fermé et distingué de G, alors G/H est un groupe algébrique affine (*cf.* TD).

Chapitre 7

Structure des groupes résolubles connexes

7.1 Groupes diagonalisables, tores

Un *caractère* de G est un morphisme de groupes algébriques $G \to \mathbb{G}_m$. Un morphisme de groupes algébriques $\mathbb{G}_m \to G$ est un *cocaractère* ou sous-groupe à un paramètre.

Exemple : $X^*(D_n) \simeq \mathbb{Z}^n$, $X_*(D_n) \simeq \mathbb{Z}^n$.

Remarque : les caractères $\chi \in X^*(D_n)$ forment une base de $k[D_n]$ et $k[D_n]$ est isomorphe à l'algèbre de groupes $k[\mathbb{Z}^n]$.

Un groupe *diagonalisable* est un groupe isomorphe à un sous-groupe fermé de D_n.

Un *tore* est un groupe diagonalisable connexe.

ex : en caractéristique $\neq 2$, posons $S := \mathrm{SO}_2(k) := \{\begin{pmatrix} x & -y \\ y & x \end{pmatrix} : x^2 + y^2 = 1\}$. On a $S \simeq \mathbb{G}_m$ d'où le nom ($S \times S \simeq \mathbb{G}_m^2$) !

Théorème 7.1.1 *Pour un groupe algébrique G, sont équivalentes :*

i) *G diagonalisable ;*

ii) *le groupe abélien $X^*(G)$ est de type fini et $X^*(G)$ forme une $k-$base de $k[G]$;*

iii) *toute représentation rationnelle de G est somme directe de représentations de dimension* 1.

Remarque : la condition *ii* du théorème montre que l'algèbre $k[G]$ est isomorphe à l'algèbre de groupe

$$k[X^*(G)] := \oplus_{\chi \in X^*(G)} k.\chi \ .$$

Démonstration : On utilisera le lemme d'Artin :

Lemme 7.1.2 (*cf.* **Lang,** *Algèbre, ch. VI, th. 4.1*) *Soit K un corps quelconque (commutatif). Si G est un groupe quelconque, alors, dans le $K-$espace vectoriel des applications $G \to K$, les caractères $\chi : G \to K^\times$ sont $K-$linéairement indépendants.*

$i \Rightarrow ii$

Supposons que G est un sous-groupe fermé de D_n.

Remarquons que ii est vérifié pour $G = D_n$. Comme la restriction $k[D_n] \to k[G]$ est un morphisme surjectif, $k[G]$ est engendré par les caractères $\chi|_G$ où $\chi \in X^*(D_n)$. Soit $\chi \in X^*(G)$. On a $\chi \in k[G]$. Donc est une combinaison linéaire de caractères de D_n restreints à G. D'après le lemme de Dedekind, les caractères de G sont $k-$linéairement indépendants donc χ se prolonge en un caractère de D_n. On en déduit que la restriction à G induit un morphisme surjectif $X^*(D_n) \to X^*(G)$ Donc le groupe $X^*(G)$ est bien abélien de type fini et $X^*(G)$ forme bien une base de $k[G]$.

$ii \Rightarrow iii$

Soit $f \in k[G]$, on a : $f(gh) = f(hg)$ pour tous $g, h \in G$ (il suffit en effet de le vérifier pour les $f \in X^*(G)$). On en déduit que G est abélien. De même, on montre que si $g \in G$, alors $f(g_u) = f(e) = 1$ pour tout $f \in k[G]$ (c'est facile si f est un caractère). Donc pour tout $g \in G$, $g_u = e$ et tout $g \in G$ est semisimple.

Supposons que V est une représentation rationnelle de G de dimension finie (il suffit de traiter ce cas). Notons$\rho : G \to \mathrm{GL}(V)$ le morphisme de groupes algébriques correspondant. Si $\chi \in X^*(G)$, on pose :

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

c'est l'espace propre associé à χ. Comme G est abélien et comme tous ses éléments sont semisimples, on peut diagonaliser simultanément les $\rho(g)$, $g \in G$. On en déduit :

$$V = \sum_\chi V_\chi$$

et il est facile de voir que cette somme est directe.

$iii \Rightarrow i$

On peut supposer que $G \subseteq \mathrm{GL}_n(k)$ pour un certain n. La représentation correspondante est somme directe de représentations de dimension 1. On peut donc trouver une base de diagonalisation commune à tous les $g \in G$ *i.e.* G est conjugué à un sous-groupe fermé de D_n.

Q.e.d.

On déduit du théorème précédent (et de laremarque sur l'algèbre de groupe) le théorème suivant :

Théorème 7.1.3 *Soit G diagonalisable. Alors : i) $G \simeq$ tore $\times A$ où A est abélien, fini, d'ordre premier à p ;*

ii) G est un tore $\Leftrightarrow$ G connexe ;
iii) G est un tore $\Leftrightarrow$ $X^*(G)$ libre.

Exercice 41 *Vérifier que dans un tore les éléments d'ordre fini forment une partie dense (indication : il suffit de traiter le cas de $\mathbb{G}_m^n$).*

7.1.1 Rigidité

Proposition 7.1.4 (Rigidité) *G, H diagonalisables. V variété connexe affine.*

Soit $\phi : V \times G \to H$ un morphisme tel que :

$$\forall\, v \in V, \phi(v, \cdot) : G \to H \text{ est un morphisme de groupes algébriques}$$

alors $\phi(v, \cdot)$ est indépendant de V.

Démonstration : Soit $\psi \in X^*(H)$. Alors

$$\forall\, v \in V, \forall\, g \in G,\ \chi(\phi(v, g)) = \sum_{\chi \in X^*(G)} f_{\chi,\psi}(v)\chi(g)$$

pour certains coefficients $f_{\chi,\psi} \in k[V]$. Comme les caractères de G sont linéairement indépendants, tous les $f_{\chi,\psi}(v)$ sont nuls sauf un qui vaut 1. Donc :

$$f_{\chi,\psi}^2 = f_{\chi,\psi} \ .$$

Comme V est connexe, $f_{\chi,\psi} = 0$ ou 1 dans $k[V]$. Donc $f_{\chi,\psi} = 0$ pour tous les χ (ψ étant fixé) sauf pour un où l'on a $f_{\chi,\psi} = 1$. **Q.e.d.**

Corollaire 7.1.4.1 *Soit H un sous-groupe de G diagonalisable. Alors $N_G(H)^\circ = Z_G(H)^\circ$; en particulier, $N(H)/Z(H)$ est fini.*

Théorème 7.1.5 *Soit G un groupe algébrique connexe de dimension 1. Alors :*

$$G \simeq \mathbb{G}_a \text{ ou } \mathbb{G}_m \ .$$

Démonstration :

On sait déjà que G est commutatif et que $G = G_s$ ou G_u.

Si $G = G_s$, alors G est un *tore*. Pour des raisons de dimension : $G \simeq \mathbb{G}_m$.

Si $G = G_u$, alors supposons d'abord k de caractéristique nulle. Rappelons que dans l'anneau $\mathbb{Z}[[T]]$, on a :

$$\exp(\log(1+T)) = 1 + T \text{ et } \log(\exp(T)) = T$$

où

$$\exp(T) := 1 + T + ... + \frac{T^n}{n!} + ... \text{ et } \log(1+T) := T + ... + (-1)^{n-1}\frac{T^n}{n} + ...$$

Soit $I_n \neq g \in G$. On pose $N := \log g := \sum_{j>0}(-1)^{j-1}\frac{(g-1)^j}{j}$. Soit ϕ : $\mathbb{G}_a \to \mathrm{GL}_n(k)$, $t \mapsto \exp(tN)$.

Alors ϕ est un morphisme de groupes algébriques. De plus, $\phi(\mathbb{G}_a) \subseteq G$. En effet : pour tout entier $l \in \mathbb{Z}$, $\phi(l) = g^l \in G$ donc $\phi(\mathbb{G}_a) \cap G$ est infini et donc $\phi(\mathbb{G}_a) \cap G = \phi(\mathbb{G}_a)$.

D'un autre côté, l'application induite :

$$\phi : \mathbb{G}_a \overset{\simeq}{\to} G$$

est un isomorphisme de groupes car l'application :

$$G \to kN \simeq \mathbb{G}_a,\ g \mapsto \log g$$

est un morphisme de variétés. **Q.e.d.**

7.2 Automorphismes semisimples

Soit G un groupe algébrique. Soit $\sigma : G \to G$ un automorphisme de groupe algébrique ; on dit que σ est semisimple si $\sigma^* : k[G] \to k[G]$ est un isomorphisme semisimple.

Proposition 7.2.1 *Un automorphisme σ est semisimple si et seulement s'il existe un morphisme injectif de groupes algébbriques : $\phi : G \to \mathrm{GL}_n$ et $s \in \mathrm{GL}_n$ une matrice diagonalisable qui normalise $\phi(G)$ telle que :*

$$\forall\, g \in G\, \phi(\sigma(g)) = s\phi(g)s^{-1}\ .$$

Démonstration : On pose $\delta(g)f = f(\cdot g)$ pour tout $f \in k[G]$.

On a $\sigma^* \circ \delta(\sigma(g)) = \delta(\sigma(g)) \circ \sigma^*$ pour tout $g \in G$.

Soient $f_1, ..., f_n \in k[G]$ tels que $k[G] = k[f_1, ..., f_n]$. Il existe un sous-espace V de $k[G]$ de dimension finie qui contient $f_1, ..., f_n$ et qui est stable par σ^* et par tous les $\delta(g)$, $g \in G$. On pose $\phi(g) = \delta(g)|_V$ et $s := \sigma^*|_V$.

Q.e.d.

Théorème 7.2.2 *soit G un groupe algébrique d'algèbre de Lie $\mathfrak{g}$. Soit σ : $G \to G$ un automorphisme semisimple. On note $G^\sigma := \{g \in G\ :\ \sigma(g) = g\}$ et $\mathfrak{g}^\sigma := \{\xi \in \mathfrak{g}\ :\ d\sigma|_e\xi = \xi\}$. Alors :* $\mathrm{Lie}(G^\sigma) = \mathfrak{g}^\sigma$.

Démonstration :

Q.e.d.

7.3 Groupes résolubles

Soit G un groupe non forcément algébrique. On définit, par récurrence, la suite de ses groupes dérivés :

$$\mathcal{D}^0(G) := G \; ; \; \mathcal{D}^i(G) := (\mathcal{D}^{i-1}(G), \mathcal{D}^{i-1}(G)) \text{ si } i > 0$$

(si G est un groupe algébrique, alors d'après la proposition 2.7.1, les groupes $\mathcal{D}^i(G)$ sont des sous-groupes fermés de G).

On dit que G est *résoluble* s'il existe $n \geq 0$ tel que : $\mathcal{D}^n(G) = 1$.

Exercice : le groupe $G = B_n(k)$ est résoluble (*indication :* $\mathcal{D}^1(G) = U_n(k)$ *et plus généralement, si* $g \in \mathcal{D}^l(G)$, *alors* $g_{i,i} = 1$ *et* $g_{i,j} = 0$ *si* $1 \leq |i-j| < l$).

7.3.1 Théorème de Lie-Kolchin

Théorème 7.3.1 *Tout sous-groupe connexe résoluble de* $GL_n(k)$ *est conjugué à un sous-groupe de* $B_n(k)$.

Exercice : le sous-groupe de GL_2 engendré par les matrices :

$$\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$

est isomorphe au groupe S_3 donc résoluble mais n'est pas inclus dans un conjugué de B_n (non connexité).

Démonstration : On raisonne par récurrence sur $n + \dim G$. Pas de problème pour l'initialisation. Il suffit de montrer qu'il existe un vecteur propre commun à toutes les matrices $g \in G$. On peut supposer que G agit irréductiblement sur k^n. Comme $G' := (G, G) < G$ et comme G' est connexe, par hypothèse de récurrence, il existe au moins un vecteur propre commun à tous les $g \in (G, G)$. Si χ est un caractère de (G, G), on note :

$$V_\chi := \{v \in k^n \; : \; \forall \, g \in (G, G), gv = \chi(g)v\} \; .$$

Comme (G, G) est distingué dans G, $gV_\chi \subseteq V_{\chi_g}$ où $\chi_g : G' \to \mathbb{G}_m$ est le caractère $\chi_g : x \mapsto \chi(g^{-1}xg)$.

Donc le sous-espace $\oplus_\chi V_\chi$ de k^n est $G-$stable. comme on a supposé k^n irréductible, comme au moins un des $V_\chi \neq 0$, on a :

$$k^n = \oplus_\chi V_\chi \; .$$

Notons $\chi_1, ..., \chi_r$ les caractères χ de G' tel que $V_\chi \neq 0$. Le groupe G permute les V_{χ_i} donc les caractères χ_i. Comme g est connexe, forcément G

laisse fixe chaque χ_i *i.e.* $g(V_\chi) = V_\chi$ pour tout χ. Comme k^n est irréductible, $r = 1$ et $k^n = V_{\chi_1}$. En particulier,

$$G' = \left\{ \begin{pmatrix} \chi_1(g) & & \\ & \ddots & \\ & & \chi_1(g) \end{pmatrix} \right\} .$$

Donc : pour tout $g \in G'$, $\chi_1(g)^n = 1$ (car $G' \leq \mathrm{SL}_n$). Comme G' est connexe, $\chi_1(g) = 1$ pour totu $g \in G'$ et G' est réduit à la matrice I_n. En particulier, G est abélien et il existe bien un vecteur propre commun à tous les $g \in G$ (et donc $n = 1$). **Q.e.d.**

Voici quelques conséquences :

Corollaire 7.3.1.1 *Soit G un groupe connexe résoluble.*

i) *Le sous-groupe dérivé (G, G) est fermé, connexe, unipotent et distingué ;*

ii) *l'ensemble G_u des éléments unipotents de G est un sous-groupe fermé, unipotent connexe et distingué de G ;*

iii) *le quotient G/G_u est un tore ;*

iv) *si de plus, G est nilpotent, alors l'ensemble G_s des éléments semisiples de G est un sous-groupe fermé et un tore contenu dans le centre de G. De plus, l'application « produit » : $G_s \times G_u \to G$ est un isomorphisme de groupes algébriques.*

Remarque : le point iii) est faux pour B_n : si $n \geq 2$, l'ensemble des matrices semisimples de B_n n'est pas un sous-groupe de B_n.

Démonstration :

D'après le théorème de Lie-Kolchin, on peut supposer que G est un sous-groupe fermé de B_n.

i) On a bien $(G, G) \subseteq (B_n, B_n) = U_n$. On a $G_u = G \cap U_n$.

ii) Il est facile de voir que G_u est fermé et distingué. Pour montrer que G_u est connexe on se ramène au cas où G_u est fini en quotientant par G_u^0. Or d'après *i)*, (G, G) est connexe et $(G, G) \subseteq G_u$. Donc $(G, G) = e$ et G est abélien. Dans ce cas, on a déjà vu que $G \simeq G_s \times G_u$ et en particulier, G_u est connexe (donc trivial).

iii) G/G_u est connexe et isomorphe à un sous-groupe fermé de $B_n/U_n \simeq D_n$. Donc, c'est un tore.

iv) Si G est nilpotent : soit $s \in G_s$. Le morphisme : $\chi : G \to G$, $g \mapsto sgs^{-1}g$ a son image fermée et $d\chi|_e : \mathfrak{g} \to T_e\chi G$ est surjective. Or $d\chi|_e = \mathrm{Ad}(s) - \mathrm{Id}$ est un endomorphisme semisimple de $\mathfrak{g}$ et nilpotent car : $\forall\, g \in G$, $\chi^n(g) \in \mathscr{C}^n G = \{e\}$ pour n assez grand. Donc ${d\chi|_e}^n = 0$ pour n assez grand. Ainsi, $d\chi|_e = \mathrm{Ad} s - \mathrm{Id} = 0$ et $\chi G = e$ *i.e.* $s \in Z(G)$.

On peut donc trouver une base de diagonalisation commune des $g \in G_s$. Comme dans le cas commutatif, on peut décomposer $k^n = \oplus E_i$ où chaque E_i est une intersection d'espaces propres communs à tous les $g \in G_s$: E_i est de la forme $\bigcap_{g \in G_s} \ker(g - \lambda_g)$ pour certaines fonctions $\lambda : G_s \to k$. En particulier les E_i sont $G-$stables. On peut donc appliquer Lie-Kolchin dans chaque E_i. On peut donc supposer que non seulement $G \leq B_n$ mais aussi que chaque matrice $g \in G$ est triangulaire par blocs avec des blocs de matrices triangulaires supérieures à diagonale constante. Pour une telle matrice g, la partie semisimple est simplement la diagonale. Donc $G \to G_s$, $g \mapsto g_s$ est un morphisme algébrique qui préserve le produit (car la diagonale d'un produit de matrices triangulaires est le produit des diagonales) donc G_s est bien un sous-groupe fermé de G et on en déduit un morphisem :

$$G \to G_s \times G_u,\ g \mapsto (g_s, g_s^{-1}g)$$

qui est bien la réciproque de $g \mapsto (g_s, g_u)$.

Q.e.d.

Corollaire 7.3.1.2 *Si G est un groupe résoluble connexe, alors il existe des sous-groupes fermés, connexes et distingués de G :*

$$G = G_0 \geq G_1 \geq ... \geq G_N = e$$

tels que $\forall\, i$, $G_i/G_{i+1} \simeq \mathbb{G}_a$ ou $\mathbb{G}_m$. On peut même choisir les G_i tels que pour un certain $0 \leq q \leq N$, on ait :

$$\forall\, 1 \leq i \leq q,\ G_i/G_{i+1} \simeq \mathbb{G}_m,\ \forall\, q < i \leq N,\ G_i/G_{i+1} \simeq \mathbb{G}_a\ .$$

Démonstration : *cf.* td (fiche 7). **Q.e.d.**

7.3.2 Résultats de base sur les groupes résolubles connexes

On déduit facilement du corollaire 7.3.1.2 le :

Lemme 7.3.2 *Si G est résoluble connexe et n'est pas un tore, alors il existe un sous-groupe fermé connexe et distingué N de G contenu dans le centre de G_u et isomorphe à $\mathbb{G}_a$.*

Démonstration : soit $G = G_0 \geq G_1 \geq ... \geq G_N = e$ comme dans le corollaire 7.3.1.2. Comme G_u est nilpotent, il existe i tel que $\mathscr{C}^i(G_u) \neq 0$ et $\mathscr{C}^{i+1}(G_u) = e$. Il suffit de prendre le plus grand p pour que $\dim \mathscr{C}^i(G_u) \cap G_p > 0$. On a forcément $\dim \mathscr{C}^i(G_u) \cap G_p = 1$ et il suffit de poser $N := (\dim \mathscr{C}^i(G_u) \cap G_p)^0$. **Q.e.d.**

Lemme 7.3.3 *Soit d un groupe diagonalisable qui agit par automorphismes de groupes sur G un groupe connexe (par exemple, D est un sous-groupe diagonalisable de G qui agit par conjugaison). On note :*

$$Z_G(D) := \{g \in G : \forall d \in D,\, d.g = g\} \text{ et } \mathfrak{z}_{\mathfrak{g}}(d) := \{\xi \in \mathfrak{g} : \forall d \in D,\, d.\xi = \xi\}\,.$$

On a : $\mathrm{Lie}(Z_G(D)) = \mathfrak{z}_{\mathfrak{g}}(D)$.

Démonstration : On raisonne par récurrence sur $\dim G$. Si $Z_G(D) = G$, c'est évident. Sinon, soit $d \in D$ tel que $Z_G(d) < G$. On pose $H := Z_G(d)^0$. Comme D est dommutatif, D laisse stable H et donc :

$$Z_G(D)^0 \leq Z_H(D) \leq Z_G(D)\ .$$

Par hypothèse de récurrence, $\mathrm{Lie}(Z_H(D)) = \mathfrak{z}_{\mathfrak{h}}(D)$. Or, d est un automorphisme semisimple ; donc $\mathfrak{h} = \mathfrak{z}_{\mathfrak{g}}(d)$. On a donc :

$$\mathrm{Lie} Z_G(D) = \mathrm{Lie} Z_H(D) = \mathfrak{z}_{\mathfrak{h}}(D) = \mathfrak{z}_{\mathfrak{g}}(D)\ .$$

Q.e.d.

Corollaire 7.3.3.1 *Soit $\phi : H \to H'$ un morphisme surjectif de groupes. on suppose qu'il existe un groupe diagonalisable D qui agit par automorphismes de groupes sur H et H' et que ϕ est $H-$équivariant. Alors $\phi(H^D)^0 = (H'^D)^0$.*

Démonstration : Commençons par le cas où $H' = H/K$ pour un certain sous-groupe fermé distingué de H et où ϕ est la surjection canonique. Alors, $d\phi$ est surjective de noyau $\mathrm{Lie}(K) = \mathfrak{k}$. Soit $\mathfrak{n}$ un supplémentaire $D-$stable de $\mathrm{Lie}(K)$ dans $\mathrm{Lie}(G)$. On a :

$$\dim \mathrm{Lie}(\phi(H^D)) \geq \dim d\phi(\mathfrak{h}^D) = \dim \mathfrak{h}^D - \dim \mathfrak{k}^D = \dim \mathfrak{n}^D = \dim \mathfrak{h}'^d\ .$$

Donc $\dim \phi(H^D) = \dim H'^D$. Or $\phi(H^D)^0 \subseteq (H'^D)^0$ d'où :

$$\phi(H^D)^0 = (H'^D)^0\ .$$

Q.e.d.

Théorème 7.3.4 *Soit G un groupe résolubles connexe. On dira qu'un tore T contenu dans G est maximal si* $\dim T = \dim G/G_u$.

i) Si $s \in G$ est semisimple, alors s appartient à un tore maximal de G (en particulier, il existe des tores maximaux) ;

ii) le centralisateur d'un élément semisimple s, $Z_G(s)$ est connexe ;

iii) deux tores maximaux sont conjugués dans G ;

iv) si T est un tore maximal, alors l'application produit : $T \times G_u \to G$ est un isomorphisme de variétés.

v) G a un seul tore maximal si et seulement si G est nilpotent.

Démonstration :

Si G est nilpotent, il n'y a rien à faire car dans ce cas, il y a un seul tore maximal : G_S et $G \simeq G_s \times G_u$. On suppose donc que G n'est pas nilpotent *i.e.* $G^\infty := \bigcap_i \mathscr{C}^i G$ est un sous-groupe connexe (et unipotent) de dimension > 0.

Si G a un seul tore maximal, on vérifie que $\mathscr{C}^i(G) \leq \mathscr{C}^{i-1}(G_u)$ si $i > 0$: il suffit de montrer que si s est semisimple, si $g \in G_u$, $sg = gs$; soit $sg = xy$ la décomposition de Jordan de sg avec x semisimple, y unipotent et $xy = yx$. Alors comme on le montrera plus tard, s, x sont dans l'unique tore maximal de G donc $x^{-1}s = yg^{-1}$ est semisimple et unipotent donc trivial. Donc $x = s$ et $y = g$ commutent.

Pour *iv)* : $T \to G/G_u$ est injective donc bijective. Donc le produit : $p : T \times G_u \to G$ est bijectif. Deplus, p est $T \times G_u-$équivariant et $T \times G_u$ et G sont $T \times G_u$ homogènes. Il suffit donc de montrer que $dp|_{e,e}$ est surjective *i.e.* injective en raison de l'égalité des dimensions. C'est le cas car $\ker dp = \{x \oplus y \in \mathrm{Lie}(T) + \mathrm{Lie}(G_u) \ : \ x + y = 0 \in \mathrm{Lie}(G)\}$ et $\mathrm{Lie}(T) \cap \mathrm{Lie}(G_u) = 0$ (car si $x \in \mathrm{Lie}(T) \cap \mathrm{Lie}(G_u)$, x est semisimple et nilpotent).

On raisonne par récurrence sur $\dim G$. Si G est nilpotent, c'est facile.

Soit N un sous-groupe unipotent central connexe de dimension 1. Soit $\overline{G} := G/N$. Soit $s \in G$ semisimple. Soit $G_1 := \{g \in G : gsg^{-1}s^{-1} \in N\}$; c'est un sous-groupe fermé de G qui contient $Z_G(s)$ et N. De plus, $G_1/N \simeq Z_{\overline{G}}(\overline{s})$. Par hypothèse de récurrence, $Z_{\overline{G}}(\overline{s})$ est connexe donc G_1 est connexe car $G_1/N = G_1^0/N$. Si $G_1 \neq G$, $Z_G(s) = Z_{G_1}(s)$ est connexe par hypothèse de récurrence. Si $G_1 = G$, soit $Z := Z_G(s)$. Il existe un isomorphisme : $\phi : \mathbb{G}_a \to N$ et un caractère χ de G tel que :

$$\forall\, g \in G, \forall\, a \in \mathbb{G}_a, \, g\phi(a)g^{-1} = \phi(\chi(g)a) \ .$$

Soit $\pi : G \to G/N$. On a : $(\mathrm{Ad}(s) - \mathrm{Id})\mathfrak{g} + \mathfrak{z} = \mathfrak{g}$ où $\mathfrak{z} := \mathrm{Lie}(Z)$. Or, si $G_1 = G$, $d\pi \circ (\mathrm{Ad} s - \mathrm{Id}) = 0$. Donc $\mathrm{Ad} s - \mathrm{Id}(\mathfrak{g}) \subseteq \ker d\pi = \mathrm{Lie}(N)$. Mais alors : $\dim \mathfrak{z} \geq \dim G - 1$. Comme s est non central, $\dim Z = \dim G - 1$ et $G = Z^0 N$.

Si $\chi(s) = 1$, alors $N \subseteq Z$ et $G = Z^0$ *absurde.* Donc $\chi(s) \neq 1$ et $Z \cap N = e$. Donc $G = Z^0 N \Rightarrow Z = Z^0$ est connexe. D'où *ii)*.

Soit $s \in G$ semisimple non central. Soit $H := Z_G(s)^0 = Z_G(s)$. Par hypothèse de récurrence, H contient un tore maximal qui contient s. Or, $\pi : G \to G/G_u$ est $D-$équivariant où $D = \langle s \rangle$ agit par conjugaison. G/G_u est abélien donc $(G/G_u)^D = G/G_u$. On a $\pi(H) = G/G_u$ d'après le corollaire 7.3.3.1. Alors $\dim H/H_u = \dim G/G_u$ et un tore maximal de H est un tore maximal de G d'où i) (si s est semisimple central, alors pour tout tore maximal T de G on a : $G = TG_u$ donc $s = tx$ pour un $t \in T$ et un $x \in G_u$; comme s est central, $x = t^{-1}s$ est semisimple donc $s = t^{-1}s = e \Rightarrow s = t \in T$).

Soient T, T' deux tores maximaux de G. Soit $\overline{G} := G/N$. Les tores $\overline{T} := \pi T$ et $\overline{T'} := \pi T'$ sont maximaux dans $\overline{G}$. Donc il existe $x \in g$ tel que $xT'x^{-1} \subseteq NT$. Si $NT < G$ on applique l'hypothèse de récurrence. Si $G = NT$, alors comme ci-dessus : il existe un isomorphisme : $\phi : \mathbb{G}_a \to N$ et un caractère χ de G tel que :

$$\forall\, g \in G, \forall\, a \in \mathbb{G}_a,\ g\phi(a)g^{-1} = \phi(\chi(g)a)\ .$$

comme on suppose G non nilpotent, les éléments de T et de N ne commutent pas tous. Donc il existe $t \in T$ tel que $\chi(t) \neq 1$. On a alors $T = Z_G(t)$. De même il existe $t' \in T'$ tel que $\chi(t') \neq 0$ et $T' = Z_G(t')$.

Soit $a \in \mathbb{G}_a$ tel que $t' = \phi(a)t$. Si $b := -a/(1 - \chi(t)) \in \mathbb{G}_a$, alors on a :

$$\phi(b)t'\phi(b)^{-1} = \phi(b)\phi(a)t\phi(b)^{-1} = t$$

donc $\phi(b)Z_G(t')\phi(b)^{-1} = Z_G(t) = T$.

$$\phi(b)t'\phi(b)^{-1} =$$

Q.e.d.

Corollaire 7.3.4.1 *Soit $H \subseteq G$ un sous-groupe dont tous les éléments sont semisimples.*

i) H est contenu dans un tore maximal de G ; en particulier, tout tore est contenu dans un tore maximal ;

ii) le centralisateur $Z_G(H)$ est connexe et $Z_G(H) = N_G(H)$.

Démonstration : Si H est central, c'est facile.

On raisonne ensuite par récurrence. Soit $s \in H$ non central. Alors $Z := Z_G(s)$ est connexe et contient H. Il existe un tore maximal T qui contient s. On a alors $T \subseteq Z$. Donc un tore maximal de Z est un tore maximal de G. Par hypothèse de récurrence, H est contenu dans un tore maximal de Z donc de G. Toujours par hypothèse de récurrence, $Z_G(H)$ est connexe. Si $x \in N_G(H)$, alors pour tout $h \in H$, on a :

$$xhx^{-1}h^{-1} \in H \cap (G, G) \subseteq H \cap G_u = e$$

donc $x \in Z_G(H)$. **Q.e.d.**

Remarque : il résulte de i) qu'un tore maximal pour l'inclusion est un tore maximal.

Exercice. Soit G un groupe nilpotent connexe et soit $H \leq G$ un sous-groupe fermé. Alors $\dim N_G H > \dim H$. En particulier, si $\dim H = \dim G - 1$, H est distingué dans G *(indication : raisonner par récurrence sur* $\dim H$ *; soit Z la composante neutre du centre de G,* $\dim Z > 0$ *et on peut considérer G/Z si $Z \subseteq H$ et $HZ > H$ si $Z \nsubseteq H$).*

Chapitre 8

Sous-groupes paraboliques, sous-groupes de Borel et sous-groupes de Cartan

8.1 Variétés complètes

Une variété algébrique X est *complète* si pour toute variété algébrique Y, la projection $X \times Y \to Y$ est fermée (envoie fermé sur fermé).

Proposition 8.1.1 *Soit X complète.*

i) Un fermé de X est complet ;

ii) Si $\phi : X \to Y$ est un morphisme alors ϕX est fermé est complet ;

iii) si X irréductible, alors $k[X] = k$;

iv) si X est affine alors X est fini.

Exercice : si G est un groupe algébrique (où on retire l'hypothèse affine) complet. Alors G est commutatif.

Proposition 8.1.2 *Une variété projective est complète.*

Démonstration : Il suffit de démontrer que $p : \mathbb{P}^n \times \mathbb{A}^l \to \mathbb{A}^l$ est fermé : soit F un fermé de $\mathbb{P}^n \times \mathbb{A}^l$. Alors F est défini par des équations $f_i \in k[X_0, ..., X_n; Y_1, ..., Y_l]$ homogènes en les X_j (*exo*). On peut supposer que les f_i sont en nombre fini : $1 \leq i \leq N$. On a :

$$p(F) = \{y \in \mathbb{A}^l \ : \ \exists\, x \in \mathbb{A}^{n+1} \setminus \{0\}, \forall\, i,\ f_i(x, y) = 0\} \ .$$

Notons k_i le degré de f_i en les variables X_j.

Donc si $y \in \mathbb{A}^l$, alors :

$$y \in p(F) \Leftrightarrow (X_0, ..., X_n) \not\subseteq \sqrt{(f_i(X; y) \ : \ 1 \leq i \leq N)}$$

$$\Leftrightarrow \forall\, s \geq 1,\, (X_0, ..., X_n)^s \not\subseteq (f_i(X; y)\ :\ 1 \leq i \leq N)$$

$$\Leftrightarrow \forall\, \alpha \in \mathbb{N}^{n+1},\, |\alpha| = s \Rightarrow X^\alpha \in (f_i(X; y)\ :\ 1 \leq i \leq N)$$

$$\Leftrightarrow \forall \alpha \in \mathbb{N}^{n+1},\, |\alpha| = s \Rightarrow X^\alpha \in \mathrm{vect}\{X^\beta f_i(X, y) : 1 \leq i \leq N,\, \beta \in \mathbb{N}^{n+1},\, |\beta| = s - k_i\}.$$

Soient $a_{\alpha;\beta,i} \in k[Y]$ des coefficients tels que :

$$X^\beta f_i = \sum_{\alpha,\beta,i} a_{\alpha;\beta,i} X^\alpha$$

où α décrit les $n+1-$uplets tels que $|\alpha| = s$, $1 \leq i \leq N$, $\beta \in \mathbb{N}^{n+1}$, $|\beta| = s - k_i$.

Soit $A := (a_{\alpha;\beta,i})_{\alpha,(\beta,i)} \in \mathscr{M}_{m_s,n_s}(k[Y])$ où $m_s = |\{\alpha \in \mathbb{N}^{n+1}\ :\ |\alpha| = s\}|$ et $n_s = |\{(\beta, i)\ :\ 1 \leq i \leq N,\, \beta \in \mathbb{N}^{n+1},\, |\beta| = s - k_i\}|$.

On a donc

$$y \in p(F) \Leftrightarrow \forall\, s,\, \mathrm{rg}A < m_s$$

ce qui est une « condition fermée ».

Q.e.d.

8.2 Théorème du point fixe de Borel

Théorème 8.2.1 *Soit G un groupe résoluble connexe qui agit sur une variété complète X. Alors, G a au moins un point fixe dans X.*

Démonstration : Par le corollaire 7.3.1.2, on se ramène au cas où $G = \mathbb{G}_a$ où $\mathbb{G}_m$. Dans ce cas, si $G.x$ est une orbite fermée dans X, alors $G/G_x \to G.x$ est un morphisme qui est un homéomorphisme donc G/G_x est à la fois affine et complet. Donc $G/G_x = 1$ *i.e.* x est un point fixe. **Q.e.d.**

8.3 Sous-groupes paraboliques

Soit G un groupe algébrique.

Un sous-groupe P de G est *parabolique* si le quotient G/P est une variété complète.

Remarque : si P est parabolique, alors G/P est projective.

Lemme 8.3.1

Lemme 8.3.2 *Soient X, Y des espaces $G-$homogènes et $\phi : X \to Y$ un $G-$morphisme bijectif. Alors X complet $\Leftrightarrow$ Y complet.*

Démonstration : En effet, pour toute variété Z, le morphisme $\phi \times \mathrm{Id} : X \times Z \to Y \times Z$ est un homéomorphisme. **Q.e.d.**

Lemme 8.3.3 (transitivité) *Soient $Q \leq P \leq G$ des sous-groupes fermés. Si P est parabolique dans G et Q dans P, alors Q est parabolique dans G.*

Démonstration : On note $p_P : G \to G/P$, $p_Q : G \to G/Q$ les projections canoniques. Soit $m : P \times G \to G : (p, g) \mapsto gp$. Soit Z une variété ; on a un diagramme commutatif :

$$\begin{tikzcd}
P \times G \times Z \arrow[r, "m\times 1"] \arrow[dd, "p_Q\times 1"] & G \times Z \arrow[r, "p_Q\times 1"] & G/Q \times Z \arrow[d, "\pi_Z"] \\
 & & Z \\
P/Q \times G \times Z \arrow[r, "\pi_{G\times Z}"] & G \times Z \arrow[r, "p_P\times 1"] & G/P \times Z \arrow[u, "\pi_Z"']
\end{tikzcd}$$

Soit $F \subseteq G/Q \times Z$ un fermé. Alors $((m \times 1)(p_Q \times 1))^{-1}F$ est un fermé, notons le A de $P \times G \times Z$ qui vérifie :

$$(p, g, z) \in A \Rightarrow \forall\, q \in Q,\ (pq, g, z) \in A\ .$$

Comme $p_Q \times 1$ est ouverte, on en déduit que $(p_Q \times 1)A$ est fermé dans $P/Q \times G \times Z$. Comme P/Q est complète, $\pi_{G\times Z}(p_Q \times 1)A$ est un fermé B de $G \times Z$ et $(p_P \times 1)B$ est fermé dans $G/P \times Z$ (car $(g, z) \in B \Rightarrow \forall\, p \in P,\ (gp, z) \in B$). Comme G/P est complète on en conclut que $\pi_Z p_P \times 1B = \pi_Z F$ est fermé dans Z.

Q.e.d.

Lemme 8.3.4 *i) Soit P un sous-groupe parabolique de G alors si Q contient P, Q est parabolique dans G.*

ii) P parabolique dans G si et seulement si P° parabolique dans G°.

Démonstration : $i)$: facile !

$ii)$: si P est parabolique dans G, alors comme P^0 est parabolique dans P, P^0 est parabolique dans G. Or G^0/P^0 est une composante connexe de G/P^0 donc P^0 est parabolique dans G^0. Réciproquement, si P^0 est parabolique dans G^0, alors toutes les composantes connexes de G/P^0 sont complètes car isomorphes à G^0/P^0 donc G/P^0 est complète. Mais alors G/P est complète d'après $i)$. **Q.e.d.**

Proposition 8.3.5 *Soit G connexe. G contient un parabolique propre si et seulement si G non résoluble.*

Démonstration : Si G est résoluble et si $P \leq G$ est parabolique, alors G a un point fixe dans G/P par le théorème du point fixe. Donc $P = G$.

Si G n'est pas résoluble, on peut supposer que G est un sous-groupe fermé de $\mathrm{GL}(V)$ pour un certain espace V de dimension finie. Soit $x \in \mathbb{P}(V)$ tel que l'orbite $G.x$ est fermée. Soit $P := G_x$. Si $P \neq G$, on a terminé. Sinon on remplace V par V/kx ... à la fin on trouve un stabilisateur différent de G sinon, si G stabilise un drapeau complet, alors G est résoluble. **Q.e.d.**

8.4 Sous-groupes de Borel

Un *sous-groupe de Borel* est un sous-groupe connexe résoluble maximal pour ces propriétés (et pour l'inclusion).

Théorème 8.4.1 *i) Un sous-groupe fermé de G est parabolique $\Leftrightarrow$ il contient un Borel de G ;*

ii) En particulier, un sous-groupe de Borel B est parabolique i.e. *G/B est projective ;*

iii) les sous-groupes de Borel sont conjugués (en particulier de même dimension).

Démonstration : Le *iii*) résulte de *ii*) et du théorème de point fixe de Borel.

Démontrons *i*) : si G/P est complète et si B est un groupe résoluble connexe, alors d'après le théorème du point fixe de Borel, B est conjugué à un sous-groupe de P. Réciproquement, si P contient un sous-groupe de Borel B, alors G/B est projective (*cf.* td) et donc G/P aussi. **Q.e.d.**

Exemple : si $G = \mathrm{GL}_n$, les sous-groupes de Borel sont les conjugués de B_n et GL_n/B_n est isomorphe à la variété des drapeaux complets (*cf.* td).

On dit que les G/B sont des variétés de drapeaux.

Remarque : on obtient une caractérisation géométrique des sous-groupes de Borel : un sous-groupe B résoluble connexe est un sous-groupe de Borel si et seulement si la variété G/B est complète.

Corollaire 8.4.1.1 *Soit $\phi : G \to G'$ un morphisme surjectif de groupes algébriques. Soit H un parabolique , respectivement un sous-groupe de Borel, respectivement un tore maximal, de G. Alors, ϕH est un parabolique, respectivement un sous-groupe de Borel, respectivement un tore maximal, de G'.*

Démonstration : Si H est un sous-groupe parabolique, alors G/H est complète donc $\phi G/\phi H$ aussi. Donc ϕH est un sous-groupe paranolique de $\phi G = G'$. En particulier, si H est un sous-groupe de Borel, ϕB est un sous-groupe parabolique de G' qui est résoluble et connexe : c'est donc un sous-groupe de Borel de G'.

Soit T un tore maximal de G, soit B un sous-groupe de Borel de G qui contient T. Alors $B' := \phi B$ est un sous-groupe de Borel de G' contenant ϕT. Soit T' un tore maximal de B' (donc de G') qui contient ϕT. Alors si $t' \in T'$, $t' = \phi(tu)$ pour un certain $t \in T$, et un certain $u \in B_u$. Donc $\phi(t^{-1})t' \in T' \cap B'_u = \{e\}$.

Donc $t' = \phi t \in \phi T$ et $\phi T = T'$ est un tore maximal de G' **Q.e.d.**

Corollaire 8.4.1.2 *Si G est connexe, alors $Z(G)^\circ \subseteq Z(B) \subseteq Z(G)$.*

Démonstration : Pour la première inclusion, on remarque que $Z(G)^0$ est résoluble connexe donc contenu dans un Borel et comme tous les Borel sont conjugués ... Pour la deuxième inclusion : soit $x \in Z(B)$. On considère : $\phi : G \to G$, $y \mapsto xyx^{-1}y^{-1}$. Alors $\phi(B) = \{e\}$ donc ϕ se factorise en un morphisme $\overline{\phi} : G/B \to G$. En particulier, $\phi(G) = \overline{\phi}(G/B)$ est fermé (donc affine) et complet dans G donc fini. Comme G est connexe, $\phi(G) = e$ et $x \in Z(G)$. **Q.e.d.**

Corollaire 8.4.1.3 *Soit G un groupe connexe.*

i) si B est un sous-groupe de Borel nilpotent alors $G = B$;

ii) le groupe G est nilpotent $\Leftrightarrow$ G contient un seul tore maximal.

Démonstration : *i*) On raisonne par récurrence sur $\dim G$. Si $\dim G = 0$, c'est facile. Si $\dim G > 0$, alors $\dim B > 0$ (car sinon $B = e$ et $G/e = G$ n'est pas complet). Donc $\dim Z(B) > 0$ (considérer le dernier terme non nul de la suite centrale). Comme $Z(G)^0 \leq Z(B) \leq Z(G)$, on peut appliquer l'hypothèse de récurrence à $G/Z(G)^0$ où $B/Z(G)^0$ est un Borel. Donc $B/Z(G)^0 = G/Z(G)^0 \Rightarrow G = B$.

ii) : si G a un seul tore maximal T, soit B un sous-groupe de Borel le contenant. Alors B est nilpotent donc $G = B$ aussi. La réciproque est facile.

Q.e.d.

8.5 Tores maximaux

Soit G un groupe algébrique.

Un *tore maximal* est un tore maximal pour l'inclusion.

Théorème 8.5.1 *Les tores maximaux sont conjugués.*

Démonstration : En effet, les tores maximaux d'un Borel le sont et les Borel sont conjugués. **Q.e.d.**

Soit T tore maximal et soient $C := Z_G(T)$, $N := N_G(T)$. On dit que C est un *sous-groupe de Cartan*.

Lemme 8.5.2 *i) C est un sous-groupe distingué de N et $W := N/C$ est fini ;*

ii) C^0 est nilpotent ;

iii) Soit $X := \{(xC^0, y) \in G/C^0 \times G \ : \ x^{-1}yx \in C^0\}$; l'image de la projection $p_G : X \to G$ contient un ouvert non vide de G.

Démonstration : *i)* : vrai pour un tore S de G quelconque à la place de G : *cf.* la rigidité ;

ii) : T est le seul tore maximal de C^0 donc C^0 est nilpotent.

iii) : Comme G^0 est ouvert dans G, il suffi de traiter le cas où G est connexe. Soit $\widetilde{X} := \{(x, y) \in G \times G \ : \ x^{-1}yx \in C^0\}$. On remarque que $\widetilde{X}$ est fermé dans $G \times G$ isomorphe à $G \times C^0$ (*exo*)donc $\dim G + \dim C^0 = \dim \widetilde{X}$ et $\widetilde{X}$ est irréducible. Or, la projection : $\pi : G \times G \to G/C^0 \times G$, $(g_1, g_2) \mapsto (g_1C^0, g_2)$ est ouverte. On en déduit que $X = p\widetilde{X} = X$ est un fermé irréductible de $G/C^0 \times G$. Soit $p : X \to G$ la projection. Il suffit donc de montrer qu'il existe $a \in X$ tel que $p^{-1}pa$ est fini (*cf.* le lemme 6.2.7). Soit $t \in T$ tel que $Z_G(t) = Z_G(T)$ (*exo*). On peut prendre $a = (C^0, t)$.

En effet, dans ce cas, $p^{-1}pa \simeq \{gC^0 \ : \ t \in gC^0g^{-1}\}$. Or, si $t \in gC^0g^{-1}$, $t \in gTg^{-1}$ le seul tore maximal de gC^0g^{-1}. Donc $gTg^{-1} \leq C^0 = Z_Gt^0$. Or, T est le seul tore maximal de C^0 donc $gTg^{-1} = T$ et $g \in N$. Donc $p^{-1}pa$ est isomorphe à N/C^0 qui est fini. **Q.e.d.**

Le groupe fini W est le *groupe de Weyl* de (G, T), il opère fidèlement sur T.

Remarque : on a : $p_G(X) = \cup_{x \in G} xC^0x^{-1}$. En particulier, si $G = \mathrm{GL}_n$ et si T est le tore (maximal) des matrices diagonales inversibles, alors $C = C^0 = T$ et $p_GX = \cup_{g \in G} gTg^{-1}$ est l'ensemble des matrices diagonalisables.

8.5.1 Propriétés supplémentaires dans le cas connexe

Soit G un groupe **connexe**.

Théorème 8.5.3 *Tout élément de G est contenu dans un sous-groupe de Borel.*

Démonstration : Soit T un tore maximal ; soit B un Borel qui contient $C^0 = Z_G(T)^0$. Soit :

$$Y := \{(xb, y) \in G/B \times G \ : \ x^{-1}yx \in B\} \ .$$

Y est un fermé de $G/B \times G$ et la projection $p : Y \to G$ est fermée car G/B est complète. D'après le lemme 8.5.2 *iii*), $p(Y)$ contient un ouvert non vide de G. Donc p est surjective (car G est connexe). **Q.e.d.**

Corollaire 8.5.3.1 *Tout élément semisimple est dans un tore maximal de G.*

Démonstration : Grâce au lemme précédent, on se ramène au cas où G est résoluble ... **Q.e.d.**

Théorème 8.5.4 *Soit $S \leq G$ un tore.*

i) Le centralisateur $Z_G S$ est connexe ; en particulier, les sous-groupes de Cartan sont connexes.

ii) Si $B \geq S$ est un sous-groupe de Borel contenant S, alors $Z_G(S) \cap B$ est un sous-groupe de Borel de $Z_G(S)$ et tous les sous-groupes de Borel de $Z_G S$ s'obtiennent ainsi..

Démonstration : *i*) : Soit $S \leq G$ un tore. Soit $x \in Z_G(S)$. Le groupe S agit sur la sous-variété fermée de G/B :

$$\{yB \ : \ y^{-1}xy \in B\}$$

donc laisse fixe un point d'après le théorème du point fixe de Borel. On trouve donc un Borel B qui contient S et x. Donc $x \in Z_B(S)$ qui est connexe. Or $Z_B(S) \leq Z_G(S)^0$ donc $x \in Z_G(S)^0$.

ii) : Soit $Z := Z_G S$. On sait déjà que $Z_G S \cap B = Z_B S$ est résoluble connexe. Il reste donc à montrer que $Z/Z \cap B$ est complète. On a un morphisme bijectif : $Z/Z \cap B$ sur l'image de ZB dans G/B. Il suffit donc de montrer que l'image de Y de ZB dans G/B est complète. Or Y est irréductible (c'est une image de $Z \times B$). Comme la surjection canonique $G \to G/B$ est ouverte, il suffit de montrer que ZB est fermé dans G :

si $y \in Y$, $y^{-1}Sy \subseteq B$. c'est donc vrai aussi si $y \in \overline{Y}$. Considérons le morphisme :

$$\phi : \overline{Y} \times S \to B/B_u,\ (y,s) \mapsto y^{-1}sy \bmod B_u \ .$$

D'après le théorème de rigidité, $y^{-1}sy = s \bmod B_u$ pour tout $y \in \overline{Y}$.Donc $y^{-1}Sy$ est un tore maximal de SB_u. Or S est aussi un tore maximal de SB_u donc :

$$y^{-1}Sy = z^{-1}Sz$$

pour un certain $z \in B_u$. Donc $zy^{-1} \in N := N_G S$. On a donc $ZB \leq \overline{Y} \leq NB$. Or N/Z est fini donc NB est une réunion (disjointe) finie de $Z \times B-$orbites doncZB est une $Z \times B-$orbite ouverte et fermée. Donc $\overline{Y} = ZB$ est fermé. **Q.e.d.**

Corollaire 8.5.4.1 *Si B est un Borel qui contient T, alors B contient $Z_G(T)$.*

8.5.2 Théorème du normalisateur

Soit G un groupe **connexe**.

Lemme 8.5.5 *Soit B un sous-groupe de Borel de G. Alors $B = N_G(B)^0$.*

Démonstration : Le groupe B est le seul sous-groupe de Borel de N^0. Or, tout élément de N^0 est dans un sous-groupe de Borel. Donc $N^0 = B$. **Q.e.d.**

Théorème 8.5.6 *Soit B un sous-groupe de Borel de G. Alors $B = N_G(B)$.*

Démonstration : Posons $N := N_G(B)$.

Par récurrence sur $\dim G$: c'est évident si $\dim G = 0$; si $\dim G > 0$, soit T un tore maximal de B. Si $x \in N$, alors xTx^{-1} est un tore maximal de B donc $xTx^{-1} = bTb^{-1}$ pour un certain $b \in B$. Donc quitte à remplacer x par $b^{-1}x$, on peut supposer que $x \in N_G(T)$. Soit $\phi : T \to T$, $t \mapsto xtx^{-1}t^{-1}$. Distinguons deux cas :

a) ϕ n'est pas surjectif. Dans ce cas $S := (\ker \phi)^0$ est un sous-tore non trivial de T et $x \in Z_G S$. Il est clair que x est dans le normalisateur du sous-groupe de Borel $Z_G S \cap B$ de $Z_G S$. Si $Z_G S \neq G$, alors par hypothèse de récurrence, $x \in B$. Si $Z_G S = G$, alors $S \leq Z(G)$ et on peut appliquer l'hypothèse de récurrence à G/S.

b) ϕ est surjectif. Soit $r : G \to \mathrm{GL}(V)$ une représentation rationnelle de dimension finie et $0 \neq v \in V$ tels que :

$$n = \{g \in G \ : \ r(g)v \in kv\} \ .$$

Si $g \in B_u$, alors $r(g)v = v$ (car un groupe unipotent a un seul caractère : le caractère trivial). Si $t \in T$, alors $t = xt_1x^{-1}t_1^{-1}$ pour un certain $t_1 \in T$; on a donc $r(t)v = v$. Donc $r(B)v = v$ d'où un morphisme :

$$G/B \to V, \ gB \mapsto r(g)v \ .$$

Ce morphisme a son image complète et affine (car fermé dans un affine) (et irréductible) donc pour tout $g \in G$, $r(g)v = v$. Ainsi, $G = N$. Or, $B = N^0$. Donc $B = N$. **Q.e.d.**

Corollaire 8.5.6.1 *Soit P un sous-groupe parabolique de G. Alors $P = N_G P$ et P est connexe.*

Démonstration : Soit $B \leq P^0$ un sous-groupe de Borel de G. Si $x \in N_G P$, alors xBx^{-1} est aussi un sous-groupe de Borel de P^0. Donc il existe $y \in P^0$ tel que $xBx^{-1} = yBy^{-1}$. Donc $y^{-1}x \in N_G B = B \Rightarrow x \in P^0$. **Q.e.d.**

Corollaire 8.5.6.2 *Soient P, Q deux sous-groupes paraboliques de G qui contiennent un même sous-groupe de Borel de G. Si P, Q sont conjugués, alors $P = Q$.*

Soit $\mathscr{B}$ l'ensemble des sous-groupes de Borel de G. Fixons $B \in \mathscr{B}$, l'application $gB \mapsto gBg^{-1}$ est une bijection entre G/B et $\mathscr{B}$. On en déduit une structure de variété projective sur $\mathscr{B}$ (indépendante de B) ; c'est la *variété des sous-groupes de Borel de G*.

Corollaire 8.5.6.3 *Soit B un sous-groupe de Borel de G et soit $U := B_u$. Alors $B = N_G U$.*

Démonstration : Soit $N := N_G U$. Soit $x \in (N_G U)^0$ unipotent. Il existe $g \in N_G U$ tel que $gxg^{-1} \in B$. Donc $gxg^{-1} \in U \Rightarrow x \in U$. Donc N^0/U est formé d'éléments semisimples ; c'est donc un tore. En particulier, N^0 est résoluble et comme $B \subseteq N^0$, forcément $B = N^0$. Or $N \subseteq N_G N^0 = N_G B = B$. Donc $N = B$. **Q.e.d.**

Corollaire 8.5.6.4 *Soit T tore maximal. Soit B un Borel contenant T. L'application : $x \mapsto xBx^{-1}$ induit une bijection entre $N_G(T)/Z_G(T)$ et l'ensemble des Borel qui contiennent T.*

Démonstration : Soit $x \in N_G(T)$ tel que $xBx^{-1} = B$. Alors $x \in N_B T$. Donc pour tout $t \in T$, $xtx^{-1}t^{-1} \in (B, B) \cap T = e$. D'où $x \in Z_G T$. **Q.e.d.**

Exercice : si $|W| = 1$, alors G est résoluble *(indication : soit B un sous-groupe de Borel qui contient T ; alors si* $\dim G/B > 0$*, T a au moins* 2 *points fixes dans G/B (pour cela, on choisit une représentation rationnelle de dimension finie V de G telle que G/B est isomorphe à une orbite fermée de $\mathbb{P}(V)$, et un sous-groupe à un paramètre $\nu : \mathbb{G}_m \to T$ tel que si $\chi_1, ..., \chi_n$ sont les caractères propres de T dans V, $\forall i \neq j$, $\chi_i \circ \nu \neq \chi_j \circ \nu$ (c'est possible ! (exo)) et on utilise la démonstration de la proposition 9.2.1).*

8.6 Radical

Soit G un groupe algébrique. Le *radical* de G, noté $R(G)$ est le plus grand sous-groupe fermé, connexe, résoluble et distingué de G. Le *radical unipotent* de G, noté $R_u(G)$ est le plus grand sous-groupe fermé, connexe, unipotent de G.

On dit que G est *semisimple* si $RG = e$, réductif si $R_u G = 1$.

Exercice : $R(G)$ et $R_u(G)$ existent et $R_u G = (RG)_u$. De plus, on a :

$$R(G) = \langle S \subseteq G \ : \ S \text{ est fermé, connexe, résoluble et distingué } \rangle \ .$$

On a aussi : $R(G) = \left(\bigcap_{\substack{B \leq G \\ \mathrm{sous-groupe\,de\,Borel}}} B\right)^0$.

Exercice : Soit G un sous-groupe fermé de $\mathrm{GL}(V)$ qui agit irréductiblement sur V (*i.e.* 0 et V sont les seuls sous-espaces $G-$invariants de V).

En considérant

$$V^{R_u(G)} = \{v \in V \;:\; \forall\, g \in R_u(G),\, g(v) = v\}$$

montrer que G est réductif.

Exemple : GL_n est réductif, $\mathbb{G}_m^n$ aussi mais non B_n (si $n > 1$) ; SL_n est semisimple.

Proposition 8.6.1 *Si G est réductif, alors RG est un tore contenu dans le centre de G^0*

Démonstration : On utilise la rigidité des tores. **Q.e.d.**

Lemme 8.6.2 *G réductif connexe. Alors : $R(G) = Z(G)^\circ$. De plus, (G, G) est connexe et $R(G) \cap (G, G)$ est fini.*

Démonstration : Pour l'intersection finie, on suppose que G est un sous-groupe fermé de $\mathrm{GL}V$. Soient $\chi_1, ..., \chi_n$ les caractères propres de l'action de $(ZG)^0$ sur V. On a : $V = V_{\chi_1} \oplus ... \oplus V_{\chi_n}$. Et dans une bonne base de V, les matrices de RG sont des blocs diagonaux de diagonales constantes. Forcément, pour un élément de $(G, G) \cap RG$, les valeurs de ces diagonales constantes sont des racines de l'unité. **Q.e.d.**

Chapitre 9

Groupes réductifs

Dans ce chapitre, G est un groupe connexe.

9.1 Racines

Soit T un tore maximal de G. Soient $X := X^*T$ et $X^\vee := X_*T := \mathrm{Hom}(\mathbb{G}_m, T)$. Si $\lambda \in X$, $\nu \in X^\vee$, alors $\circ\, \nu : \mathbb{G}_m \to \mathbb{G}_m$ est un morphisme de groupes donc il existe un entier noté $\langle \lambda, \nu \rangle$, tel que :

$$\forall\, z \in \mathbb{G}_m,\ \lambda(\nu(z)) = z^{\langle \lambda, \nu \rangle}\ .$$

Soit $\widetilde{R} \subseteq X$ l'ensemble fini des craractères propres non nuls de T dans $\mathfrak{g}$ (T agit sur $\mathfrak{g}$ par la représentation adjointe). Si $\alpha \in \widetilde{R}$, on pose $T_\alpha := (\ker \alpha)^0$, c'est un sous-tore de codimension 1 de T. On note $G_\alpha := Z_G T_\alpha$ son centralisateur : c'est un sous-groupe fermé connexe de G. Si $\alpha \in \widetilde{R}$ est tel que G_α est non résoluble, on dit que α est une *racine de G par rapport à T*. On note $R(G,T)$ l'ensemble des racines.

Lemme 9.1.1 *i) Le groupe G est engendré par les G_α, $\alpha \in \widetilde{R}$.*
ii) Si tous les G_α sont résolubles, alors G aussi.

Démonstration : *i*) En effet, l'algèbre de Lie de G est engendré par les sous-algèbres de Lie des G_α.

ii) Soit B un sous-groupe de Borel de G contenant T. D'après le théorème 8.5.4, B contient G_α si G_α est résoluble. Donc $G = B$ est résoluble si tous les G_α le sont. **Q.e.d.**

9.2 Le groupe de Weyl

Soit T un tore maximal de G. Soit $W := W(G,T) := N_G T / Z_G T$ le groupe de Weyl. C'est un groupe fini. Si S est un sous-tore de T, alors

$W(Z_G S, T)$ est un sous-groupe de W. De plus si S est contenu dans le centre de G, la surjection canonique : $G \to G/S$ induit un isomorphisme : $W(G,T) \to W(G/S, T/S)$ (en effet : si $n \in G$ est tel que $\forall\, t$, $ntn^{-1} = t \bmod S$, alors $\forall\, t$, $ntn^{-1}t^{-1} \in S \cap (G,G)$. Or, $S \cap (G,G)$ est fini (*cf.* la démonstration du lemme 8.6.2). Donc l'image de $T \to S \cap (G,G)$, $t \mapsto ntn^{-1}t^{-1}$ est réduite à un point : e. D'où$ntn^{-1} = t$ ($\forall\, t \in T$)).

Soit α une racine, le sous-tore T_α est central dans le groupe $G_\alpha = Z_G(T_\alpha)$. D'après ce qui précède, le groupe de Weyl $W_\alpha := W(G_\alpha, T)$ est un sous-groupe de W isomorphe à $W(G_\alpha/T_\alpha, T/T_\alpha)$.

De plus $\dim T/T_\alpha = 1$.

Exercice :

a) Le groupe W agit fidèlement et transitivement sur l'ensemble des sous-groupes de Borel de G qui contiennent T.

b) Soit B un sous-groupe de Borel de G contenant T ; il y a une bijection : $W \overset{1:1}{\leftrightarrow} (G/B)^T$, $w \mapsto wB$.

9.2.1 Rang un

On suppose que G n'est pas résoluble et que $\mathrm{rang} G = 1$.

Soit T un tore maximal de G et B un sous-groupe de Borel contenant T.

Proposition 9.2.1 *i) Le groupe de Weyl W de (G,T) est d'ordre 2 ;*

ii) si B est un sous-groupe de Borel, alors $\dim G/B = 1$.

Démonstration : i) Comme $\mathrm{Aut}\mathbb{G}_m$ est d'ordre 2, $|W| \leq 2$.

Il y a une bijection entre W et les $T-$points fixes de G/B : $w \mapsto wB$.

Comme G n'est pas résoluble, $\dim G/B > 0$. Pour finir de montrer *i*), on va montrer que G/B a au moins 2 points fixes en montrant *ii*).

ii) : Fixons $\lambda : \mathbb{G}_m \to T$ un isomorphisme. Soient $r : G \to V$ une représentation de G et $v \in V$ tels que B est le groupe d'isotropie de $[v] \in \mathbb{P}V$ et $G/B \simeq G.[v]$, $gB \mapsto [r(g)v]$. On identifiera G/B à l'orbite $G.[v]$ (qui est fermée dans $\mathbb{P}(V)$. On suppose aussi que V est engendré par les $r(g)v$, $g \in V$. Soit $e_1, ..., e_n$une base de $T-$vecteurs propres de V. On suppose que : $r(\lambda(a))e_i = a^{m_i}$ pour tout $a \in \mathbb{G}_m$, pour tout i et pour certains entiers $m_1 \geq ... \geq m_n$. Soit $0 \neq x \in V$ tel que $[x] \in G/B \setminus (G/B)^T$. Il existe $1 \leq i_0 < i_\infty \leq n$ tel que :

$$x = x_{i_0} e_{i_0} + ... + x_{i_\infty} e_{i_\infty}$$

où les ... sont des $x_i e_i$ avec $i_0 < i < i_\infty$ et où $x_{i_0}, x_{i_\infty} \neq 0$. On pose alors $\lambda(0).x := x_0 := x_{i_0}$ et $\lambda(\infty).x := x_\infty := x_{i_\infty}$. Le morphisme $\mathbb{G}_m \to \mathbb{P}(V)$, $a \mapsto [\lambda(a).x]$ se prolonge en un morphisme $\mathbb{P}^1 \to \mathbb{P}(V)$:

$$[u:v] \mapsto \begin{cases} [\lambda(v/u).x] & \text{si } u \neq 0, \\ [\lambda(\infty).x] & \text{si } u = 0. \end{cases}$$

Comme $[x] \in G/B$, alors $[\lambda(0).x]$ et $[\lambda(\infty).x] \in G/B$. On obtient deux $T-$points fixes : $[\lambda(0).x], [\lambda(\infty).x] \in G/B$. Soit l une forme linéaire sur V qui vaut 1 en x_∞ et 0 en x_0. Soit $F := \{[x] \in G/B \; : \; l(x) = 0\}$. Les composantes de F sont $T-$stables. Si l'une de ces composantes est de dimension > 0, alors on peut trouver deux $T-$points fixes de G/B distincts de $[x_\infty]$: absurde car G/B a seulement 2 points fixes. Or, l permet de définir une fonction régulière sur un voisinage ouvert de $[x_0]$: $f : G/B - - > \mathbb{A}^1$, $[y] = [y_1 e_1 + ... + y_n e_n] \mapsto \frac{l(y)}{y_{i_0}}$. Comme f n'est pas constante (car sinon $G.v \leq \ker l < V$), f est dominant et comme $f^{-1}f([x_0]) \subseteq F$ est fini, on a $\dim G/B = 1$ (*cf.* le lemme 6.2.7). **Q.e.d.**

9.2.2 Action du groupe de Weyl sur les racines

Le groupe de Weyl $W = N_G T / Z_G T$ agit sur T par conjugaison, on en déduit une action sur X (et sur $X^\vee$) qui laisse stable $R(G,T)$. Si $\alpha \in R$, on choisit $n_\alpha \in N_{G_\alpha} T \setminus Z_{G_\alpha} T$ et on pose $s_\alpha := n_\alpha \bmod Z_G T \in W$.

Posons $V := \mathbb{R} \otimes X$ et $V^\vee := \mathbb{R} \otimes X^\vee$. La paire de dualité $\langle \cdot, \cdot \rangle$ s'étend à $V \times V^\vee$.

Il est commode d'introduire une forme bilinéaire définie positive sur V qui est $W-$invariante :

$$(\cdot, \cdot) : V \times V \to V \ .$$

Lemme 9.2.2 *i) Il existe un unique $\alpha^\vee \in V^\vee$ tel que $\langle \alpha, \alpha^\vee \rangle = 2$ et :*

$$\forall\, x \in X,\; s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha \ .$$

ii) Si β est une racine, et si $G_\alpha = G_\beta$, alors $s_\beta = s_\alpha$.

Démonstration : Pour i) : on a $s_\alpha^2 = 1$ dans W_α donc $v \mapsto s_\alpha(v)$ est une réflexion orthogonale pour le produit scalaire $(\cdot,\cdot)$. Or, $\ker s_\alpha - 1$ est un hyperplan. En effet, montrons que $\mathrm{rang}(s_\alpha - 1) = 1$. Dans T/T_α, on a : $n_\alpha t n_\alpha^{-1} = t^{-1}$ donc $s_\alpha \alpha = -\alpha$. Or, $\ker(s_\alpha - 1) \oplus \ker(s_\alpha + 1) = V$ et donc $\mathrm{rang}(s_\alpha - 1) > 0$. Soit $\chi \in X$. Posons $(s_\alpha - 1)(\chi) = \chi'$. On a : $\forall\, t \in T_\alpha$, $\chi'(t) = \chi(n_\alpha t n \alpha^{-1} t^{-1}) = 1$ car T_α est central dans G_α. Mais alors $t_\alpha \leq \ker \chi'$. Or $X^*(T/T_\alpha)$ est un groupe abélien libre de rang 1 où α est non nul. Donc $\chi' \in \mathbb{R}\alpha$ (dans V). Donc $\mathrm{rang}(s_\alpha - 1) = 1$. Comme s_α est une réflexion orthogonale (par rapport à un hyperplan, comme $s_\alpha \alpha = -\alpha$, on a :

$$s_\alpha x = x - 2\frac{(x,\alpha)}{(\alpha,\alpha)}\alpha \ .$$

Il suffit alors de poser $\alpha^\vee \in V^\vee$ l'unique élément tel que :

$$\langle \cdot, \alpha^\vee \rangle = \frac{2}{(\alpha,\alpha)}(\alpha, \cdot) \ .$$

Q.e.d.

Théorème 9.2.3 *Le groupe de Weyl W est engendré par les s_α.*

Démonstration : On raisonne par récurrence sur $\dim G$.
Soit $w \in W$ représenté par $x \in N_G T$. On considère :

$$\psi : T \to T,\ t \mapsto xtx^{-1}t^{-1} \ .$$

1er cas : Comme on l'a déjà vu dans la démonstration de la proposition 9.2.1, ψ est un morphisme de groupes. Si $\mathrm{im}\,\psi < T$, alors posons $S := (\ker \psi)^0$. Si $Z_G S < G$, par hypothèse de récurrence, $W(Z_G S, T)$ est engendré par les s_α ; or, $w \in W(Z_G S, T) \leq W(G,T)$. Si $Z_G S = G$, alors S est central et on peut appliquer l'hypothèse de récurrence à G/S.

2ème cas : Si ψ est surjective, alors $w - 1 : V \to V$ est injective (car $w - 1 = 1 \otimes \psi^*$) donc bijective. Soit α une racine. Il existe $v \in V$ tel que $(w-1)v = \alpha$. Alors :

$$(v,v) = (wv,wv) = (v+\alpha, v+\alpha) = (v,v) + 2(v,\alpha) + (\alpha,\alpha)\,,$$

d'où : $s_\alpha v = v + \alpha = wv$. Donc $s_\alpha w$ a 1 comme valeur propre et on est ramené au premier cas. **Q.e.d.**

Remarque : on rappelle que le groupe de Weyl est fini.

Lemme 9.2.4 *Si $\alpha \neq \beta$ sont des racines non proportionnelles, alors :*

i) $0 \leq \langle \alpha, \beta^\vee \rangle \langle \beta, \alpha^\vee \rangle \leq 3$.

ii) $|\langle \alpha, \beta^\vee \rangle| > 1 \Rightarrow |\langle \beta, \alpha^\vee \rangle| = 1$.

iii) $\langle \alpha, \beta^\vee \rangle = 0 \Leftrightarrow \langle \beta, \alpha^\vee \rangle = 0$.

Démonstration : On considère la matrice de$s_\alpha s_\beta$, vu comme automorphisme du sous-espace engendré par α, β dans $\mathbb{R} \otimes_{\mathbb{Z}} X$, dans la base α, β :

$$M_{\alpha,\beta} \begin{pmatrix} \langle \alpha, \beta^\vee \rangle \langle \beta, \alpha^\vee \rangle - 1 & \langle \beta, \alpha^\vee \rangle \\ -\langle \alpha, \beta^\vee & -1 \end{pmatrix} \ .$$

Or W est fini donc $M_{\alpha,\beta}$ est d'ordre fini. Donc ses valeurs propres sont de module 1 et la $|\mathrm{Tr} M_{\alpha,\beta}| \leq 2$. De plus, $s_\alpha \neq s_\beta$ donc les valeurs propres ne sont pas toutes égales à 1 ... **Q.e.d.**

9.3 Groupes semisimples de rang un

On fixe $n \in N_G T \setminus Z_G T$ un relevé de l'élément non trivial de W. On a $ntn^{-1} = t^{-1}$ pour tout $t \in T$ et $n^2 \in Z_G T$. Posons $U := B_u$.

Lemme 9.3.1 *i) G est l'union disjointe de B et UnB ;*

ii) $\dim U/U \cap nUn^{-1} = 1$ *;*

iii) $RG = (U \cap nUn^{-1})^0$.

Démonstration : *i)* : Soit $x := B/B$. Comme $nx \neq x$, x et nx sont les deux points fixes de T dans G/B. Comme $n^{-1}Bn \neq B$, $Unx \neq nx$. Or Unx est connexe et contient nx donc Unx est ouvert dans G/B (car $\dim G/B = 1$). Donc $S := G/B \setminus Unx$ est fini. Or T normalise U, donc T laisse fixe chaque point de S. Mais alors $G/B \setminus Unx = \{x\}$ *i.e.* $G = B \cup UnB$.

ii) : Comme $U \cap nUn^{-1}$ est le sous-groupe d'isotropie de nx dans U, on a $\dim U/nUn^{-1} = \dim Unx = 1$.

iii) : Le groupe $(U \cap nUn^{-1})^0$ est distingué dans U d'après *ii)* et l'exercice ci-dessous. Comme T et n normalisent U , aussi, le groupe $(U \cap nUn^{-1})^0$ est distingué dans G. Donc $(U \cap nUn^{-1})^0 \leq R(G)$ qui est la composante neutre de l'intersection de tous les sous-groupes de Borel de G.

Or $R(G)$ ne contient pas de tore (sinon pour des raisons de dimension, $T \leq R(G)$ mais alors l'image de T dans $G/R(G)$ est trivial et donc $G/R(G)$ a pour tore maximal le tore trivial (*cf.* le corollaire 8.4.1.1) ; mais alors G/RG serait unipotent donc résoluble et donc G aussi serait résoluble : *absurde !*). Donc $R(G) = (U \cap nUn^{-1})^0$. **Q.e.d.**

Exercice : soit G un groupe unipotent connexe et H un sous-groupe fermé connexe propre de G. Alors $H < N_G H$ *(indication : raisonner par récurrence sur* $\dim G$*, on rappelle que* $\dim Z(G) > 0$*, considérer* $Z(G)H$*).*

On note $\mathfrak{g}$ l'algèbre de Lie de G et $\mathfrak{t}$ celle de T.

Lemme 9.3.2 *On suppose que G est semisimple de rang* 1.

i) $\dim U = 1$*,* $Z_G T = T$*,* $U \cap nU^{-1} = e$ *;*

ii) il existe un unique poids α de T dans $\mathfrak{g}$, tel que :

$$\mathfrak{g} = \mathfrak{t} \oplus \mathfrak{g}_{-\alpha} \oplus \mathfrak{g}_\alpha$$

$$\mathrm{Lie}(U) = \mathfrak{g}_\alpha,\ \mathrm{Lie}(nUn^{-1}) = \mathfrak{g}_{-\alpha}\ .$$

iii) L'application produit : $(u, b) \mapsto unb$ est un isomorphisme de variétés $U \times B \to UnB = G - B$.

Démonstration : *i)* D'après le lemme précédent, $\dim U = 1$. Donc $\dim B = 2$. De plus, $U \cap nUn^{-1}$ est fini et unipotent. Or T normalise ce groupe fini, T est connexe donc $U \cap nUn^{-1} \subseteq Z_G T$. Or $Z_G T$ est connexe et contenu dans B. Comme $\dim B = 2$, $Z_G T = T$ ou B. Le deuxième cas est impossible (sinon B est nilpotent et alors $G = B$). Donc $Z_G T = T$ et $U \cap nUn^{-1} \leq T \Rightarrow U \cap nUn^{-1} = e$.

ii) : Soit $u : \mathbb{G}_a \to U$ un isomorphisme. Il existe $\alpha \in X^*T$ tel que :

$$\forall\, a \in \mathbb{G}_a, \forall\, t \in T,\ tu(a)t^{-1} = u(\alpha(t)a)\ .$$

Le caractère α est non trivial car $Z_G T = T$.

Soit X un élément non nul de $\mathrm{im}\, du$. On a :

$$\forall\, t \in T,\ \mathrm{Ad}tX = \alpha(t)X,\ \mathrm{Ad}t\mathrm{Ad}nX = \alpha(t)^{-1}\mathrm{Ad}nX\ .$$

En effet, $u^{-1} \circ \mathrm{ad}(t) \circ u : \mathbb{G}_a \to \mathbb{G}_a$ est la multiplication par $\alpha(t)$ ($t \in \mathbb{G}_m$ fixé). Donc :

$$du|_0{}^{-1} \circ \mathrm{Ad}(t) \circ du|_0\ : \mathrm{Lie}(\mathbb{G}_a) \to \mathrm{Lie}(\mathbb{G}_a)$$

est aussi la multiplication par $\alpha(t)$. De plus, $\mathrm{Ad}(t)\mathrm{Ad}(n) = \mathrm{Ad}(n)\mathrm{Ad}(n^{-1}tn) = \mathrm{Ad}(n)\mathrm{Ad}(t^{-1})$.

Comme UnB est ouvert dans G, $\dim G \leq 3$. Or, $\mathfrak{t} \oplus kX \oplus k\mathrm{Ad}nX \leq \mathfrak{g}$. Donc $\dim \mathfrak{g} = \dim G = 3$.

iii) : L'application $n^{-1}Un \times B \to n^{-1}UnB$, $n^{-1}un, b \mapsto n^{-1}unb$ est bijective d'après i et de plus, sa différentielle est aussi bijective d'après *ii)*. C'est $n^{-1}Un \times B-$équivariant, on en déduit que c'est un isomorphisme. **Q.e.d.**

Théorème 9.3.3 *Soit G un groupe connexe semisimple de rang* 1*, alors* $G \simeq \mathrm{SL}_2$ *ou* PGL_2.

Démonstration : On a $\dim U = 1$, $\dim T = 1$. On fixe des isomorphismes :

$$t : \mathbb{G}_m \to T,\ x \mapsto t(x),\ u : \mathbb{G}_a \to U,\ y \mapsto u(y)\ .$$

Il existe $m \in \mathbb{Z}$ tel que $\forall x \in \mathbb{G}_m$, $\forall y \in \mathbb{G}_a$, $t(x)u(y)t(x^{-1}) = u(x^m y)$, $nt(x)n^{-1} = t(x^{-1})$. Soit ϵ tel que $t(\epsilon = n^2$. Alors $nt(\epsilon)n^{-1} = t(\epsilon) \Rightarrow \epsilon = \pm 1$. On a un isomorphisme de variétés :

$$\mathbb{G}_a \times \mathbb{G}_m \times \mathbb{G}_a \to G \setminus B,\ x, y, z \mapsto u(x)nt(y)u(z)\ .$$

Or, $nu(y)n^{-1} \notin U$ si $y \neq 0$ d'après 9.3.2. Donc :

$$\forall\, y \neq 0,\ nu(y)n^{-1} = u(f(y))nt((g(y))u(h(y)) \tag{9.1}$$

pour certaines fonctions rationnelles non nulles $f, g, h \in k[y, y^{-1}]$.

On conjugue (9.1) par $t(z)$ et on obtient :

$$nu(z^{-m}y)n^{-1} = u(z^m f(y))nt(z^{-2}g(y))u(z^m h(y))$$

d'où :

$$f(z^{-m}y) = z^m f(y),\ g(z^{-m}y) = z^{-2}g(y),\ h(z^{-m}y) = z^m h(y)\ .$$

Donc : $g(y^m) = y^2 g(1)$, $f(y) = ay^{-1}$, $h(y) = by^{-1}$ pour certains $a, b \in k$. En particulier, $m = 1$ ou 2. En prenant l'inverse des deux membres de (9.1), on trouve que : $a = b$ et $g(-y) = \epsilon g(y)$. Comme $n \notin B$, $a, b \neq 0$. Quitte à changer n en $nt(y_0)$ pour un certain y_0, on peut supposer que $a = b = -1$.

Si $m = 1$, alors $g(y) = cy^2$ pour un certain $c \in k^\times$ et $\epsilon = 1$; si $m = 2$, alors $g(y) = cy$ pour un certain $c \in k^\times$ et $\epsilon = -1$.

On a donc :

$$\forall\, y \neq 0,\ nu(y)n^{-1} = u(-y^{-1})nt(g(y))u(-y^{-1})\ . \tag{9.2}$$

En remarquant que :

$$nu(y+1)n^{-1} = nu(y)n^{-1}nu(1)n^{-1}$$

on trouve :

$$g(y)^m = y^2\ .$$

Si $m = 2$, on a $g(y) = \eta y$ avec $\eta = \pm 1$. Quitte à remplacer n par $nt(\eta)$, on a : $g(y) = y$.

On peut donc supposer que l'on a les relations :

$$\forall\, y \neq 0,\ nu(y)n^{-1} = u(-y^{-1})nt(y^{m'})u(-y^{-1}),\ n^2 = t((-1)^{m'}$$

$$\forall x, y \in \mathbb{G}_a,\ \forall z \in \mathbb{G}_m,\ u(x+y) = u(x)u(y),\ t(zw) = t(z)t(w),\ t(z)u(x)t(z)^{-1} = u(z^m x)$$

où $mm' = 2$.

Ces relations déterminent la structure de groupe de G.

Soit $G_1 := \mathrm{SL}_2$. On note T_1 les sous-groupe des matrices diagonales de G_1, B_1 le sous-groupe des matrices triangulaires supérieures de G_1, U_1 le sous-groupe des matrices triangulaires supérieures à diagonale constante 1 de G_1et n_1 la matrice :

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\ .$$

On a $G \setminus B_1 = U_1 n_1 B_1$ et des isomorphismes de variétés :

$$\begin{array}{ccccc} G_1 \setminus B_1 & \longleftarrow & \mathbb{G}_m \times \mathbb{G}_a \times \mathbb{G}_m & \longrightarrow & G \setminus B \\ u_1(x)n_1t_1(y)u_1(z) & \longleftarrow\!\shortmid & x, y, z & \longmapsto & u(x)nt(y)u(z) \end{array}$$

où

$$u_1(x) := \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \; t_1(y) = \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix} .$$

qui induisent un morphisme surjectif de groupes $\phi : G_1 \to G$. De plus, si $m = 2$, ϕ est un isomorphisme sur l'ouvert $U_1 n B_1$ et donc sur tous ses translatés donc $\mathrm{SL}_2 \simeq G$. Si $m = 1$, on montre que $G \simeq \mathrm{PGL}_2$.

Q.e.d.

Lemme 9.3.4 *Pour tout $\alpha \in R$, Il existe un unique $\alpha^\vee \in X^\vee$ tel que :*

$$\forall\, x \in X,\; s_\alpha.x = x - \langle x, \alpha^\vee \rangle \alpha$$

$$\forall\, x^\vee \in X^\vee,\; s_\alpha.x^\vee = x^\vee - \langle \alpha, x^\vee \rangle \alpha^\vee$$

de plus, $\langle \alpha, \alpha^\vee \rangle = 2$ et $s_\alpha^2 = 1$ et $\mathrm{im}\, \alpha^\vee \leq (G, G)$.

Démonstration : On montre que dans le lemme 9.2.2, on a $\alpha^\vee \in X$. Pour cela, on peut supposer que $G = G_\alpha$ et que G est réductif. Alors comme les tores maximaux de G sont conjugués, on peut supposer que T contient un tore maximal T_1 de $G_1 := (G, G)$. Comme $R(G) = (\ker \alpha)^0$ et comme $R(G) \cap (G, G)$ est fini, G_1 est semisimple de rang 1. Soit $\alpha_1^\vee : \mathbb{G}_m \to T_1$ un isomorphisme. On peut considérer $\alpha_1^\vee$ comme un élément de $X^\vee$. Il résulte de la démo du théorème 9.3.3 que $\langle \alpha, \alpha_1^\vee \rangle = \pm 1$ ou ± 2. Or on a : $s_{\alpha_1}(t) = t^{-1}$ donc :

$$\alpha_1^\vee - \langle \alpha, \alpha_1^\vee \rangle \alpha^\vee = -\alpha_1^\vee$$

d'où $\alpha^\vee = \pm \alpha_1^\vee$ ou $\pm 2\alpha_1^\vee$.

Q.e.d.

Soit B un sous-groupe de Borel de G contenant T dont l'algèbre de Lie est $\mathfrak{t} \oplus \mathfrak{g}_\alpha$.

Corollaire 9.3.4.1 *Soit $f \in k[G]$ dont la restriction à (G, G) n'est pas constante. On suppose qu'il existe χ un caractère de B tel que $f(gb) = \chi(b) f(g)$ pour tout $g \in G$ et tout $b \in B$. Alors, $\langle \chi, \alpha^\vee \rangle > 0$.*

9.4 Données radicielles

Une donnée radicielle est un quadruplet $(X, R, X^\vee, R^\vee)$ où : X et $X^\vee$ sont des réseaux en dualité :

i.e. :

$$X \times X^\vee \to \mathbb{Z}$$

$$(x, x^\vee) \mapsto \langle x, x^\vee \rangle$$

est bilinéaire et induit des isomorphismes : $X \simeq \hom_{\mathbb{Z}}(X^\vee, \mathbb{Z})$, $X^\vee \to \hom_{\mathbb{Z}}(X, \mathbb{Z})$; où R et $R^\vee$ sont des parties finies respectivement de X et $X^\vee$ en bijection :

$$R \overset{1:1}{\leftrightarrow} R^\vee$$

$$\alpha \mapsto \alpha^\vee$$

tels que d'une part $\langle \alpha, \alpha^\vee \rangle = 2$ pour tout $\alpha \in R$ et si l'on pose :

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha \text{ et } s_\alpha(x^\vee) = x^\vee - \langle \alpha, x^\vee \rangle \alpha^\vee$$

on ait :

$$s_\alpha(R) = R \text{ et } s_\alpha(R^\vee) = R^\vee \ .$$

Remarque : on a automatiquement $s_\alpha^2 = 1$ et $s_\alpha \alpha = -\alpha$.

9.4.1 Systèmes de racines

Soit $\Psi := (X, R, X^\vee, R^\vee)$ une donnée radicielle. On suppose $R \neq \emptyset$. On note Q le sous-groupe de X engendré par R et $V := Q \otimes \mathbb{R}$. Alors $R (= R \otimes 1)$ est un système de racine de V au sens où :

1) R est fini et engendre V ;
2) si $\alpha \in R$, il existe $\alpha^\vee \in V^\vee$, le dual de V, tel que : $\langle \alpha, \alpha^\vee \rangle = 2$ et $s_\alpha := \mathrm{Id} - \langle \cdot, \alpha^\vee \rangle \alpha$ laisse stable R ;
3) si $\alpha, \beta \in R$, $\langle \alpha, \beta^\vee \rangle \in \mathbb{Z}$.

Proposition 9.4.1 *Soit G un groupe réductif connexe non résoluble et T un tore maximal de G. Soit $R(G, T)$ l'ensemble des racines de (G, T). Soit Q le sous-groupe de X^*T engendré par $R(G, T)$ et $V := \mathbb{R} \otimes Q$. Alors $R(G, T)$ est un système de racines réduit de V (*i.e. *si $c\alpha \in R$ avec $\alpha \in R(G, T)$, $c \in \mathbb{Q}$, alors $c = \pm 1$).*

Soit R un système de racines d'un $\mathbb{R}-$espace vectoriel V. On note W le sous-groupe de $\mathrm{GL}(V)$ engendré par les s_α, $\alpha \in R$. Un *système de racines positives de* R est une partie R^+ de R telle que :

1) $R = R^+ \cup -(R^+)$;
2) pour toute famille finie de racines $\alpha_i \in R^+$, et toute famille d'entiers $n_i > 0$, $\sum_i n_i \alpha_i \neq 0$.

Si R^+ est un système de racines positives, il existe une unique partie $D \subseteq R^+$ telle que tout élément de R^+ est une combinaison linéaire à coefficients entiers ≥ 0 d'éléments de D ; on dit que D est la base de R associée à R^+. Dans ce cas, W est engendré par les s_α, $\alpha \in D$.

9.5 Caractérisation du radical unipotent

Exercice. Soit $G = \mathrm{SL}_2$. On note B le sous-groupe de G formé des matrices triangulaires supérieures. Soit $f \in k[G]$ telle que :

$$\forall\, g \in G,\, \forall\, b \in B,\; f(gb) = \chi(b)f(g)$$

pour un certain caractère χ de B. Alors, montrer que :

$$\forall\, x \in k^{\times},\, \forall\, y\; ink,\; \chi\left(\begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix}\right) = x^m$$

pour un certain entier $m \geq 0$. De plus $m > 0$ si f est non constante. Vérifier les mêmes résultats pour PGL_2 à la place de SL_2 (*cf.* l'examen partiel).

On fixe $T \leq G$ un tore maximal. Si α est une racine de (G, T), alors $G_\alpha/R(G_\alpha)$ est semisimple de rang 1. Donc :

$$\mathrm{Lie}(G_\alpha/R_u(G_\alpha)) = \mathrm{Lie}(Z_G T/Z_G T \cap R_u G_\alpha) \oplus kX_\alpha \oplus kX_{-\alpha},$$

où X_α, $X_{-\alpha}$ sont des vecteurs propres de α et $-\alpha$ respectivement. Si B est un sous-groupe de Borel de G contenant T, alors $B \cap G_\alpha$ est un sous-groupe de Borel de G_α. On a donc :

$$\mathrm{Lie}(B \cap G_\alpha/R_u(G_\alpha)) = \mathrm{Lie}(Z_G T/Z_G T \cap R_u G_\alpha) \oplus kX_\beta$$

où $\beta = \pm\alpha$. Soit $R^+(B)$ l'ensemble des β ainsi obtenus, α décrivant $R(G, T)$.

On pose $R := R(G, T)$.

Proposition 9.5.1 *$R^+(B)$ est un système de racines positives pour R* i.e. *$R = R^+(B) \cup -R^+(B)$ et une combinaison linéaire d'éléments de $R^+(B)$ à coefficients ≥ 0 non tous nuls est non nulle.*

Démonstration : Si $G = B$, il n'y a rien à montrer. Supposons $G \neq B$. Si $\alpha \in R$, alors posons $G_\alpha := Z_G(T_\alpha$ où $T_\alpha := (\ker \alpha)^0$.

Comme $B \cap G_\alpha$ est un sous-groupe de Borel de G_α, on a α ou $-\alpha \in R^+(B)$. Soit $r : G \to GL(V)$ un morphisme injectif de groupes algébriques (où V est un $k-$espace vectoriel de dimension finie) tel qu'il existe $0 \neq v \in V$ vérifiant $B = \{g \in G \;:\; gv \in kv\}$. Soit $\lambda : B \to \mathbb{G}_m$ le caractère avec lequel B agit sur kv. Soit l une forme linéaire sur V qui vaut 1 en v. On pose :

$$F : G \to k,\; g \mapsto F(g) := l(g.v)\ .$$

On a $F(gb) = \chi(b)F(g)$ pour tout $g \in g$, tout $b \in B$. Soit $\alpha \in R^+(B)$. On restreint au sous-groupe $G'_\alpha := (G_\alpha, G_\alpha)$ qui est isomorphe à SL_2 ou PGL_2, on a d'après l'exercice ci-dessus, $F(g\alpha^\vee(s)) = s^{\langle \chi, \alpha^\vee \rangle}F(g)$ avec $\langle \chi, \alpha^\vee \rangle \geq 0$.

Si $\langle \chi, \alpha^\vee \rangle = 0$ pour une certaine racine $\alpha \in R^+(B)$, alors F est constante sur G_α pour toute forme linéaire l. Donc $G_\alpha \leq B$ absurde car G_α n'est pas résoluble. On a donc $\forall\, \alpha \in R^+(B)$, $\langle \chi, \alpha^\vee \rangle > 0$.

Donc si on considère $V := \mathbb{R} \otimes_{\mathbb{Z}} X$ et $(\cdot, \cdot)$ un produit scalaire $W-$invariant sur V on a :

$$\forall\, \alpha \in R^+,\ (\chi, \alpha) > 0\ .$$

On en déduit l'existence d'un $\nu \in X_*(T)$ tel que $\forall\, \alpha \in R^+$, $\langle \alpha, \nu \rangle > 0$. On en déduit que si $\sum_{\alpha \in R^+} n_\alpha \alpha = 0$ pour certains entiers $n_\alpha \in \mathbb{N}$, alors :

$$\langle \sum_{\alpha \in R^+} n_\alpha \alpha, \nu \rangle = 0 \Rightarrow \forall\, \alpha n_\alpha = 0\ .$$

Q.e.d.

Théorème 9.5.2 *Soit G un groupe connexe et T un tore maximal de G. Alors, $R_u G = \left(\cap_{B \geq T} B_u\right)^0$ où B décrit les sous-groupes de Borel qui contiennent T.*

Démonstration : On utilise le lemme suivant

Lemme 9.5.3 *Soit R un système de racines avec R^+ un système de racines positives, soient $\alpha, \beta \in R$ deux racines non colinéaires. Il existe alors un $w \in W$ tel que $w\alpha, w\beta \in R^+$.*

Démonstration : On note $\delta > 0$ (*respectivement* $\delta < 0$) si $\delta \in R^+$ (*respectivement* $-R^+$). On peut supposer $\alpha < 0$ et $\beta > 0$ (quitte à échanger α et β ou à remplacer α, β par $s_\alpha \alpha, s_\alpha \beta$) et ensuite on peut supposer que $s_\alpha \beta < 0$ en particulier, $\langle \beta, \alpha^\vee \rangle < 0$.

Soit $a := \langle \alpha, \beta^\vee \rangle \langle \beta, \alpha^\vee \rangle$. On sait que $a = 0, 1, 2$ ou 3. Si $a = 0$, $w = s_\alpha$ convient.

Si $a = 1$, $w = s_\alpha s_\beta$ convient.

Si $a = 2, 3$, alors $(s_\alpha s_\beta)^a = -1$ (considérer la matrice $M_{\alpha,\beta}$ comme dans le lemme 9.2.4). Donc on peut si nécessaire remplacer α, β par $-\beta, -\alpha$ et supposer que :

$$\langle \alpha, \beta^\vee = -1 \text{ et } \langle \beta, \alpha^\vee \rangle = -a\ .$$

Si $a = 2$, alors on prend $w = s_\alpha$ si $2\alpha + \beta > 0$, $w = -s_\beta$ si $\alpha + \beta < 0$, $w = s_\alpha s_\beta$ sinon.

Si $a = 3$, $w = s_\alpha, -s_\beta, s_\alpha s_\beta, -s_\beta s_\alpha$ ou $s_\alpha s_\beta s_\alpha$ convient.

Si $a =$

Q.e.d.

Q.e.d.

Corollaire 9.5.3.1 *Soit S un sous-tore fermé de G. Alors $R_u(Z_G S) \subseteq R_u G$. En particulier, si G est réducif, $Z_G S$ aussi.*

Corollaire 9.5.3.2 *Soit G un groupe réductif. Si T est un tore maximal de G, alors $Z_G T = T$* i.e. *les sous-groupes de Cartan et les tores maximaux coïncident.*

Proposition 9.5.4 *Soit G un groupe réductif connexe. Soit R l'ensemble des racines de (G, T). On note $\mathfrak{g}$ l'algèbre de Lie de G.*

i) *Pour tout $\alpha \in R$, il existe un unique sous-groupe fermé U_α tel qu'il existe un isomorphisme $x_\alpha : \mathbb{G}_a \to U_\alpha$ vérifiant :*

$$\forall\, t \in T, a \in k,\ t x_\alpha(a) t^{-1} = x_\alpha(\alpha(t)a) \ ;$$

de plus, $\operatorname{im} du_\alpha = \mathfrak{g}_\alpha$, *l'espace propre de $\mathfrak{g}$ de poids α.*

ii) *T et les U_α, $\alpha \in R$ engendrent G.*

Les U_α sont les *groupes radiciels* de G.

Corollaire 9.5.4.1 *Les racines de R sont les poids non nuls de T dans l'algèbre de Lie de G et* $\dim \mathfrak{g}_\alpha = 1$ *pour tout $\alpha \in R$;*

Corollaire 9.5.4.2 *Soit B un sous-groupe de Borel de G contenant T. Soit $\alpha \in R$. On note $\mathfrak{b}$ l'algèbre d Lie de B.*

i) *Sont équivalentes : a) $\alpha \in R^+(B)$, b) $X_\alpha \leq B$, c) $\mathfrak{g}_\alpha \leq \mathfrak{b}$;*

ii) *soit $r := \dim T$ le rang de G ; alors :* $\dim B = r + \frac{|R|}{2}$, $\dim G = r + R$.

9.5.1 Groupes semisimples

Théorème 9.5.5 *Soit G un groupe semisimple connexe.*

i) *Les U_α engendrent G ;*

ii) *$(G, G) = G$;*

iii) *l'ensemble des sous-groupes fermé distingués de G de dimension > 0 minimale est fini ; notons le $G_1, ..., G_n$;*

iv) *pour tous $i \neq j$, $(G_i, G_j) = e$;*

v) *l'application produit $G_1 \times ... \times G_n \to G$ est surjective de noyau fini.*

Corollaire 9.5.5.1 *Soit G un groupe réductif connexe. Alors $G = R(G).(G, G)$ et (G, G) est semisimple.*

Démonstration : On remarque que $G/R(G)$ est semisimple donc $(G/R(G), G/R(G)) = G/R(G)$. **Q.e.d.**

Soit $(X, R^\vee, X^\vee, R^\vee)$ une donnée radicielle. On note Q le sous-groupe de X engendré par R. C'est le réseau radiciel.

Lemme 9.5.6 *Le groupe G est semisimple si et seulement si Q est d'indice fini dans X.*

Si G est semisimple soit $V := \mathbb{R} \otimes X$. On pose :

$$P := \{v \in V \ : \ \langle v, R^\vee \rangle \subseteq \mathbb{Z}\} \ .$$

C'est le *réseau des poids*. On a $Q \leq X \leq P$.

Remarque : P/Q est fini et le système de racines R étant fixé, il y a un nombre fini de posiibilités pour X.

On dit que G est *adjoint* si $X = Q$, *simplement connexe* si $X = P$.

Proposition 9.5.7 *Le groupe semisimple G est quasisimple si et seulement si R est irréductible. Dans ce cas, le centre de G est isomorphe à X/Q.*

9.6 Classification des groupes quasisimples

Un groupe connexe est *quasisimple* s'il n'a pas de sous-groupe fermé distingué de dimension > 0.

Soit G un groupe semisimple connexe. Soient B un sous-groupe de Borel de G et $T \leq B$ un tore maximal. Notons $R = R(G,T)$ le système de racines et $D \leq R$ la base associés.

On associe un graphe $\mathscr{D}$ à $G \geq B \geq T$:

a) les sommets sont les éléments de D.

b) deux sommets α, β sont reliés par $\langle \alpha, \beta^\vee \rangle \langle \beta, \alpha^\vee \rangle$ arêtes avec une flèche qui pointe de α vers β (*respectivement* dans l'autre sens) si $0 > \langle \alpha, \beta^\vee \rangle > \langle \beta, \alpha^\vee \rangle$ (*respectivement* si $\langle \alpha, \beta^\vee \rangle < \langle \beta, \alpha^\vee \rangle < 0$).

Remarque : d'après le lemme 9.2.4, $\langle \alpha, \beta^\vee \rangle \langle \beta, \alpha^\vee \rangle = 0, 1, 2$ ou 3.

9.7 Existence et unicité

Théorème 9.7.1 *i) (existence) : Soit Ψ une donnée radicielle. Il existe un groupe réductif connexe G et un tore maximal T de G tel que $\Psi = \Psi(G,T)$.*

ii) (unicité) : Soient G, G' deux groupes réductifs connexes, T, T' deux tores maximaux (respectifs). Si $f : \Psi(G,T) \to \Psi(G',T')$ est un isomorphisme de données radicielles, alors il existe un isomorphisme de groupes algébriques :

$$\phi : G \to G'$$

tel que $f = f(\phi)$. Si $\phi_1 : G \to G'$ est un autre isomorphisme tel que $f(\phi_1) = f(\phi) = f$, alors il existe un $t \in T$ tel que :$\phi_1(g) = \phi(tgt^{-1})$ pour tout $g \in G$.

9.8 Décomposition de Bruhat

9.8.1 Sous-groupes paraboliques associés à un sous-groupe à un paramètre

Soit G un groupe réductif *connexe*. Soit $\lambda : \mathbb{G}_m \to G$ un morhisme de groupes. Si P est un sous-groupe parabolique de G, on dit qu'un sous-groupe fermé $L \leq P$ est un *sous-groupe de Levi* si la muliplication : $L \times R_u P \to P$ est un isomorphisme de variétés.

Proposition 9.8.1 *i) L'ensemble de* $g \in G$ *tels que* $\mathbb{G}_m \to G$, $t \mapsto \lambda(t) g \lambda(t)^{-1}$ *se prolonge en un morphisme :* $\mathbb{A}^1 \to G$ *est un sous-groupe parabolique de* G *noté* $P(\lambda)$*. Si* $g \in P(\lambda)$*, on note* $\lim_{t\to 0} \lambda(t) g \lambda(t)^{-1}$ *l'image de* 0 *par le prolongement. Le centralisateur de* $\lambda(\mathbb{G}_m)$ *est un sous-groupe de Levi de* $P(\lambda)$ *et :*

$$R_u P(\lambda) = \{g \in G \ : \ \lim_{t \to 0} \lambda(t) g \lambda(t)^{-1} = e \ .\}$$

ii) Tous les sous-groupes paraboliques de G *sont de la forme* $P(\lambda)$*.*

Démonstration : Supposons que G est un sous-groupe fermé de GL_n. On peut supposer que ν est de la forme : $\nu : \mathbb{G}_m \to \mathrm{GL}_n, t \mapsto \mathrm{diag}(t^{a_1}, ..., t^{a_n})$ pour certains entiers a_i. Alors on a :

$$P(\nu) = \{g = (g_{i,j}) \in G \ : \ \forall\, i, j, \ a_i - a_j < 0 \Rightarrow g_{i,j} = 0\} \ .$$

Donc $P(\nu)$ est fermé dans G. Soit T un tore maximal de G qui contient $\nu(\mathbb{G}_m)$.

On a $P(\nu) \geq T$ donc $\mathrm{Lie}(P(\nu)$ est un sous-$T-$module de $\mathfrak{g}$ l'algèbre de Lie de G. Soit $R := R(G,T)$. Si α est une racine de (G,T), alors $U_\alpha \leq P(\nu) \Leftrightarrow \mathfrak{g}_\alpha \leq \mathrm{Lie}(P(\nu) \Leftrightarrow \langle \alpha, \nu \rangle \geq 0$. On en déduit que si on note $R(P)$ les racines de (P,T), alors $R(P) \cup -R(P) = R$; donc P est parabolique.

(ii) : Soit P un parabolique de G. On raisonne comme dans la démonstration de la porposition 9.5.1 : soient $r : G\mathrm{GL}(V)$ un morphisme injectif de groupes algébriques et $0 \neq v \in V$ tels que :

$$P = \{g \in G \ : \ r(g)v \in kv\} \ .$$

Soit χ le caractère avec lequel P agit sur kv.

Soient $T \leq B$ un tore maximal et un sous-groupe de Borel de P donc de G. Alors on vérifie que si $\alpha \in R(G,T)$, alors $\alpha \in R(P,T) \Leftrightarrow U_\alpha \leq P \Leftrightarrow \langle \chi, \alpha^\vee \rangle \geq 0$. Il existe certainement un sous-groupe à un paramètre ν de T tel que si $\alpha \in R$, $\langle \alpha, \nu \rangle \geq 0$(*respectivement* > 0) $\Leftrightarrow \langle \chi, \alpha^\vee \rangle \geq 0$(*respectivement* > 0). On a alors $P = P(\nu)$. **Q.e.d.**

Application : Construction de B^- et U^-.

Si G est réductif connexe et si $T \leq B$ sont un tore maximal et un sous-groupe de Borel. Notons R^+ le système positif de racines associé. Il existe un cocaractère ν de T tel que $\forall\, \alpha \in R^+$, $\langle \alpha, \nu \rangle > 0$.

Alors $B = P(\nu)$. On pose $B^- = P(-\nu)$. On a : $B^- \cap B = T$ et B^- est un sous-groupe de borel de G ; On note $U^- := B_u$.

Remarque : U^- est le sous-groupe de G engendré par les $U_{-\alpha}$, $\alpha \in R^+$ et B^- est le sous-groupe de G engendré par les $U_{-\alpha}$, $\alpha \in R^+$ et T.

9.8.2 Sous-groupes directement engendrés

Soit H un groupe et $H_1, ..., H_n$ des sous-groupes de H. On dira que H est *directement engendré* par $H_1, ..., H_n$ si la multiplication : $H_1 \times ... \times H_n \to H$ est un morphisme bijectif.

Remarque : si de plus, les H_i sont connexes et si la différentielle en $(1, ..., 1)$ est injective (donc surjective), alors $H_1 \times ... \times H_n \to H$ est un isomorphisme de variétés.

Soit G un groupe réductif connexe. On fixe T un tore maximal de G et $T \leq B$ un sous-groupe de Borel. On note $U := B_u$. Pour tout racine α de (G, T), on note U_α le sous-groupe unipotent fermé de dimension 1 de G d'algèbre de Lie $\mathfrak{g}_\alpha$.

Proposition 9.8.2 *Soit H un sous-groupe fermé de U, normalisé par T. Alors H est directement engendré par les U_α, où α décrit les racines de (G, T) telles que $\mathfrak{g}_\alpha \leq \mathfrak{h}$, l'algèbre de Lie de H. En particulier, H est connexe.*

Démonstration : On démontre par récurrence le lemme suivant :

Lemme 9.8.3 *Soit H un $T-$groupe unipotent connexe d'algèbre de Lie $\mathfrak{h}$ tel que :*

(i) $H^T = e$;

*(ii) les poids α de T dans $\mathfrak{h}$ sont tels que les noyaux connexes $T_\alpha := (\ker \alpha)^0$ sont deux à deux distincts (*i.e. *les poids α sont deux à deux non proportionnels) .*

Alors pour tout α poids de T dans $\mathfrak{h}$, $H_\alpha := Z_H(T_\alpha)$ est l'unique sous-groupe fermé de H d'algèbre de Lie $\mathfrak{h}_\alpha$ et H est directement engendré par les $H_\alpha := Z_H(T_\alpha)$ (peu importe l'ordre).

On commence par le cas où H est commutatif. On numérote les poids de T dans $\mathfrak{h}$; $\alpha_1, ..., \alpha_n$, ... **Q.e.d.**

Soit R^+ le système de racines positives de R défini par B. Si $\alpha \in R$, on notera $\alpha > 0$ si $\alpha \in R^+$. On note W le groupe de Weyl $N_G T/T$. On notera U^- le sous-groupe de G engendré par les $U_{-\alpha}$, $\alpha > 0$. On notera $R_w^+ := \{\alpha > 0 \,:\, w^{-1}\alpha > 0\}$, $R_w^- := \{\alpha > 0 \,:\, w^{-1}\alpha < 0\}$.

Corollaire 9.8.3.1 *i) Le groupe U est directement engendré par les U_α, $\alpha > 0$.*

ii) Si $w \in W$, on note $U_w := U \cap wUw^{-1}$ et $U'_w := U \cap wU^- w^{-1}$. Alors $U = U_w U'_w = U'_w U_w$ et U_w (respectivement U'_w) est engendré par les sous-groupes U_α, $\alpha \in R_w^+$ (respectivement R_w^-).

9.8.3 Racines simples

Soit $G \geq B \geq T$ un groupe réductif connexe, un sous-groupe de Borel et un tore maximal. Soit R^+ le système de racines associées. Soit Δ l'ensemble des racines de R^+ indécomposables : ce sont les *racines simples*.

Proposition 9.8.4 *i) Δ est une base de R au sens où :*

$$\forall\, \alpha \in R, \exists\,!\, (n_\delta)_{\delta\in\Delta} \in \mathbb{N}^\Delta \cup (-\mathbb{N})^\Delta,\ \sum_\delta n_\delta \delta = \alpha\ .$$

ii) Si $\alpha \in \Delta$, alors $s_\alpha(R^+ \setminus \{\alpha\}) = R^+ \setminus \{\alpha\}$.

iii) $W\Delta = R^+$.

iv) W est engendré par les s_α, $\alpha \in \Delta$.

v) $|w^{-1}R^+ \cap (-R^+)|$ est le plus petit entier l tel qu'il existe $\alpha_1, ..., \alpha_l \in \Delta$ vérifiant : $s_{\alpha_1}...s_{\alpha_l} = w$.

On note $l(w) := |w^{-1}R^+ \cap (-R^+)|$: c'est la *longueur* de w.

Démonstration : $i)$ il suffit de démontrer que les $\delta \in \Delta$ sont $\mathbb{Z}-$linéairement indépendants. Or si $\sum_\delta n_\delta \delta = 0$ pour certains entiers $n_\delta \in \mathbb{Z}$, on a :

$$\sum_{\substack{\delta \\ n_\delta > 0}} n_\delta \delta = \sum_{\substack{\delta \\ n_\delta < 0}} -n_\delta \delta$$

Notons λ de caractère. Soit $V := \mathbb{R} \otimes_{\mathbb{Z}} X$. Il existe un produit scalaire $W-$invariant sur V tel que pour tout $\lambda \in X$ et tout $\alpha \in R$, $\langle \lambda, \alpha^\vee \rangle = 2\frac{(\lambda,\alpha)}{(\alpha,\alpha)}$. On a $(\lambda, \lambda) > 0$ (si au moins un des coefficients $n_\delta \neq 0$) ; or, si $\alpha \neq \beta \in \Delta$, $(\alpha, \beta) \leq 0$. En effet, $s_\alpha(\beta) = \beta - 2\frac{(\beta,\alpha)}{(\alpha,\alpha)}\alpha \in R$; comme β et α sont indépendantes et indécomposables,, $s_\alpha(\beta) \in R^+$ et donc $(\beta, \alpha) \leq 0$. En particulier, on a :

$$(\lambda, \lambda) = \sum_{\substack{\delta,\delta' \\ n_\delta > 0,\, n_{\delta'} < 0}} -n_\delta n_{\delta'} (\delta, \delta') \leq 0$$

d'où la contradiction.

$ii)$: facile.

iii) Soit $\beta = \sum_{\delta\in\Delta} n_\delta \delta \in R^+$, avec $\forall \delta,\, n_\delta \in \mathbb{N}$. On montre par récurrence sur $N := \sum_\delta n_\delta$ qu'il existe $w \in W$ tel que $w\beta \in \Delta$. Comme $(\beta,\beta) > 0$, il existe au moins un $\delta_0 \in \Delta$ tel que $(\beta, \delta_0) > 0$ *i.e.* : $\langle \beta, \delta_0^\vee\rangle > 0$. Mais alors :

$$s_{\delta_0}\beta = \beta - \langle \beta, \delta_0^\vee\rangle \delta_0 \in R^+$$

si $\beta \neq \delta_0$. On a donc :

$$s_{\delta_0}\beta = (n_{\delta_0} - \langle \beta, \delta_0^\vee\rangle) + \sum_{\delta\neq\delta_0} n_\delta \delta$$

et $((n_{\delta_0} - \langle \beta, \delta_0^\vee\rangle) + \sum_{\delta\neq\delta_0} n_\delta < \sum_{\delta\in\Delta} n_\delta$. On peut donc appliquer l'hypothèse de récurrence à $s_\delta\beta$: il existe $w \in W$ tel que $ws_{\delta_0}\beta \in \Delta$.

iv) Soit $w \in W$. On montre par récurrence sur $N_w := |w^{-1}(R^+) \cap (-R^+)|$ que $w \in \langle s_\alpha \;:\; \alpha \in \Delta\rangle$. Si $n_w = 0$, alors $w^{-1}(R^+) = R^+$ donc $\forall\, \alpha \in R^+$, $w(\alpha) \in R^+$. Or, $w(R^+)$ est l'ensemble des poids non nuls de wBw^{-1}. On a donc $wBw^{-1} \geq B$ *i.e.* $w = 1$. Si $N_w > 0$, alors il existe $\delta \in \Delta$ tel que $w^{-1}\delta \in -R^+$. Alors d'après *iv*), on a :

$$(s_\delta w)^{-1}(R^+) \cap (-R^+) = w^{-1}(R^+) \cap (-R^+) \;\setminus\; \{w^{-1}(\delta)\}$$

donc $N_{s_\delta w} = N_w - 1$. Par hypothèse de récurrence, $s_\delta w \in \langle s_\alpha \;:\; \alpha \in \Delta\rangle$. Du coup on a aussi montré *v*). **Q.e.d.**

Corollaire 9.8.4.1 *Si α est une racine simple, alors U_{s_α} est de codimension 1 dans U et $N_G U_{s_\alpha} \geq G_\alpha$.*

Démonstration : Comme U est unipotent, $\dim N_U U_{s_\alpha} > \dim U_{s_\alpha}$. Donc U_{s_α} est normalisé par U, par s_α et par T donc par G_α (qui est engendré par U_α, s_α et T. **Q.e.d.**

Lemme 9.8.5 *Soit α une racine. Si $w \in W$, alors $G_\alpha wB = U_\alpha wB \cup U_\alpha s_\alpha wB$.*

Démonstration : Le stabilisateur de wB vu comme élément de G/B est le Borel wBw^{-1}. Soit $B_\alpha := G_\alpha \cap wBw^{-1}$. C'est un sous-groupe de Borel de G_α. On a donc un morphisme bijectif : $G_\alpha/B_\alpha \to G_\alpha wB/B$. En particulier, $G_\alpha wB/B$ est une $G_\alpha-$variété complète de dimension 1 avec exactement 2 points fixes de T : wB/B et $s_\alpha wB/B$. Comme $\dim(B_\alpha)_u = 1$, U_α ou $U_{-\alpha} \not\subseteq B_\alpha$. Supposons par exemple que U_α ne laisse pas fixe wB/B. Alors $U_\alpha wB/B$ est localement fermé de dimension 1 dans $G_\alpha wB/B$. mais alors $U_\alpha wB/B$ est ouvert dans $G_\alpha wB/B$. Donc $G_\alpha wB/B \;\setminus\; U_\alpha wB/B$ est fini et stable par T. Comme T est connexe, T laisse fixe tous les points de $G_\alpha wB/B \;\setminus\; U_\alpha wB/B$ donc forcément, $G_\alpha wB/B = s_\alpha wB/B \cup U_\alpha wB/B$.

Donc : $G_\alpha wB/B = U_\alpha wB/B \cup U_\alpha s_\alpha wB/B$. Si c'est $U_{-\alpha}$ qui ne laisse pas fixe wB/B, alors :

$$G_\alpha wB = U_{-\alpha}wB \cup s_\alpha wB \Rightarrow s_\alpha G_\alpha wB = G_\alpha wB = s_\alpha U_{-\alpha}wB \cup wB = U_\alpha s_\alpha wB \cup wB.$$

Q.e.d.

Théorème 9.8.6 (Décomposition de Bruhat) *On a une décomposition en réunion disjointe :*

$$G = \cup_{w \in W} BwB \ .$$

De plus, si n_w est un représentant de w dans $N_G T$, alors on a un isomorphisme de variété algébriques :

$$U'_w \times B \to BwB,\ (u,b) \mapsto un_w b \ .$$

Lemme 9.8.7 *Le groupe G est engendré par les G_α, $\alpha \in \Delta$.*

Exercice. On a aussi une décomposition de Bruhat sous la forme : $G = \cup_{w \in W} BwB^-$. De plus, BwB^- est de codimension $l(w)$ dans G où $l(w) = |\{\alpha \in R^+ \ : \ w^{-1}(\alpha) < 0\}$ = la longueur minimale l d'une décomposition $w = s_{\alpha_1}...s_{\alpha_l}$ où les α_i sont des racines simples.

9.8.4 La grosse cellule

Proposition 9.8.8 *L'application produit : $U \times B^- \to G$ est un isomorphisme sur l'ouvert UB^- de G.*

Démonstration : L'application est bijective, UB^- est une $U \times B^-$ orbite de codimension 0 c'est donc un ouvert de G. De plus la différentielle est injective donc surjective donc on a un morphisme bijectif séparable donc birationnel. Comme G est lisse, G est normale et d'après le théorème principal de Zariski, c'est un isomorphisme. **Q.e.d.**

Chapitre 10

Représentations des groupes réductifs

Soit G un groupe réductif connexe. On fixe un tore maximal et un sous-groupe de Borel de G : $T \leq B$. On note $X := X^*T$, R, R^+ ;

Si $r : G \to \mathrm{GL}(V)$ est une représentation rationnelle, on a une décomposition :

$$V = \oplus_{\lambda \in X} V_\lambda$$

où $V_\lambda := \{v \in V \ : \ \forall\, t \in T,\, t.v = \lambda(t)v\}$.end

Lemme 10.0.9 *Si α est une racine si $u \in U_\alpha$ alors :*

$$\forall\, \chi \in X, \forall\, v \in V_\chi,\; u.v - v \in \oplus_{n>0} V_{\chi+n\alpha} \ .$$

Lemme 10.0.10 *Supposons V irréductible.*

i) *Il existe une unique droite propre pour B : c'est un espace propre V_μ pour un certain $\mu \in X$;*

ii) *pour un μ comme ci-dessus, on a : $\forall\, \alpha \in R^+$, $\langle \mu, \alpha^\vee \rangle \geq 0$;*

iii) *si μ est comme ci-dessus et si λ est un autre caractère propre de V, alors : $\mu - \lambda$ est une somme de racines positives et* $\dim V_\mu = 1$. *en particulier μ est unique : on dit que μ est le plus haut poids de V.*

iv) *Si V' est une autre représentation irréductible de poids μ', alors $V \simeq V' \Leftrightarrow \mu = \mu'$.*

Un caractère μ qui vérifie $\forall\, \alpha \in R^+$, $\langle \mu, \alpha^\vee \rangle \geq 0$ est appelé *dominant.*

Théorème 10.0.11 *Pour un poids dominant $\mu \in X$ il existe une unique représentation irréductible v de G de plus haut poids μ, à isomorphisme près.*

Si $\lambda \in X$, on pose $H^0(\lambda) := \{f \in k[G] \ : \ \forall\, g \in G, \forall\, b \in B^-,\, f(gb) = \lambda^{-1}(b)f(g)\}$ où λ est étendu à B^- de manière traditionnelle.

L'espace $H^0(\lambda)$ est un $G-$module pour l'action suivante :

$$\forall\, g \in G,\, \forall\, f \in H^0(\lambda),\, \forall\, x \in G,\, G.f(x) = f(g^{-1}x)\ .$$

Théorème 10.0.12 *Soit $\lambda \in X$. Sont équivalentes :*

i) *λ dominant ;*

ii) *$H^0(\lambda) \neq 0$;*

iii) *Il existe un $G-$module V tel que $(V^U)_\lambda \neq 0$.*

Démonstration : Si λ est dominant, soit $f_\lambda \in k[UB^-]$ définie par :

$$\forall\, u \in U,\, \forall\, t \in t,\, \forall\, u' \in U^-,\, f_\lambda(utu') := \lambda(t)^{-1}\ .$$

Soit α une racine simple. On choisit $u_{\pm\alpha}$ et n_α comme dans le lemme 10.0.13.

Posons $U_1 := \langle U_\beta\ :\ \beta > 0, \beta \neq \alpha\rangle$. Alors s_α normalise U_1 et :

$$U_1 \times k \times T \times U^- \to s_\alpha UB^-,\, (u_1, x, t, u') \mapsto u_1 n_\alpha u_\alpha(x) tu'$$

est un isomorphisme de variétés.

D'après le lemme 10.0.13, si $x \neq 0$, $u_1 n_\alpha u_\alpha(x)tu' \in UB^-$ et :

$$f_\lambda(u_1 n_\alpha u_\alpha(x)tu') = \lambda(t^{-1})(-x)^{\langle\lambda,\alpha^\vee\rangle}\ .$$

Donc f_λ se prolonge à $s_\alpha UB^-$ pour toute racine simple α.

Or, lorsque α décrit l'ensemble des racines simples, $\cup_\alpha s_\alpha UB^-$ est un ouvert dont le complémentaire est de codimension ≥ 2. Comme G est normale, $k[G] = k[\cup_\alpha s_\alpha UB^-]$. Donc $f_\lambda \in H^0(\lambda)$. **Q.e.d.**

Lemme 10.0.13 *Si $\alpha \in R$, alors il existe $u_\alpha : \mathbb{G}_a \simeq U_\alpha$, $u_{-\alpha} : \mathbb{G}_a \to U_{-\alpha}$ tels que :*

$$\forall\, x \in k,\, \forall\, t \in T,\, tu_{\pm\alpha}(x)t^{-1} = u_{\pm\alpha}(\alpha^{\pm}(t)x)\ .$$

$$\forall\, x \in k^\times,\, u_\alpha(-x^{-1})\alpha^\vee(-x^{-1})u_{-\alpha}(x^{-1}) = n_\alpha u_\alpha(x)$$

pour un certain élément de $N_{G_\alpha}T \setminus Z_{G_\alpha}T$.

Proposition 10.0.14 *Si $\mu \in X$ est un caractère dominant, alors $H^0(\mu)$ contient un unique sous-G$-$module irréductible $L(\mu)$. Ce $G-$module $L(\mu)$ est de plus haut poids μ.*

Bibliographie

[1] S. Lang. *Cours d'algèbre*. Dunod, 2004.