Rapport de M2
Groupes algébriques unipotents

par Raphaël Achet
sous la direction de Bertrand Rémy

Table des matières

1 Généralités sur les groupes algébriques **3**
1.1 Préliminaires algébriques . . . 3
1.2 Langage des variétés . . . 3
1.3 Langage des schémas . . . 4
1.4 k-structure . . . 4
1.5 Action du groupe de Galois . . . 5
1.6 Groupes algébriques . . . 5
1.7 Schémas en groupes affines . . . 6

2 Groupes diagonalisables et tores **8**
2.1 Groupes diagonalisables . . . 8
2.2 Action du groupe de Galois . . . 10
2.3 Tores déployés et tores anisotropes . . . 10

3 Groupes unipotents **11**
3.1 Définitions . . . 11
3.2 Extension de Ga par Ga . . . 12
3.3 p-polynôme et applications . . . 13
3.4 Groupes unipotents commutatifs d'exposant p . . . 15
3.5 Groupes totalement ployés . . . 17
3.6 Noyau cckp et applications . . . 19
3.7 Structure des groupes unipotents . . . 21
3.8 Action des tores sur les groupes unipotents . . . 22

4 Annexes **23**
4.1 Extension de groupes algébriques commutatifs . . . 23
4.2 Systèmes de facteurs . . . 24
4.3 Restriction de Weil et applications . . . 25
4.4 Algèbres formellement lisses . . . 29

Introduction

Une motivation élémentaire, de l'étude des groupes unipotents vient de la décomposition de Dunford multiplicative : si A est une matrice inversible à coefficient dans un corps algébriquement clos, alors il existe un unique couple de matrices (A_s, A_u) où A_s est diagonale inversible, A_u unipotente (c'est à dire $A_u - Id$ est nilpotente), A_s et A_u commutent et vérifient $A = A_u.A_s$. Soit G un groupe algébrique commutatif, G peut être vu comme sous groupe d'un GL_n, une conséquence de Dunford multiplicatif est que l'on peut définir $G_s = \{g_s | g \in G\}$ et $G_u = \{g_u | g \in G\}$. On peut alors décomposer G de la façon suivante :

0.1 Théorème. *[Spr98, 3.1.1]*
Soit G un groupe algébrique commutatif.

1. *Les ensembles G_s et G_u sont des sous-groupes fermés de G.*
2. *L'application produit $G_s \times G_u \to G$ est un isomorphisme de groupes algébriques.*

Ce théorème peut donner l'idée d'étudier les groupes unipotents commutatifs, ce qui est fait dans les paragraphes 3.4 et 3.5.

De façon plus générale, on considère G un groupe algébrique défini sur un corps k. On note $\mathcal{R}_{u,k}(G)$ le radical unipotent rationnel de G c'est-à-dire le plus grand sous-groupe de G distingué, connexe, unipotent et défini sur k. Le groupe G est dit pseudo-réductif si $\mathcal{R}_{u,k}(G) = \{1\}$.

On a en toute généralité une suite exacte :

$$\{1\} \to \mathcal{R}_{u,k}(G) \to G \to G/\mathcal{R}_{u,k}(G) \to \{1\}. \tag{1}$$

Le groupe $\mathcal{R}_{u,k}(G)$ est unipotent, le groupe $G/\mathcal{R}_{u,k}(G)$ est pseudo-réductif. Une bonne compréhension de ces deux classes de groupes doit donc permettre de mieux comprendre les groupes algébriques en général. Un résumé de l'étude des groupes pseudo-réductifs et de ses applications peut être trouvé dans [Rém10].

Dans le présent rapport on va s'intéresser aux groupes algébriques unipotents sur un corps quelconque dont l'étude a été commencée par J. Tits [Tits67], continuée par

J.Oesterlé [Oest84] et complétée dans l'annexe B de [CGP10]. L'étude des groupes unipotents est précédée de celle plus simple des tores qui permet de faire quelques analogies.

Je tiens à remercier Philippe Gille et Michel Brion pour leur aide, Ziyang Gao pour m'avoir fait découvrir [Tits67] (une merveille de simplicité et concision), Magali Moureau ma mère pour la correction de l'orthographe et bien sûr Bertrand Rémy toujours disponible et ponctuel.

1 Généralités sur les groupes algébriques

La première section rassemble un certain nombre de conventions, de définitions et de propriétés utiles pour la suite. On peut trouver dans [Spr98] des précisions sur le contenu des paragraphes 1.1 et 1.2 (la présentation de [Bor91] est assez différente, au moins dans le vocabulaire). Les deux paragraphes sur les schémas 1.3 et 1.7 sont strictement inclus dans le premier chapitre de [Wat79], les définitions élémentaires sur les foncteurs peuvent être trouvées dans [Dou05]. Quant aux paragraphes 1.4, 1.5 et 1.6, le lecteur peut chercher des précisions dans [Spr98] ou [Bor91].

1.1 Préliminaires algébriques

Soit K un corps algébriquement clos.

Soit $V = K^n$, $S = K[T_1, \dots, T_n]$. les éléments de S sont vus comme des fonctions sur V. Si I est un idéal de V, on note $\mathcal{V}(I)$ l'ensemble des zéros communs à tous les éléments de I. Si X est un sous ensemble de V alors on note $\mathcal{I}(X)$ l'idéal des éléments de S qui s'annulent sur X.

1.1 Proposition (Nullstellensatz)**.** $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$

Les ensembles $\mathcal{V}(I)$ pour I idéal de S sont les fermés d'une topologie, dite topologie de Zariski. Un ensemble fermé pour cette topologie est dit ensemble algébrique.

1.2 Définition. Une K-algèbre est dite affine si elle est de type fini comme K-algèbre.

Une K-algèbre est dite réduite si 0 est son seul élément nilpotent.

On remarque que si X est un ensemble algébrique alors $K[X] := S/\mathcal{I}(X)$ est une algèbre affine réduite.

1.3 Remarque. Cette notation bien que standard pose problème car elle est en conflit avec celle d'algèbre de groupe. On signalera donc systématiquement quand cette notation signifie algèbre de groupe.

En fait la donnée de X est équivalente à la donnée de $K[X]$. En effet si A est une algèbre affine réduite alors il existe un entier r et un ensemble algébrique $X \subset K^r$ tel que $K[X] = A$.

1.2 Langage des variétés

Soit K un corps algébriquement clos.

Soit $X \subset K^n$ un ensemble algébrique. Une fonction f définie sur U voisinage de X est dite régulière en x s'il existe $g, h \in K[X]$ et V voisinage ouvert de x, $V \subset U \cap \{z |\ h(z) \neq 0\}$ tel que $\forall y \in V$ on ait $f(y) = \frac{g(y)}{h(y)}$.

f est dite régulière sur U si elle est régulière en tout point de U. On note $\mathcal{O}_X(U)$ la K-algèbre des fonctions régulières sur U.

Un espace annelé est appelé K-variété algébrique affine s'il est isomorphe à un tel couple $(X, \mathcal{O}_X)$. Par abus de notation on parle de la K-variété X, en sous entendant $\mathcal{O}_X$.

1.3 Langage des schémas

Soit k un corps et K une extension de k algébriquement close.

Soit F un foncteur covariant de la catégorie des k-algèbres dans la catégorie des ensembles.

Un tel foncteur F est dit représentable s'il existe une k-algèbre A tel que F est isomorphe au foncteur $R \mapsto \mathrm{Hom}_k(A, R)$. On appelle alors F un schéma affine.

1.4 Lemme (Lemme de Yoneda)**.** *[Wat79, 1.3]*

Soient E et F deux schémas affines représentés par des k-algèbres A et B, alors les transformations naturelles $E \to F$ correspondent bijectivement aux morphismes de k-algèbre $B \to A$.

De plus $E \to F$ est un isomorphisme si et seulement si $B \to A$ est un isomorphisme de k-algèbres.

On va maintenant montrer que l'on peut voir les variétés algébriques affines comme des schémas.

Soit X une K-variété algébrique affine on note $A = K[X]$. On note $\mathrm{Max}(A)$ l'ensemble des idéaux maximaux de A.

1.5 Proposition. *[Spr98, 1.3.3]*

L'application

$$x \in X \mapsto \mathcal{I}(\{x\}) \in \mathrm{Max}(A) \tag{2}$$

est une bijection.

De plus $\mathrm{Max}(A)$ est en bijection avec $\mathrm{Hom}_{K-alg}(A, K)$. Si l'on note X' le schéma représenté par A, on peut donc voir X comme $X'(K)$.

Dans la suite on note indifféremment X vue comme variété algébrique et schéma affine.

1.4 k-structure

Soit k un corps et K une extension de k algébriquement close.

Soit V un K-espace vectoriel, une k-structure sur V est un k-espace vectoriel $V_k \subset V$ tel que $V \cong V_k \otimes_k K$. Soit $f : V \to W$ une application linéaire entre deux K-espace vectoriel muni de k-structure, f est dite définie sur k ou k-morphisme si $f(V_k) \subset W_k$.

Soit A une K-algèbre, une k-structure sur A est une k-algèbre $A_k \subset A$ tel que $A \cong A_k \otimes_k K$. Soit $f : A \to B$ un morphisme de K-algèbre entre deux K-algèbres munies de k-structure, f est dite définie sur k ou k-morphisme s'il est un k-morphisme en tant qu'application linéaire.

Soit X une K-variété algébrique affine, on dit que X est définie sur k si l'idéal $\mathcal{I}(X)$ est engendré par des polynômes à coefficients dans k. C'est-à-dire si $\mathcal{I}(X)$ admet une k-structure, ou encore s'il existe une k-algèbre de type fini A_0 sous

algèbre de $K[X]$ telle que $K \otimes_k A_0 \to K[X]$ soit un isomorphisme. On note alors $A_0 = k[X]$ et on dit que X est une k-variété algébrique affine.

L'ensemble $X(k)$ des points k-rationnels correspond aux morphismes de k-algèbres $A_0 \to k$.

Soient X et Y deux k-variétés, $\alpha : X \to Y$ est dit k-morphismes si le morphisme de K-algèbre $\alpha' : K[X] \to K[Y]$ est défini sur k.

On note k_s la clôture séparable de k.

1.6 Proposition. *[Bor91, AG.13.3]*
Soit X une k-variété, alors $X(k_s)$ est dense dans X.

1.5 Action du groupe de Galois

On note $\Gamma = \mathrm{Gal}(k_s/k)$ où k_s est la clôture séparable de k.

Soit V un K-espace vectoriel avec une k-structure V_k, c'est à dire $V \cong V_k \otimes_k K$. Alors Γ opère sur $V_{k_s} = k_s \otimes_k V_k$ via le premier facteur. On a alors $V_k = V_{k_s}^{\Gamma}$.

Soit V une k-variété, on va définir une action de Γ sur $V(k_s)$ qui est dense dans V selon 1.6.

En effet, l'on peut identifier $V(k_s)$ avec $\mathrm{Hom}_{k_s-alg}(k_s[V], k_s)$ donc $x \in V(k_s)$ correspond à un morphisme d'algèbre e_x. Si $\gamma \in \Gamma$ on définit alors :

$$e_{\gamma(x)} = \gamma \circ e_x \circ \gamma^{-1} \tag{3}$$

où le γ de gauche agit sur k_s, celui de droite sur $k_s[V] = k_s \otimes_k k[V]$.

1.7 Théorème. *[Bor91, AG.14.4]*
Soient V une k-variété et Z une sous-variété fermée, alors les conditions suivantes sont équivalentes :

1. *Z est définie sur k.*
2. *Z est définie sur k_s et $Z(k_s)$ est Γ-stable.*
3. *Il existe $E \subset Z \cap V(k_s)$ tel que E est Γ-stable et dense dans Z.*

1.6 Groupes algébriques

Soient k un corps et K une extension de k algébriquement close.

1.8 Définition. Un groupe algébrique affine $(G, +)$ est une K-variété algébrique affine G munie de :

1. un élément $e \in G$;
2. un morphisme $\mu : G \times G \to G$;
3. un morphisme $i : G \to G$.

qui vérifient les axiomes de groupes usuels.

Si en plus G est une k-variété, si μ et i sont définis sur k ($e \in G(k)$ est alors automatique) alors G est dit k-groupe.

Si G, G' sont deux groupes algébriques affines. Un morphisme f de groupes algébriques affines de G dans G' est un morphisme de variétés qui est aussi un morphisme de groupes. Si en plus G et G' sont des k-groupes et f est défini sur k alors f est appelé k-morphisme.

1.9 Définition. Soit G un groupe algébrique, la composante connexe de $\{Id\}$ est notée G°.

1.10 Proposition. *[Bor91, 1.2] Soit G un groupe algébrique.*

1. *G est lisse (comme variété).*
2. *G° est un sous groupe normal d'indice fini dans G, et dont les classes sont les composantes irréductibles de G. Si G est défini sur k alors G° l'est aussi*
3. *Tout sous groupe d'indice fini contient G°.*

1.11 Théorème. *[Tits67] Soit G, H deux groupes algébriques définis sur k. Soit $\varphi : G \to H$ une k-isogénie bijective de $G(\overline{k})$ dans $H(\overline{k})$, alors φ est un k-isomorphisme si et seulement si $d\varphi : \mathrm{Lie}(G) \to \mathrm{Lie}(H)$ est surjective.*

1.12 Proposition. *[Bor91, 1.10] Soit G un k-groupe affine, alors G est isomorphe à un k-sous-groupe d'un certain GL_n.*

1.13 Corollaire. *[Bor91, 2.3] Soit G' un k-groupe, G et H des k-sous-groupes avec G connexe, alors le commutateur [G,H] est un k-sous-groupe.*

1.14 Théorème (Décomposition de Jordan)**.** *[Bor91, 4.2]*

Soit G un k-groupe, soit $g \in G$. Il existe un unique couple $(g_s, g_u) \in G^2$ tel que $g = g_s g_u$.

De plus si $G \subset GL_n$ alors la décomposition de Jordan ci-dessus coïncide avec la décomposition de Dunford multiplicative donnée dans l'introduction.

1.15 Proposition. *[Bor91, 4.6] Soit $M \subset M_n(k)$ une famille d'endomorphismes qui commutent 2 à 2. Soit L l'extension de k engendrée par les valeurs propres des éléments de M.*

1. *M est trigonalisable sur L*
2. *Si les éléments de M sont diagonalisables sur $\overline{k}$, alors $L \subset k_s$ et M est diagonalisable sur L.*

1.7 Schémas en groupes affines

Soit k un corps.

Soit G un foncteur représentable de la catégorie des k-algèbres dans la catégorie des groupes. On appelle alors G un schéma en groupe affine.

Le lemme de Yoneda 1.4 nous permet à partir des transformations naturelles *mult* et *inv* de définir deux morphismes de k-algèbres $\Delta : A \to A \otimes A$ dit comultiplication et $\iota : A \to A$ dit antipode. De plus e peut être vu comme une transformation naturelle $\{1\} \to G$, il induit donc un morphisme de k-algèbres $\varepsilon : A \to k$.

Les axiomes de groupes se traduisent en la commutativité des trois diagrammes suivants :

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes A \\ \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle id \otimes \Delta} \\ A \otimes A & \xrightarrow{\Delta \otimes id} & A \otimes A \otimes A \end{array} \tag{4}$$

$$\begin{array}{ccc} A \otimes A & \xrightarrow{\iota \otimes id} & A \otimes A \\ {\scriptstyle \Delta}\uparrow & & \downarrow{\scriptstyle mult} \\ A & \xrightarrow{\varepsilon} & A \\ \downarrow{\scriptstyle \Delta} & & \uparrow{\scriptstyle mult} \\ A \otimes A & \xrightarrow{id \otimes \iota} & A \otimes A \end{array} \tag{5}$$

$$\begin{array}{ccccc} A & & \xleftarrow{\varepsilon \otimes id} & & A \otimes A \\ {\scriptstyle id \otimes \varepsilon}\uparrow & & \nwarrow^{id} & & \uparrow{\scriptstyle \Delta} \\ A \otimes A & & \xleftarrow[\Delta]{} & & A \end{array} \tag{6}$$

1.16 Définition. Une k-algèbre A munie d'applications Δ, ε, ι qui rendent les diagrammes (4), (5) et (6) commutatifs est appelée une algèbre de Hopf.

Les schémas en groupes affines sur k correspondent donc aux k-algèbres de Hopf.

1.17 Exemple. Exemples de schémas en groupes classiques et de leurs algèbres de Hopf A :

1. $G_a : R \mapsto (R, +)$, $A = k[T]$.
2. $GL_1 = G_m : R \mapsto (R^*, \times)$, $A = k[T, T^{-1}]$
3. $GL_n : R \mapsto GL_n(R)$, $A = k[X_{1,1}, \ldots, X_{n,n}, Y]/(\det(X_{i,j})Y - 1)$

Un k-groupe G défini dans la section 1.6, peut être vu comme un schéma en groupe affine dont l'algèbre de Hopf est $A = k[G]$. Dans ce cas, l'algèbre de Hopf A est affine et réduite.

Les schémas en groupes sont donc des généralisations des k-groupes qui permettent entre autre de considérer des points dans des k-algèbres qui ne sont pas forcément des corps comme dans le théorème 3.41.

1.18 Définition. Soit G un schéma en groupe algébrique affine sur un corps k tel que $k[G] \otimes \overline{k}$ est réduite, alors G est dit lisse.

On a vu selon le théorème 1.10 que les groupes algébriques sont toujours lisses au sens des variétés. Mais les opérations usuelles comme l'intersection (!) font parfois apparaitre des objets qui sont toujours des schémas en groupes algébriques affines mais qui ne sont pas lisses comme le montre l'exemple ci-dessous.

1.19 Exemple. [Gil14, 1.1.2]

Ici k est un corps algébriquement clos de caractéristique $p > 0$.

Soient $G = G_a^2$, H_1 défini par l'équation $x^p + x = y$, H_2 défini par l'équation $x = y$, alors H_1 et H_2 sont des k-sous groupes isomorphes à G_a et $H = H_1 \cap H_2$ est donné par l'équation $x = y$ et $x^p = 0$.

Du point de vue des variétés, l'intersection est triviale. Du point de vue des schémas, elle est isomorphe à μ_p d'algèbre de Hopf $k[t]/t^p$ qui n'est pas réduite alors que H_1 et H_2 sont lisses.

1.20 Proposition. *Soit $f : G \to H$ un morphisme surjectif de k-schéma en groupe algébrique, alors $f_k : G(k) \to H(k)$ est surjective.*

Démonstration. Le morphisme f est surjectif donc $f^* : A = k[H] \to B = k[G]$ est injectif. Or selon [Wat79, 14.1] si $A \subseteq B$ sont deux algèbres de Hopf sur un corps k alors B est fidèlement plat sur A. On applique alors l' assertion (iv) de la proposition 8 de [Bou61, chapitre 1, §3, N° 5], selon laquelle tout idéal maximal de A est l'intersection de A avec un idéal maximal de B. Donc tout morphisme de k-algèbre de A dans k s'étend en un morphisme de k-algèbre de B dans k. □

2 Groupes diagonalisables et tores

Le but de cette partie est de rappeler les principaux résultats de la théorie des tores. Les résultats de cette section et beaucoup d'autres peuvent être trouvés dans [Bor91, chapitre III] et [Spr98, chapitre 3].

Dans toute la suite K/k est une extension de corps avec K algébriquement clos et G est un k-groupe sauf si le contraire est explicitement mentionné.

2.1 Groupes diagonalisables

2.1 Lemme (lemme de Dedekind)**.** *Soit H un groupe quelconque, soit X un ensemble de morphismes $G \to K^*$, alors X est linéairement indépendant en tant que sous ensemble de l'ensemble des fonctions de H dans K.*

Démonstration. [Bor91, 8.1]

Par l'absurde, si ce n'est pas le cas alors il existe $n > 0$ minimal tel que $(\chi_1, \dots, \chi_n) \in X^n$ sont liés, c'est-à-dire :

$$f = \sum_{i<n} \alpha_i \chi_i + \chi_n = 0. \tag{7}$$

Soit $h_0 \in H$ tel que $\chi_n(h_0) \neq \chi_1(h_0)$, alors pour tout $h \in H$,

$$0 = f(h_0 h) - \chi_n(h_0) f(h) = \sum_{i<n} \alpha_i (\chi_i(h_0) - \chi_n(h_0)) \chi_i(h) \tag{8}$$

c'est une relation de dépendance linéaire non triviale de longueur strictement plus faible. □

On note $A = K[G]$, $X(G) = \mathrm{Hom}(G, GL_1)$ le groupe des caractères de G, et $X(G)_k$ le sous-groupe de $X(G)$ constitué des caractères de G définis sur k. On remarque que $X(G)$ peut être vu comme un sous-groupe de A.

2.2 Définition. G est dit diagonalisable si $X(G)$ engendre A comme K-espace vectoriel. Si de plus $X(G)_k$ engendre A alors G est dit déployé sur k.

Étant donné que $A = K \otimes_k A_k$ la condition ci-dessus est équivalente à $X(G)_k$ engendre $A_k = k[G]$ comme k-espace vectoriel.

2.3 Proposition. *Supposons que $Y \subseteq X(G)_k$ engendre A_k, alors :*

1. *$Y = X(G)$, en particulier les caractères de G sont définis sur k.*
2. *$A_k = k[X(G)]$ (où $k[X(G)]$ est l'algèbre de groupe), de plus la structure d'algèbre de Hopf sur A est induite par le plongement diagonal $X(G) \to X(G) \times X(G)$ et l'inversion $X(G) \to X(G)$.*

3. *Si H est un k-sous-groupe de G alors H est diagonalisable et déployé sur k. De plus H est défini comme intersection de noyaux de caractères définis sur k. Enfin tout caractère de H s'étend en caractère de G.*
4. *Si $\rho : G \to GL_n$ est une représentation k-rationnelle, alors $\rho(G)$ est conjuguée sur k à un sous-groupe de D_n. En particulier G est k-isomorphe à un sous-groupe fermé de D_n.*

Démonstration. [Bor91, 8.2]

Prouvons 1 : selon le lemme de Dedekind 2.1 appliqué à $X(G)_k \subset A_k$, les éléments de $X_k(G)$ sont libres. Donc $Y \subseteq X(G)_k$ engendre A_k, ce qui implique $Y = X(G)_k$ et G déployé sur k, ainsi $Y = X(G)$.

Au tour de 2 : toujours selon le lemme de Dedekind 2.1 $X(G)$ est libre donc $A_k = k[X(G)]$. De plus Δ est le comorphisme de $mult : G \times G \to G$, or la restriction de $mult$ aux caractères $X(G) \to X(G \times G) = X(G) \times X(G)$ est exactement la plongement diagonal.

Montrons 3 : $B = K[H]$ est engendrée par l'image de la restriction à H des caractères de G, donc B est diagonalisable et par 2 on a $B = K[X(H)]$. La surjection $p : A \to B$ envoie $X(G)$ sur $X(H)$ donc p est la surjection induite sur l'algèbre de groupe par le morphisme de groupe surjectif $X(G) \to X(H)$. Or $X(G) = X(G)_k$, donc H est défini comme intersection de noyaux de caractères définis sur k et $X(H) = X(H)_k$ ce qui signifie H déployé sur k et termine la preuve de 3.

Enfin en ce qui concerne 4 : $X(G)$ fournit un morphisme injectif de G dans $(GL_1)^d$ pour un certain $d > 0$, donc G est commutatif et constitué d'éléments semi-simples. Soit $\rho : G \to GL(V)$ une représentation k-rationnelle, selon la proposition 1.15 $\rho(G)$ est diagonalisable. De plus pour tout $\chi \in X(G)$ selon [Bor91, 5.2] l'espace propre $V_\chi = \{x \in V |\ \forall g \in G\ \ \rho(g)x = \chi(g)x\}$ est défini sur k. Donc $\rho(G)$ est diagonalisable sur k. Pour montrer la seconde partie il suffit de remarquer que selon la proposition 1.12 il existe une représentation k-rationnelle et injective.

□

2.4 Corollaire. *[Bor91, 8.3] Le foncteur contravariant $G \mapsto X(G)$ est fidèlement plat de la catégorie des groupes diagonalisables déployés sur k munie des k-morphismes dans la catégorie des $\mathbb{Z}$-modules de type fini.*

2.5 Corollaire. *[Bor91, 8.4] Les assertions suivantes sont équivalentes :*

1. *G est diagonalisable .*
2. *G est isomorphe à un sous groupe de D_n pour un certain $n > 0$.*
3. *Si $\pi : G \to GL_n$ est une représentation rationnelle alors $\pi(G)$ est conjugué sur k à un sous groupe de D_n.*

2.6 Corollaire. *[Bor91, 8.4] Les assertions suivantes sont équivalentes :*

1. *G est diagonalisable et déployé sur k.*
2. *G est k-isomorphe à un sous groupe de D_n pour un certain $n > 0$.*
3. *Si $\pi : G \to GL_n$ est une k-représentation alors $\pi(G)$ est conjugué sur k à un sous groupe de D_n.*

2.7 Proposition. *Soit G un groupe diagonalisable, alors G est déployé sur une extension finie séparable de k.*

Démonstration. [Bor91, 8.11]

On choisit un plongement $G \subset GL_n$. Selon la proposition 1.6 il suffit de diagonaliser $G(k_s)$ par conjugaison par un élément de $GL_n(k_s)$. Ce qui est vrai selon la proposition 1.15. □

2.2 Action du groupe de Galois

Soit G un groupe diagonalisable, la proposition 2.7 nous assure que G est déployé sur k_s. Soit $A = K[G]$, selon 2.3 $A_{k_s} = k_s[X(G)]$.

Soit $\gamma \in \Gamma = \mathrm{Gal}(k_s/k)$, γ agit sur A_{k_s} via :

$$\left(\sum_{\alpha \in X(G)} a_\alpha \alpha\right)^\gamma = \sum_{\alpha \in X(G)} a_\alpha^\gamma \alpha^\gamma \tag{9}$$

avec cette action $A_k = A_{k_s}^\Gamma$. En tant que k-groupe G est donc entièrement déterminé par la connaissance de $X(G)$ et de sa structure comme Γ-module.

En fait, on a une équivalence de catégorie.

2.8 Proposition. *[Bor91, 8.12]*

Soit $\mathcal{A}$ la catégorie dont les objets sont les k-groupes diagonalisables, et dont les morphismes sont les k-morphismes.

Soit $\mathcal{B}$ la catégorie dont les objets sont les $\mathbb{Z}$ modules de type fini sans p torsion si $p = \mathrm{char}(k) > 0$ sur lesquels Γ agit de façon continue, et dont les morphismes sont les morphismes de $\mathbb{Z}$-modules Γ-équivariant, alors

$$X : \mathcal{A} \to \mathcal{B} \tag{10}$$

est une équivalence de catégorie.

2.3 Tores déployés et tores anisotropes

2.9 Définition. Un groupe algébrique isomorphe à $D_n = (G_m)^n$ pour un certain $n \geq 0$ est dit un tore de dimension n.

2.10 Proposition. *Soit T un k-groupe. Les assertions suivantes sont équivalentes :*

1. *T est un tore de dimension n.*
2. *T est connexe, diagonalisable de dimension n.*
3. *T est diagonalisable et $X(T) \cong \mathbb{Z}^n$.*

Démonstration. [Bor91, 8.5]

$1 \Rightarrow 2$ est évident.

$2 \Rightarrow 3$: GL_1 est connexe et de dimension 1, ses seuls sous-groupes connexes sont GL_1 et $\{Id\}$. Donc l'image de T par un caractère est GL_1 ou $\{Id\}$. En particulier $X(G)$ est sans torsion. De plus T est diagonalisable donc $K[T] = K[X(t)]$, et enfin $n = \dim(T) = \deg.\mathrm{tr}(K(T))$ est le rang du groupe abélien libre $X(T)$.

$3 \Rightarrow 1$: soit $\alpha_a, \ldots, \alpha_n$ une base de $X(T)$. Alors $K[T] = K[\alpha_1, \alpha_1^{-1}, \ldots, \alpha_n, \alpha_n^{-1}]$ et $\varphi : t \to \mathrm{diag}(\alpha_1(t), \ldots, \alpha_n(t))$ donne un isomorphisme de T dans D_n. □

2.11 Définition. Soit T un k-tore, T est dit k-anisotrope sur k si $X(T)_k = \{1\}$ ou de façon équivalente si $X(T)^\Gamma = \{1\}$.

Soit T un k-tore, on va définir le plus grand sous tore de T qui est k-anisotrope T_a et le plus grand sous tore de T qui est k-déployé T_d :

On définit T_a comme le sous tore de T qui correspond au Γ-module sans torsion $X(T)/X(T_k) = X(T)/X(T)^\Gamma$.

On a donc

$$X(T_a) = \frac{X(T)}{X(T_k)} = \frac{X(T)}{X(T^\Gamma)} \tag{11}$$

et selon 2.3 3.

$$T_a = \bigcap_{\alpha \in X(T)_k} \ker(\alpha) \tag{12}$$

Par construction il est clair que T_a est anisotrope.

En ce qui concerne T_d on peut le définir comme le sous-tore engendré par $\{\mathrm{Im}(\alpha) | \alpha \in X(T)_k\}$. De façon évidente T_d est déployé et contient tout sous-tore déployé.

Un sous-tore de $T_a \cap T_d$ est à la fois déployé et anisotrope donc trivial. Donc $(T_a \cap T_d)^\circ$ est trivial, donc $T_a \cap T_d$ est fini.

De plus, on peut montrer que $\dim(T_a) + \dim(T_d) = \dim(T)$ donc $T_a \times T_d \to T$ est surjective.

On peut résumer le travail ci-dessus par la proposition suivante :

2.12 Proposition. *[Bor91, 8.15]*
Soit T un k-tore, T_a et T_d sont définis comme ci-dessus, alors

1. *T_a est le plus grand sous tore anisotrope de T défini sur k. T_d est le plus grand sous tore déployé de T défini sur k.*
2. *$T_a \cap T_d$ est fini et $T = T_a T_d$.*
3. *Si $\alpha : T \to T'$ est un k-morphisme de k-tore alors $\alpha(T_a) \subset T'_a$ et $\alpha(T_d) \subset T'_d$. Autrement dit $T \mapsto T_a$ et $T \mapsto T_d$ sont fonctoriels.*

3 Groupes unipotents

Tous les groupes sont des k-groupes, algébriques, affines sauf si le contraire est explicitement mentionné.

3.1 Définitions

On rappelle qu'un endomorphisme g est unipotent si $g - Id$ est nilpotent. On note U_n l'ensemble des matrices carrées, de taille n, triangulaires supérieures, et dont les éléments diagonaux sont tous 1.

3.1 Théorème. *[Bor91, 4.8] Soit G un sous-groupe de $GL_n(k)$ non nécessairement défini sur k dont tous les éléments sont unipotents, alors G est conjugué sur k à un sous-groupe de $U_n(k)$.*

3.2 Définition. Un k-groupe G est dit unipotent si $G = G_u = \{g_u | g \in G\}$.

3.3 Corollaire. *Soit U un k-groupe unipotent, U est isomorphe à un k-sous-groupe de U_n pour un certain entier n.*

Démonstration. [Bor91, 4.8]
C'est une conséquence de la proposition 1.12 et du théorème 3.1. □

3.4 Proposition. *Soit U un groupe unipotent, tout morphisme $U \to G_m$ est trivial.*

Démonstration. En effet un tel morphisme est une représentation de dimension 1, donc triviale. □

3.2 Extension de G_a par G_a

On a vu dans le paragraphe 2.1 la définition de groupe diagonalisable déployé. En fait, la notion de déploiement est plus générale : un k-groupe G est dit déployé s'il admet une suite de composition dont les quotients successifs sont k-isomorphes à G_a ou G_m. Dans le cas d'un groupe unipotent U les quotients successifs sont tous des G_a.

Dans le cas des groupes unipotents, cette définition mène naturellement à s'intéresser aux extensions de G_a par G_a.

La théorie des extensions de groupes algébriques commutatifs est faite en annexe 4.1 et 4.2.

Dans la suite du paragraphe k est algébriquement clos.

Selon la proposition 4.5 $\mathrm{Ext}(G_a, G_a) \cong H^2_{reg}(G_a, G_a)_s$, on recherche donc des applications régulières $f : G_a \times G_a \to G_a$, c'est-à-dire des polynômes en deux variables, qui vérifient la relation de cocycle suivante :

$$\forall x, y, z \in A,\ f(y,z) - f(x+y,z) + f(x,y+z) - f(x,y) = 0 \tag{13}$$

On remarque que si k est de caractéristique $p > 0$ alors

$$F(x,y) = \frac{1}{p}\left(x^p + y^p - (x+y)^p\right) \tag{14}$$

vérifie la relation de cocycle (13).

3.5 Proposition. *[Laz55, III]*

Si k est de caractéristique $p > 0$ alors $H^2_{reg}(G_a, G_a)_s$ admet pour base les puissances p-iémes de la fonction F définie en (14).

Si k est de caractéristique 0 alors $H^2_{reg}(G_a, G_a)_s$ est trivial.

On a donc en particulier des extensions de G_a par G_a non triviales sur un corps algébriquement clos en caractéristique positive, et seulement dans ce cas.

Mais même s'il y a des extensions non triviales sur un corps algébriquement clos, le corollaire 3.6 nous assure que tous les groupes unipotents sur un tel corps sont déployés.

3.6 Corollaire. *[Bor91, 15.5 (ii)]*

Soit k un corps parfait et G un k-groupe unipotent, G est déployé sur k.

Le corollaire 3.6 n'est malheureusement pas généralisable au cas des corps non parfaits comme le montre l'exemple ci-dessous.

3.7 Exemple. En effet, considérons un corps k non parfait de caractéristique p. Soit $a \in k - k^p$, le k groupe $U = \{y^p = x - ax^p\}$ est isomorphe à G_a sur l'extension purement inséparable $k(a^{1/p})$ mais n'est pas déployé. En effet s'il était déployé, il serait isomorphe à G_a sur k, or la compactification de U a un unique point à l'infini dont le corps des résidus est $k(a^{1/p})$.

Notre objectif va être d'étudier les groupes unipotents avec des outils plus explicites que ceux qu'utilise Borel pour démontrer 3.6.

3.3 p-polynôme et applications

Ici k est un corps de caractéristique $p > 0$.

3.8 Définition. Un polynôme $P \in k[X_1, \dots, X_n]$ est dit un p-polynôme si les monômes qui le composent sont de la forme $c_{i,j} X_i^{p^j}$.

3.9 Remarque. On peut écrire P sous la forme $P = \sum_{i=1}^{n} P_i(X_i)$ où les P_i sont des p-polynômes à une variable.

De plus $P(0) = 0$ et $\forall i, P_i(0) = 0$

3.10 Proposition. *Un polynôme $P \in k[X_1, \dots, X_n]$ est un p-polynôme si et seulement si c'est un k-morphisme vu comme application $G_a^n \to G_a$*

Démonstration. [Tits67, 3.3.4]

Montrons que si $P(x_1 + y_1, \dots, x_n + y_n) = P(x_1, \dots, x_n) + P(y_1, \dots, y_n)$ alors P est un p-polynôme, le reste étant clair.

On raisonne par récurrence sur le degré de P.

Pour tout $y \in k^n$, $P(X + y) = P(X) + P(y)$ donc $\forall i$, $\frac{\partial P}{\partial X_i}(X + y) = \frac{\partial P}{\partial X_i}(X)$.

Donc $\frac{\partial P}{\partial X_i}(X) = \gamma_i$ est constant, et $P - \sum_{i=1}^{n} \gamma_i Xi$ est additif de dérivée partielle nulle. Donc $P - \sum_{i=1}^{n} \gamma_i Xi = Q(X_1^p, \dots, X_n^p)$.

Pour conclure on applique l'hypothèse de récurrence à Q. □

Un polynôme sur k non nul est dit séparable si son schéma des zéros est génériquement lisse, c'est-à-dire s'il est sans facteur carré dans $\overline{k}$.

3.11 Proposition. *Soit $P \in k[X_1, \dots, X_n]$ un polynôme non nul tel que $P(0) = 0$. Alors le sous-schéma $P^{-1}(0) \subseteq G_a^n$ est un k-sous-groupe si et seulement si P est un p-polynôme séparable.*

Démonstration. [Tits67, 3.3.4]

Si P est un p-polynôme séparable alors $P^{-1}(0)$ k-sous-groupe est clair par ce qui vient d'être vu.

Reste la réciproque : on note $G = P^{-1}(0)$, la lissité de G implique P séparable. Selon la proposition 3.10 il suffit de montrer que P est un k-morphisme.

Soit $\alpha \in G(k)$, le schéma des zéros de $P(x+\alpha)$ et $P(x)$ est G. Donc $P(x+\alpha) = c(\alpha)P(x)$ où $c(\alpha) \in k^*$.

La fonction c est une fonction polynomiale de α et vérifie :

$$c(\alpha + \beta)P(x) = P(\alpha + \beta + x) = c(\alpha)c(\beta)P(x) \tag{15}$$

Donc $c : G \to GL_1$ est un k-morphisme. Mais G est unipotent donc selon la proposition 3.4 $c = 1$. Donc $\forall \alpha \in G(k), P(x + \alpha) = P(x)$.

Soit $\beta \in k^n$, $\forall \alpha \in G(k)$ $P(\alpha + \beta) - P(\beta) = 0$, donc $P(\alpha + \beta) - P(\beta)$ s'annule sur G, donc $P(\alpha + \beta) - P(\beta) = g(\beta)P(x)$ où $g(\beta) \in k$ et $g(0) = 1$.

Donc pour tout $\gamma \in k^n$ on a :

$$P(\alpha + \gamma + x) - P(\beta + \gamma) = g(\beta + \gamma)P(x). \tag{16}$$

De plus on a :

$$P(\alpha+\gamma+x) = P(\beta) + g(\beta)P(x+\gamma) = P(\beta) + g(\beta)P(\gamma) + g(\beta)g(\gamma)P(x). \quad (17)$$

En comparant les termes de plus haut degré on trouve que $g(\beta+\gamma) = g(\beta)g(\gamma)$, donc $g(\beta)^p = g(0) = 1$, donc P est bien additive.

□

3.12 Corollaire. *Soit $G \subset G_a^n$ un k-sous-groupe de codimension 1, alors G est le schéma des zéros d'un p-polynôme séparable de $k[X_1, \ldots, X_n]$.*

Démonstration. [CGP10, B.1.5]
G est de codimension 1 dans G_a^n donc c'est le schéma des zéros d'un polynôme séparable qui est un p-polynôme selon la proposition 3.11.

□

3.13 Définition. Un groupe vectoriel sur k est un k-groupe commutatif V qui est isomorphe à G_a^n pour un certain $n \geq 0$. L'action de GL_1 issue de cet isomorphisme est appelée structure linéaire sur V.

3.14 Définition. Si $P = \sum_{i=1}^{n} P_i(X_i)$ est un p-polynôme sur k en n variables, alors la partie de P noté P_{princ} est la somme des termes de plus haut degré des P_i.

3.15 Lemme. *Soit V un groupe vectoriel sur k de dimension $n > 0$, soit $f : V \to G_a$ un k-morphisme, alors les assertions suivantes sont équivalentes :*

1. *Il existe un morphisme de k-schémas non constant $f' : \mathbb{A}_k^1 \to V$ tel que $f \circ f' = 0$.*
2. *Pour tout k-isomorphisme $h : G_a^n \cong V$, la partie principale du p-polynôme $f \circ h \in k[X_1, \ldots, X_n]$ a un zéro non trivial dans k.*
3. *Il existe un isomorphisme de k-groupes $h : G_a^n \cong V$ tel que $\ker(f \circ h)$ contient le premier facteur de G_a^n.*

Démonstration. [CGP10, B.1.7]
On va montrer que $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$.
Supposons 1, on considère alors $\varphi = h^{-1} \circ f' : \mathbb{A}_k^1 \to G_a^n$, l'on note $\varphi_i : \mathbb{A}_k^1 \to G_a$ la i-ème composante de φ et $a_i t^{s_i}$ le monôme dominant de $\varphi_i(t)$, où $s_i = 0$ si $\varphi_i = 0$.
f' est non constant donc φ aussi, donc pour un certain i on a $s_i > 0$.
Soit $\sum_{i=1}^{n} c_i x_i^{p^{m_i}}$ la partie principale de $f \circ h$.
On a alors :

$$0 = f(h(\varphi(t)) = \sum_{i=1}^{n} c_i a_i^{p^{m_i}} t^{s_i p^{m_i}} + \ldots \quad (18)$$

On note $N = \max s_i p^{m_i}$, et on définit $b_i = a_i$ si $s_i p^{m_i} = N$, $b_i = 0$ sinon. Le coefficient de degré N de $f(h(\varphi(t))$ est 0 donc $\sum_{i=1}^{n} c_i b_i^{p^{m_i}} = 0$ où les b_i sont dans k non tous nuls. C'est exactement 2.

Montrons $2 \Rightarrow 3$:
Soit $h : G_a^n \cong V$ un isomorphisme de k-groupes. On peut supposer que f est non nul, donc la partie principale de $f \circ h$ est non nulle.

On raisonne par récurrence sur la somme des degrés des monômes de la partie principale de $f \circ h$, toujours notée $\sum_{i=1}^{n} c_i x_i^{p^{m_i}}$.

Si l'un des c_i est 0, quitte à permuter les variables 3 est vrai. Sinon, on suppose que tous les c_i sont non nuls et que $m_1 \geq \cdots \geq m_n \geq 0$. Par hypothèse il existe $(a_1, \ldots, a_n) \in k^n - \{0\}$ tel que $\sum_{i=1}^{n} c_i a_i^{p^{m_i}} = 0$. Soit $r \geq 0$ le plus petit entier tel que a_r est non nul.

On considère $h' : G_a^n \cong G_a^n$ défini par

$$h'(y_1, \ldots, y_n) = \left(y_1, \ldots, y_{r-1}, a_r y_r, y_{r+1} + a_{r+1} y_r^{p^{m_r - m_{r+1}}}, \ldots, y_n + a_n y_r^{p^{m_r - m_n}}\right) \tag{19}$$

Alors $f \circ h \circ h'$ est un p-polynôme dont la partie principale est $\sum_{i \neq r} c_i y^{p^{m_i}}$ de somme des degrés strictement inférieurs d'où 3 par récurrence.

Il reste à montrer que 3 implique 1 :

Soit h vérifiant 3 et $\varphi : t \in G_a \mapsto (t, 0, \ldots, 0) \in G_a^n$, alors $f' = h \circ \varphi$ convient.

□

3.16 Lemme. *Soit K/k une extension galoisienne. Si un p-polynôme de la forme $\sum_{i=1}^{n} c_i x_i^{p^{m_i}}$ a un zéro dans $K^n - \{0\}$ alors il a un zéro dans $k^n - \{0\}$.*

Démonstration. [CGP10, B.1.8]

On peut supposer que $m_1 \geq \cdots \geq m_n$. On raisonne par récurrence sur n. Si $n = 1$ alors $c_1 a_1^{p^{m_1}} = 0$ avec $a_1 \in K^*$ implique $c_1 = 0$. Donc le polynôme est nul.

Supposons $n > 1$, alors il existe $a \in K^n - \{0\}$ tel que $\sum_{i=1}^{n} c_i a_i^{p^{m_i}} = 0$. Si l'un des a_i est nul le théorème est vrai par récurrence. Sinon on peut supposer $a_n = 1$. Pour tout $\sigma \in \mathrm{Gal}(K/k)$, alors $a - \sigma(a)$ est un zéro du polynôme. Si $a \in k^n$ alors il n'y a rien à faire, sinon il existe $\sigma \in \mathrm{Gal}(K/k)$ tel que $a - \sigma(a) \neq 0$ or $a_n - \sigma(a_n) = 0$. On peut alors conclure par récurrence.

□

3.17 Lemme. *Soit V un groupe vectoriel sur k, soit K/k une extension galoisienne et soit $f : V \to G_a$ un k-morphisme, alors les conditions équivalentes du lemme 3.15 sont vraies sur K si et seulement si elles sont vraies sur k.*

Démonstration. [CGP10, B.1.9]

C'est une conséquence immédiate de 3.15 et 3.16. □

3.4 Groupes unipotents commutatifs d'exposant p

Ici k est un corps de caractéristique $p > 0$.

3.18 Théorème. *Soit G un k-groupe commutatif d'exposant p, alors G est k-isomorphe à un k-sous-groupe d'un certain G_a^N.*

3.19 Remarque. Ce théorème est vrai sur un corps de caractéristique nulle, et la preuve est beaucoup plus simple : G peut être vu comme un sous-groupe d'un certain GL_n et donc de M_n par passage au logarithme.

La preuve ci-dessous due à Tits, et que l'on peut trouver dans [Tits67] utilise des astuces pour pallier au manque d'exponentielle.

Démonstration. [Tits67, 3.3.1]

On peut supposer que $G \subset GL_n \subset M_n$. Soit A le k-espace vectoriel engendré par $\{g - I_n |\ g \in G\}$. On note A^i le k-espace vectoriel engendré par $\{a^i |\ a \in A\}$.

On a alors $(g - I_n)(h - I_n) = (gh - I_n) - (g - I_n) - (h - I_n)$ donc $\{0\} = A^p \subset \cdots \subset A^2 \subset A$.

Soit $(a_1, \ldots, a_r)$ une base de A telle que pour tout j, A^j est engendré par $(a_{i_j}, \ldots, a_r)$ pour un certain i_j.

On considère l'application suivante :

$$\begin{array}{rccc} \varphi : & A & \to & I_n + A \\ & \sum_{i=1}^{n} x_i a_i & \mapsto & \prod_{i=1}^{n} \exp x_i a_i \end{array} \tag{20}$$

où $\exp x_i a_i = \sum_{k=1}^{p-1} \frac{(x_i a_i)^k}{k!}$.

On remarque que $\exp((x+y)a) = \exp(xa)\exp(ya)$. De plus A est commutatif donc $\varphi : A \to I_n + A$ est un k-morphisme du groupe additif A dans le groupe multiplicatif $I_n + A$ qui contient G. Montrons que φ est inversible.

Or $\prod_{i=1}^{n} \exp x_i a_i = I_n + \sum_{i=1}^{n} y_i a_i$, où y_i est de la forme $x_i + P_i(x_1, \ldots, x_{i-1})$ par construction des a_i. □

3.20 Proposition. *Soit $V_1, \ldots, V_n$ des k-groupes isomorphes à G_a et soit $V = \prod_{i=1}^{n} V_i$.*

Soit U un k-sous groupe de V tel que $U(k_s)$ est le k_s sous groupe de $V(k_s)$ engendré par l'image d'une famille de morphismes de k_s-schémas $\mathbb{A}^1_{k_s} \to V(k_s)$ qui passent par 0.

Alors il existe un automorphisme de k-groupe $h : V \cong V$ tel que $h(U)$ est le produit de certains des V_i. En particulier, U est un groupe vectoriel.

Démonstration. [CGP10, B.1.11]

On raisonne par récurrence sur n. Si $n = 1$ c'est évident.

On suppose $n > 1$, dans le cas où $U = V$ la proposition est claire, on peut donc supposer que $\dim(U) \leq n - 1$. Si la dimension de U est $n - 1$ alors selon le corollaire 3.12, U est le noyau d'un k-morphisme $f : V \to G_a$. Par hypothèse il existe un morphisme de k_s-schéma non constant $\mathbb{A}^1_{k_s} \to U_{k_s}$, donc selon le lemme 3.15 appliqué à $k = k_s$ et le lemme 3.16 il existe h' k-automorphisme de V tel que $V_1 \subset h'(U)$.

Alors $h'(U) = V_1 \times U'$ où U' est la projection de $H'(U)$ sur $V' = \prod_{i \geq 2} V_i$.

L'hypothèse de récurrence appliquée à U' et V' nous permet de conclure.

Reste le cas $\dim(U) < n - 1$, soit U' la projection de U sur V'. Par hypothèse de récurrence, après renumérotation il existe $h_1 : V' \cong V'$ tel que $h_1(U') = \prod_{i=2}^{r} V_i$ pour $r < n$. Alors $h' = id_{V_1} \times h_1 : V \cong V$ vérifie $h'(U) \subset \prod_{i=1}^{r} V_i$, ce qui permet de conclure par récurrence.

□

3.21 Corollaire. *Soit G un groupe d'exposant p, commutatif, alors tout k-sous groupe qui est un groupe vectoriel est un facteur direct de G.*

Démonstration. [CGP10, B.1.12]

C'est une conséquence immédiate de 3.20 et 3.18. □

3.22 Proposition. *Soit k un corps de caractéristique $p > 0$ et de cardinal infini. Soit U un k-groupe commutatif d'exposant p.*

Alors U est k-isomorphe à un k-sous-groupe de codimension 1 d'un k-groupe vectoriel. En particulier, U est isomorphe au schéma des zéros d'un p-polynôme non nul et séparable sur k.

Démonstration. [CGP10, B.1.13]

Selon le théorème 3.18 U peut être identifié avec un k-sous-groupe d'un k-groupe vectoriel V. Si $m = \dim(V) - \dim(U) \leq 1$ alors on applique le corollaire 3.12.

Sinon supposons $m > 1$, on va montrer que U peut être identifié à un k-sous-groupe de W groupe vectoriel de dimension $\dim(W) = \dim(V) - 1$.

$\mathrm{Lie}(U)$ est un sous-k-espace vectoriel de $\mathrm{Lie}(V) \cong V$ de codimension m. On note $G_a.U$ l'adhérence de Zariski de l'image de l'application produit $G_a \times U \to V$. C'est un sous-schéma de V de codimension strictement positive. V étant irréductible l'union $\mathrm{Lie}(U) \cup G_a.U$ est strictement inclus dans V.

Le corps k est supposé infini donc $V(k)$ est Zariski dense dans V, donc il existe $v \in V(k)$ tel que $v \notin \mathrm{Lie}(U) \cup G_a.U$.

Soit L le k-sous groupe de V correspondant à la droite vectorielle engendrée par v. Soit $\varphi : V \to W = V/L$ et $\psi = \varphi_{|U}$, on va montrer que $\ker(\psi) = \{1\}$, ce qui permet d'identifier U avec un sous-groupe de W.

Selon le théorème 1.11 il suffit de montrer que $d(\psi)$ est bijective et que $\psi_{|U(\overline{k})}$ est bijective.

L'application $\mathrm{Lie}(\psi)$ a pour noyau $L \cap \mathrm{Lie}(U) = \{0\}$. Si $\psi_{|U(\overline{k})}$ n'est pas injective alors L serait inclus dans $G_a.U$. Or $v \in L(k)$ et $v \notin G_a.U(\overline{k})$. □

3.5 Groupes totalement ployés

Ici k est un corps de caractéristique $p > 0$.

La notion de groupe unipotent totalement ployé est l'analogue de la notion de tore anisotrope.

On rappelle qu'un tore est anisotrope s'il n'y a pas de morphisme de k-groupe $T \to G_m$ non trivial.

3.23 Définition. Un k-groupe unipotent U est dit k-totalement ployé si tout morphisme de k-schéma $\mathbb{A}^1_k \to U$ est constant, d'image un point de $U(k)$.

3.24 Remarque. On dit aussi k-ployé à la place de k-totalement ployé.

La définition de k-ployé a un sens en caractéristique 0, mais elle implique alors U trivial.

3.25 Exemple. On suppose que k est non parfait, soit $a \in k - k^p$. Le k groupe

$$U := \{y^p = x - ax^p\} \tag{21}$$

est un sous groupe de G_a^2 qui devient isomorphe à G_a sur $k(a^{1/p})$ mais qui est k-ployé.

3.26 Remarque. Supposons k infini. Selon la proposition 3.22 les k-groupes G commutatifs d'exposant p sont exactement les schémas des zéros des p-polynômes séparables non nuls.

Or G est connexe si et seulement si P irréductible sur k.

Supposons G connexe, si la partie principale P_{prin} de P n'a pas de zéro dans $k^n - \{0\}$ alors selon le lemme 3.15 G est k-ployé. Mais la réciproque est fausse.

Par contre si P est un p-polynôme dont la partie principale P_{prin} a un zéro sur $k^n - \{0\}$, alors la preuve de l'implication entre la seconde et la troisième assertion du lemme 3.15 montre que l'on peut trouver un p-polynôme Q qui a un schéma des zéros isomorphe à celui de P et dont la somme des degrés des monômes de la partie principale est strictement inférieure à celle de P. Par récurrence immédiate on peut obtenir un p-polynôme R dont le schéma des zéros est k-isomorphe à celui de P, et dont la partie principale n'a pas de zéro non trivial.

Dans ce sens, les schémas des zéros des p-polynômes irréductibles dont la partie principale n'a pas de zéro non trivial sont exactement les k-groupes k-ployés, commutatifs et d'exposant p.

3.27 Théorème. *Soit U un k-groupe commutatif connexe d'exposant p. Alors U est le produit direct d'un k-groupe vectoriel et W k-groupe connexe unipotent tel que W_{k_s} est k_s-ployé.*

De plus le facteur vectoriel est engendré par les images des morphismes de k_s-schémas $\mathbb{A}^1_{k_s} \to U_{k_s}$ passant par l'identité.

Démonstration. [CGP10, B.2.5]

Soit V le sous-groupe de G engendré par les images de tous les k_s-morphismes $\varphi : G_a \to U_{k_s}$ qui passent par l'identité. Ce groupe V est défini sur k_s et est invariant par l'action de $\mathrm{Gal}(k_s/k)$ donc V est défini sur k selon le théorème 1.7. Selon le lemme 3.18, on peut identifier U avec un sous-groupe d'un k-groupe vectoriel. Donc selon la proposition 3.20 V est un groupe vectoriel sur k. Selon le corollaire 3.21 on a $U = V \times W$ où W est un k-sous groupe de U. Le groupe U est connexe et unipotent donc W aussi, et par définition de V, W est k_s-ployé.

Il reste à montrer que V est unique. Soit $U = V' \times W'$ une autre décomposition, l'image des morphismes de k_s-schémas $\varphi : \mathbb{A}^1_{k_s} \to U_{k_s}$ qui passent par l'identité est contenue dans V'_{k_s} car W' est k_s-ployé.

Donc $V \subset V'$ donc $V' = V \times V'_1$ où V'_1 est l'image de V' par $U \twoheadrightarrow W$ or W_{k_s} est k_s-ployé et V' groupe vectoriel donc $V'_1 = \{0\}$.

□

3.28 Corollaire. *Soit U un k-groupe connexe commutatif d'exposant p, alors les assertions suivantes sont équivalentes :*

1. *U est k-ployé ;*
2. *U_{k_s} est k_s-ployé ;*
3. *il n'y a pas de morphisme de k-groupe non trivial $G_a \to U$.*

De plus le k-groupe U est un groupe vectoriel sur k si et seulement si U_{k_s} est un k_s-groupe vectoriel.

Démonstration. [CGP10, B.2.6]

C'est une conséquence immédiate de 3.27 □

3.29 Lemme. *Tout $\overline{k}$-groupe G totalement ployé, connexe, commutatif, d'exposant p est trivial.*

Démonstration. [Tits67, 3.3.13]

Par l'absurde, si $\dim(G) \geq 1$. Selon 3.22 on peut supposer que G est le noyau de $f : G_a^n \to G_a$. Selon le lemme 3.15 il existe $f' : G_a \to V$ non constant tel que $f \circ f' = 0$ (en effet 2 est toujours vrai sur $\overline{k}$), contradiction avec G ployé. □

3.30 Théorème. *Si k est un corps parfait et G est un k-groupe connexe commutatif d'exposant p alors G est k-isomorphe à un groupe vectoriel.*

Démonstration. [Tits67, 3.3.14]

Selon 3.28 on peut supposer $k = \overline{k}$ on applique ensuite le théorème 3.27 puis le lemme 3.29.

□

3.31 Remarque. Ce théorème est prouvé dans [SGA3, exposé XVII, lemme 4.1.5] comme conséquence de Hilbet 90 pour la dimension 1, par récurrence pour les dimensions supérieures

3.6 Noyau cckp et applications

Ici k est un corps de caractéristique $p > 0$.

3.32 Définition. Soit U un k-groupe unipotent connexe, le noyau cckp de U est le k-sous-groupe maximal de U qui est connexe, central et d'exposant p.

La définition ci-dessus a un sens car deux k-sous-groupes, connexes, centraux et d'exposant p engendrent un groupe avec les même propriétés.

3.33 Proposition. *Soit U un k-groupe connexe et unipotent, soit K/k une extension séparable. On note F le noyau cckp de U. Alors U est k-ployé si et seulement si U_K est K-ployé. Si U est k-ployé alors U/F l'est aussi.*

De plus les conditions suivantes sont équivalentes :

1. *U est k-ployé.*
2. *U n'a pas de k-sous groupe central k-isomorphe à G_a.*
3. *F est k-ployé.*

3.34 Remarque. Cette proposition implique que U est k-ployé si, et seulement si, il n'y a pas de k-morphisme non trivial de G_a dans U. Cette propriété est exactement analogue à la définition de l'anisotropie pour les tores. La définition 3.23 est donc une astuce qui simplifie les preuves.

Le fait d'être ployé n'est pas modifié par passage à une extension séparable ; alors que les tores se déploient sur une extension séparable, mais les extensions purement inséparables conservent l'anisotropie. En fait le théorème 3.39 montre que la situation est vraiment inversée : les groupes unipotents se déploient sur des extensions purement inséparables.

Démonstration. [CGP10, B.3.2]

On commence par montrer l'équivalence des trois conditions : $1 \Rightarrow 2$ est évidente. Selon le corollaire 3.28 les conditions 2 et 3 sont équivalentes.

Pour montrer que 3 implique 1 on va montrer que si U_{k_s} n'est pas k_s-ployé alors F n'est pas k-ployé. Et on aura en même temps montré que si K/k est une extension séparable alors U est k-ployé implique U_K est K-ployé.

Soit $\varphi : \mathbb{A}^1_{k_s} \to U_{k_s}$ un morphisme de k_s-schéma non constant. Quitte à composer avec une translation, on peut supposer que $\varphi(0) = 1$.

Si $\varphi(\mathbb{A}^1_{k_s})$ n'est pas central alors U n'est pas commutatif et il existe $g \in U(k_s)$ qui ne centralise pas $\varphi(\mathbb{A}^1_{k_s})$. Le morphisme de k_s-schémas $\varphi' : \mathbb{A}^1_{k_s} \to U_{k_s}$ défini par $\varphi'(x) = g^{-1}\varphi(x)^{-1}g\varphi(x)$, est non constant et son image est incluse dans le groupe dérivé $\mathcal{D}(U_{k_s}) = \mathcal{D}(U)_{k_s}$. Le k-groupe $\mathcal{D}(U)$ est de dimension inférieure à U et est non trivial, donc par itération on obtient $\varphi : \mathbb{A}^1_{k_s} \to U_{k_s}$ qui est central non constant. De plus on peut supposer que $\varphi(\mathbb{A}^1_{k_s})$ est d'exposant p quitte à remplacer φ par φ^{p^e} pour e entier bien choisi.

On a donc obtenu $\varphi : \mathbb{A}^1_{k_s} \to U_{k_s}$ non constant dont l'image est incluse dans F_{k_s}. Ainsi le groupe F_{k_s} n'est pas k_s-ployé, et donc selon le corollaire 3.28 le groupe F n'est pas k-ployé.

Pour prouver notre proposition, il reste donc à montrer que si U est k-ployé alors U/F l'est aussi. En vertu du travail fait ci-dessus on peut supposer que $k = k_s$.

Supposons que U est k-ployé mais que U/F n'est pas k-ployé, alors U/F admet un k-sous groupe central k-isomorphe à G_a noté A. Soit π la surjection canonique de U dans U/F, le k-sous groupe $\pi^{-1}(A)$ est unipotent et connexe.

Si $\pi^{-1}(A)$ n'est pas central dans U alors, il existerait $g \in U(k)$ qui ne centralise pas $\pi^{-1}(A)$ et on aurait un morphisme de k-schéma non constant :

$$\varphi : xF \in \pi^{-1}(A)/F \cong \mathbb{A}^1_k \mapsto gxg^{-1}x^{-1} \in F \tag{22}$$

ce qui est exclu car F est k-ployé. Donc $\pi^{-1}(A)$ est central dans U.

De même $\pi^{-1}(A)$ est de p-torsion car sinon on aurait un morphisme non constant de k-schémas $\psi : xF \in \mathbb{A}^1_k \mapsto x^p \in F$.

Ainsi $\pi^{-1}(A)$ est inclus dans F donc $\pi^{-1}(A) = F$, ce qui implique $A = 1$ ce qui est absurde car $A \cong G_a$.

□

3.35 Théorème. *Soit U un k-groupe connexe, unipotent.*

1. *Il existe un unique k-sous groupe U_{dep} de U, connexe, normal et k-déployé tel que U/U_{dep} est k-ployé.*
2. *Le sous-groupe U_{dep} contient l'image de tout k-morphisme d'un k-groupe, connexe, unipotent et k-déployé dans U.*
3. *Le noyau de tout k-morphisme de U dans un k-groupe, connexe, unipotent et k-ployé contient U_{dep}.*
4. *La définition de U_{dep} commute avec les extensions séparables de k.*

3.36 Remarque. Le théorème ci-dessus est l'analogue du théorème de structure des tores 2.12.

Démonstration. [CGP10, B.3.4]

Si U est k-ployé alors $U_{dep} = \{1\}$ convient. Sinon on suppose que U n'est pas k-ployé et on raisonne par récurrence sur la dimension de U. Soit A un k-sous groupe central, isomorphe à G_a (A existe selon la proposition 3.33).

Soit $H = U/A$, par récurrence, il existe un k-sous groupe H_{dep} de H qui est connexe, normal, k-déployé et vérifie les autres propriétés du théorème. Soit

U_{dep} le k-sous groupe correspondant à H_{dep} contenant A, il est k-déployé et $U/U_{dep} \cong H/H_{dep}$ est k-ployé.

Prouvons 2 : Soit U' un k-groupe connexe, unipotent qui a une suite de composition $(U'_i)_i$ où $U'_0 = U'$ et dont les quotients successifs sont isomorphes à G_a. Soit $\varphi : U' \to U$ un k-morphisme. Il existe un indice i minimal tel que $\varphi(U'_i) \subseteq U_{dep}$. Si $i > 0$ alors φ induit un k-morphisme de $G_a \cong U'_{i-1}/U'_i \to U/U_{dep}$ d'image non triviale. Ce qui est exclu car U/U_{dep} est k-ployé. On en déduit que $i = 0$, et donc $\varphi(U') \subseteq U_{dep}$; c'est l'unicité de U_{dep}.

Soit $\varphi : U \to U''$ un k-morphisme où U'' est un k-groupe connexe, unipotent et k-ployé. Par 2 on a $\varphi(U_{dep}) \subset U''_{dep} = \{1\}$.

Il reste 4 : Soit K/k une extension séparable on note $U' := U_K$ alors $(U_{dep})_K \subset U'_{dep}$. De plus le quotient $U'_{dep}/(U_{dep})_K$ est un K-sous groupe de $(U/U_{dep})_K$ qui est selon la proposition 3.33 K-ployé. Or $U'_{dep}/(U_{dep})_K$ est K-déployé, donc trivial.

□

3.7 Structure des groupes unipotents

Ici k est un corps de caractéristique $p > 0$.

3.37 Définition. Soit G et H deux k-groupes, G est dit une k-forme de H si G et H sont isomorphes en tant que $\overline{k}$-groupes.

3.38 Théorème. *Soit U un k-groupe connexe et unipotent, alors U admet une suite centrale de k-sous-groupes :*

$$\{1\} = U_n \subset \cdots \subset U_0 = U \tag{23}$$

telle que pour tout i, U_i/U_{i+1} est une k-forme de $G_a^{m(i)}$ pour $m(i) \geq 0$.

Démonstration. [KMT74, 8.1]

On note $H_1 = \mathcal{D}(U) = [U, U]$ et pour $i > 1$, $H_i = [U, H_{i-1}]$. Selon le corollaire 1.13 ce sont des k-sous-groupes de U. On a donc une suite centrale descendante :

$$\{1\} = H_g \subset \cdots \subset H_1 \subset U \tag{24}$$

où H_i et H_{i-1}/H_i sont connexes. De plus H_{i-1}/H_i est commutatif. On peut donc supposer que U est en plus commutatif.

Soit U^{p^n} l'image de U par $x \in U \mapsto x^{p^n} \in U$; c'est un k-groupe et on a $\{1\} = U^{p^N} \subset \cdots \subset U^p \subset U$.

On a donc obtenu une suite centrale de k-groupes dont les quotients successifs sont connexes, commutatifs, unipotents et d'exposant p. Selon le théorème 3.30 ce sont bien des k-formes de G_a^N. □

3.39 Théorème. *Soit U un k-groupe connexe et unipotent. Il existe une extension purement inséparable K/k telle que U_K est K-déployé.*

Démonstration. On peut le voir comme un raffinement du théorème 3.38, l'hypothèse dans le théorème 3.30 est k parfait donc les quotients sont isomorphes à G_a sur $k^{p^{-\infty}}$. On en déduit que $U_{k^{p^{-\infty}}}$ est $k^{p^{-\infty}}$-déployé. Donc il existe des extensions $k^{p^{-\infty}}/K/k$ où K/k est finie et U_K est K-déployé. □

3.40 Remarque. On peut trouver une autre preuve dans [Bor91, 15.5].

3.8 Action des tores sur les groupes unipotents

Ici k est un corps de caractéristique $p > 0$.

3.41 Proposition. *Soit U k-groupe unipotent, alors U est totalement ployé sur k si et seulement si $U(k[[T]]) = U(k((T)))$*

Démonstration. [Oest84, V.8]

Si U n'est pas totalement ployé sur k alors il possède selon le théorème 3.33 un sous groupe H isomorphe à G_a qui vérifie donc $H(k[[T]]) \neq H(k((T)))$ a fortiori $U(k[[T]]) \neq U(k((T)))$.

Réciproquement, supposons U totalement ployé sur k, alors selon le théorème 3.33 U est aussi totalement ployé sur k_s, or

$$U(k[[T]]) = U(k((T))) \cap U(k_s[[T]]) \tag{25}$$

on est donc ramené au cas où $k = k_s$.

On remarque que si l'on a une suite exacte $1 \to U' \to U \xrightarrow{\pi} U'' \to 1$ telle que $U'(k[[T]]) = U'(k((T)))$ et $U''(k[[T]]) = U''(k((T)))$.

Selon la proposition 1.20 $U(k((T))) \to U''(k((T)))$ est surjective.

On montre dans l'annexe 4.4 que l'application $U(k[[T]]) \to U''(k[[T]])$ est surjective.

On a donc le diagramme commutatif

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U'(k[[T]]) & \longrightarrow & U(k[[T]]) & \longrightarrow & U''(k[[T]]) & \longrightarrow & 1 \\ & & \| & & \downarrow & & \| & & \\ 1 & \longrightarrow & U'(k((T))) & \longrightarrow & U(k((T))) & \longrightarrow & U''(k((T))) & \longrightarrow & 1 \end{array} \tag{26}$$

où les lignes sont exactes, on en déduit par le lemme des 5 que $U(k[[T]]) = U(k((T)))$.

Compte tenu du théorème 3.33, on applique la remarque ci-dessus avec $U' = F$ le noyau cckp de U et $U'' = U/F$. Si $U \neq F$ alors on conclut par récurrence sur la dimension.

Sinon on peut donc supposer que U est en plus d'exposant p, commutatif et connexe. Selon le théorème 3.22 et la remarque 3.26, le groupe U est isomorphe au schéma des zéros d'un p-polynôme séparable P de G_a^{n+1} dont la partie principale P_{princ} ne s'annule pas sur $k^{n+1} - \{0\}$. Un élément de $U(k((T)))$ est de la forme $(f_1, \ldots, f_{n+1})$ où les f_i sont dans $k((T))$, il vérifie $P(f_1, \ldots, f_{n+1}) = 0$.

On note $P_{princ} = \sum_{i=1}^{n+1} a_i T_i^{p^{m_i}}$, et ν_i l'ordre de la série de Laurent f_i. Si l'un des ν_i est négatif alors on note $\nu = \inf_{1 \leq i \leq n+1} p^{m_i} \nu_i$. L'annulation du monôme en T^ν dans $P(f_1, \ldots, f_n)$ donne un zéro de P_{princ} dans $k^{n+1} - \{0\}$. Ce qui est exclu donc les ν_i sont tous positifs et donc les f_i sont tous dans $k[[T]]$. □

On rappelle que si G, H sont des foncteurs en groupes alors une action de G sur H correspond à la donnée d'une transformation naturelle $G \times H \to H$ telle que $\forall R,\ G(R) \times H(R) \to H(R)$ soit une action au sens usuel.

3.42 Théorème. *Soit T un tore k-déployé et U un k-groupe unipotent k-ployé. Alors la seule action de T sur U est triviale.*

Démonstration. Une action de T sur U implique des actions de G_m sur U.

Or tous les k-morphismes $G_m \to U$ sont triviaux. En effet ils correspondent à des points de $U\left(k[T,T^{-1}]\right)$.

Mais $U\left(k[T,T^{-1}]\right) \subseteq U\left(k((T))\right) = U\left(k[[T]]\right)$ selon le théorème 3.41. Donc $U\left(k[T,T^{-1}]\right) = U\left(k[T]\right)$. Les application orbites sont donc triviales et l'action aussi. □

Une conséquence de ce théorème est que l'action d'un tore déployé maximal ne permet pas de décomposer l'algèbre de Lie d'un groupe unipotent totalement ployé.

4 Annexes

4.1 Extension de groupes algébriques commutatifs

Ici k est algébriquement clos.

Soit A, B et C trois groupes algébriques commutatifs, une suite exacte

$$0 \to B \to C \to A \to 0 \tag{27}$$

est dite strictement exacte si elle est exacte et si la structure algébrique de B est induite par celle de C et la structure algébrique de A est la structure quotient de celle de C par B.

4.1 Lemme. *[Ser59, chapitre VII §1. 1.]*

La suite (27) *est strictement exacte si et seulement si la suite* (27) *est exacte et si la suite d'espaces tangents à l'identité correspondante l'est aussi.*

Une suite strictement exacte (27) est appelée une extension de A par B. Par abus de langage, on parle de C extension de A par B.

Deux extensions C et C' sont isomorphes s'il existe $f : C \to C'$ tel que le diagramme

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & C & \longrightarrow & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle id} & & \\ 0 & \longrightarrow & B & \longrightarrow & C' & \longrightarrow & A & \longrightarrow & 0 \end{array} \tag{28}$$

est commutatif. Et dans ce cas f est automatiquement un isomorphisme selon le lemme des cinq. On note $\mathrm{Ext}(A,B)$ l'ensemble des classes d'extension de A par B.

Définissons le poussé en avant et le tiré en arrière d'une extension :

1. Soit $f : B \to B'$ et $C \in \mathrm{Ext}(A,B)$. Alors $f_*(C)$ est l'unique extension C' de A par B' tel qu'il existe $F : C \to C'$ rendant le diagramme

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & C & \longrightarrow & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle id} & & \\ 0 & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & A & \longrightarrow & 0 \end{array} \tag{29}$$

commutatif.

De façon explicite $f_*(C) = C \times B'/\{(-b, f(b)), b \in B\}$.

2. De même, soit $g : A' \to A$ et $C \in \mathrm{Ext}(A, B)$. Alors $g^*(C)$ est l'unique extension C' de A' par B tel qu'il existe $G : C' \to C$ rendant le diagramme

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & C' & \longrightarrow & A' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle G} & & \downarrow{\scriptstyle g} & & \\ 0 & \longrightarrow & B & \longrightarrow & C & \longrightarrow & A & \longrightarrow & 0 \end{array} \tag{30}$$

commutatif.

De façon explicite $g^*(C) = \{(a', c) \in A' \times C | g(a') = c\}$.

Avec ces deux opérations on va définir une loi de groupe sur $\mathrm{Ext}(A, B)$:

Soit C et C' deux éléments de $\mathrm{Ext}(A, B)$, on peut voir $C \times C'$ comme un élément de $\mathrm{Ext}(A \times A, B \times B)$.

On considère le plongement diagonal $d : A \to A \times A$ et la multiplication $s : B \times B \to B$. On définit alors $C + C' := d^* s_* C \times C'$.

4.2 Proposition. *[Ser59, chapitre VII §1. 1.]*
$(\mathrm{Ext}(A, B), +)$ *est un groupe abélien.*

La preuve étant assez longue et fastidieuse, contentons nous de remarquer que :

1. L'extension triviale $A \times B$ est le neutre.
2. Si $C \in \mathrm{Ext}(A, B)$, alors $-C = (-1)^*(C)$ où $(-1) : a \in A \mapsto -a \in A$

4.2 Systèmes de facteurs

Ici k est un corps algébriquement clos.

On se donne deux groupes algébriques commutatifs A et B.

On appelle système de facteurs sur A à valeurs dans B une application $f : A \times A \to B$ qui vérifie :

$$\text{pour tout } x, y, z \in A, f(y, z) - f(x + y, z) + f(x, y + z) - f(x, y) = 0 \tag{31}$$

Soit $g : A \to B$ est une application, on note δg la fonction

$$\delta g : (x, y) \in A \times A \mapsto g(x + y) - g(x) - g(y) \in B \tag{32}$$

δg vérifie l'identité 31, c'est donc un système de facteurs. Un tel système de facteurs est dit trivial.

4.3 Définition. $H^2(A, B)$ est l'ensemble des systèmes de facteurs modulo les systèmes de facteurs triviaux.

Un système de facteurs f est dit symétrique si $f(x, y) = f(y, x)$ pour tout x, y dans A.

Les classes de systèmes de facteurs symétriques forment un sous groupe de $H^2(A, B)$ noté $H^2(A, B)_s$.

Si l'on se restreint aux applications f régulières vérifiant (31) modulo les systèmes de facteurs triviaux issus d'applications régulières, on obtient un sous-groupe de $H^2(A, B)$ noté $H^2_{reg}(A, B)$.

4.4 Proposition. $H^2_{reg}(A, B)_s$ *est isomorphe au sous-groupe de* $\mathrm{Ext}(A, B)$ *formé des extensions qui admettent une section régulière.*

Démonstration. [Ser59, chapitre VII §1. 4.]

Si $C \in \mathrm{Ext}(A,B)$ admet une section régulière $s : A \to C$, on pose $f(x,y) = s(x+y) - s(x) - s(y)$. Alors f est une application régulière symétrique de A dans le noyau de $C \to A$, c'est à dire dans B. De plus f vérifie l'équation (31) et changer de section s revient à ajouter un système de facteurs trivial.

Si l'on note $\mathrm{Ext}(A,B)_*$ l'ensemble des extensions admettant une section régulière, on a défini une application $\theta : \mathrm{Ext}(A,B)_* \to H^2_{reg}(A,B)_s$. On admet que θ est un morphisme de groupes, il reste donc à montrer que θ est une bijection.

Si $\theta(C) = 0$ alors C admet une section s qui est un morphisme, donc $C \cong A \times B$. Ainsi θ est injective.

De plus si $f \in H^2_{reg}(A,B)_s$ alors on définit $A \times_f B$ comme étant $A \times B$ muni de la loi de groupe suivante :

$$(a,b) + (a',b') = (a+a', b+b'+f(a,a')) \tag{33}$$

qui fait de $A \times_f B$ un groupe algébrique commutatif extension de A par B admettant une section rationnelle. □

Un peu plus de travail permet de démontrer la proposition suivante que l'on admet ici :

4.5 Proposition. *[Ser59, VII proposition 7]*
Si A et B sont linéaires alors,

$$\mathrm{Ext}(A,B) \cong H^2_{reg}(A,B)_s \tag{34}$$

Cette proposition permet de simplifier le travail de recherche d'extension en le ramenant à la recherche de solutions de l'identité (31).

4.3 Restriction de Weil et applications

Soit K/k une extension de corps, soit G un schéma en groupes sur K, on note $A = K[G]$.

4.6 Définition. On considère le foncteur

$$\begin{array}{rccc} R_{K/k}(G) : & k-alg & \to & groupes \\ & R & \mapsto & G(R \otimes_k K) \end{array} \tag{35}$$

Ce foncteur est appelé restriction de Weil.

4.7 Lemme. *Si K/k est une extension finie séparable alors $R_{K/k}(G)$ est représentable donc c'est un k-schéma en groupe affine.*

Démonstration. [KMRT98, 20.6]

Soit $X = X(K)$ l'ensemble des morphismes de k-algèbres $\tau : K \to k$.

Le groupe de Galois $\Gamma = \mathrm{Gal}(k_s/k)$ agit sur X par ${}^{\gamma}\tau = \gamma \circ \tau$.

Soit $\tau \in X$, on note $A_\tau = A \otimes_K k_s$ où K agit sur k_s via τ c'est-à-dire pour tout $a \in A,\ l \in L$ et $x \in k_s$

$$al \otimes x = a \otimes \tau(l)x. \tag{36}$$

Soit $\gamma \in \Gamma$, on considère

$$\begin{array}{rccc} \tilde{\gamma_\tau} : & A_\tau & \to & A_{\gamma\tau} \\ & a \otimes x & \mapsto & a \otimes \gamma(x) \end{array} \tag{37}$$

c'est un isomorphisme d'anneaux qui vérifie pour tout $x \in k_s$ et $u \in A_\tau$

$$\tilde{\gamma_\tau}(xu) = \gamma(x)\tilde{\gamma_\tau}(u). \tag{38}$$

On considère $\widetilde{B} = \bigotimes_{\tau \in X} A_\tau$. Le groupe Γ agit sur $\widetilde{B}$ de façon continue via

$$\gamma\left(\bigotimes_{\tau \in X} a_\tau\right) = \bigotimes_{\tau \in X} \tilde{\gamma}(a_\tau). \tag{39}$$

De plus $\widetilde{B}$ est une k_s-algèbre et $\widetilde{B} = \bigotimes_{\tau \in X} A_\tau = \bigotimes_{\tau \in X} (A \otimes_{K,\tau} k_s)$. La structure d'algèbre de Hopf de A implique une structure d'algèbre de Hopf pour B qui est compatible avec l'action de Γ.

Soit $B = \widetilde{B}^\Gamma$, c'est une k-algèbre de Hopf. On va montrer que B représente le foncteur $R_{K/k}(G)$.

Soit R une k-algèbre,

$$\mathrm{Hom}_{k-alg}(B, R) \cong \mathrm{Hom}_{k_s-alg}(\widetilde{B}, R \otimes_k k_s)^\Gamma. \tag{40}$$

Un élément de $\mathrm{Hom}_{k_s-alg}(\widetilde{B}, R \otimes_k k_s)^\Gamma$ est déterminé par une collection de morphismes de k_s-algèbres que l'on note $(f_\tau)_{\tau \in X}$ où $f_\tau : A_\tau \to R \otimes_k k_s$ vérifie pour tous $\gamma \in \Gamma$ et $\tau \in X$ que le diagramme

$$\begin{array}{ccc} A_\tau & \xrightarrow{f_\tau} & R \otimes_k k_s \\ {\scriptstyle \tilde{\gamma_\tau}}\downarrow & & \downarrow{\scriptstyle id \otimes \gamma} \\ A_{\gamma\tau} & \xrightarrow[f_{\gamma\tau}]{} & R \otimes_k k_s \end{array} \tag{41}$$

est commutatif.

On considère $g_\tau = (f_\tau)_{|A}$, le morphisme g_τ vérifie alors $(id \otimes \gamma) \circ g_\tau = g_{\gamma\tau}$. Donc en particulier $\mathrm{Im}(g_\tau)$ est invariant sous l'action de $\mathrm{Gal}(k_s/\tau K) \subset \Gamma$ et $\mathrm{Im}(g_\tau) \subset R \otimes_k \tau K$.

L'application $h = (id \otimes \tau)^{-1} \circ g_\tau : A \to R \otimes_k K$ est indépendante du choix de τ et est un morphisme de K-algèbres.

Réciproquement pour tout morphisme de K-algèbres $h : A \to R \otimes_k K$ définit des applications $f_\tau : a \otimes x \mapsto (id \otimes \tau)h(a)(x)$.

Selon le lemme 4.8 on a $B \otimes_k k_s \cong \widetilde{B}$.

Soit R une k-algèbre, par définition de $R_{K/k}(G)$,

$$R_{K/k}(G)(R) = \mathrm{Hom}_{K-alg}(A, R \otimes_k K) = \mathrm{Hom}_{k-alg}(B, R). \tag{42}$$

□

4.8 Lemme (Descente de Galois)**.** *Soit k un corps quelconque, on note Γ le groupe de Galois $\mathrm{Gal}(k_s/k)$. Soit V un k_s-espace vectoriel, si Γ agit de façon continue sur V par automorphismes semi-linéaires alors*

$$V^\Gamma = \{v \in V |\ \forall \gamma \in \Gamma,\ \gamma.v = v\} \tag{43}$$

est un k-espace vectoriel.

De plus $v \otimes x \in V^\Gamma \otimes k_s \mapsto xv \in V$ est un isomorphisme de k_s-espaces vectoriels.

Démonstration. [KMRT98, 18.1]

Il est clair que V^Γ est un k-espace vectoriel. Il reste à montrer que $V^\Gamma \otimes k_s \to V$ est un isomorphisme de k_s-espace vectoriel.

On note $\star$ l'action de Γ sur V.

Montrons tout d'abord la surjectivité : soit $v \in V$, le groupe Γ agit de façon continue sur V donc il existe L extension galoisienne de k dans k_s tel que $\mathrm{Gal}(k_s/L)$ agit trivialement sur v.

Soit $(m_i)_{1\leq i\leq n}$ une base de L sur k et $(\gamma_i)_{1\leq i\leq n}$ un ensemble de représentants du quotient à gauche de $\Gamma/\mathrm{Gal}(k_s/L)$. Donc $\Gamma\star v = \{\gamma_1\star v, \dots, \gamma_n\star v\}$ où l'on peut choisir $\gamma_1 \star v = v$.

Pour tout $1 \leq j \leq n$, on note

$$v_j = \sum_{i=1}^{n} \gamma_i(m_j)(\gamma_i \star v). \tag{44}$$

On remarque que pour tout $\gamma \in \Gamma$, $1 \leq i \leq n$, il existe $1 \leq l \leq n$ et $\gamma' \in \mathrm{Gal}(k_s/L)$ tel que $\gamma\gamma_i = \gamma_l\gamma'$. L'action de Γ sur la somme (44) est une permutation, donc $v_j \in V^\Gamma$.

De plus $(\gamma_i(m_j))_{i,j}$ est inversible dans $GL_n(L)$ selon le lemme de Dedekind 2.1. On note $(m'_{i,j})$ la matrice inverse. On a alors :

$$v = \gamma_1 \star v = \sum_{i=1}^{n} m'_{i,1} v_i \tag{45}$$

d'où la surjectivité.

Pour montrer l'injectivité, on montre que l'image d'une famille k-libre est k_s-libre.

Par l'absurde, soit $v_1, \dots, v_r \in V^\Gamma$ une famille de vecteurs k-libres telle qu'il existe $m_1, \dots, m_r \in k_s$ non tous nuls qui vérifient

$$\sum_{i=1}^{r} m_i v_i = 0. \tag{46}$$

On peut supposer que $r > 1$ est minimal et que $m_1 = 1$.

Par hypothèse les m_i ne sont pas tous dans k, quitte à renuméroter les m_i on peut supposer que $m_2 \notin k$. En conséquence il existe $\gamma \in \Gamma$ tel que $\gamma(m_2) \neq m_2$.

On a donc

$$\sum_{i=2}^{r} \left(m_i - \gamma(m_2)\right) v_i = 0 \tag{47}$$

qui est une relation de dépendance linéaire de longueur strictement inférieure.

□

4.9 Définition. Soit G un schéma en groupes sur k, le foncteur

$$\begin{array}{rccc} G_K : & K-alg & \to & groupes \\ & R & \mapsto & G(R) \end{array} \tag{48}$$

est représenté par $k[G] \otimes_k K$. On l'appelle restriction de G à K.

4.10 Proposition. *[KMRT98, 20.7]*

Soit K/k est une extension finie séparable. Les foncteurs restriction et restriction de Weil sont adjoints. C'est-à-dire pour tout H schéma en groupe sur k, pour tout G schéma en groupe sur K il y a une transformation naturelle bijective :

$$\mathrm{Hom}_k(H, R_{K/k}(G)) \cong \mathrm{Hom}_K(H_K, G) \tag{49}$$

de plus on a :

$$\big(R_{K/k}(G)\big)_{|k_s} \cong \prod_{\tau \in X} G_\tau \tag{50}$$

où $G_\tau = G_{k_s}$ et k_s est vue comme une K-algèbre via τ.

Ce qui est fait ci-dessus sur la restriction de Weil peut être grandement généralisé. Une présentation de la restriction de Weil et de ses propriétés basiques peut être trouvée dans [BLR91, 7.6]. En particulier, il est en fait possible de montrer le lemme 4.3 avec des hypothèses beaucoup plus faibles.

4.11 Proposition. *[CGP10, A.5.1]*

Soit k un corps et k' une k-algèbre réduite de dimension finie non triviale (c'est-à-dire selon [Wat79, 6.2] que k' est en tant que k-algèbre le produit d'un nombre fini d'extensions séparables de k). Soit G un k'-schéma en groupes dont l'algèbre de Hopf est de type fini. Alors la restriction de Weil $G = R_{k'/k}(G')$ est un k-schéma en groupe dont l'algèbre de Hopf est de type fini.

La proposition suivant est énoncé dans [CGP10] comme l'équation (A.5.1), il est prouvé dans un contexte plus général dans [BLR91, 7.6 lemme 1].

4.12 Proposition. *Soit k un corps et k' une k-algèbre réduite de dimension finie non triviale,*

$$\mathrm{Hom}_k(H, R_{K/k}(G)) \cong \mathrm{Hom}_{k'}(H_{k'}, G) \tag{51}$$

4.13 Corollaire. *Soit k'/k une extension de corps. Soient H un k' schéma en groupes, G un k schéma en groupes. Il existe un k'-morphisme surjectif $\rho : R_{k'/k}(H) \to H$. Et pour tout k'-morphisme $f : G \to H$, il existe un unique k-morphisme g tel que le diagramme*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ & \searrow^{g} & \uparrow{\scriptstyle \rho} \\ & & R_{k'/k}(H) \end{array} \tag{52}$$

est commutatif.

La restriction de Weil va nous servir à construire des exemples de groupes unipotents.

4.14 Exemple. Soit k un corps de caractéristique $p > 0$ non parfait. Soit $a \in k - k^p$, on note $k = k[a^{1/p}]$. On a la suite exacte suivante :

$$1 \to \mu_p \to G_m \xrightarrow{x \mapsto x^p} G_m \to 1 \tag{53}$$

à laquelle on applique la restriction de Weil.

$$1 \to R_{k'/k}(\mu_p) \to R_{k'/k}(G_m) \xrightarrow{x \mapsto x^p} R_{k'/k}(G_m) \tag{54}$$

On note $\alpha = a^{1/p}$, on a la décomposition suivante de k' : $k' \cong k1 \oplus \cdots \oplus k\alpha^{p-1}$.

Soit B une k-algèbre, par définition de la restriction de Weil,

$$R_{k'/k}(\mu_p)(B) = \mu_p(B \otimes_k k') \cong \{(x_0, \ldots, x_{p-1}) \in B \mid x_0^p + \cdots + a^{p-1}x_{p-1}^p = 1\}. \quad (55)$$

$R_{k'/k}(\mu_p)/\mu_p$ est un groupe unipotent de dimension $p-1$ (alors que μ_p est de dimension 0) totalement ployé selon la remarque 3.26.

4.4 Algèbres formellement lisses

L'objectif de cette annexe est de montrer que, avec les notations et hypothèses de la proposition 3.41, l'application $U(k[[T]]) \to U''(k[[T]])$ est surjective.

4.15 Définition. Soient A un anneau topologique, B une A-algèbre topologique. On dit que B est une A-algèbre formellement lisse si pour toute A-algèbre topologique discrète C, tout idéal J de C nilpotent, et tout A-morphisme continue $u : B \to C/J$ il existe un A-morphisme continu $v : B \to C$ qui induit u par passage au quotient.

C'est-à-dire v est tel que le diagramme

$$\begin{array}{ccc} B & \xrightarrow{u} & C/J \\ {\scriptstyle\rho}\uparrow & \swarrow_{v} & \uparrow{\scriptstyle\pi} \\ A & \xrightarrow[\rho']{} & C \end{array} \quad (56)$$

est commutatif.

Si l'on montre que $k_s[U]$ est une $k_s[U'']$-algèbre formellement lisse, on en déduit que $U\left(k[[T]]/(T^n)\right) \to U''\left(k[[T]]/(T^n)\right)$ est une surjection pour tout n. Ce qui implique en passant à la limite inductive que $U\left(k[[T]]\right) \to U''\left(k[[T]]\right)$ est surjective.

4.16 Définition. Soient k un anneau, A une k-algèbre et $(x_i)_{i\in I}$ une famille d'éléments de A. On note A' la sous-algèbre de A engendrée par les x_i. On dit que $(x_i)_{i\in I}$ est une famille essentiellement génératrice de A si pour tout $a \in A$, il existe $s \in A'$ inversible dans A tel que $sa \in A'$.

On dit que A est essentiellement de type fini si elle admet une famille essentiellement génératrice finie.

4.17 Définition. Soit A un anneau local noethérien, on note m son idéal maximal et $k = A/m$. L'anneau local A est dit régulier si $\dim_k(m/m^2) = \dim(A)$. La dimension de A étant la dimension de Krull de Spec(A).

Soit A un anneau commutatif noethérien, A est dit régulier si pour tout $\mathfrak{p}$ idéal premier de A, le localisé $A_\mathfrak{p}$ de A en $\mathfrak{p}$ est régulier.

4.18 Définition. Soient k un corps, A une k-algèbre. A est dite absolument régulière si $A \otimes_k k'$ est régulière pour toute extension k'/k radicelle de dimension finie.

4.19 Théorème. *[Bou98, AC X.103, théorème 4]*

Soit A un anneau noethérien, B une A-algèbre essentiellement de type fini. Les assertions suivantes sont équivalentes :

1. *La A-algèbre B est formellement lisse*
2. *Le A-module B est plat et, pour tout $\mathfrak{p} \in \mathrm{Spec}(A)$, la $\kappa(\mathfrak{p}) = \mathrm{Frac}(A/\mathfrak{p})$-algèbre $\kappa(\mathfrak{p}) \otimes_A B$ est absolument régulière.*

Le fait que $k_s[U]$ est un $k_s[U'']$-module plat est donné par le théorème [Wat79, 14.1].

De plus $k_s[U]$ est de type fini comme k_s-algèbre donc comme $k_s[U'']$-algèbre donc en particulier est essentiellement de type fini. Enfin π est lisse c'est à dire $k_s[U]$ est une $k_s[U'']$-algèbre lisse. Donc selon le théorème [Wat79, 11.6] la condition 2 est vérifiée.

On peut donc conclure que $U(k[[T]]) \to U''(k[[T]])$ est surjective.

Références

[BLR91] S. Bosch, W. Lütkebohmert et M. Raynaud – *Néron models*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **21**. Springer, 1991.

[Bor91] A. Borel – *Linear algebraic groups*, second edition. Graduate Texts in Mathematics **126**. Springer, 1991.

[Bou61] N. Bourbaki – *Algèbre commutative. Chapitres 1 à 3.* Éléments de mathématique, seconde édition. Springer, 2007.

[Bou98] N. Bourbaki – *Algèbre commutative. Chapitre 10.* Éléments de mathématique, seconde édition. Springer, 2007.

[CGP10] B. Conrad, O. Gabber et G. Prasad – *Pseudo-reductive groups*. New Mathematical Monographs **17**. Cambridge University Press, 2010.

[Dou05] R. Douady et A. Douady – *Algèbre et théories galoisiennes*, seconde édition. Nouvelle bibliothèque mathématique **4**. Cassini, 2005.

[Gil14] P. Gille – *Introduction to affine algebraic groups in positive caracteristic.* Note d'exposé à Lyon. Juin 2014.

[KMRT98] M.-A. Knus, A. Merkurjev, M. Rost et J.-P. Tignol – *The book of involutions*, avec une préface de J. Tits. Colloquium Publications **44**. Amer. Math. Soc., 1998.

[KMT74] T. Kambayashi, M. Miyanishi et M. Takeuchi – *Unipotent algebraic groups*. Graduate Texts in Mathematics **414**. Springer, 1974.

[Laz55] M. Lazard – *Sur les groupes de Lie formels à un paramètre.* Bulletin de la S.M.F., tome 83, 1955.

[Oest84] J. Oesterlé – *Nombres de Tamagawa et groupes unipotents en caractéristique p.* Invent. Math. **78** (1984) 13-88.

[Rém10] B. Rémy – *Groupes algébriques pseudo-réductifs et applications.* Séminaire BOURBAKI. 62ième année, 2009-2010, n° 1021.

[Ser59] J.-P. Serre – *Groupes algébriques et corps de classes, second edition.* Université de Nancago, 1959.

[SGA3] M. Demazure et A.Grothendieck – *Schémas en groupes.* Séminaire de géométrie algébrique du Bois Marie. Springer, 1970.

[Spr98] T.A. Springer – *Linear algebraic groups, second edition.* Progress in Mathematics **9**. Birkhäuser, 1998.

[Tits67] J. Tits – *Lectures on algebraic groups*. Mimeographed Notes, Yale Univ., 1967.

[Wat79] W.C. Waterhouse – *Introduction to affine group schemes*. Graduate Texts in Mathematics **66**. Springer-Verlag, 1979.