QUESTIONS DE RATIONALITÉ SUR LES GROUPES ALGÉBRIQUES LINÉAIRES

M2, PARIS 6, 2008

Philippe Gille

Ce cours porte sur les groupes algébriques réductifs définis sur un corps k non algébriquement clos. De façon plus précise, on présente la théorie de Borel-Tits avec la cohomologie galoisienne des groupes algébriques linéaires. On s'intéresse aux invariants de ces groupes, par exemple l'approximation faible et la R-équivalence.

Nous utilisons principalement les références suivantes:

- A. Borel, *Introduction aux groupes arithmétiques*, Hermann.
- A. Borel, *Linear algebraic groups*, second edition, Springer.
- M. Demazure et P. Gabriel, *Groupes algébriques*, Masson (1970).
- P. Gille, T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics **101** (2006), Cambridge University Press.
- P. Polo, Notes de cours de M2 (2006 et 2007): *Groupes algébriques et groupes de Lie I*, http://www.math.jussieu.fr/ polo/M2/
- J.-P. Serre, *Cohomologie galoisienne, 5-ième édition*, LN 5, Springer.
- T.A. Springer, *Linear Algebraic Groups*, second edition (1998), Birkäuser.
- V.I. Voskresenskiĭ, *Algebraic Groups and their birational invariants*, AMS, 1998.

Contents

Descente galoisienne, tores algébriques.

Soit k un corps.

1. Généralités

Dans ce cours, une k–variété algébrique affine est un k–schéma affine de type fini. En d'autres mots, une k-variété algébrique affine V est une k-sous-variété fermée d'un espace affine $\mathbb{A}^n_k$ et on a $V = \mathrm{Spec}(k[V])\,\mathrm{Spec}(k[t_1, ..., t_n]/\mathcal{I})$ où $\mathcal{I}$ est un idéal de $k[t_1, ..., t_n]$.

La k–variété V est réduite si $k[V]$ n'a pas d'élément nilpotent non nul.

1.1. **Remarque.** Si V est réduite, il n'est pas vrai en général que l'extension des scalaires $V \times_k K$ le soit pour une extension de corps K/k. C'est la raison pour laquelle nous prenons une définition plus souple de k–variétés affines (par rapport à [Po]) afin qu'elle soit stable par extension des scalaires.

Ceci est vrai cependant lorsque K/k est une extension séparable de k [Ha, §3.3]. Si k est parfait, le produit $V_1 \times_k V_2$ de deux k–variétés affines réduites est une k–variété affine réduite.

1.2. **Notation.** *Si W est un k–espace vectoriel de dimension finie, on note*

$$\mathbb{A}(W) = \mathrm{Spec}\big(\mathrm{Sym}_k(W^*)\big)$$

le k-espace affine sous–jacent à W. On a $\mathbb{A}(W)(k) = W$.

1.3. **Définition.** Un k–groupe algébrique affine $G = \mathrm{Spec}(A)$ est une k–variété algébrique affine munie de:

(1) un point $e \in G(k)$,
(2) un produit $\mu : G \times_k G \to G$, noté $(g_1, g_2) \to g_1\, g_2$,
(3) un morphisme d'inversion $\iota : G \to G$, noté $g \to g^{-1}$,

satisfaisant aux compatibilités suivantes:

(1) (associativité) $\mu^* \otimes_k id : A \otimes_k A \otimes_k A \to A$ et $id \otimes_k \mu^* : A \otimes_k A \otimes_k A \to A$ coïncident,
(2) (existence d'un inverse) $m \circ (\iota^* \otimes_k id) \circ \mu^* = m \circ (id \otimes_k \iota^*) \circ \mu^* = \epsilon$,
(3) (existence de e) $(e^* \otimes_k id) \circ \mu^* = (id \otimes_k e^*) \circ \mu^*)$,

où $e^* : A \to k$ est la co-unité (i.e. représente e), $\mu^* : A \to A \otimes_k A$ est la comultiplication et $\iota^* : A \to A$ est l'application antipode, $m : A \otimes_k A \to A$ désigne la multiplication et $\epsilon = A \to A$ est le composé de e^* et du morphisme structural $k \to A$.

Voir [Po, §7] pour plus de détails sur cette définition en termes d'algèbres de Hopf, qui vaut sur un corps de base arbitraire.

1.4. **Exemples.** (a) Si Γ est un groupe fini, l'algèbre de groupes $k[\Gamma]$ est une algèbre de Hopf et $\mathrm{Spec}(k[\Gamma])$ est le k–schéma en groupes constant associé à Γ. On le note souvent abusivement encore Γ.

b) On note $\mathbb{G}_a = \mathrm{Spec}(k[t])$ le groupe additif et $\mathbb{G}_m = \mathrm{Spec}(k[t, t^{-1}])$ le groupe multiplicatif.

c) Soit n un entier ≥ 1. On note

$$\mathrm{GL}_n = \mathrm{Spec}\Big(k[x_{i,j}, t]_{1\leq i,j\leq n} \,/\, det(x_{i,j})t = 1\Big)$$

et

$$\mathrm{SL}_n = \mathrm{Spec}\Big(k[x_{i,j}]_{1\leq i,j\leq n} \,/\, det(x_{i,j}) = 1\Big).$$

c') De façon intrinsèque, si V un k–espace vectoriel de dimension finie, on peut définir les k–groupes linéaires $\mathrm{GL}(V)$ et $\mathrm{SL}(V)$ de la façon suivante. Le k–groupe $\mathrm{GL}(V)$ est la sous–variété fermée de $\mathbb{A}\big(\mathrm{End}_k(V)\big)) \times_k \mathbb{G}_a$ formée des (f, u) satisfaisant $\det(f)\, u = 1$.

d) Soit B une k–algèbre (associative, unitaire) de dimension finie. Le morphisme de k–espaces vectoriels $B \to \mathrm{End}_k(B)$, $b \mapsto L_b$ donne lieu à un morphisme $\phi : \mathbb{A}(B) \to \mathbb{A}(\mathrm{End}_k(B))$ On pose alors

$$\mathrm{GL}_1(B) := \mathbb{A}(B) \times_{\mathbb{A}\big(\mathrm{End}_k(B)\big)} \mathrm{GL}(B).$$

On a $\mathrm{GL}_1(B)(k) = B^\times$.

1.5. **Théorème.** *Soit G/k un groupe algébrique affine. Alors G/k est un sous–groupe algébrique fermé d'un k–groupe algébrique* $\mathrm{GL}(V)$ *où V est un k–groupe algébrique linéaire.*

En d'autres mots, G admet une représentation linéaire fidèle. Pour la démonstration, nous renvoyons à [Po, §7] ou [DG, II.2.3.3].

1.6. **Remarque.** Il faut prendre garde que ce théorème n'entraîne pas que G est un k–groupe algébrique linéaire au sens de Borel [Bo] puisque cette définition requiert en plus que G soit absolument réduit, c'est-à-dire que $G \otimes_k K$ soit réduit pour toute extension de corps K/k.

Si le corps k est de caractéristique positive p, le k–groupe

$$\mu_p = \mathrm{Spec}(k[t]/t^p - 1)$$

est un k–groupe affine mais n'est pas un k–groupe algébrique linéaire.

La nuance précédente n'apparaît qu'en caractérique positive.

1.7. **Théorème.** *(Cartier) Soit G un k–groupe algébrique affine.*

(1) *On suppose k parfait et réduit. Alors G est une k–variété lisse.*
(2) *Si k est de caractéristique nulle, alors G est lisse.*

Pour un énoncé plus précis, voir [DG, §II.5.2, II.6].

Esquisse de preuve: (1) Sans perte de généralité, on peut supposer que k est algébriquement clos. C'est un fait général de géométrie algébrique qu'il existe un ouvert dense U de G qui est lisse sur k [DG, §I.4.4.1]. Mais $G = \cup_{g\in G(k)}\, gU$, donc G est lisse sur k.
(2) Nous renvoyons à la démonstration élémentaire de Oort [Oo] (ou [Wa, 11.4]). □

2. Caractères, groupes diagonalisables

Soit G un k–groupe algébrique affine.

2.1. Caractères.

2.1. **Définition.** Un caractère de G est un homomorphisme de k–groupes $G \to \mathbb{G}_m$.

On note $\widehat{G}(k) = \mathrm{Hom}_{k-gr}(G, \mathbb{G}_m)$ le groupe des caractères de G. Si $f : G_1 \to G_2$ est un morphisme de k–groupes algébriques affines, la composition produit un morphisme naturel $f^* : \widehat{G}_2(k) \to \widehat{G}_1(k)$. Par ailleurs, on sait que [Po, lemme 10.30]

$$\widehat{G_1 \times_k G_2}(k) = \widehat{G}(k) \oplus \widehat{G}_2(k).$$

2.2. **Exemple.** $\widehat{\mathrm{GL}_n}(k) = \mathbb{Z}.\det$.

Nous démontrerons aussi ultérieurement le fait suivant.

2.3. **Proposition.** *(Rosenlicht) Soit G un k–groupe algébrique linéaire connexe. Alors $k[G]^\times = k^\times \oplus \widehat{G}(k)$.*

"Démonstration". On peut supposer que k est algébriquement clos. Si X et Y sont des k–variétés affines lisses connexes, le lemme de Rosenlicht (voir [CT, §3]) est l'isomorphisme

$$k[X]^\times/k^\times \oplus k[X]^\times/k^\times \xrightarrow{\sim} k[X \times_k Y]^\times/k^\times.$$

Ainsi on a un isomorphisme $k[G]^\times/k^\times \oplus k[G]^\times/k^\times \xrightarrow{\sim} k[G \times_k G]^\times/k^\times$ ou encore

$$\ker\bigl(k[G]^\times \xrightarrow{e^*} k^\times\bigr) \oplus \ker\bigl(k[G]^\times \xrightarrow{e^*} k^\times\bigr) \xrightarrow{\sim} \ker\bigl(k[G \times_k G]^\times \to k^\times\bigr).$$

Soit $f \in k[G]^\times$. On peut supposer que $f(e) = e$. On considère le défaut $\Delta : G \times G \to \mathbb{G}_m$, $(g_1, g_2) \mapsto f(g_1 g_2)\, f(g_1)^{-1}\, f(g_2)^{-1}$. Il s'ecrit $\Delta(g_1, g_2) = f_1(g_1) f_2(g_2)$ suivant l'identité ci-dessus. Vu que $\Delta(g_1, e) = \Delta(e, g_2) = e$, on conclut que $f_1 = f_2 = e$ et $\Delta = e$. Le morphisme f est donc un caractère. $\square$

En d'autres mots, toute fonction inversible sur G est le produit d'une constante et d'un caractère.

2.2. **Groupes diagonalisables.** Soit M un $\mathbb{Z}$-module de type fini. On définit l'algèbre commutative $k[M]$ par générateurs et relations suivantes:

Générateurs : $(e_m)_{m \in M}$;

Relations : $e_{m+m'} = e_m\, e_{m'}$ pour $m, m' \in M$.

Cette algèbre est commutative, unitaire. Elle est munie d'une structure d'algèbre de Hopf:

- co-unité : $k[M] \to k$, $[e_m] \to 1$;
- co-multiplication : $k[M] \to k[M] \otimes_k k[M]$, $[e_m] \mapsto [e_m] \otimes [e_m]$;

- antipode : $k[M] \to k[M]$, $[e_m] \mapsto [e_{-m}]$.

On pose
$$D(M) = \mathrm{Spec}(k[M]),$$
c'est un k–groupe algébrique commutatif affine. On a $k[M \oplus M'] = k[M] \otimes_k k[M']$, d'où un isomorphisme $D(M) \cong D(M) \times_k D(M')$ pour des $\mathbb{Z}$–modules libres de type fini.

2.4. **Définition.** Un k–groupe algébrique affine est diagonalisable s'il est isomorphe à un k–groupe $D(M)$,

2.5. **Exemples.** (a) Si $M = \mathbb{Z}$, $D(M) = \mathrm{Spec}(k[t, t^{-1}]) = \mathbb{G}_m$.
(b) Si $M = \mathbb{Z}/n\mathbb{Z}$, $D(M) = \mathrm{Spec}(k[t]/t^n - 1) = \mu_n$, le k–groupe des racines de l'unité.

2.6. **Lemme.** (1) *$M \cong \widehat{D(M)}(k)$;*
(2) *Si M_1, M_2 sont des $\mathbb{Z}$–modules de type fini, alors* $\mathrm{Hom}_{k-gp}(M_1, M_2) \xrightarrow{\sim} \mathrm{Hom}_{gr}(M_2, M_1)$.

Démonstration. (1) Par additivité en M, on est ramené au cas des deux exemples fondamentaux (a) et (b) ci-dessus.
(2) Par additivité des deux cotés, il y a quatre cas à vérifier. □

En d'autres mots, le foncteur (additif) D produit une équivalence de catégories additives de la catégorie des $\mathbb{Z}$–modules de type fini et la catégorie des k–groupes diagonalisables.

2.7. **Definition.** On dit qu'une suite de morphismes
$$1 \to H \xrightarrow{i} G \xrightarrow{p} Q \to 1$$
de k–groupes algébriques affines est exacte si
(1) $p \circ i$ est le morphisme trivial,
(2) i est une immersion fermée,
(3) $H = \ker(p)$,
(4) p est fidèlement plat.

2.8. **Lemme.** *Soit* $0 \to M_1 \xrightarrow{p^*} M_2 \xrightarrow{i^*} M_3 \to 1$ *une suite exacte de $\mathbb{Z}$-modules. Alors la suite de k–groupes algébriques*
$$0 \to D(M_3) \xrightarrow{i} D(M_2) \xrightarrow{p} D(M_1) \to 1$$
est exacte.

Démonstration. On va vérifier les propriétés de la définition. La première propriété est évidente.

Le morphisme $k[M_2] \to k[M_3]$ est surjectif, donc $D(M_3) \to D(M_2)$ est une immersion fermée.

Le noyau est un sous–groupe algébrique affine de $D(M_2)$, i.e. $\ker(p) = \mathrm{Spec}(B)$ avec $B = k[M_2] \otimes_{k[M_1]} k$. Le morphisme $D(M_3) \to \ker(p)$ produit un morphisme $\phi : B \to k[M_3]$ qui applique $[e_{m_2}] \otimes 1$ sur $[e_{i^*(m_3)}] \otimes 1$. Vu que i^* est surjectif, ϕ est surjectif. De même, l'exactitude en M_2 entraîne l'injectivité de ϕ.

Il reste à établir que p est fidèlement plat. Soit $s : M_3 \to M_2$ une section ensembliste de i^*. On observe alors que le $k[M_1]$–module $k[M_2]$ est libre de base $s(M_2)$. Il est donc fidèlement plat. □

Ainsi la catégorie des k–groupes multiplicatifs est une catégorie abélienne. On peut résumer ce paragraphe de la façon suivante.

2.9. **Théorème.** *(dualité de Cartier) Le foncteur "caractère" produit une anti-équivalence de catégories abéliennes*

$$k\text{-groupes diagonalisables} \quad < - - - > \quad \mathbb{Z}\text{-modules de type fini.}$$

2.10. **Remarque.** Si M est un $\mathbb{Z}$–module de type fini, alors on a une suite exacte canonique

$$0 \to M_{tors} \to M \to M_{libre} \to 0.$$

Par dualité, on a donc une suite exacte canonique de k–groupes

$$1 \to D(M_{libre}) \to D(M) \to D(M_{tors}) \to 1.$$

En d'autres mots, un k–groupe de type diagonalisable se dévisse comme extension d'un k–groupe diagonalisable fini et d'un k–tore algébrique déployé.

3. Descente galoisienne

Soit K/k une extension finie galoisienne. On note $\Gamma = \mathrm{Gal}(K/k)$.

3.1. Le lemme de Speiser.

3.1. **Définition.** Soit V un K–espace vectoriel. Une action Γ sur V est dite K/k-semi-linéaire si si

$$\sigma.(\lambda.v) = \sigma(\lambda).\sigma(v) \ \ \forall v \in V \, \forall \sigma \in \Gamma.$$

Sous les hypothèses de la défintion, l'espaces des points fixes V^Γ est un k–espace vectoriel.

Si V_0 est un k-espace vectoriel, le K–espace vectoriel $K \otimes_k V_0$ est muni de l'action semi-linéaire standard définie par $\sigma(\lambda \otimes v_0) = \sigma(\lambda) \otimes v_0$.

3.2. **Lemme.** *(Speiser) Soit V un K-espace vectoriel muni d'une action semi-linéaire de Γ. Alors on a un isomorphisme canonique de K–espaces vectoriels (qui respecte l'action de Γ)*

$$K \otimes_k V^\Gamma \xrightarrow{\sim} V, \ \ \lambda \otimes w \mapsto \lambda w.$$

En d'autres mots, il revient au même se se donner un k-espace vectoriel ou un K–espace vectoriel muni d'une action semi-linéaire de Γ. En outre, on a une équivalence de catégories abéliennes

$$\begin{array}{ccc} \mathrm{Vect}(k) & \longrightarrow & \mathrm{Vect}_\Gamma(K) \\ V_0 & \mapsto & K \otimes_k V_0 \\ V^\Gamma & \longleftarrow & V \end{array}$$

où $\mathrm{Vect}_\Gamma(K)$ désigne la catégorie des K–espaces vectoriels munis d'une action semi-linéaire de Γ.

Démonstration: Puisque K est galoisienne sur k, il existe $\alpha \in K$ tel que K/k est engendré par les conjugués $\sigma(\alpha)$. On pose $P(X) = \prod_{\sigma\in\Gamma}(X-\sigma(\alpha)) \in k[X]$. On dédouble la notation en posant $\widetilde{k} = K = k[X]/P(X)$. L'idée de montrer que la flèche $K \otimes_k V^\Gamma \otimes_k \widetilde{k} \xrightarrow{\sim} V \otimes_k \widetilde{k}$ est un isomorphisme. Les racines de P dans K produisent un Γ-isomorphisme

$$\begin{array}{ccc} K \otimes_k \widetilde{k} = K[X]/P(X) = K[X]/\prod_{\sigma\in\Gamma}(X-\sigma(\alpha)) & \xrightarrow{\sim} & K^{(\Gamma)} \\ Q(X) & \mapsto & \big(Q(\sigma(\alpha))\big)_{\sigma\in\Gamma} \end{array}$$

Identifiant le facteur K en σ et $\widetilde{k}$ via σ^{-1}, on constate que l'on a un $\widetilde{k}$-isomorphisme Γ-équivariant $K \otimes_k \widetilde{k} \xrightarrow{\sim} (\widetilde{k})^{(\Gamma)} = \bigoplus_{\sigma\in\Gamma} \widetilde{k}\,.e_\sigma$. Alors il existe un $\widetilde{k}$-espace vectoriel $\widetilde{W}$ tel que

$$V \otimes_k \widetilde{k} \xrightarrow{\sim} \bigoplus_{\sigma\in\Gamma} \widetilde{W} e_\sigma.$$

L'espace des points fixes $V^\Gamma \otimes_k \widetilde{k} \xrightarrow{\sim} (V \otimes_k \widetilde{k})^\Gamma$ n'est pas autre chose que le $\widetilde{W}$ diagonal. On a bien un un isomorphisme $K \otimes_k V^\Gamma \otimes_k \widetilde{k} \xrightarrow{\sim} V \otimes_k \widetilde{k}$. $\square$

3.2. **Cohomologie galoisienne non abélienne et K/k–formes.** Si A est un Γ–groupe (i.e. un groupe muni d'une action à gauche de Γ), un 1–cocycle est une application $z : \Gamma \to A$ satisfaisant la règle suivante

$$z_{\sigma\tau} = z_\sigma\, \sigma(z_\tau) \;\; \forall \sigma, \tau \in \Gamma$$

On note $Z^1(\Gamma, A)$ l'ensemble des 1–cocycles. Deux cocycles z, z' sont dits cohomologues s'il existe $a \in A$ satisfaisant

$$(*) \qquad z_\sigma = a^{-1}\, z'_\sigma\, \sigma(a).$$

On pose $H^1(\Gamma, A) = Z^1(\Gamma, A)/\sim$, c'est l'ensemble pointé (par la classe du cocycle trivial) de cohomologie galoisienne du Γ-groupe A.

3.3. **Remarques.** (a) Si A est abélien, $H^1(\Gamma, A)$ est un groupe abélien et coïncide avec le groupe correspondant de cohomologie des groupes.

(b) Si deux cocycles z et z' sont cohomologues, il faut prendre garde que l'élément a ci-dessus (*) n'est pas unique en général.

(c) Une autre façon de définir $Z^1(\Gamma, A)$ et $H^1(\Gamma, A)$ est la suivante. On définit $Z^1(\Gamma, A)$ comme l'ensemble des sections de $A \rtimes \Gamma \to \Gamma$ et $H^1(\Gamma, A)$ comme l'ensemble des sections de $A \rtimes \Gamma \to \Gamma$ modulo conjugaison de A (le vérifier !). Ceci montre qu'un 1–cocycle est défini par sa valeur sur des générateurs de Γ.

Soit V_0 un k–espace vectoriel de dimension finie et Φ_0 un tenseur, c'est-à-dire un élément de $V^{\otimes p} \otimes_k (V^*)^q = \mathrm{Hom}_k(V^{\otimes q}, V^{\otimes p})$.

Une K/k–forme de (V_0, Φ_0) est un couple (V, Φ) où V est un k–espace vectoriel de dimension finie et Φ un tenseur tel que $(V_0, \Phi_0) \otimes_k K \cong (V, \Phi) \otimes_k K$. On considère le k-groupe algébrique affine

$$G_0 := \Big\{ g \in \mathrm{GL}(V_0) \mid g^* \circ \Phi_0 = \Phi_0 \Big\}.$$

Par exemple, si Φ_0 est une forme quadratique (i.e. un tenseur de type $(0,2)$), le k–groupe G_0 est le groupe orthogonal de Φ_0.

On va construire une flèche naturelle

$$\begin{array}{ccc} \text{Classes de } k\text{–isomorphie de } K/k\text{–formes de } (V_0,\Phi_0) & \longrightarrow & H^1\big(\Gamma, G_0(K)\big) \\ (V,\Phi) & \mapsto & [(V,\Phi)]. \end{array}$$

Si (V, Φ) est une K/k–forme de (V_0, Φ_0), il existe un K-isomorphisme $\phi : (V_0, \Phi_0) \otimes_k K \cong (V, \Phi) \otimes_k K$. On définit le conjugué $\sigma(\varphi)$ par le diagramme commutatif suivant

$$\begin{array}{ccc} (V_0,\Phi_0)\otimes_k K & \xrightarrow{\phi} & (V,\Phi)\otimes_k K \\ {\scriptstyle id\otimes\sigma}\uparrow & & {\scriptstyle id\otimes\sigma}\uparrow \\ (V_0,\Phi_0)\otimes_k K & \xrightarrow{\sigma(\phi)} & (V,\Phi)\otimes_k K. \end{array}$$

Alors le composé $a_\sigma = \phi^{-1}\,\sigma(\phi) : (V_0, \Phi_0) \otimes_k K \to (V_0, \Phi_0) \otimes_k K$ appartient à $G_0(K)$. Un calcul classique (à vérifier) montre que $\sigma \to a_\sigma$ est un 1-cocycle. De plus, changer ϕ par un automorphisme de $(V_0, \Phi_0) \otimes_k K$ revient à modifier a_σ par un cobord. Ainsi la classe $[a_\sigma]$ dans $H^1\big(\Gamma, G_0(K)\big)$ est bien définie, on la note $[X]$.

3.4. **Lemme.** *Soient $(V, \Phi), (V', \Phi')$ deux K/k-formes de (V_0, Φ_0). Alors $(V, \Phi) \xrightarrow{\sim} (V', \Phi')$ si et seulement si $[(V, \Phi)] = [(V', \Phi')] \in H^1\big(\Gamma, G_0(K)\big)$. En particulier, $(V, \Phi) \xrightarrow{\sim} (V_0, \Phi_0)$ si et seulement si $[(V, \Phi)] = 1$.*

Démonstration: On se donne $\phi : (V_0, \Phi_0) \otimes_k K \cong (V, \Phi) \otimes_k K$. tel qu'il existe $a \in G_0(K)$ satisfaisant $(\phi')^{-1}\sigma(\phi') = a^{-1}\phi^{-1}\sigma(\phi)\sigma(\phi)$. Alors $\phi' \circ a \circ \phi^{-1} = \sigma\big(\phi' \circ a \circ \phi^{-1}\big)$. En d'autres mots, le K–isomorphisme $\phi' \circ a \circ \phi^{-1} : (V, \Phi) \otimes_k K \to (V', \Phi') \otimes_k K$ est Γ–invariant. On conclut que $(V, \phi) \xrightarrow{\sim} (V', \phi')$. □

3.5. **Théorème.** *On a une bijection naturelle*

Classes de k–isomorphie de K/k–formes de $(V_0, \Phi_0) \;\; < - - - > \;\; H^1\big(\Gamma, G_0(K)\big)$.

Démonstration: On va construire la flèche réciproque. Soit $a \in Z^1\big(\Gamma, G_0(K)\big)$. On peut définir alors l'action tordue de Γ sur $(V_0, \Phi_0) \times_k K$ par

$$\sigma * v = a_\sigma \,.\, \sigma(v)$$

La condition de cocycle entraîne que l'on a bien une action de Γ sur $(V_0, \Phi_0) \times_k K$. En outre, celle-ci est semi-linéaire. Le lemme de Speiser montre que

$$V := \Big\{ v \in V_0 \times_k K \mid (a_\sigma) \,.\, \sigma(v) = v \;\; \forall \sigma \in \Gamma \Big\}$$

satisfait $\phi : V \otimes_k K \cong V_0 \times_k K$. Par construction, le K–tenseur $\phi^{-1}(\Phi_0)$ sur $V \otimes_k K$ est invariant par K. Il produit donc un k-tenseur Φ sur V tel que $\phi : (V, \Phi) \xrightarrow{\sim} (V_0, \Phi_0)$. Ainsi (V, Φ) est une K/k-forme de (V_0, Φ_0). Les vérifications suivantes sont laissées au lecteur.

1) Changer le cocycle a par un cobord produit un espace (V', Φ') k–isomorphe à (V_0, Φ_0).

2) Les deux flèches sont inverses l'une de l'autre, c'est-à-dire que $a_\sigma = \phi^{-1}\sigma(\phi)$. □

En appliquant ceci au tenseur nul, on obtient le :

3.6. **Théorème.** *(Théorème 90 de Hilbert) Pour tout entier $n \geq 1$, on a*

$$H^1(\Gamma, \mathrm{GL}_n(K)) = 1.$$

Si l'on part d'une forme quadratique Φ_0, on obtient que l'ensemble pointé $H^1(\Gamma, O(\Phi_0))$ classifie les k-formes quadratiques qui deviennent isomorphes à Φ_0 après extension des scalaires à K.

Le théorème 3.5 se généralise à d'autres structures algébriques.

3.7. **Exemples.** Soit n un entier ≥ 1.

(a) *Algèbres étale* : Une k–algèbre étale de degré n est un produit $A = k_1 \times \cdots k_r$ d'extensions séparables sur k et de dimension n. L'algèbre étale de dimension n standard (ou encore déployée) est l'algèbre $A_0 = k \times \cdots \times k$ (n fois). Si l'extension K contient les clôtures galoisiennes des k_i, alors $A \otimes_k K \cong A_0 \otimes_k K$. On dit alors que l'extension K/k déploie (ou trivialise A). Le groupe des K–automorphismes de l'algèbre étale K^n est le groupe symétrique S_n. La descente galoisienne produit donc une correspondance

Classe d'isomorphie de k–algèbres étales déployées par K/k

$$< -- > \quad H^1(\Gamma, S_n) = \mathrm{Hom}_{gr}(\Gamma, S_n)/\mathrm{int}(S_n).$$

Dans cette correspondance, le nombre de facteurs r de $A = k_1 \times \cdots k_r$ est le nombre d'orbites de Γ sur $\{1, ..., n\}$ pour l'action d'un homomorphisme $f : \Gamma \to S_n$; en particulier, les corps sont associés aux actions transitives. Pour cette généralisation de la théorie de Galois, voir [KMRT, §18] et [KT].

(b) *Algèbres simples centrales*: Une k–algèbre simple centrale A de degré n est une k-algèbre de dimension n^2, de centre k et dont les seuls idéaux bilatères sont 0 et A. La k–algèbre simple centrale standard (ou encore déployée) de degré n est l'algèbre de matrices $M_n(k)$. Si $A \otimes_k K \cong M_n(k) \otimes_k K$, on dit que K/k déploie A (A est toujours déployée par une extension convenable, voir [GS, §2]). Par ailleurs, il est bien connu que le groupe de

K-automorphismes de l'algèbre $M_n(K)$ est $\mathrm{PGL}_n(K) = \mathrm{GL}_n(K)/K^\times$. La descente galoisienne produit donc une correspondance

Classe d'isomorphie de k–algèbres simples centrales déployées par K/k

$$< -- > \quad H^1(\Gamma, \mathrm{PGL}_n(K)).$$

Voir [GS, §2] pour plus de détails.

3.3. K/k–formes de variétés.

3.8. **Définition.** Soit X_0 une k–variété (par exemple affine). On dit qu'une k–variété X est une K/k–forme de X si $X \times_k K$ est isomorphe à $X_0 \times_k K$.

Le même principe va s'appliquer avec des conventions appropriées pour la définition de l'action du groupe de Galois.

Tout d'abord, étant donné deux k–variétés affines $X = \mathrm{Spec}(A)$, $Y = \mathrm{Spec}(B)$, l'ensemble $\mathrm{Hom}_K(X \times_k K, Y \times_k K) = \mathrm{Hom}_K(B \otimes_k K, A \otimes_k K)$ est muni d'une action naturelle (à gauche) de Γ définie par le diagramme

$$\begin{array}{ccc} X \times_k \mathrm{Spec}(K) & \longrightarrow & Y \times_k \mathrm{Spec}(K) \\ {\scriptstyle id\times(\sigma^{-1})^*}\uparrow & & {\scriptstyle id\times(\sigma^{-1})^*}\uparrow \\ X \times_k \mathrm{Spec}(K) & \longrightarrow & Y \times_k \mathrm{Spec}(K) \end{array}$$

pour $f \in \mathrm{Hom}_K(X \times_k K, Y \times_k K)$ et $\sigma \in \Gamma$. En termes d'algèbres, on a une action de Γ (à droite) sur $\mathrm{Hom}_K(B \otimes_k K, A \otimes_k K)$ définie par le diagramme

$$\begin{array}{ccc} B \otimes_k K & \xrightarrow{f^*} & A \otimes_k K \\ {\scriptstyle id\otimes\sigma^{-1}}\downarrow & & {\scriptstyle id\otimes_\sigma -1}\downarrow \\ B \otimes_k K & \xrightarrow{\sigma(f)^*} & A \otimes_k K. \end{array}$$

On a $\mathrm{Hom}_k(X, Y) \xrightarrow{\sim} \mathrm{Hom}_K(X_K, Y_K)^\Gamma$. En particulier, $\mathrm{Hom}_K(X \times_k K, X \times_k K)$ et $\mathrm{Aut}_K(X \times_k K, X \times_k K)$ sont munis d'une action de Γ. On va construire une flèche naturelle

$$\begin{array}{ccc} \text{Classes de } k\text{–isomorphie de } K/k\text{–formes de } X_0 & \longrightarrow & H^1\big(\Gamma, \mathrm{Aut}_K(X_0 \times_k K)\big) \\ X & \mapsto & [X]. \end{array}$$

Si X est une K/k–forme de X_0, il existe un K-isomorphisme

$$\phi : X_{0,K} \xrightarrow{\sim} X_K.$$

Alors le composé $a_\sigma \phi^{-1}\, \sigma(\phi) : X_{0,K} \to X_K \to X_{0,K}$ est un K-automorphisme de X_K. Un calcul classique (à vérifier) montre que $\sigma \to a_\sigma$ est un 1-cocycle. De plus, changer ϕ par un automorphisme de $X_{0,K}$ revient à modifier a_σ par un cobord. Ainsi la classe $[a_\sigma]$ dans $H^1\big(\Gamma, \mathrm{Aut}_K(X_0 \times_k K)\big)$ est bien définie, on la note $[X]$.

3.9. **Lemme.** *Soient* X, X' *deux* K/k*-formes de* X_0. *Alors* $X \xrightarrow{\sim} X'$ *si et seulement si* $[X] = [X'] \in H^1\bigl(\Gamma, \mathrm{Aut}_K(X_0 \times_k K)\bigr)$. *En particulier,* $X \xrightarrow{\sim} X_0$ *si et seulement si* $[X] = 1$.

Démonstration: On se donne $\phi : X_{0,K} \xrightarrow{\sim} X_K$ et $\phi' \xrightarrow{\sim} X'_K$ tels qu'il existe $a \in \mathrm{Aut}_K(X_0 \times_k K)$ tel que $(\phi')^{-1}\sigma(\phi') = a^{-1}\phi^{-1}\sigma(\phi)\sigma(\phi)$. Alors $\phi' \circ a \circ \phi^{-1} = \sigma\bigl(\phi' \circ a \circ \phi^{-1}\bigr)$. En d'autres mots, le K–isomorphisme $\phi' \circ a \circ \phi^{-1}$: $X \to X'$ est Γ–invariant. On conclut que $X \xrightarrow{\sim} X'$. □

3.10. **Théorème.** *On suppose* X_0 *affine (ou plus généralement quasi-projective). On a une bijection naturelle*

Classes de k*–isomorphie de* K/k*–formes de* X_0 $\quad < - - - > \quad H^1\bigl(\Gamma, \mathrm{Aut}_K(X_0 \times_k K)\bigr)$.

Démonstration: On suppose tout d'abord $X_0 = \mathrm{Spec}(A_0)$ affine. On va construire la flèche $\leftarrow$. Soit $a \in Z^1\bigl(\Gamma, \mathrm{Aut}_K(X_0 \times_k K)\bigr)$. On peut définir alors l'action (à droite) tordue de Γ sur $A_0 \times_k K$ par

$$\sigma * f = (a_\sigma)^* \,.\, \sigma^{-1}(f)$$

La condition de cocycle entraîne que l'on a bien un action de Γ sur $A_0 \times_k K$. En outre, celle-ci est semi-linéaire. Le lemme de Speiser montre que

$$A := \Bigl\{ f \in A_0 \times_k K \ \mid\ (a_\sigma)^* \,.\, \sigma^{-1}(f) = f \,\forall \sigma \in \Gamma \Bigr\}$$

satisfait $A \otimes_k K \cong A_0 \times_k K$. Ainsi $X := \mathrm{Spec}(A)$ est une K/k-forme de X_0. Les vérifications suivantes sont laissées au lecteur.

1) Changer a par un cobord produit une k–variété k–isomorphe à X.

2) Les deux flèches sont inverses l'une de l'autre, c'est-à-dire que si ϕ : $A \otimes_k K \cong A_0 \times_k K$ est l'isomorphisme de Speiser, alors $a_\sigma = \phi^{-1}\sigma(\phi)$.

On passe au cas quasi-projectif par recollement d'ouverts affines de X_0, voir [S2, V.4.20].

□

3.11. **Remarque.** Avec les notations de la démonstration, on note ${}_aX = \mathrm{Spec}(A)$ la tordue de X_0 par le cocycle a.

Il faut prendre garde que si a et a' sont des cocycles cohomologues, les variétés ${}_aX_0$ et ${}_{a'}X_0$ sont isomorphes à isomorphisme non unique près. On ne peut donc pas identifier les variétés tordues ${}_aX_0$ et ${}_{a'}X_0$.

3.12. **Exercice.** Montrer que les K/k-formes de la droite affine $\mathbb{A}^1_k$ sont triviales.

3.13. **Exemple.** Espaces affines tordus: Soit n un entier ≥ 2. Le groupe des K–automorphismes de l'espace affine $\mathbb{A}_K$ est un objet de dimension infinie assez mal compris (conjecture jacobienne !). C'est un théorème de Shafarevitch que K/k-formes du plan affine $\mathbb{A}^2_k$ sont triviales [Sh], [Km]. Pour $n \geq 3$, c'est un problème ouvert.

3.14. **Exemple.** Variétés de Severi-Brauer: Soit $n \geq 2$. Une k–variété (projective) X est une variété de Severi-Brauer de dimension $n-1$ s'il existe une extension finie de corps F/k telle que $X \times_k F \cong \mathbb{P}^{n-1} \times_k F$. Le groupe des K–automorphismes de $\mathbb{P}^{n-1} \times_k K$ est $\mathrm{PGL}_n(K)$. Selon l'exemple 3.7.b, on obtient donc une correspondance entre les classes d'isomorphies de k–variétés de Severi-Brauer de degré $n-1$ déployées par K/k et les classes d'isomorphie des algèbres simples centrales, le tout étant classifié par l'ensemble pointé dans $H^1(\Gamma, \mathrm{PGL}_n(K))$.

En fait, on sait associer directement à une algèbre simple centrale une variété de Severi-Brauer [KMRT, I.C] et inversement à une variété de Severi-Brauer une algèbre centrale [Sz]. Pour en savoir plus sur ce lien, consulter [J], [GS, §4].

La descente galoisienne se généralise à des morphismes de variétés. En particulier, si G_0/k est un groupe algébrique affine, les classes d'isomorphie de K/k–formes (en tant que groupe algébrique) de G_0 sont décrites par $H^1(\Gamma, \mathrm{Aut}_{K-gr}(G_{0,K}))$. Le morphisme $G_0(K) \overset{\mathrm{int}}{\to} \mathrm{Aut}_{K-gr}(G_{0,K})$. Si on se donne un 1–cocycle z_σ à valeurs dans $G_0(K)$, le k-groupe ${}_{int(z)}G_0$ est appelé le k–groupe tordu de G_0 par le cocycle z par automorphismes intérieurs. On le note souvent (abusivement) ${}_zG_0$.

3.15. **Lemme.** *Soit $f : X \to Y$ un morphisme de k–variétés quasi–projectives. Alors f est plat (resp. fidèlement plat, lisse, propre, fini, une immersion ouverte, une immersion fermée) si et seulement si le morphisme $f_K : X_K \to Y_K$ est plat (resp. fidèlement plat, lisse, propre, fini, une immersion ouverte, immersion fermée).*

Démonstration: Pour plat, fidèlement plat et lisse, cela se lit sur la définition. Pour les autres, voir par exemple [J, lemma 2.12]. $\square$

3.16. **Corollaire.** *Soit $f : X_0 \to Y_0$ un morphisme de k–variétés quasi–projectives. Soit $z \in Z^1(\Gamma, \mathrm{Aut}_K(X_{0,K} \to Y_{0,K}))$. Alors f est plat (resp. fidèlement plat, lisse, fini, une immersion ouverte, une immersion fermée) si et seulement si le morphisme tordu ${}_zf : {}_zX_0 \to {}_zY_0$ est plat (resp. fidèlement plat, lisse, propre, fini, une immersion ouverte, immersion fermée).*

3.4. **Restriction des scalaires à la Weil, I.** Soit n un entier. Soit X_0 une k–variété affine (ou quasi-projective). La k–variété produit $X_0^n = X_0 \times_k \cdots X_0$ est munie d'une action naturelle de S_n En d'autres mots, on a défini un morphisme

$$can : S_n \to \mathrm{Aut}_k(X_0^n) \to \mathrm{Aut}_K(X_{0,K}^n)$$

qui est Γ–équivariant. En passant aux cocycles, on obtient une application

$$can_* : H^1(\Gamma, S_n) \to \mathrm{Aut}_K(X_{0,K}^n).$$

On peut donc associer à un homomorphisme $f : \Gamma \to S_n$ la forme tordue ${}_{can(f)}(X_0^n)$. Si A_f désigne l'algèbre étale associé à f, on note $R_{A_f/k}(X_0)$

cette variété, puisque l'on verra plus loin qu'il s'agit d'un cas particulier de restriction des scalaires à la Weil.

En d'autres mots, $R_{A_f/k}(X_0)$ est la tordue de $R_{k^n/k}(X_0) = X_0^n$ par f.

Cette variété ne dépend que de l'algèbre étale $A = A_f$ et pas de K (dans la mesure où $A \otimes_k K \overset{\sim}{\longleftarrow} K^n$).

Cette construction vérfie les propriétés formelles suivantes.

(1) Le morphisme "diagonal" $\Delta : X_0 \to X_0^n$ se descend en un morphisme canonique $X_0 \to R_{A/k}(X_0)$.
(2) Si F est une extension de k, on a $R_{A/k}(X_0) \times_k F \overset{\sim}{\longrightarrow} R_{A\otimes_k F/F}(X_{0,F})$.
(3) Si A' est une k–algèbre étale, on a un isomorphisme

$$R_{A\times_k A'/k}(X_0) = R_{A/k}(X_0) \times R_{A'/k}(X_0).$$

Par suite, on peut travailler en pratique dans le cas où A est un corps.

3.17. **Exercice.** Identifier $R_{K/k}(\mathrm{Spec}(K))$, puis montrer que $R_{A/k}(\mathbb{A}^1) \overset{\sim}{\longrightarrow} \mathbb{A}(A)$.

3.18. **Proposition.** *Soit L une sous-extension de K. La k–variété $R_{L/k}(X_0)$ est caractérisée par la propriété suivante:*
Pour toute k–variété affine Z_0, on a

$$\mathrm{Hom}_L\big(Z_{0,L}, X_{0,L}\big) \overset{\sim}{\longrightarrow} \mathrm{Hom}_k\big(Z_0, R_{L/k}(X_0)\big).$$

En particulier, $X_0(L) = R_{L/k}(X_0)(k)$.

On montrera ultérieurement une version plus générale de cette proposition. Contentons nous ici de décrire les flèches d'adonction.

(a) Etant donné un L–morphisme $g : Z_{0,L} \to X_{0,L}$, on associe le k-morphisme composé $Z_0 \overset{can}{\to} R_{L/k}(Z_0) \overset{g_*}{\to} R_{L/k}(X_0)$.

(b) Pour construire la flèche réciproque, le point est que le morphisme d'algèbres étales $L \to L \otimes_k L$, $l \to l \otimes 1$, admet le scindage canonique produit $l_1 \otimes l_2 \to l_1 l_2$. Ceci produit la décomposition d'algèbres étales

$$L \otimes_k L \cong L \times L'.$$

Etant donné un k–morphisme $h : Z_0 \to R_{L/k}(X_0)$, l'extension des scalaires à L produit un L–morphisme

$$h_L : Z_{0,L} \to R_{L\otimes_k L/L}(X_{0,M}) \overset{\sim}{\longrightarrow} R_{L\times_k L'}(X_{0,L}) \overset{\sim}{\longrightarrow} R_{L/L}(X_{0,L}) \times_L R_{L'/L}(X_{0,L})$$

où l'on a utilisé la troisième propriété ci-dessus. La première projection définit un homomorphisme $Z_{0,L} \to X_{0,L}$.

Pour voir que tout est cohérent, la technique éprouvée est d'étendre les scalaires à $\widetilde{k} = K$ afin de travailler avec la $\widetilde{k}$–algèbre étale triviale $\widetilde{k}^n$.

3.5. **Passage à la limite.** Soit k_s une clôture séparable de k contenant K. Soit K'/k est une extension galoisienne contenant K de groupe $\Gamma' = \mathrm{Gal}(K'/k)$. On a une surjection naturelle $\Gamma' \to \Gamma$ et l'extension des scalaires de K à K' donne lieu à un plongement de groupes

$$\mathrm{Aut}_K(X_{0,K}) \to \mathrm{Aut}_{K'}(X_{0,K'})$$

qui est Γ'–équivariant. Le composé

$$Z^1\big(\Gamma, \mathrm{Aut}_K(X_{0,K})\big) \to \ Z^1\big(\Gamma', \mathrm{Aut}_K(X_{0,K})\big) \to \ Z^1\big(\Gamma', \mathrm{Aut}_{K'}(X_{0,K'})\big)$$

induit une application

$$H^1\big(\Gamma, \mathrm{Aut}_K(X_{0,K})\big) \to H^1\big(\Gamma', \mathrm{Aut}_{K'}(X_{0,K'})\big).$$

Le théorème de descente galoisienne indique que cette flèche est injective (cela peut aussi se vérifier directement sur les cocycles). On pose

$$H^1\big(k_s/k, \mathrm{Aut}_{k_s}(X_{0,k_s})\big) := \bigcup_{L/k} H^1\big(\, \mathrm{Gal}(L/k), \mathrm{Aut}_L(X_{0,L})\big)$$

où L/k parcourt les sous-extensions galoisiennes finies de k_s/k. Par ailleurs, une k_s/k–forme de X_0 est une k–variété telle qu'il existe une sous-extension galoisienne finie L/k de k_s/k satisfaisant $X_{0,L} \xrightarrow{\sim} X_L$.

Par passage à la limite du théorème de descente galoisienne, on obtient une bijection naturelle

Classes de k–isomorphie de k_s/k–formes de X_0 $\quad < -- > \quad H^1\big(k_s/k, \mathrm{Aut}_{k_s}(X_0 \times_k k_s)\big)$.

Par abus de notation, il arrive que l'on omette k_s dans les ensembles ci-dessus.

4. Groupes de type multiplicatif

4.1. **Définition.**

4.1. **Définition.** Un k–groupe algébrique affine G est de type multiplicatif si G est une k_s/k–forme d'un k–groupe diagonalisable.

Si G est un tel k–groupe, il existe un $\mathbb{Z}$–module de type fini M_O (unique à isomorphisme près) et une extension galoisienne finie K/k tels que $D(M_0) \times_k K \cong G \times_k K$.

Si M_0 est fini, le groupe G est fini sur k; le k–groupe G est donc fini de type multiplicatif.

Si $M_0 = \mathbb{Z}^r$, on dit que G est un k–tore algébrique de dimension r, c'est le cas $\mathbb{G}_m^r \times_k k_s \cong G \times_k k_s$.

Vu que $\mathrm{Aut}_K(D(M_0) \times_k K) = \mathrm{Aut}_{\mathbb{Z}}(M_0)$, la correspondance ci-dessus s'écrit

Classes de k–isomorphie de K/k–formes de $D(M_0)$ $\quad < -- > \quad \mathrm{Hom}(\mathrm{Gal}(K/k), \mathrm{Aut}_{\mathbb{Z}}(M_0))/\sim$

$< -- >$ Structures de Γ–modules sur M_0.

Une façon de voir cette correspondance est d'associer à G son groupes des caractères

$$\widehat{G}(K) = \mathrm{Hom}_{K-gr}(\mathbb{G}_{m,K}, G_K).$$

C'est un Γ–module et la classe $[G] \in \mathrm{Hom}(\mathrm{Gal}(K/k), \mathrm{Aut}_{\mathbb{Z}}(M_0))/\sim$ n'est pas autre chose que la classe d'isomorphie du Γ–module $\widehat{G}(K)$ composée de M_0 et d'une action de $\mathrm{Gal}(K/k)$ sur M_0.

En particulier on a la correspondance

k–tores algébriques de dimension r déployés par K/k $<-->$ $\mathrm{Hom}(\mathrm{Gal}(K/k), \mathrm{GL}_r(\mathbb{Z}))/\sim$.

$<-->$ Γ–réseaux de dimension r.

4.2. **Exemples.** Premiers exemples

(a) Le Γ–module libre $\mathbb{Z}[\Gamma]$ correspond au k–tore $R_{K/k}(\mathbb{G}_m)$ (à vérifier).

(b) Le morphisme $N : \mathbb{Z} \to \mathbb{Z}[\Gamma]$, $1 \mapsto \sum\limits_{\sigma \in \Gamma} \sigma$ donne lieu à un morphisme $N_{K/k} : R_{K/k}(\mathbb{G}_m) \to \mathbb{G}_m$. On appelle ce morphisme la norme; en effet, sur les k–points rationnels, $N_{K/k}$ donne lieu à la norme usuelle $K^\times = R_{K/k}(\mathbb{G}_m)(k) \to (\mathbb{G}_m)(k) = k^\times$.

Par ailleurs, on a morphisme naturel $i_{K/k} : \mathbb{G}_m \to R_{K/k}(\mathbb{G}_m)$ provenant de l'augmentation $\mathbb{Z}[\Gamma] \to \mathbb{Z}$, $\sigma \mapsto 1$.

(c) Plus généralement, si $L = K^H$ pour $H \subset \Gamma$, le Γ–module de permutation $\mathbb{Z}[\Gamma/H]$ donne lieu au tore (dit induit ou encore quasi–trivial) $R_{L/k}(\mathbb{G}_m)$ et à des morphismes $i_{L/k} : \mathbb{G}_m \to R_{L/k}(\mathbb{G}_m)$ et $N_{L/k} : R_{L/k}(\mathbb{G}_m) \to \mathbb{G}_m$.

4.2. **Catégorie des k–groupes de type multiplicatif.**

4.3. **Théorème.** *(dualité de Cartier) On pose* $\Gamma = \mathrm{Gal}(K/k)$.

(1) Le foncteur "caractère" produit une anti-équivalence de catégories additives

groupes de type multiplicatifs déployés par K/k $<-->$ $\mathrm{Gal}(K/k)$*-modules de type fini.*

(2) Une suite

$$1 \to G_1 \to G_2 \to G_3 \to 1$$

de groupes de types mutiplicatifs (déployés par K/k) est exacte si et seulement si

$$0 \to \widehat{G}_3(K) \to \widehat{G}_2(K) \to \widehat{G}_1(K) \to 0$$

est exacte.

La seconde assertion montre que la catégorie des groupes de type multiplicatifs est une catégorie abélienne. De plus la dualité de Cartier est une anti–équivalence de catégories abéliennes.

Démonstration.

(1) Il faut vérifier que si G et G' sont des k–groupes de type multiplicatif déployés par K/k, alors le morphisme $\mathrm{Hom}_{K-gr}(G, G') \xrightarrow{\sim} \mathrm{Hom}_\Gamma(\widehat{G}'(K), \widehat{G}(K))$. L'injectivité se voit après extension des scalaires à K, on est donc ramené au cas des groupes diagonalisables déjà établi. On note M_0 (resp. M_0') le

$\mathbb{Z}$–module sous–jacent à $\widehat{G}(K)$ (resp. $\widehat{G}'(K)$) et $f : \Gamma \to \mathrm{Aut}_{\mathbb{Z}}(M_0)$ (resp. $f' : \Gamma \to \mathrm{Aut}_{\mathbb{Z}}(M_0')$) sa structure de Γ-modules. Alors $\widehat{G}(K) \cong (M_0, f)$ et $\widehat{G}'(K) \cong (M_0, f')$. Par suite, un morphisme Γ-équivariant $M_0' \to M_0$ donne lieu à un morphisme ${}_fD(M_0) \to {}_{f'}D(M_0')$, c'est-à-dire à un morphisme de k–groupes $G \to G'$ qui est dual du Γ–morphisme $M_0' \to M_0$.
(2) Suivant la proposition 3.15, la suite de k–groupes $1 \to G_1 \to G_2 \to G_3 \to 1$ est exacte si et seulement si la suite de K–groupes $1 \to G_{1,K} \to G_{2,K} \to G_{3,K} \to 1$ est exacte. Par ailleurs, la suite de Γ–modules $0 \to \widehat{G}_3(K) \to \widehat{G}_2(K) \to \widehat{G}_1(K) \to 0$ est exacte si et seulement si la suite exacte sous-jacente de $\mathbb{Z}$-modules $0 \to \widehat{G}_3(K) \to \widehat{G}_2(K) \to \widehat{G}_1(K) \to 0$ est exacte. On est donc ramené au cas des groupes mutiplicatifs déjà considéré en (2.8). $\square$

4.4. **Remarque.** De même qu'en 2.10, un k–groupe de type multiplicatif G admet un dévissage canonique

$$1 \to T \to G \to \mu \to 1$$

où T est un k–tore algébrique et μ un k–groupe fini de type multiplicatif. Si μ est étale sur k, T est la composante connexe de l'origine de G.

La connaissance des sous–groupes finis (ou plus exactement de leurs classes de conjugaison) de $\mathrm{GL}_n(\mathbb{Z})$ pour les petites valeurs de n permet de comprendre les k–tores algébriques de petite dimension.

4.5. **Exemples.** (a) *Tores de dimension 1:* On a $\mathrm{GL}_1(\mathbb{Z}) = \{\pm 1\}$. Les Γ–modules sont donc donnés par des caractères d'ordre 2 de Γ. Du coté galoisien, les k-tores de rang 1 sont les k–tores normiques $\ker\bigl(R_{A/k}(\mathbb{G}_m) \to \mathbb{G}_m\bigr)$ pour A une algèbre étale de degré 2. Ce tore est noté $R^1_{A/k}(\mathbb{G}_m)$.
(b) *Tores de dimension 2:* Les sous–groupes finis maximaux de $\mathrm{GL}_2(\mathbb{Z})$ sont bien connus. Le premier, noté W_1, est d'ordre 8, c'est le groupe $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$. Le second est $S_3 \times \mathbb{Z}/2\mathbb{Z}$ agissant sur $\mathbb{Z}^3/\mathbb{Z}$. Ce dernier cas donne lieu à des tores $\ker\Bigl(R_{L/k}\bigl(R^1_{A/k}(\mathbb{G}_m)\bigr) \to R^1_{A/k}(\mathbb{G}_m)\Bigr)$ pour une algèbre étale cubique A et une algèbre étale quadratique L/k.
(c) *Tores de dimension 3:* La classification des sous–groupes finis de $\mathrm{GL}_3(\mathbb{Z})$ est due à Tahara [Ta]. Elle indique que l'ordre d'un sous–groupe fini de $\mathrm{GL}_3(\mathbb{Z})$ divise 48. Les tores de dimension 3 ont été étudiés par B. Kunyavskiĭ [Ku].

Un autre point de vue est de regarder les k–tores déployés algébriques déployés par une extension galoisienne K/k de groupe de Galois Γ petit, par exemple cyclique ou bicyclique.

4.6. **Lemme.** *Soit $\Gamma = \mathbb{Z}/n\mathbb{Z}$ un groupe cyclique de générateur σ. On pose $J_\Gamma = \mathbb{Z}[\Gamma]/\mathbb{Z}$ et $I_\Gamma = \ker\bigl(\mathbb{Z}[\Gamma] \to \mathbb{Z}\bigr)$. Alors $\sigma - 1$ induit un isomorphisme*

$$J_\Gamma \xrightarrow{\sim} I_\Gamma.$$

□

Ainsi si A/k est une $\mathbb{Z}/n\mathbb{Z}$–algèbre étale, on a un isomorphisme

$$R_{A/k}(\mathbb{G}_m)/\mathbb{G}_m \xrightarrow{\sim} R^1_{A/k}(\mathbb{G}_m).$$

4.7. **Théorème.** *(Diederichsen-Reiner,* [R], [CR, §34.B]*) Soit p un nombre premier. On note h le nombre de classes de l'anneau $\mathbb{Z}[e^{2\pi\, i/p}]$ des entiers cyclotomiques. Il existe $(2h+1)$ $\mathbb{Z}/p\mathbb{Z}$–modules indécomposables non isomorphes.*

Dans le cas $h = 1$, c'est-à-dire lorsque $\mathbb{Z}[e^{2\pi\, i/p}]$ est un anneau principal, cela signifie que les seuls $\mathbb{Z}/p\mathbb{Z}$–modules indécomposables sont $\mathbb{Z}$, $\mathbb{Z}[\mathbb{Z}/p\mathbb{Z}]$ et $I_{\mathbb{Z}/p\mathbb{Z}}$. Dans le cas $p = 2$, il existe une démonstration élémentaire. Rappelons le fait suivant.

4.8. **Lemme.** *Soit M un réseau et N un sous-réseau. Alors le "saturé"*

$$N^\sharp := \Big\{ m \in M \ \mid \ \textit{il existe } a \in \mathbb{Z} \textit{ tel que } a\, m \in N \Big\}$$

est facteur direct de M et est de même rang que N.

Démonstration du théorème 4.7 pour $p = 2$ (M. Florence): Soit R un Γ-réseau indécomposable de $\mathbb{Z}$-rang ≥ 2. Si l'involution σ n'est pas la multiplication par -1, il existe une suite exacte équivariante:

$$0 \to K \to R \to \mathbb{Z} \to 0.$$

En effet, on choisit un vecteur primitif dans le $\mathbb{Z}$-dual de R, qui est invariant par l'involution; cela donne un plongement $\mathbb{Z} \to \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Z})$ puis la suite exacte ci-dessus en dualisant. Cette suite est non scindée. Soit v dans R s'envoyant sur 1 par la surjection; et soit P un plan de R, contenant v, invariant par l'involution. Quitte à remplacer P par son saturé $P^\sharp$, on peut supposer que P est facteur direct de R (comme $\mathbb{Z}$-module seulement, bien sur). On a alors une suite exacte non scindée de Γ–modules

$$0 \to L \to P \to \mathbb{Z} \to 0,$$

où L est isomorphe a $\mathbb{Z}[\Gamma]/\mathbb{Z}$ puisqu'il est $\mathbb{Z}$-libre de rang 1 avec action non triviale de σ. On peut montrer que P est $\mathbb{Z}[\Gamma]$ avec de la cohomologie des groupes (i.e. $\mathrm{Ext}^1_\Gamma(\mathbb{Z}, \mathbb{Z}[\Gamma]/\mathbb{Z}) = H^1(\Gamma, \mathbb{Z}[\Gamma]/\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$), mais aussi de la façon suivante.

Soit l un générateur du groupe abélien L; on a $\sigma(l) = -l$. La préimage de 1 par la surjection $P \to \mathbb{Z}$ est $v + \mathbb{Z}l$. On peut écrire $v - \sigma(v) = m\, l$, avec m entier. Du coup, pour un entier n, on a $(v + n\, l) - \sigma(v + nl) = (m + 2n)l$. Par suite, vu que 1 n'a pas d'antécédent fixe par σ, m est impair et on peut choisir un antécédent w de 1 tel que $w - \sigma(w) = l$. On constate alors que le Γ–morphisme $\mathbb{Z}[\Gamma] \to P$, envoyant 1 sur w, est un isomorphisme.

Le Γ–module P, étant projectif et facteur direct de R comme $\mathbb{Z}$-module, est facteur direct de R comme $\mathbb{Z}[\Gamma]$-module (pour le voir, considérer la suite exacte $0 \to P \to R \to Q \to 0$, ou tout est $\mathbb{Z}$-libre de type fini; dualiser, il y a une section puisque le dual de P est projectif et redualiser). On a donc une décomposition $R = P \oplus R'$ qui permet de conclure que $R = P = \mathbb{Z}[\Gamma]$. $\square$

Si K/k est une extension de corps quadratique étale, les k–tores déployés par $\mathrm{Gal}(K/k)$ sont des produits des k–tores suivants $\mathbb{G}_m$, $R_{K/k}(\mathbb{G}_m)$, $R^1_{K/k}(\mathbb{G}_m)$.

4.3. **Unirationalité des tores algébriques.**

4.9. **Définition.** Soit X une k–variété séparée, intègre et irréductible.
(1) X est k–unirationnelle s'il existe un k–morphisme dominant $W \to X$ où W est un ouvert non vide d'un espace affine.

(2) X est k–rationelle s'il existe un ouvert non vide $U \subset X$ k–isomorphe à un ouvert d'un espace affine.

Pour l'unirationalité, il revient au même de demander que le corps de fonctions $k(X)$ est un sous k–corps d'un corps transcendant pur $k(t_1, \cdots, t_n)$. De même, la k–rationalité se lit sur le corps des fonctions de X, c'est-à-dire $k(X)$ est k–isomorphe à un corps $k(t_1, ..., t_n)$.

4.10. **Proposition.** *Soit T un k–tore algébrique. Alors T est une variété k–unirationnelle.*

Démonstration: Soient K/k une extension galoisienne finie et Γ son groupe de Galois. On note $M = \widehat{T}(K)$ le Γ–module des caractères de T_K. L'idée est de plonger M dans un $\mathbb{Z}[\Gamma]$–module libre. On procède de la manière suivante. Le morphisme $N : \mathbb{Z} \to \mathbb{Z}[\Gamma]$ produit le plongement

$$M \hookrightarrow \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} M$$

Nous affirmons que le Γ–module $\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} M$ est libre, plus précisèment que la flèche

$$\mathrm{Hom}_\Gamma(M \otimes_{\mathbb{Z}} \mathbb{Z}[\Gamma], N) \to \mathrm{Hom}_{\mathbb{Z}}(M, N), \quad h \mapsto h(m \otimes [e])$$

est un isomorphisme pour tout Γ-module N. Cette flèche est en effet injective et son inverse applique $f : M \to N$ sur le Γ–morphisme $F : M \otimes_{\mathbb{Z}} \mathbb{Z}[\Gamma] \to N$ défini par $\sigma \otimes m \mapsto \sigma \,.\, f(\sigma^{-1}.m)$. Ce plongement $M \to \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} M \cong \mathbb{Z}[\Gamma]^r$ produit par dualité un morphisme (surjectif dans la catégorie des k–groupes de type multiplicatifs)

$$R_{K/k}(\mathbb{G}_m)^r \to T \to 1.$$

Vu que $R_{K/k}(\mathbb{G}_m)^r$ est un ouvert de l'espace affine $\mathbb{A}(K^r)$, on conclut que T est une variété k–unirationnelle. $\square$

4.11. **Corollaire.** *Si k est infini, $T(k)$ est Zariski dense dans T.*

4.4. **Un énoncé d'approximation faible.**

4.12. **Proposition.** *Soit T un $\mathbb{Q}$–tore algébrique. Alors $T(\mathbb{Q})$ est dense dans $T(\mathbb{R})$ muni de la topologie réelle.*

Si $T \subset \mathbb{A}^n_{\mathbb{Q}}$, on a $T(\mathbb{R}) \subset \mathbb{R}^n$ et la topologie réelle sur $T(\mathbb{R})$ est la topologie induite par celle de de $\mathbb{R}^n$. La définition intrinsèque de cette topologie est due à Weil [W, appendice III]..

Démonstration: Soit $K/\mathbb{Q}$ une sous-extension K de $\mathbb{C}$ stable par la conjugaison complexe, déployant T et galoisienne de groupe de Galois Γ fini. On pose $L = \{x \in K \mid \overline{x} = x\}$. Alors K/L est une extension quadratique. On note $M = \widehat{T}(K)$ le Γ-réseau des caractères de T. Le plongement

$$M \hookrightarrow M \otimes_{\mathbb{Z}} \mathbb{Z}[\Gamma/\operatorname{Gal}(K/L)]$$

définit par dualité le morphisme de norme

$$N_{L/\mathbb{Q}} : R_{L/\mathbb{Q}}(T) \to T.$$

Vu que $L \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R} \times A$ pour une $\mathbb{R}$–algèbre étale A, on a $R_{L/\mathbb{Q}}(T) \times_{\mathbb{Q}} \mathbb{R} \cong T_{\mathbb{R}} \times R_{A/\mathbb{R}}(T_{\mathbb{R}})$ et ainsi la flèche

$$\big(R_{L/\mathbb{Q}}(T)\big)(\mathbb{R}) \to T(\mathbb{R})$$

est (scindée) surjective. On est donc ramené à voir que l'adhérence de $\big(R_{L/\mathbb{Q}}(T)\big)(\mathbb{Q})$ dans $\big(R_{L/\mathbb{Q}}(T)\big)(\mathbb{R})$ contient le facteur $T(\mathbb{R})$, c'est-à-dire que $T_L(L)$ est dense dans $T_L(\mathbb{R})$ pour le plongement $L \to \mathbb{R}$ ci-dessus. Le tore T_L est déployé par l'extension quadratique K/L, il est donc un produit de tores (4.7) $\mathbb{G}_{m,L}$, $R_{K/L}(\mathbb{G}_m)$ et $R^1_{K/L}(\mathbb{G}_m) \cong R_{K/L}(\mathbb{G}_m)/\mathbb{G}_m$. Il suffit donc de traiter ces trois cas. Pour le premier, $L^\times$ est dense dans $\mathbb{R}^\times$, pour le second $K^\times$ est dense dans $(K \otimes_L \mathbb{R})^\times = \mathbb{C}^\times$. Le tore $R_{K/L}(\mathbb{G}_m)/\mathbb{G}_m$ est un ouvert de l'espace projectif $\mathbb{P}^1(L)$, donc $\big(R_{K/L}(\mathbb{G}_m)/\mathbb{G}_m\big)(L)$ est dense dans $\big(R_{K/L}(\mathbb{G}_m)/\mathbb{G}_m\big)(\mathbb{R})$. □

Nous reviendrons sur l'approximation faible sur les tores. Le résulat le plus basique est le suivant.

4.13. **Lemme.** *Soient T un k–tore et K/k une extension galoisienne déployant T. Soient $v_1, ..., v_n$ des valuations de k indépendantes deux à deux et k_{v_i} les complétés respectifs de k. Alors*

$$[K:k]\,.\operatorname{Coker}\Big(\overline{T(k)} \to \prod_i T(k_{v_i})\Big) = 0,$$

où $\overline{T(k)}$ désigne l'adhérence de $T(k)$ dans les $\prod_i T(k_{v_i})$ suivant le plongement diagonal.

Démonstration. Le composé $T \to R_{K/k}(T) \overset{N_{K/k}}{\to} T$ est la multiplication par $[K:k]$ et on a déjà vu que $R_{K/k}(T) \cong R_{K/k}(\mathbb{G}_m^r)$ est un ouvert du k–espace affine $\mathbb{A}(K^r)$. Le groupe $T(K) = R_{K/k}(T)(k)$ est donc dense dans

$\prod_i R_{K/k}(T)(k)(k_{v_i})$ suivant le théorème d'indépendance des valuations. Le diagramme commutatif

$$\begin{array}{ccccc} T(k) & \longrightarrow & R_{K/k}(T)(k) & \xrightarrow{N_{K/k}} & T(k) \\ \downarrow & & \downarrow & & \downarrow \\ \prod_i T(k_{v_i}) & \longrightarrow & \prod_i R_{K/k}(T)(k_{v_i}) & \xrightarrow{N_{K/k}} & \prod_i T(k_{v_i}) \end{array}$$

permet de conclure que le défaut d'approximatioin faible de T

$$\mathrm{Coker}\Big(\overline{T(k)} \to \prod_i T(k_{v_i})\Big)$$

est annulé par $[K:k]$. $\square$

4.5. **Un résultat de J. Tits.**

4.14. **Théorème.** [T3, III.1.6] *On suppose que le corps k n'est pas une extension algébrique d'un corps fini. Soit T/k un tore algébrique. Alors il existe $t \in T(k)$ tel que le groupe $t^{\mathbb{Z}}$ est Zariski dense dans T.*

L'hypothèse sur le corps de base est nécessaire. En effet, tout élément de $\overline{\mathbf{F}}_p^\times$ est d'ordre fini. Cet énoncé est donc inexact dans le cas du tore $\mathbb{G}_m$ et de $\overline{\mathbf{F}}$. Ce résultat est donc de nature différente par rapport au Corollaire 4.11.

4.15. **Exemples.** (a) Si $T = \mathbb{G}_m^r$, la proposition énonce qu'il existe des éléments $t_1, \cdots, t_r \in k^\times$ tels que $t_1, ..., t_r$ engendrent un réseau de rang r dans $T(k)$. Ceci est clair par réduction au cas de $k = \mathbb{Q}$.
(b) Plus généralement si $T = R_{K/k}(\mathbb{G}_m)^r$ pour une extension finie galoisienne K/k de groupe Γ. Alors le Théorème énonce en fait qu'il existe des éléments $t_1, \cdots, t_r \in K^\times$ tels que les $(\sigma(t_i))_{\sigma\in\Gamma, i=1,\dots,r}$ engendrent un réseau de rang $[K:k]r$ dans $T(K) = (K^\times)^{[K:k]r}$.

Démonstration du théorème 4.14 si k n'est pas dénombrable: Il existe K/k galoisienne finie (de groupe Γ) et un morphisme surjectif $\big(R_{K/k}\mathbb{G}_m\big)^r \to T$. Il suffit de montrer la proposition pour le tore $E := \big(R_{K/k}\mathbb{G}_m\big)^r$. Si $\underline{n} = (n_{\sigma,i})_{\sigma\in\Gamma, i=1,\dots,r}$ sont des entiers indexés par Γ et $[1,n]$, on définit le sous–tore $E_{\underline{n}}$ de E par l'équation

$$\prod_{i=1,\dots,r \,|\, \sigma\in\Gamma} \sigma(t_i)^{n_{i,\sigma}} = 1.$$

Mais E est un ouvert de l'espace affine $\mathbb{A}(K^r)/k$. Vu que k n'est pas dénombrable, l'ensemble

$$E(k) \setminus \bigcup_{\underline{n}} E_{\underline{n}}(k)$$

est non vide où $\underline{n}$ parcourt toutes les familles d'entiers. Soit x un élément de cet ensemble. On note $G \subset E$ l'adhérence de Zariski de $\langle x \rangle$. C'est un sous-groupe de type multiplicatif et $x \in G(k)$. Alors G^0 est un k–tore. Comme G^0 est d'indice fini dans G, il existe un entier d tel que $g^d \in G^0(k)$. Si $G^0 \neq G$, alors G^0 est un sous-tore d'un $E_{\underline{n}}$ et alors $g^d \in E_{\underline{n}}(k)$ et $g \in E_{d\underline{n}}(k)$, ce qui est une contradiction. Il résulte que $x^{\mathbb{Z}}$ est Zariski dense dans E. □

Le cas général est une autre affaire. La démonstation originale de Tits traite le cas du tore E ci-dessus. Nous suivons ici essentiellement la démonstration de Raghunathan [R] qui met en évidence le résultat intermédiaire suivant.

4.16. **Proposition.** *Sous les hypothèses du Théorème 4.14, le groupe abélien $T(k)$ est de rang infini.*

Démonstration:
Premier cas: k est un corps global: D'après le théorème de Cebotarev, il existe une infinité de places v de k telles que $K \otimes_k k_v = k_v \times ...k_v$ (i.e. places totalement décomposées). Alors le tore $T \times_k k_v$ est déployé pour une telle place. Soit $v_1, ..., v_m$ de telles places. Le plongement $T(k_v) \to (k_v^\times)^{r\,\sharp\,\mathrm{Gal}(K/k)}$ permet de parler d'éléments entiers de $T(k_v)$, c'est-à-dire de la préimage de $(O_v^\times)^{r\,\sharp\,\mathrm{Gal}(K/k)}$. Soit $t_i \in T(k_{v_i})$ un élément non entier. Soit $\tau_i \in T(k)$ une bonne approximation de $(1, \cdots, t_i^{[K:k]}, 1, \cdots)$ (donnée par le Lemme 4.13), c'est-à-dire telle que la composante en v_i soit non entière et les autres entières. Alors les τ_i engendrent un sous–réseau de $T(k)$ de rang m. En effet, supposons que l'on ait une relation

$$\prod_i \tau_i^{r_i} = 1$$

avec $r_i \in \mathbb{Z}$. Alors $t_i^{[K:k]\,,\,r_i}$ est entier pour la valuation v_i pour tout i, donc $r_i = 0$.
Cas général (esquisse): On procède par récurrence sur le le degré de transcendance sur k sur le corps premier. On écrit alors $k = k_0(C)$ où C/k_0 est une courbe algébrique lisse. Soit c un point fermé de C où le tore T/k a bonne réduction, c'est-à-dire s'étend en un schéma en groupes lisse $\mathcal{T}$ sur l'anneau local $R := \mathcal{O}_{C,c}$ et tel que la fibre spéciale $\mathcal{T} \times_R k_0(c)$ est un $k_0(c)$-tore. On a alors une flèche de spécialisation $\mathcal{T}(R) \to \mathcal{T}(k_0(c))$. Le même type de techniques[1] que pour l'approximation faible permet de montrer l'inclusion

$$\mathcal{T}(k_0(c))^{[K:k]} \subset \mathrm{Im}\Big(\mathcal{T}(R) \to \mathcal{T}(k_0(c))\Big).$$

Par récurrence, $\mathcal{T}(k_0(c))$ est de rang infini, on en déduit que $\mathcal{T}(R)$ est de rang infini. Mais $\mathcal{T}(R)$ est un sous–groupe de $T(k)$, donc $T(k)$ est de rang infini. □

---

[1]de façon précise, la théorie des R–tores algébriques, voir [CTS2, §7].

4.17. **Remarque.** La démonstration montre en fait que les éléments d'ordre infini de $T(k)$ sont Zariski dense dans T.

4.18. **Définition.** Soit T un k–tore algébrique T et $\phi : \mathrm{Gal}(K/k) \to \mathrm{GL}_r(\mathbb{Z})$ un morphisme le définissant. On dit que T est irréductible si la représentation rationnelle $\phi : \mathrm{Gal}(K/k) \to \mathrm{GL}_r(\mathbb{Q})$ est irréductible.

La définition ne dépend pas du choix de K/k et de ϕ. Si T est irréductible et si $T_1 \times T_2 \to T$ est un morphisme surjectif à noyau fini de k–tores, alors T_1 ou T_2 est trivial. Tout k–tore est un quotient fini d'un produit de k–tores irréductibles.

Démonstration du théorème 4.14 dans le cas général: Soit K/k une une extension galoisienne déployant T.
Cas T irréductible: Le lemme 4.16 produit un élément $t \in T(k)$ d'ordre infini. Soit S la composante connexe de l'adhérence de Zariski de $t^{\mathbb{Z}}$ dans T. Alors l'extension K/k déploie S et on a un morphisme surjectif $\widehat{T}(K) \to \widehat{S}(K)$. Puisque T est irréductible et S non trivial, on a $\widehat{T}(K) \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} \widehat{S}(K) \otimes_{\mathbb{Z}} \mathbb{Q}$. Par suite le résau $\ker\bigl(\widehat{T}(K) \to \widehat{S}(K)\bigr)$ est trivial, d'où $S = T$.
Cas T^n avec T irréductible: On procède par récurrence sur $n \geq 1$. Soit $(t_1, ..., t_{n-1}) \in T(k)^{n-1}$ engendrant T^{n-1}. On considère le sous–groupe $M \subset K^\times$ engendré par les $\chi(t_i)$ pour χ parcourant $\widehat{T}^{n-1}(K)$. Le groupe M est un réseau. Soit $\chi_0 \in \widehat{T}(K)$, $\chi_0 \neq 0$. Ce caractère définit un morphisme $f : T \to R_{K/k}(\mathbb{G}_m)$ non trivial dont le noyau est fini puisque T est irréductible. D'après le lemme 4.16, $f(T(k))$ est un sous–groupe de rang infini de $K^\times$. Il existe donc $t_n \in T(k)$ tel que $f(t_n)$ et M engendrent un réseau de rang $\mathrm{rg}(M) + 1$. Il reste à vérifier que $(t_1, ..., t_{n-1}, t_n)$ engendre T. On raisonne par l'absurde en supposant qu'il existe un K-caractère non trivial $\theta = \theta_1 \oplus \cdots \oplus \theta_n \in \widehat{T^n}(K)$ satisfaisant

$$1 = \theta(t_1, ..., t_n) = \prod_{i=1,...,n} \theta_i(t_i).$$

On a $\theta_n \neq 0$ en utilisant l'hypothèse de Par conjugaison, il vient

$$\sigma(\theta_n)(t_n) = \prod_{i=1,...,n-1} \sigma(\theta_i)(t_i) \quad \forall \sigma \in \mathrm{Gal}(K/k). \tag{4.19}$$

Puisque T est irréductible, les $\sigma(\theta_n)$ engendrent le $\mathbb{Q}$-vectoriel $\widehat{T}(K) \otimes_{\mathbb{Z}} \mathbb{Q}$. Il existe donc un entier $N \geq 1$ et une relation

$$N\,\chi_0 = \sum_{\sigma \in \mathrm{Gal}(K/k)} m_\sigma\, \sigma(\theta_n).$$

En multipliant les identités (4.19) pondérées par m_σ, on tire une relation

$$\chi_0(t_n)^{-N}(t_n) = \prod_{i=1,...,n-1, \sigma \in \mathrm{Gal}(K/k)} \sigma(\theta_i)^{m_\sigma}(t_i)$$

qui contredit le choix de t_n.

Cas général: On réalise T comme un quotient fini de $\prod_i T_i^{r_i}$ où les T_i sont des tores irréductibles de sorte que les représentations galoisiennes $\widehat{T}_i(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ doient deux à deux non isomorphes. Le cas précédent produit des éléments $\tau_i \in T_i^{r_i}(k)$ engendrant $T_i^{r_i}$. Nous affirmons que $\tau := (\tau_1, ..., \tau_r)$ engendre $\prod_i T_i^{r_i}$ et partant T. En effet, le sous–tore S de T engendré par τ se surjecte sur chaque facteur $T_i^{r_i}$. Par suite, le morphisme de $\mathrm{Gal}(K/k)$-représentations

$$\oplus_i \widehat{T}_i(K) \otimes_{\mathbb{Z}} \mathbb{Q} \to \widehat{S}(K)$$

est injectif sur chaque composante isotypique, il est donc injectif. Comme au premier cas, on conclut que $S = T$. $\square$

La variété des tores maximaux des groupes réductifs

Soit k un corps, k_s une clôture séparable et $\overline{k}$ une clôture algébrique.

5. Action de groupes

Soit G un k–groupe algébrique affine agissant (à gauche) sur une k–variété X séparée. Si Y' et Y sont des sous k–variétés fermées de X, on considère les foncteurs $\underline{Tranp}_G(Y',Y)$, $\underline{N}_G(Y)$, $\underline{Z}_G(Y)$ et $\underline{X}^G$ qui associent repsectivement à toute k–algèbre R le sous-ensemble

$$\underline{Tranp}_G(Y',Y)(R) := \bigl\{g \in G(R) \mid p_1^*(g).p_2^*(Y(S)) \subset Y(R\otimes_k S) \text{ pour toute } k\text{–algèbre } S\bigr\}.$$

$$\underline{N}_G(Y)(R) := \bigl\{g \in G(R) \mid p_1^*(g).p_2^*(Y(S)) = Y(R\otimes_k S) \text{ pour toute } k\text{–algèbre } S\bigr\}.$$

$$\underline{Z}_G(Y)(R) := \bigl\{g \in G(R) \mid p_1^*(g).p_2^*(y) = p_2^*(y) \text{ pour toute } k\text{–algèbre } S \text{ et tout } y \in Y(S)\bigr\}.$$

$$\underline{X}^G(R) := \bigl\{x \in X(R) \mid p_2^*(g).p_1^*(x) = p_1^*(x) \text{ pour toute } k\text{–algèbre } S \text{ et tout } g \in G(S)\bigr\}.$$

5.1. **Théorème.** [DG, II.3.6] *ou* [SGA3, XI.6] *Ces quatre foncteurs sont représentables par des k–variétés. En outre, $\underline{Z}_G(Y)$ et $\underline{N}_G(Y)$ sont des k–sous-groupes algébriques fermés de G.*

Ces variétés sont alors notées $Tranp_G(Y',Y)$ (transporteur de Y' dans Y), $N_G(Y)$ (normalisateur ou stabilisateur de Y), $Z_G(Y)$ (centralisateur ou fixateur de Y) et X^G (variétés des points fixes).

6. Espaces homogènes et cohomologie galoisienne

Pour simplifier, on suppose dans ce paragraphe que k est de caractéristique nulle.

Soit G un k–groupe algébrique affine et soit X une k–variété (non vide) munie d'une action (à droite) de G. On dit que X est un espace homogène sous G (resp. principal homogène) si $G(k_s)$ agit de façon transitive (resp. simplement transitive) sur $X(k_s)$.

Les G-espaces principaux homogènes sont aussi appelés G–torseurs, ou encore G–torseurs sur Spec(k).

6.1. **Exemples.** (a) Etant donné une forme quadratique non dégénérée q, la quadrique projective $\{q = 0\}$ est homogène sousle groupe orthogonal $O(q)$.
(b) Etant donné un entier $n \geq 1$ et $a \in k^\times$, la variété $\{x^n = a\}$ est un espace principal homogène sur $\mu_n = \mathrm{Spec}(\frac{k[t]}{(t^n-1)})$.

On observe que le groupe $G(k)$ (agissant par translations à droite sur lui-même) est le groupe des k–automomorphismes du G–espace principal homogène G. La descente galoisienne indique la correspondance suivante

Classes de k–isomorphie de G–espaces principaux homogènes $< -- >$ $H^1(k,G)$.

Si H est un k–sous–groupe de G, on rappelle que le théorème des semi-invariants de Chevalley [Po, §10] permet de définir le quotient $H\backslash G$. C'est une variété quasi-projective et le morphisme quotient $G \to H\backslash G$ est lisse et surjectif.

6.2. **Lemme.** *Soit X un espace homogène sous G. Alors les assertions suivantes sont équivalentes:*

(1) *$X(k) \neq \emptyset$,*
(2) *$X \cong H\backslash G$ pour un certain $H \subset G$.*

Démonstration: (1) $\Longrightarrow$ (2) est trivial. Réciproquement un point $x \in X(k)$ produit un isomorphisme $G_x\backslash G \xrightarrow{\sim} X$, $g \mapsto x\,.\,g$. □

6.3. **Remarque.** Le groupe H n'est pas unique, il existe des isomorphismes G-équivariants $H\backslash G \cong H'\backslash G$ pour des k–groupes H et H' non isomorphes. Voir §8.2.

On considère maintenant des G–espaces homogènes à gauche. Pour un quotient $X := G/H$, il n'est pas vrai en général que l'application $\pi : G(k) \to X(k)$ est surjective. Par exemple, $\mathbb{G}_m$ est le quotient de $\mathbb{G}_m$ par μ_n et l'application $k^\times \to k^\times$, $x \mapsto x^n$, n'est pas surjective. La cohomologie galoisienne est le cadre approprié. En effet, on a la suite exacte d'*ensembles pointés*[2]

$$1 \to H(k) \to G(k) \to X(k) \xrightarrow{\varphi} H^1(k,H) \to H^1(k,G).$$

L'application φ est appelée l'application caractéristique. En termes de cocycles, elle est définie de la façon suivante. Si $x \in X(k)$, il existe une extensions galoisienne finie K/k (avec $K \subset k_s$) et un élément g de $G(K)$ tel que $\pi(g) = x$. Vu que $\pi(\sigma(g)) = x$ pour tout $\sigma \in \mathrm{Gal}(K/k)$, $z_\sigma := g^{-1}\,\sigma(g)$ est un 1-cocycle à valeurs dans $H(K)$. La classe $[z]$ ne dépend pas du choix de g, et on pose $\phi(x) = [z]$.

6.4. **Remarque.** (a) De façon intrinsèque, on peut définir $\phi(x)$ comme la classe d'isomorphie dans $H^1(k,H)$ du H–espace principal homogène $\pi^{-1}(x)$.
(b) Il est commode de voir les éléments de $X(k)$ comme des classes $[gH]$ with $g \in G(K)$ (pour K/k galoisienne convenable) et satisfaisant $g^{-1}\,\sigma(g) \in H(K)$ pour tout $\sigma \in \Gamma$.

---

[2]Un morphisme d'ensembles pointés est une application $f : (E,e) \to (E',e')$ appliquant e sur e'. Le noyau $\ker(f)$ est la préimage de e'. Une suite exacte d'ensembles pointés est une suite d'applications

$$\cdots \to (E_0,e_0) \xrightarrow{f_0} (E_1,e_1) \xrightarrow{f_1} (E_2,e_2) \to \cdots$$

telle que $(f_{i+1} \circ f_i)(E_i) = \{e_i\}$ et $\mathrm{Im}(f_i) = \ker(f_{i+1})$ pour tout $i \in \mathbb{Z}$.

6.5. **Proposition.** *L'application caractéristique induit une bijection*

$$G(k)\backslash X(k) \xrightarrow{\sim} \mathrm{Ker}\Big(H^1(k,H) \to H^1(k,G)\Big).$$

En d'autres mots, les $G(k)$-orbites de $X(k)$ sont décrites en termes de cohomologie galoisienne. Ceci est particulir̀ement intéressant si $G = \mathrm{GL}_n$ puisque alors $H^1(k,\mathrm{GL}_n) = 1$ (Hilbert 90). Si $X = \mathrm{GL}_n/H$, on a donc

$$\mathrm{GL}_n(k)\backslash X(k) \xrightarrow{\sim} H^1(k,H).$$

En particulier, si H est fini, cela établit un lien entre la théorie de Galois et les points rationnels de certains espaces homogènes.

Démonstration: Il reste à établir l'injectivité de $G(k)\backslash X(k) \xrightarrow{\sim} \mathrm{Ker}\big(H^1(k,H) \to H^1(k,G)\big)$. Soient $x = [gH]$, $x' = [g'H]$ des points de $X(K)$ pour K/k galoisienne finie de groupe Γ tels que $g^{-1}\sigma(g) = h^{-1}{g'}^{-1}\sigma(g')\sigma(h)$ pour un certain $h \in H(K)$. Alors $g'hg^{-1} = \sigma(g'hg^{-1})$ pour tout $\sigma \in \Gamma$, c'est-à–dire $g_0 := g'hg^{-1} \in G(k)$. Alors $g_0 x = [g_0 gH] = x'$. □

7. Généralités

7.1. Rappels sur un corps algébriquement clos.

7.1. **Définition.** Soit G un $\overline{k}$–groupe algébrique affine. Le $\overline{k}$–groupe G est unipotent[3] s'il admet une suite de composition dont les quotients successifs sont isomorphes à des sous–groupes algébriques de $\mathbb{G}_{a,\overline{k}}$.

7.2. **Remarque.** (a) Tout sous-groupe fermé et tout quotient de groupes unipotents est unipotent. Toute extension de groupes unipotents est unipotent.

(b) En caractéristique nulle, le groupe additif $\mathbb{G}_a$ n'admet aucun sous–groupe propre non trivial. Dans ce cas, le $\overline{k}$–groupe G est unipotent si il admet une suite de composition dont les quotients successifs sont isomorphes à des groupes additifs $\mathbb{G}_{a,\overline{k}}$.

(c) En caractéristique $p > 0$, les sous–groupes propres de $\mathbb{G}_{a,\overline{k}}$ sont les les sous–groupes finis constants $\mathbb{Z}/p^r\mathbb{Z}$ et les k–sous–groupes infinitésimaux comme $\alpha_{p^r} = \mathrm{Spec}(\frac{k[t]}{t^{p^r}})$. Si U est un k-groupe unipotent lisse et connexe, alors il admet une suite de composition dont les quotients successifs sont isomorphes à des groupes additifs $\mathbb{G}_{a,\overline{k}}$.

7.3. **Définition.** Soit G un $\overline{k}$–groupe algébrique affine. Le $\overline{k}$–groupe G est réductif s'il est lisse, connexe, et n'admet aucun sous–groupe algébrique unipotent distingué et non trivial.

Une première propriété fondamentale des groupes réductifs est la suivante:

[3]Cette définition est celle de [SGA3]; elle est en apparence plus générale que celle de Demazure-Gabriel [DG, IV.2.2].

7.4. **Théorème.** [Bo, 11.3] *Soit G un $\overline{k}$–groupe réductif. Alors les $\overline{k}$–tores maximaux de G sont conjugués par $G(\overline{k})$.*

Le rang commun des tores maximaux de G est appelé le rang de G, noté $\mathrm{rang}(G)$. Un sous-tore T de G est donc maximal si et seulement $\mathrm{rang}(T) = \mathrm{rang}(G)$.

Une seconde propriété fondamentale est la correspondance suivante:

7.5. **Théorème.** *(voir* [SGA3, §XIII.6]*) On suppose G de centre trivial (adjoint) ou* $\mathrm{car}(\overline{k}) = 0$. *On note $\mathfrak{g}$ l'algèbre de Lie de G. Alors il y a une correspondance bijective*

$$\big\{ \textit{tores maximaux de } G \,\big\} <-- > \big\{ \textit{sous–algèbres de Cartan de } \mathfrak{g} \,\big\}$$

Une sous algèbre de Cartan est une sous–algèbre de Lie $\mathfrak{c}$ de $\mathfrak{g}$ nilpotente telle que $\mathfrak{c} = \mathfrak{n}_{\mathfrak{g}}(\mathfrak{c})$. La correspondance ci-dessus associe à un tore maximal son algèbre de Lie et réciproquement à une sous–algèbre de Cartan $\mathfrak{c}$ le centralisateur $Z_G(\mathfrak{c})$ pour l'action adjointe de G sur $\mathfrak{g}$.

7.2. **Définitions rationnelles.**

7.6. **Définition.** Soit G un k–groupe algébrique.

(1) Le k–groupe G est unipotent si $G \times_k \overline{k}$ est unipotent.

(2) Le k–groupe G est réductif si $G \times_k \overline{k}$ est réductif.

(3) Un sous k–tore algébrique T de G est maximal si $T \times_k \overline{k}$ est un $\overline{k}$–tore maximal de $G \times_k \overline{k}$.

La troisième définition est surprenante à première vue. Cependant, on a la:

7.7. **Proposition.** *Soit G un k–groupe réductif.*

(1) *Le groupe G admet un k–tore maximal.*
(2) *Soit S un sous k-tore algébrique de G. Alors S est inclus dans un k–tore maximal de G.*

La correspondance (7.5) se descend à G, c'est-à-dire qu'il revient au même de se donner un k–tore maximal ou une sous-algèbre de Cartan de $\mathfrak{g} = Lie(G)$.

7.8. **Définition.** Soit $X \in \mathfrak{g}$.

(1) X est semi-simple si $ad(X) : \mathfrak{g} \to \mathfrak{g}, Y \to [X,Y]$ est semi-simple (i.e. est k_s–diagonalisable).

(2) On note $nil(X)$ la multiplicité de la valeur propre 0 de $ad(X)$ et $n(\mathfrak{g})$ la valeur minimale de $nil(X)$ pour X parcourant $\mathfrak{g} \otimes_k \overline{k}$. On dit que X est régulier si $nil(X) = n(\mathfrak{g})$.

7.9. **Remarque.** (a) En caractéristique nulle, si X est régulier, l'espace caractéristique $\mathrm{Nil}(X)$ de la valeur propre 0 est une sous–algèbre de Cartan de $\mathfrak{g}$ [Ca, th. 3.2]; inversement, toute sous–algèbre de Cartan $\mathfrak{c}$ de $\mathfrak{g}$ apparaît

comme un $\mathrm{Nil}(X)$ pour un certain élément régulier X. En outre, X est semi–simple et on a alors $\mathfrak{z}_{\mathfrak{g}}(X) = \mathrm{Nil}(X)$.
(b) Ceci explique pourquoi d'autres auteurs [FH] [V, §2] disent que X est régulier si $\mathfrak{z}_{\mathfrak{g}}(X)$ est une sous–algèbre de Cartan de $\mathfrak{g}$.

"Démonstration de la Proposition 7.7": Nous reviendrons sur le cas d'un corps fini. On suppose ici le corps de base de caractéristique nulle.

(1) On note $\mathfrak{g} = Lie(G)$. Dans l'espace affine $\mathbb{A}(\mathfrak{g})$, les éléments réguliers forment un ouvert de Zariski. Ainsi il existe un élément régulier $X \in \mathfrak{g}$. Son centralisateur $\mathfrak{z}_{\mathfrak{g}}(X)$ est une sous–algèbre de Cartan de $\mathfrak{g}$. Ainsi G admet un k–tore maximal.
(2) On considère le k–groupe $Z_G(S)$, c'est un k–groupe réductif [Sp, 15.3.2], de même rang que G. On note $p : Z_G(S) \to Z_G(S)/S$. Soit T' un k–tore maximal de $Z_G(S)/S$. Alors $T := p^{-1}(T')$ est un k-tore maximal de $Z_G(S)$, donc de même rang que G. Le tore T est donc un k–tore maximal de G contenant S. □.

8. La variété des tores

8.1. **Définition.** Soit G un k–groupe réductif et soit T un k–tore maximal. On pose $N_T = N_G(T)$ et on considère la variété quotient $X := G/N$.

8.1. **Lemme.** *Il y a une bijection naturelle entre $X(k)$ et l'ensemble des k-tores maximaux de G.*

Démonstration (en car. nulle): Tout d'abord, on a une bijection

$$\begin{array}{ccc} X(k_s) = G(k_s)/N_T(k_s) = N_G(T)(k_s) & \xrightarrow{\sim} & \Big\{k_s\text{–tores maximaux de } G\Big\} \\ g & \mapsto & gTg^{-1} \end{array}$$

puisque tous les k_s–tores maximaux sont conjugués par $G(k_s)$. Dans la situation rationnelle, étant donné $x = [gN] \in X(k)$, on remarque que le k_s-tore $gTg^{-1} \subset G \times_k k_s$ ne dépend pas du choix de g est stable sous l'action du groupe de Galois $\mathrm{Gal}(k_s/k)$. Par suite, le k–tore $T_x := gTg^{-1}$ est défini sur k, c'est un sous–k–tore maximal de G. Nous avons ainsi défini une application de $X(k)$ vers l'ensemble des k-tores de G. La surjectivité provient de la conjugaison sur k_s. Pour l'injectivité, si $x' = [g'N] \in X(k)$ satisfait $gTg^{-1} = g'Tg'^{-1}$, alors $gg'^{-1} \in N_T(k_s)$, d'où $x = x'$. □.

Pour cette raison, la variété X est appelée la variété des tores de G.

8.2. **Exemple.** Si A est une k–algèbre étale de dimension n munie d'un isomorphisme de k–espaces $f : A \cong k^n$, on peut former le tore quasi–trivial

$$R_{A/k}(\mathbb{G}_m) = \mathrm{GL}_1(A) \subset \mathrm{GL}(A) \cong \mathrm{GL}_n$$

Les k–tores de GL_n sont tous construits de cette façon et il y a une correspondance entre les et les classes de $\mathrm{GL}_n(k)$–conjugaisons des k–tores maximaux de GL_n et les classes d'isomorphie de k–algèbres étales de dimension n.

Ceci permet d'illustrer la remarque 6.3. En effet, si A est une k–algèbre étale non triviale de dimension n, elle donne lieu à un tore T non isomorphe à $\mathbb{G}_m^n$. De plus, $N_{\mathrm{GL}_n}(T)$ et $N_{\mathrm{GL}_n}(\mathbb{G}_m^n)$ sont non isomorphes. Pourtant les espaces homogènes $\mathrm{GL}_n/N_{\mathrm{GL}_n}(T)$ et $\mathrm{GL}_n/N_{\mathrm{GL}_n}(\mathbb{G}_m^n)$ sont k–isomorphes.

8.2. **Rationalité de la variété des tores.**

8.3. **Théorème.** *(Chevalley) La variété des tores X est k–rationnelle.*

Nous nous proposons de démontrer que X est *rétracte rationnelle*, c'est un résultat plus faible, mais qui suffit dans la plupart des applications.

8.4. **Définition.** Soit X/k une k-variété séparée, réduite et irréductible (intègre). La variété X est rétracte k-rationnelle s'il existe un ouvert non vide U de X tel que l'identité de U factorise à travers un ouvert V d'un espace affine $\mathbb{A}_k^m$, i.e. il existe des morphismes $f : U \to V$ et $r : V \to U$ tels que $r \circ f = id_U$.

Ces variétés sont caractérisées par une propriété fonctorielle.

8.5. **Proposition.** *(Saltman* [Sa, theorem 3.9], *voir aussi* [CTS3, §1]*) . Soit X/k une k-variété séparée, réduite et irréductible. Les assertions suivantes sont équivalentes:*

(1) *X est rétracte k–rationnelle.*
(2) *Il existe un ouvert non vide $U \subset X$ tel que, pour toute k-algèbre locale A de corps résiduel κ, l'application $U(A) \to U(\kappa)$ est surjective.*

Démonstration: 1) $\Longrightarrow$ 2) : Par définition, il existe un ouvert (non vide) $U \subset X$ tel qu' il existe des morphismes $f : U \to V$ et $r : V \to U$ tels que $r \circ f = id_U$ où V est un ouvert d'un espace affine. Etant donné une k–algèbre locale A de corps résiduel, on considère le diagramme commutatif

$$\begin{array}{ccc} V(A) & \longrightarrow & U(A) \\ \downarrow & & \downarrow \\ V(\kappa) & \longrightarrow & U(\kappa) \end{array}$$

où les flèches horizontales sont (scindées) surjectives. Vu que que $V(A) \to V(\kappa)$ est surjective, il en est de même de $U(A) \to U(\kappa)$.

2) $\Longrightarrow$ 1) : On peut supposer que $U = \mathrm{Spec}(B)$ est affine (l'assertion 2) vaut pour tout ouvert de U). La k–algèbre B étant de type fini, on considère un morphisme surjectif d'anneaux $R = k[t_1, \cdots, t_n] \to B = R/\mathfrak{P}$. Le corps de fonctions $k(X)$ est le corps résiduel de l'anneau local $R_{\mathfrak{P}}$. Par hypothèse, la flèche $U(R_{\mathfrak{P}}) \to U(k(X))$ est surjective. Le point générique ξ de U se relève donc en un morphisme $f : \mathrm{Spec}(R_{\mathfrak{P}}) \to U$. Il s'étend en un voisinage V de $[\mathfrak{P}]$ dans $\mathbb{A}_k^n = \mathrm{Spec}(R)$ de sorte que l'on obtient un morphisme $f : V \to U$ qui admet une section rationnelle. Ainsi X est rétracte k–rationnelle. $\square$

Démonstration de la rétracte k–rationalité de la variété des tores (en car. nulle): On va voir que la rétracte rationalité de X est une conséquence de la correspondance entre tores maximaux et sous–algèbres de Cartan. Si $y \in \mathfrak{g}$ est un élément régulier, $\mathfrak{z}_{\mathfrak{g}}(y)$ est une sous–algèbre de Cartan de $\mathfrak{g}$ qui est l'algèbre de Lie du tore $T_y := Z_G(\mathfrak{z}_{\mathfrak{g}}(y))$ (aussi égal à $Z_G(y)$).

Soit V l'ouvert de $\mathbb{A}(\mathfrak{g})$ consistant en les éléments réguliers. On définit[4] alors un morphisme de k–variétés $f : V \to X$ en appliquant $y \to T_y$. Vu que tous les k–tores maximaux de G sont construits de cette façon, la flèche $V(k) \to X(k)$ est surjective. En appliquant ceci au corps $k(X)$ et au point générique de X, il résulte que $f : V \to X$ admet une section rationnelle. Il existe donc $U \subset X$ et $r : U \to V$ tel que $f \circ r = id_U$. Ainsi id_U factorise par l'ouvert $V' = f^{-1}(U) \subset V$. On conclut que X est rétracte k–rationnelle.

Pour établir la k–rationalité, on doit raffiner l'argument précédent.

Esquisse de démonstration de la k–rationalité (d'après Borel-Springer [BSp, 7.9] *(en car. nulle)*: On note $\mathfrak{t}$ l'algèbre de Lie de T. Soit $t \in \mathfrak{t}$ un élément régulier. Soit W l'ouvert de $\mathbb{A}(\mathfrak{g})$ consistant en les éléments $x \in \mathfrak{g}$ tels que $t + x$ est régulier, c'est-à-dire tels que l'algèbre de Lie $\mathfrak{h}_X = \mathfrak{C}_{\mathfrak{g}}(t + x)$ est une sous–algèbre de Cartan de $\mathfrak{g}$. On fixe une décomposition de k–espaces vectoriels $\mathfrak{g} = \mathfrak{t} \oplus \mathfrak{m}$. Ceci permet de définir la sous–variété ouverte (non vide) $V \subset W$ des éléments $x \in W$ satisfaisant $\mathfrak{m} \cap \mathfrak{h}_x = 0$. On montre alors que le morphisme $V \to G/N_G(T)$, $x \mapsto Z_G(\mathfrak{h}_x)$ est une immersion ouverte, l'image s'identifiant à la la sous–variété de $G/N_G(T)$ consistant en les sous–algèbres de Cartan $\mathfrak{h}$ telles que $\mathfrak{h} \cap \mathfrak{m} = 0$. $\square$.

9. Unirationalité des groupes réductifs

9.1. **Théorème.** *Soit G un k–groupe réductif. Alors G est une variété k–unirationnelle.*

9.2. **Corollaire.** *Si k est infini, alors $G(k)$ est Zariski dense dans G.*

Démonstration (en car. nulle): On note $\Omega := G^{ss,reg}$ l'ouvert des éléments semi-simples réguliers de G consistant en les $g \in G$ tels que $Z_G(g)$ est un k–tore maximal. Soit T un k–tore maximal de G et $X = G/N_G(T)$ la variété des tores de G. On définit le k–morphisme de variétés $\pi : \Omega \to X$, $g \to [Z_G(g)]$.

Si T est un k–tore maximal de G, on note T^{reg} l'ouvert de T des éléments réguliers de T. Vu que $T(k)$ est Zariski-dense dans T (4.11), il existe $t \in T(k)$ satisfaisant $T = Z_G(t)$. Par suite, $\pi : \Omega(k) \to X(k)$ est surjective et la fibre en $[T]$ est T^{reg}. On note $T_{gen}/k(X)$ le tore générique de G, c'est-à-dire le $k(X)$–tore défini par le point générique $\xi : \mathrm{Spec}(k(X)) \to X$. Alors

$$k(G) = k(X)(\pi^{-1}(\xi_x)) = k(X)(T_{gen}).$$

Le corps de fonctions $k(X)$ est k-unirationnel (sous–corps d'un $k(t_1, ..., t_n)$) et $k(X)(T_{gen})$ est un sous–corps de $k(X)(t_{n+1}, ..., t_m)$ (4.10). Par suite, $k(X)$ est un sous–corps de $k(t_1, ..., t_m)$, i.e. X est k–unirationnelle. $\square$

[4] Une façon de voir que cela définit bien un k–morphisme est de passer par la théorie des schémas en groupes [SGA3, XI].

10. Un exemple d'approximation faible

Le résultat suivant est un cas particulier d'un article de Kunyavskiĭ-Skorobogatov [KS].

10.1. **Proposition.** *Soit G un $\mathbb{Q}$-groupe réductif. Alors $G(\mathbb{Q})$ est dense dans $G(\mathbb{R})$.*

C'est un énoncé d'approximation faible.

10.2. **Lemme.** *Soit X une variété rétracte k–rationnelle. Soient $v_1, ..., v_n$ des valuations sur k deux à deux indépendantes. On note k_{v_i} le complété de la valuation v_i. Alors l'approximation faible vaut pour X et les places $v_1, ..., v_n$, i.e. $X(k)$ est dense dans $X(k_{v_1}) \times \cdots \times X(k_{v_n})$.*

Démonstration: De la même manière que dans la proposition 8.5, il suffit de traiter le cas d'un ouvert d'un espace affine et même de la droite affine. Dans ce cas, il s'agit de la densité de k dans $k_{v_1} \times \cdots \times k_{v_n}$, c'est-à-dire le théorème d'approximation [BAC, VI.7, corollaire 2]. □

Démonstration de la proposition 10.1. On reprend les notations de la démonstration du th. 9.1. On considère le morphisme $\pi : \Omega \to X$ de l'ouvert des éléments réguliers de G et X la variété des tores de G. Vu que $\Omega(\mathbb{R})$ est dense dans $G(\mathbb{R})$, il suffit de montrer que $\Omega(\mathbb{Q})$ est dense dans $\Omega(\mathbb{R})$. Soit $g \in \Omega(\mathbb{R})$ et posons $x = \pi(g) \in X(\mathbb{R})$. On dispose du morphisme lisse (et submersif) de variétés différentiables

$$\pi_{top} : \Omega(\mathbb{R}) \to X(\mathbb{R}).$$

D'après le théorème des fonctions implicites, il existe un voisinage topologique $V_x \subset X(\mathbb{R})$ et une section locale C^∞ $\psi : V_x \to \Omega(\mathbb{R})$ de π_{top} satisfaisant $\psi(x) = g$. Vu que $X(\mathbb{Q})$ est dense dans $X(\mathbb{R})$, on peut choisir $x_0 \in X(\mathbb{Q}) \cap V_x$ tel que $g_0 := \psi(x_0) \in \Omega(\mathbb{R})$ est très proche de g. On note T_{x_0} le $\mathbb{Q}$–tore représenté par x_0. On a $g_0 \in T_{x_0}(\mathbb{R})$. Mais $T_{x_0}(\mathbb{Q})$ est dense dans $T_{x_0}(\mathbb{R})$ (prop. 4.12), donc il existe $t \in T_{x_0}(\mathbb{Q})$ très proche de g_0.

On conclut que $\Omega(\mathbb{Q})$ est dense dans $\Omega(\mathbb{R})$. □

Sorites

11. Rigidité

Si G est un k–groupe affine, on définit son centre $Z(G)$ comme la k-sous–variété des points fixes de G pour son action sur lui-même par automorphismes intérieurs.

11.1. **Lemme.** *Soit $1 \to S \to G' \to G \to 1$ une suite exacte de k–groupes algébriques affines avec S de type mutiplicatif. On suppose G lisse, connexe.*

(1) *Alors $S \subset Z(G')$.*

(2) *Si G est un k–tore, alors G' est un k–groupe de type multiplicatif.*

Démonstration. On peut supposer k–algébriquement clos.

(1) Pour toute k–algèbre R, l'action intérieure de G' sur lui-même induit un morphisme $G'(R) \to \mathrm{Aut}_{R-gp}(S_R)$. En d'autres mots, on a défini un morphisme de k–schémas en groupes $G' \to \mathrm{Aut}(\widehat{S})$ où $\mathrm{Aut}(\widehat{S})$ désigne le k–schéma en groupes constant associé au groupe abstrait $\mathrm{Aut}_{\mathbb{Z}}(\widehat{S})$ sur k (il est localement de type fini, mais pas de type fini en général). Puisque G' est connexe, ce morphisme est trivial et $S(R)$ est distingué dans $G'(R)$ pour toute k-algèbre R/k.

(2) On a $G = \mathbb{G}_m^r$. Supposons tout d'abord que S est un k–tore, i.e. $S = \mathbb{G}_m^s$. Le morphisme $\pi : G' \to G$ est un espace principal homogène sous S. Vu que $\mathrm{Pic}(G) = 0$, il existe une section $\phi : G \to G'$ de π que l'on peut supposer appliquant e sur e'. Nous allons montrer que ϕ est un morphisme de groupes en considérant le défaut

$$\begin{array}{rcl} \Delta : G \times_k G & \longrightarrow & S = \mathbb{G}_m^s \\ g_1, g_2 & \mapsto & \phi(g_1)\phi(g_2)\phi(g_1\, g_2)^{-1}. \end{array}$$

Par rigidité, le i-ème–facteur de Δ est donné par un produit de caractères $(g_1, g_2) \to \chi_1(g_1)\chi_2(g_2)$. Par ailleurs $\Delta(g, e) = e = \Delta(e, g) = e$, donc $\chi_1 = \chi_2 = 0$. Le morphisme ϕ est donc un k–homomorphisme de groupes algébriques. L'extension est donc scindée, i.e. $G' = S \times_k G$.

Dans le cas général, on plonge S dans un tore $\mathbb{G}_m^s$. L'extension centrale du départ se "pousse en arrière" en

$$\begin{array}{ccccccccc} 1 & \longrightarrow & S & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & || & & \\ 1 & \longrightarrow & \mathbb{G}_m^s & \longrightarrow & \widetilde{G} & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

Le premier cas indique que $\widetilde{G}$ est un k–tore algébrique. Mais G' est un k–sous–groupe algébrique de $\widetilde{G}$, c'est donc un k–groupe de type multiplicatif. □

11.1. **Cas des groupes réductifs.**

11.2. **Lemme.** *On suppose k–infini. Soit G un k-groupe réductif. Alors*

$$Z(G) = \bigcap_{T \subset G} T$$

pour T parcourant les k-tores maximaux de G. En outre, Z(G) est un k–groupe de type multiplicatif.

Démonstration (en caractéristique nulle): Notons $H := \bigcap_{T \subset G} T$. Si T est un k–tore maximal de G, on a $Z(G) \subset Z_G(T) = T$. On a donc

$$Z(G) \subset H = \bigcap_{T \subset G} Z_G(T).$$

Vu que les k-tores maximaux engendrent G au sens de la topologie de Zariski, on a en fait $Z(G)(k_s) = H(k_s)$, d'où $Z(G) = H$. □

11.3. **Définition.** (a) Un groupe réductif G est semi-simple si son centre connexe $Z(G)^0$ est trivial.

(b) Un groupe réductif G est adjoint si $Z(G) = 1$.

11.4. **Exemples.** Soit $n \geq 2$ Le groupe GL_n n'est pas semi-simple. Le groupe SL_n est semi-simple mais non adjoint. Le groupe $\mathrm{PGL}_n = \mathrm{GL}_n/\mathbb{G}_m$ est adjoint (cf. Corollaire 11.6 ci-dessous).

11.5. **Proposition.** *Soit* $1 \to S \to G' \xrightarrow{\pi} G \to 1$ *une suite exacte de k–groupes avec G, G′ réductifs et S de type multiplicatif. Alors* $T \mapsto \pi^{-1}(T)$ *induit une correspondance bijective entre les k–tores maximaux de G et ceux de G′.*

Démonstration. La seule chose à montrer est que $\pi^{-1}(T)$ est un k–tore (maximal) de G'. D'après le lemme de rigidité 11.1, $\pi^{-1}(T)$ est un k–groupe de type multiplicatif. On note T' le plus grand sous–tore de $\pi^{-1}(T)$ et μ le quotient de $\pi^{-1}(T)$ par T'. Le groupe S étant central dans G', on a $S \subset T'$. On considère le diagramme commutatif

$$\begin{array}{ccccccccc}
1 & \longrightarrow & S & \longrightarrow & T' & \longrightarrow & \mathrm{Coker}(T' \to T) & \longrightarrow & 1 \\
 & & \| & & \cap & & \cap & & \\
1 & \longrightarrow & S & \longrightarrow & \pi^{-1}(T) & \longrightarrow & T & \longrightarrow & 1.
\end{array}$$

Notons $H = \mathrm{Coker}(T' \to T)$, c'est un k–groupe de type multiplicatif et le noyau de $\widehat{T} \to \widehat{H}$ est fini. Puisque $\widehat{T}$ est sans torsion, on conclut que $T' = \pi^{-1}(T)$. □

11.6. **Corollaire.** *Soit G un k-groupe réductif. Alors G/Z(G) est adjoint.*

Démonstration. On a

$$\begin{aligned} Z(G/Z(G)) &= \bigcap_{T' \subset G/Z(G)} T' \\ &= \bigcap_{T \subset G} T/Z(G) \\ &= \Big(\bigcap_{T \subset G} T\Big)/Z(G) \\ &= Z(G)/Z(G) = 1. \end{aligned}$$

□

On note $G_{ad} = G/Z(G)$ le groupe adjoint de G.

12. Groupes simplement connexes et revêtement universel

12.1. **Définition.** (a) Une isogénie (centrale) est un morphisme $\lambda : G' \to G$ de k-groupes réductifs, fidèlement plat de noyau fini.

(b) Un k-groupe semi-simple est simplement connexe si toute isogénie $G' \to G$ est un isomorphisme.

12.2. **Remarques.** (a) Si $G' \to G$ est une isogénie, G est semi-simple si et seulement si G' est semi-simple.

(b) Si $k = \mathbb{C}$ et $G/\mathbb{C}$ est simplement connexe, l'espace topologique $G(\mathbb{C})$ est simplement connexe. Ceci est faux avec $\mathbb{R}$, par exemple l'espace topologique $\mathrm{SL}_2(\mathbb{R})$ n'est pas simplement connexe.

(c) Si k est un corps algébriquement clos de caractéristique zéro, un groupe semi-simple simplement connexe G/k est simplement connexe au sens de la géométrie algébrique [SGA1], i.e. il n'admet pas de revêtement fini étale connexe non trivial.

(d) En caractéristique positive $p > 0$, deux phénomènes apparaissent. Tout d'abord, une isogénie de noyau μ_p n'est pas étale, ce n'est donc pas un revêtement au sens de [SGA1]. De plus, un groupe semi-simple simplement connexe (non trivial) n'est pas simplement connexe au sens de la géomètrie algébrique. Nous reviendrons là-dessus à propos du cas des corps finis.

12.3. **Théorème.** *Soit G un k–groupe semi-simple. Il existe une isogénie $\rho : \widetilde{G} \to G$ satisfaisant la propriété universelle suivante:*

Pour toute isogénie $\lambda : G' \to G$, il existe une unique isogénie $\phi : \widetilde{G} \to G'$ satisfaisant $\rho = \phi \circ \lambda$.

Ce groupe $\widetilde{G}$ est simplement connexe et le morphisme ρ est appelé le revêtement universel de G; son noyau, qui est un k-groupe fini de type multiplicatif, est appelé le groupe fondamental de G.

12.4. **Exemple.** L'isogénie $\mathrm{SL}_n \to \mathrm{PGL}_n$ est le revêtement fondamental de PGL_n. Le groupe fondamental de PGL_n est donc μ_n.

13. Groupe dérivé

On définit tout d'abord un foncteur.

13.1. **Définition.** Soit G un k-groupe algébrique. Pour toute k-algèbre R, on pose

$$D(G)(R) = \Big\{ g \in G(R) \mid \text{il existe } S/R \text{ fidèlement plat de présentation finie tel que } g \in [G(S), G(S)] \Big\}.$$

13.2. **Remarques.** (a) En particulier, ceci implique que $D(G)(\overline{k}) = [G(\overline{k}), G(\overline{k})]$.
(b) Demander que $D(G)(k) = [G(k), G(k)]$ est trop naïf. Par exemple, pour le groupe PGL_n, on a $\mathrm{PGL}_n(k) = \mathrm{GL}_n(k)/k^\times$. Le déterminant induit une application surjective $\mathrm{PGL}_n(k) \to k^\times/(k^\times)^n$, donc $\mathrm{PGL}_n(k)/[\mathrm{PGL}_n(k), \mathrm{PGL}_n(k)]$ se surjecte sur le groupe $k^\times/(k^\times)^n$ qui est non trivial en général. Par ailleurs, on a $\mathrm{PGL}_n(\overline{k}) = [\mathrm{PGL}_n(\overline{k}), \mathrm{PGL}_n(\overline{k})]$.

13.3. **Théorème.** *Soit G un k–groupe algébrique lisse. Alors le foncteur $D(G)$ est représentable par un sous k–groupe algébrique lisse de G.*

Voir [DG, II.5.4.8].

13.4. **Exemple.** Si G est semi-simple, on a $D(G) = G$. Le théorème ramène ce fait à voir que $[G(\overline{k}), G(\overline{k})] = G(\overline{k})$. On sait que le groupe $G(\overline{k})$ est engendré par des $\mathrm{SL}_2(\overline{k})$. On est ainsi ramené au cas bien connu de $\mathrm{SL}_2(\overline{k})$.

13.1. **Tore radical et coradical.** Si G est un k-groupe réductif, on note $\mathrm{rad}(G) = Z(G)^0$ le tore radical, i.e. la composante neutre du centre.

Le groupe des caractère $\widehat{G}(k_s) = \mathrm{Hom}_{k_s-gr}(G_{k_s}, \mathbb{G}_{m,k_s})$ est un $\mathbb{Z}$-module libre de type fini muni d'une action continue de $\mathrm{Gal}(k_s/k)$. Il définit donc un k–tore noté $\mathrm{corad}(G)$, le tore coradical de G. Etant donnée une $\mathbb{Z}$–base $\chi_1, ..., \chi_r$ de $\widehat{G}(k_s)$, on a un k_s–morphisme de groupes

$$(\chi_1, \cdots, \chi_r) : G \times_k k_s \to \mathbb{G}_{m,k_s}^r$$

qui se descend en une flèche canonique

$$\pi : G \to \mathrm{corad}(G)$$

fidèlement plate.

13.5. **Proposition.** (1) *On a une suite exacte de k-groupes algébriques*

$$1 \to D(G) \to G \xrightarrow{\pi} \mathrm{corad}(G) \to 1$$

(2) *$D(G)$ est semi-simple et les morphismes $D(G) \to G/Z(G)$, $D(G) \times \mathrm{rad}(G) \to G$ et $G \to G_{ad} \times \mathrm{corad}(G) \to G$ sont des isogénies.*

Le lemme clef est le suivant.

13.6. **Lemme.** *$Z(G) \cap \ker(\pi)$ est fini sur k.*

Démonstration. Il revient au même de montrer que $\mathrm{rad}(G) \cap \ker(\pi)$ est fini. On peut supposer le corps k séparablement clos. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire fidèle. La restriction de ρ au tore $\mathrm{rad}(G)$ donne lieu à la décomposition

$$V = \bigoplus_{\lambda \in \widehat{\mathrm{rad}(G)}} V_\lambda.$$

avec $V_\lambda = \big\{ v \in V \mid \rho(t) = \lambda(t)v \ \ \forall t \in rad(G) \big\}$. Cette décomposition est préservée par ρ qui se décompose ainsi en une somme directe $\rho_{\lambda_1} \oplus \cdots \rho_{\lambda_r}$. Les morphismes $det \circ \rho_\lambda : G \to \mathbb{G}_m$ sont des caractères de G, ils sont donc nuls sur $\ker(\pi)$. Pour tout caractère $\lambda \in \widehat{\mathrm{rad}(G)}$, on obtient alors

$$\Big(\lambda_{|\ker(\pi) \cap \mathrm{rad}(G)} \Big)^{\dim(V_\lambda)} = e.$$

Ceci montre que l'image de la surjection $\widehat{\mathrm{rad}(G)} \to \mathrm{rad}(\widehat{G) \cap \ker}(\pi)$ est de torsion. On conclut que $\mathrm{rad}(G) \cap \ker(\pi)$ est un k–groupe fini de type multiplicatif. $\square$

13.7. **Remarque.** Ce type d'argument apparaît aussi en théorie des représentations des groupes finis.

On peut maintenant passer à la preuve de la proposition 13.5.

Démonstration. On montre d'abord la seconde assertion avec $\ker(\pi)$ en lieu et place de $D(G)$. Suivant (13.4), on a $D(G_{ad}) = G_{ad}$. Vu que $D(G) \to D(G_{ad})$ est surjectif, on tire que $\ker(\pi) \to G_{ad}$ est surjectif. Mais le noyau de cette flèche est $\ker(\pi) \cap Z(G)$ qui est fini d'après le lemme. Ainsi $\ker(\pi) \to G_{ad}$ est une isogénie et $\ker(\pi)$ est semi-simple. De même, le morphisme

$$\phi : G \to G_{ad} \times \mathrm{corad}(G)$$

est surjectif et de noyau fini $Z(G) \cap \ker(\pi)$. Par ailleurs, le morphisme $\ker(\pi) \times Z(G) \to G$ est une isogénie, il en est de même de $\ker(\pi) \times \mathrm{rad}(G) \to G$.

Montrons enfin la première assertion, c'est-à-dire la coïncidence de $D(G)$ et $\ker(\pi)$. Puisque $\ker(\pi) \to G_{ad}$ est une isogénie, le morphisme $D(G) \to G_{ad}$ est a fortiori une isogénie. On a donc une inclusion de k–groupes lisses connexes $D(G) \subset \ker(\pi)$ de même dimension, donc $D(G) = \ker(\pi)$ ce qui montre (1). $\square$

13.8. **Corollaire.** *Soit G un k–groupe réductif. Alors les assertions suivantes sont équivalentes:*

(1) *G est semi-simple, i.e.* $\mathrm{rad}(G) = e$*;*
(2) $\mathrm{corad}(G) = e$*;*
(3) $D(G) = G$*.*

Dans le même cercle d'idée, nous donnons une seconde démonstration de la proposition 2.3 déterminant les fonctions globales inversibles d'un k–groupe réductif.

Démonstration. Il est loisible de supposer le corps de base séparablement clos. Si G est semi-simple, il s'agit de voir que $k^\times = k[G]^\times$. Cela peut se voir par exemple par réduction au cas de SL_2. Pour le cas réductif, on se donne une fonction $f : G \to \mathbb{G}_m$ satisfaisant $f(e) = 1$. On va montrer que f est un homomorphisme. Il suffit de voir que le composé

$$D(G) \times \mathrm{rad}(G) \xrightarrow{\lambda} G \xrightarrow{f} \mathbb{G}_m$$

est un homomorphisme. Puisque $D(G)$ est semi–simple, le premier cas indique que ce composé factorise par $G/D(D) = \mathrm{rad}(G) \longrightarrow \mathbb{G}_m$, c'est donc un caractère. $\square$

Les théorèmes de Steinberg et Raghunathan

14. Introduction

Soient k un corps et k_s/k une clôture séparable de k. On note $\Gamma_k = \mathrm{Gal}(k_s/k)$ le groupe absolu de k. Soit G/k un groupe réductif connexe. Notre but est de décrire des représentants de l'ensemble de cohomologie galoisienne $H^1(k,G)$ en fonctions de sous-groupes de G. Le premier énoncé de ce type est le suivant.

14.1. **Lemme.** [S1, III.2.2, lemme 1] *Soit $T \subset G$ un k–tore maximal. Alors l'application $H^1(k, N_G(T)) \to H^1(k,G)$ est surjective.*

Démonstration: Soit $[z] \in H^1(\Gamma_k, G(k_s))$. On considère le groupe tordu par automorphismes intérieurs ${}_zG$ et une trivialisation $\phi : G \times_k k_s \cong {}_zG \times_k k_s$ satisfaisant $\phi^{-1}\,\sigma(\phi) = int(z_\sigma)$ pour tout $\sigma \in \Gamma_k$. Soit T' un k–tore maximal de ${}_zG$. Alors $\phi^{-1}(T' \times_k k_s)$ est $G(k_s)$–conjugué a $T \times_k k_s$. Il existe $g \in G(k_s)$ satisfaisant

$$int(g^{-1}).\phi^{-1}(T' \times_k k_s) = T \times_k k_s.$$

Appliquer un élément $\sigma \in \Gamma_k$ sur cette identité donne

$$int(\sigma(g^{-1}))\,.\,\phi^{-\sigma}(T' \times_k k_s) = T \times_k k_s$$

d'où

$$int(g^{-1})\,.\,\phi^{-1}\Big(int(\sigma(g^{-1})).\phi^{-\sigma}\Big)^{-1} \in N_G(T)(k_s).$$

Finalement $g^{-1} z_\sigma\, \sigma(g) \in N_G(T)(k_s)$. On conclut que $[z] \in \mathrm{Im}\big(H^1(k, N_G(T)) \to H^1(k,G)\big)$. $\square$

Ceci a été raffiné récemment.

14.2. **Théorème.** [CGR] *On suppose* $\mathrm{car}(k) = 0$. *Soit $T \subset G$ un k–tore maximal. Il existe alors un k-sous–groupe fini $S \subset N_G(T)$ tel que l'application $H^1(F,S) \to H^1(F,G)$ est surjective pour tout F/k.*

En d'autres mots, toutes les classes de cohomologie provienned d'un k-sous–groupe fini fixé. Par exemple, pour PGL_n, on peut prendre le produit semi-direct $S = \Big((\mu_n)^n/\mu_n\Big) \rtimes S_n$.

15. Le théorème de Steinberg

On rappelle qu'un k–groupe réductif G est déployé si G admet un k-tore maximal déployé, i.e. isomorphe à $\mathbb{G}_m^{\mathrm{rang}(G)}$. On dit que G est quasi–déployé s'il admet un k-sous-groupe de Borel B, c'est-à-dire tel que $B \times_k k_s$ est un sous–groupe de Borel de $G \times_k k_s$ (par définition, il s'agit d'un k_s-sous–groupe maximal résoluble de $G \times_k k_s$).

15.1. **Théorème.** *(Steinberg, 1965,* [St]*)*
Soit G un k–groupe réductif quasi–déployé. Alors

$$H^1(k,G) = \bigcup_{T\subset G} \mathrm{Im}\Big(H^1(k,T) \to H^1(k,G)\Big)$$

où T parcourt les k–tores maximaux de G.

Quelques exemples étaient connus auparavant : PGL_n, SO_{2n}. Cela a permis de démontrer la conjecture I de Serre d'annulation pour des corps parfaits de dimension cohomologique ≤ 1, i.e. satisfaisant $H^2(k,A) = 0$ pour tout module galoisien fini A. Un exemple fondamental de tel corps est le corps de fonctions d'une courbe complexe (theorème de Tsen [S1, III.3]).

15.2. **Corollaire.** *Supposons* $\mathrm{cd}(k) \leq 1$*. Soit G/k un groupe réductif. Alors G est quasi–déployé et $H^1(k,G) = 1$.*

Pour l'annulation, on sait en effet que la cohomologie galoisienne des tores est triviale pour d'un corps de dimension cohomologique ≤ 1. La trivialité de $H^1(k,G)$ pour G quasi-déployé suit donc du théorème de Steinberg. Nous verrons plus loin qu'un groupe G/k est une forme tordue intérieure (par un cocycle à valeurs dans $G_{ad}(k_s)$ d'un k–groupe quasi-déployé, il suit que G est quasi–déployé.

Avec plus de théorie (i.e. le théorème de Grothendieck sur la trivialité des H^2 non abéliens), on peut calculer la cohomologie galoisienne d'un k–groupe algébrique linéaire arbitraire.

15.3. **Théorème.** [S1, III.2.4, corollaire 3]
On suppose k parfait et satisfaisant $\mathrm{cd}(k) \leq 1$*. Soit G/k un groupe algébrique linéaire et notons G^0 sa composante connexe. Alors le morphisme quotient $G \to G/G^0$ induit une bijection*

$$H^1(k,G) \xrightarrow{\sim} H^1(k,G/G^0).$$

16. Démonstration du théorème de Steinberg

On suppose dans cette section que k est de caractéristique nulle.

16.1. **Le quotient adjoint** [H3, III]**.** La preuve est géométrique. On considère l'anneau des fonctions centrales

$$C(G) = k[G]^{ad(G)} = \Big\{ f \in k[G] \ \mid \ f(gxg^{-1}) = f(x) \ \forall g \in G(k) \Big\}.$$

La variété $G//G := \mathrm{Spec}(C(G))$ est le quotient adjoint de G [5]. Le morphisme quotient $G \to G//G$ sépare les classes de conjugaison (géométriques) semi-simples.

---

[5] Une façon plus intrinsèque de définir le quotient à la Hilbert-Mumford $X//G$ est de poser

$$k[X//G] := \Big\{ f \in k[X] \mid \nabla(f) = 1 \otimes f \Big\}$$

où $\nabla : k[X] \to k[G] \otimes_k k[X]$ désigne la coaction.

Soit maintenant $T \subset G$ un k–tore maximal. On note $W_T := N_G(T)/T$ son groupe de Weyl qui est un k–groupe fini étale. Vu que T est commutatif, l'action de $N_G(T)$ sur T factorise par W_T; on a donc un morphisme naturel

$$T//N_G(T) = T//W_T \to G//G.$$

16.1. **Théorème.** *(Chevalley) Le morphisme $T//W_T \to G//G$ est un isomorphisme.*

Voir [H3, §3] et [SB, p. 133].

16.2. **Remarque.** Sur les points géométriques, on peut donner une explication heuristique à ce théorème. Tout d'abord, si $g \in G(k_s)$ est un élément semi-simple, il se trouve dans un k_s–tore maximal de G et est donc conjugué à élément de $T(k_s)$ suivant le théorème de conjugaison des k_s–tores maximaux. Ensuite, soient t_1, $t_2 \in T(k_s)$ deux éléments $G(k_s)$–conjugués, i.e. $t_1 = g\, t_2\, g^{-1}$ avec $g \in G(k_s)$. Le point est que T et gTg^{-1} sont des tores maximaux de $Z_G(t_2)^0$ qui est un k_s-groupe réductif [H3, §2.2]. Par suite, T et gTg^{-1} sont conjugués par un élément $h \in Z_G(t_2)^0(k_s)$, c'est-à-dire $hTh^{-1} = gTg^{-1}$. Ainsi $gh^{-1} \in N_G(T)(k_s)$ et $t_1 = gh^{-1}\, t_2\, (gh^{-1})^{-1}$.

16.2. **Cas d'un groupe semi-simple simplement connexe.** Supposons que G est semi–simple simplement connexe et quasi-déployé. Supposons en outre que T est un k–tore maximal d'un sous–groupe de Borel B de G. Alors $T//W_T$ est isomorphe à un espace affine $\mathbb{A}^r_k$. Dans le cas déployé, l'isomorphisme $G//G \to \mathbb{A}^r_k$ est produit par les caractères (poids) fondamentaux $\chi_1, \cdots, \chi_r$ of G, c'est-à-dire les caractères des représentations linéaires de G dont les plus hauts poids respectifs sont les poids fondamentaux $\overline{\omega}_1, \cdots, \overline{\omega}_r$ (relativement à $T \subset B$). Le morphisme

$$\pi : G \to G//G \cong \mathbb{A}^r_k$$

est appelé le morphisme de Steinberg de G.

16.3. **Exemple.** Si $G = \mathrm{SL}_n$, les représentations fondamentales sont les puissances alternées de la représentation standard de SL_n. Le morphisme de Steinberg applique alors un élément $g \in \mathrm{SL}_n(k)$ sur les coefficients du polynôme caractéristique de g.

Dans ce cas, la matrice "compagnon" produit un scindage de π qui est donné par

$$(a_1, \cdots, a_{n-1}) \mapsto \begin{pmatrix} 0 & 0 & . & . & 1 \\ 1 & 0 & 0 & . & a_{n-1} \\ . & . & . & . & . \\ 0 & . & 1 & 0 & a_2 \\ 0 & . & 0 & 1 & a_1 \end{pmatrix}.$$

Ceci est en fait général.

16.4. **Théorème.** [St]

Si G n'a pas de facteur de type A_{impair}, le morphisme de Steinberg $\pi : G \to \mathbb{A}^r_k$ admet une section $\mathcal{C} : \mathbb{A}^r_k \to G^{reg}$ où G^{reg} désigne l'ouvert des éléments réguliers.

La démonstation procède par la construction explicite de la section à partir du groupe de Weyl de G et des sous–groupes radiciels de G. Nous sommes intéressés par la conséquence rationnelle suivante (qui vaut aussi en type A_{impair}, mais avec un argument plus délicat).

16.5. **Corollaire.** *Soit $g \in G(k_s)$ un élément semi-simple. On suppose que la classe de conjugaison géométrique $C(g)$ est rationnelle, c'est-à-dire stable par Γ_k. Alors $C(g)$ contient un élément de $G(k)$.*

Démonstration. Notre hypothèse implique que $\pi(g) \in \mathbb{A}^r(k)$. On pose $g_0 := \mathcal{C}(\pi(g))$. Alors g_0 est semi-simple et appartient à la classe de conjugaison géométrique de g. □

16.6. **Remarque.** Pour des généralisations convenables de cet énoncé à d'autres classes de conjugaisons et des groupes réductifs arbitraires, voir Kottwitz [Ko].

On peut maintenant procéder à la démonstration du théorème de Steinberg 15.1.

Démonstration: Soit $\lambda : G^{sc} \to D(G)$ le revêtement universel du groupe dérivé de G. Les k–groupes G^{sc}, $D(G)$ et G sont quasi-déployés et ont même groupe adjoint. Ceci se traduit par le diagramme commutatif suivant

$$\begin{array}{ccccc} G^{sc} & \xrightarrow{\lambda} & D(G) & \subset & G \\ \downarrow & & \downarrow & & \downarrow \\ G^{sc}_{ad} & = & D(G)_{ad} & = & G_{ad}. \end{array}$$

En particulier, le groupe G agit par automorphismes intérieurs sur G^{sc}.

Soit $[z] \in H^1(k, G)$. On veut montrer que $[z]$ admet une réduction à un k-tore maximal de G. On considère le k-groupe tordu ${}_zG^{sc}$, et notons $g \in {}_zG^{sc}(k)$ un élément semi–simple régulier. On fixe une trivvialisation $\phi : G \times_k k_s \cong {}_zG \times_k k_s$ satisfaisant $int(z_\sigma) = \phi^{-1}\,\sigma(\phi)$ pour tout $\sigma \in \Gamma_k$.

On a

$${}_zG(k) = \phi\Big(\big\{ g \in G(k_s) \mid Ad(z_\sigma).\sigma(g) = g \big\}\Big).$$

Par suite $\phi^{-1}(g)$ définit une classe de conjugaison rationnelle de G. D'après le Corollaire 16.5, il existe $h \in G^{sc}(k_s)$ tel que $g_0 := Ad(h^{-1})\,.\,g \in G(k)$. De l'identité $Ad(z_\sigma).\sigma(g_0) = g_0$ on tire

$$Ad(z_\sigma)\,.\,\sigma(Ad(h)\,.\,g_0) = Ad(h)\,.\,g_0.$$

En poussant par $\lambda : G^{sc}(k) \to G(k)$, il vient

$$Ad\Big(\lambda(h)^{-1}\, z_\sigma\, \sigma(\lambda(h))\Big)\,.\,\lambda(g_0) = \lambda(g_0).$$

L'élément $\lambda(g_0)$ est semi-simple régulier, donc son centralisateur $T_0 := C_G(\lambda(g_0))$ est un k–tore maximal. On conclut que

$$[z_\sigma] = \big[\, \lambda(h)^{-1}\, z_\sigma\, \sigma(\lambda(h))\, \big] \in \mathrm{Im}\Big(H^1(k,T_0) \to H^1(k,G)\Big).$$

□

16.3. **Un contre-exemple.** L'hypothèse G quasi–déployé est essentielle dans le théorème 15.1. Considérons le cas $G = \mathrm{PGL}_1(Q)$ où $Q = (a,b)$ est une algèbre de quaternions $X^2 = a, Y^2 = b$, $XY + YX = 0$. Les k–tores de G sont les $R_{K/k}(\mathbb{G}_m)/\mathbb{G}_m$ où K/k parcourt les k–sous–algèbres quadratiques étales de Q. Par ailleurs, l'ensemble $H^1(k, \mathrm{PGL}_1(Q))$ classifie les k–algèbres de quaternions. Si K/k est une sous–algèbre quadratique étale de Q et $T = R_{K/k}(\mathbb{G}_m)/\mathbb{G}_m)$ le k–tore associé, et si $[z] \in H^1(k, R_{K/k}(\mathbb{G}_m)$, alors $T = {}_zT$ est un k–tore maximal de ${}_zG = \mathrm{PGL}_1(Q')$. En d'autres mots, l'énoncé du théorème 15.1 impliquerait que toute algèbre de quaterions Q' admet un sous–corps commutatif qui soit un cous–corps commutatif de Q.

Ceci est faux[6]. On peut aussi considérer l'exemple suivant. On prend $F = \mathbb{R}((t_1))((t_2))$ (séries formelles itérées) et les algèbres de quaternions $Q = (-1,-1)$ et $Q' = (t_1, t_2)$. Les extensions quadratiques de F sont les $F(\sqrt{\pm\, t_1^{n_1}\, t_2^{n_2}})$ où n_1, n_2 sont 0 ou 1. On discute alors cas par cas pour constater qu'aucune extension quadratique de F n'est commune à Q et à Q'.

17. Le théorème de Raghunathan

Dans le théorème de Steinberg, on fait apparaître en index l'ensemble des k–tores maximaux d'un groupe algébrique quasi-déployé G. Notre but est de restreindre cet index en décrivant de façon plus précise les k–tores maximaux.

On note $T \subset G$ un k–tore maximal d'un sous–groupe de Borel fixé $B \subset G$ (T est le centralisateur dans G d'un k–tore maximal déployé de G). On considère la variété $X = G/N$ des tores maximaux, où $N := N_G(T)$ désigne le normalisateur du tore T. On a une suite exacte de k–groupes algébrques $1 \to T \to N \to W_T \to 1$. Le k–groupe W_T est le groupe de Weyl; il est fini sur k. En composant l'application caractéristiquye $X(k) \to H^1(k,N)$ par l'application $H^1(k,N) \to H^1(k,W_T)$, on obtient une application

$$\mathit{Type} : X(k) \to H^1(k, W_T),$$

qui est appelé le *type* d'un tore.

Lorsque G est déployé, le groupe W_T est constant; alors l'ensemble pointé $H^1(k,W_T) = \mathrm{Hom}_{ct}(\Gamma_k, W)/int(W)$ classifie les W_T-algèbres galoisiennes sur k.

[6]On peut aussi utiliser des méthodes "génériques" en invoquant un théorème de Witt (cf. [GS, §1.4]) sur le fait qu'une algèbre de quaterions est déterminée par le corps de fonctions de la conique sous–jacente $x^2 - ay^2 = b$ qui est une extension quadratique du corps $k(x)$.

17.1. **Exemple.** Pour le groupe linéaire GL_n, les tores maximaux sont des tores $R_{E/k}(\mathbb{G}_m)$ pour E/k parcourant les k–algèbres étales de dimension n. L'application $Type$ a valeurs dans l'ensemble $H^1(k,S_n)$ qui classifie les k-algèbres étales de dimension n. Il est aisé de vérifier que $Type(R_{E/k}(\mathbb{G}_m)) = [E] \in H^1(k,S_n)$.

17.2. **Remarque.** Cet invariant est plus fin que la classe d'isomorphie du tore. Par exemple, pour GL_n, le type prend ses valeurs dans $H^1(k,S_n)$ mais l'application $H^1(k,S_n) \to H^1(k,\mathrm{GL}_n(\mathbb{Z}))$ n'est pas injective en général[7].

Cet invariant est bien lié au théorème 15.1.

17.3. **Lemme.** *Soit T_1, T_2 deux k–tores maximaux de G ayant même type dans $H^1(k,W)$. Alors*

$$\mathrm{Im}\Big(H^1(k,T_1) \to H^1(k,G)\Big) = \mathrm{Im}\Big(H^1(k,T_2) \to H^1(k,G)\Big).$$

Démonstration. On écrit $T_i = g_i.T$ avec $g_i \in G(k_s)$. L'hypothèse dit qu'il existe un élément $n \in N_G(T)(k_s)$ tel que

$$n^{-1}\, g_1^{-1}\, \sigma(g_1)\sigma(n) = g_2^{-1}\sigma(g_2) \qquad \mod \ T(k_s).$$

Quitte à remplacer g_1 par $g_1 n$, on peut supposer que $g_1^{-1}\,\sigma(g_1) = g_2^{-1}\,\sigma(g_2)$ $\mod \ T(k_s)$, ou de façon équivalente que $x_\sigma := g_1^{-1}\,\sigma(g_1)\,\sigma(g_2^{-1})g_2 \in T(k_s)$.

Soit $\sigma \to z_\sigma$ un 1–cocycle à valeurs dans $T_1(k_s)$. On écrit $z_\sigma = g_1.t_\sigma$ d'où pour tous $\sigma, \tau \in \Gamma_k$

$$g_1.t_{\sigma\tau} = (g_1.t_\sigma)\,\sigma(g_1.t_\tau) = (g_1.t_\sigma)\,(\sigma(g_1).\sigma(t_\tau)).$$

On forme alors le cocycle cohomologue

$$\begin{aligned}
(g_1\, g_2^{-1})^{-1}\, z_\sigma\, \sigma(g_1 g_2^{-1}) &= (g_1\, g_2^{-1})^{-1}\, g_1\, t_\sigma\, g_1^{-1}\, \sigma(g_1\, g_2^{-1}) \\
&= g_2\, t_\sigma\, g_1^{-1}\, \sigma(g_1)\, \sigma(g_2^{-1}) \\
&= g_2.\Big(t_\sigma\, g_1^{-1}\, \sigma(g_1)\, \sigma(g_2^{-1}) g_2\Big) \\
&= g_2.\big(t_\sigma\, x_\sigma\big),
\end{aligned}$$

qui est un 1–cocycle à valeurs dans $T_2(k_s)$. □

On peut maintenant énoncer le théorème de Raghunathan.

17.4. **Théorème.** *(2004,* [R]*) L'application de type $X(k) \to H^1(k,W_T)$ est surjective.*

Démonstration du théorème 17.4: Puisque le type d'un k–tore ne change pas par extension centrale de groupes algébriques, on peut supposer d'emblée que le groupe G est semi-simple simplement connexe. Etant donné $[\xi] \in H^1(k,W_T)$, on souhaite montrer que le tore tordu $T' = {}_\xi T$ peut se plonger dans G. On fixe une trivialisation $\phi : T \times_k k_s \xrightarrow{\sim} T' \times_k k_s$ satisfaisant $\xi_\sigma =$

[7]De tels contre-exemples proviennent de la théorie des représentations entières.

$\phi^{-1}\sigma(\phi)$ pour tout $\sigma \in \Gamma_k$. Suivant le Théorème 4.14, il existe $t' \in T'(k)$ tel que $(t')^{\mathbb{Z}}$ est Zariski dense dans T'. On pose $t := \phi^{-1}(t') \in T(k_s)$; c'est un élément régulier de G. Nous affirmons que la classe de conjugaison de $C(t')$ est rationnelle. En effet, d'après le théorème de Chevalley $T//W_T \cong G//G$ (16.1), il suffit de vérifier que les conjugués de t sont $W_T(k_s)$-conjugués à t. Mais $\sigma(t) = \sigma(\phi^{-1}(t')) = \phi^{-\sigma}(t') = (\phi^{-\sigma}\,\phi)(t) = \xi_\sigma^{-1}(t)$, d'où la rationalité de $C(t)$.

Le Corollaire 16.5 fournit des éléments $t_0 \in G(k)$ et $h \in G(k_s)$ satisfaisant $t = h^{-1}.t_0$. Alors la clôture de Zariski de $(t_0)^{\mathbb{Z}}$ dans G est un k-tore T_0 de G.

Il reste à vérifier que $Type(T_0) = [\xi]$. On a $T_0 = hTh^{-1}$ d'où le type de T_0 est donné par l'image de $h^{-1}\sigma(h)$ dans W_T. Etant donné $\sigma \in \Gamma_k$, soit n_σ un relevé de $\xi_\sigma \in N(k_s)$. De l'identité $t_0 = \sigma(t_0)$, on tire

$$\begin{aligned} h.t &= \sigma(h.t) \\ &= \sigma\big(h\,.\,\phi^{-1}(t')\big) \\ &= \sigma(h)\,.\,\phi^{-\sigma}(t') \qquad [\,t' \in T(k)\,] \\ &= \sigma(h)\,.\,n_\sigma^{-1}\,.\,t. \end{aligned}$$

Il suit que $h^{-1}\sigma(h)\,.\,n_\sigma^{-1}$ appartient à $T(k_s)$. Ainsi $h^{-1}\sigma(h) = n_\sigma \bmod T(k_s)$ On conclut que $Type(T_0) = [\xi]$. □

17.5. **Remarque.** Le théorème montre que les k–points de la variété des tores $X = G/N_G(T)$ paramètrent l'ensemble $H^1(k, W_T)$. Lorsque W_T est constant, c'est un fait remarquable du point de vue de la théorie de Galois.

Sous–groupes paraboliques, théorème de Borel-Tits

18. Introduction

Si l'on envisage de classifier les groupes réductifs sur un corps k, la première étape est de faire appel à la classification sur k_s. La seconde est de définir un invariant, l'index de Witt-Tits, qui rend compte du déploiement d'un groupe G et qui ramène la classification à celle des objets “irréductibles” ou “anisotropes”. Plutôt que de donner ici des définition précises, donnons deux exemples fondamentaux.

18.1. **Exemple. Le théorème de Wedderburn.** Soit A une k–algèbre simple centrale. Alors il existe une k–algèbre (uniquement déterminée) centrale à divisions D telle que $A \cong M_r(D)$.

18.2. **Exemple. Le théorème de Witt.** On suppose ici $\mathrm{car}(k) \neq 2$. Soit q une forme quadratique non dégénérée. Alors il existe une unique k–forme quadratique anisotrope q_0 telle que $q \cong q_0 \perp \nu(q)\mathbb{H}$, où $\mathbb{H}$ est un plan hyperbolique (i.e. la forme quadratique XY).

Ces deux énoncés sont des cas particuliers de la théorie de Borel-Tits. Dans le premier cas, il s'agit du k–groupe $\mathrm{PGL}_1(A)$ dont l'indice de Witt-Tits encode l'indice de A défini par $\deg(D)$, l'objet anisotrope sous–jacent est D. Dans le second cas, il s'agit du k–groupe $\mathrm{SO}(q)$ dont l'indice de Witt-Tits encode l'indice de Witt $\nu(q)$ de q, l'objet anisotrope sous–jacent étant la forme q_0.

19. Revue des groupes réductifs sur un corps séparablement clos

19.1. **Groupes de rang un.**

19.1. **Théorème.** [Sp, th. 7.2.4]
Soit G un F–groupe semi-simple de rang un. Alors $G = \mathrm{SL}_2$ ou $G = \mathrm{PGL}_2$.

19.2. **Données radicielles.** Soit F un corps séparablement clos. Soient G un F–groupe réductif et $\mathfrak{g}$ son algèbre de Lie. Soit $T \subset G$ un F–tore maximal. La représentation adjointe $Ad : G \to \mathrm{GL}(\mathfrak{g})$ permet d'associer au couple (G,T) une donnée de nature combinatoire appelée donnée radicielle (“root datum” en englais).

19.2. **Définition.** Une donnée radicielle est un quadruplet $(X, X^\vee, R, R^\vee)$ où X est un réseau, $X^\vee$ son dual, $R \subset X$ un ensemble fini (les racines), $R^\vee \subset X^\vee$ un ensemble fini (les coracines) muni d'une bijection $R \xrightarrow{\sim} R^\vee$, $\alpha \mapsto \alpha^\vee$. Si $\alpha \in R$, on définit la réflexion s_α de X (resp. $s_{\alpha^\vee}$ de $X^\vee$) par

$$s_\alpha(x) = x - \langle \alpha^\vee, x\rangle\, \alpha, \quad s_{\alpha^\vee}(y) = y - \langle \alpha, y\rangle \alpha^\vee.$$

On impose les deux propriétés suivantes pour tout $\alpha \in R$:

(1) $\langle \alpha^\vee, \alpha\rangle = 2$;

(2) $s_\alpha(R) = R$ et $s_{\alpha^\vee}(R^\vee) = R^\vee$.

On dit qu'une donnée radicielle $(X, X^\vee, R, R^\vee)$ est *réduite* si deux racines proportionnelles sont égales ou opposées.

19.3. **Remarque.** Si on note V le sous–espace vectoriel de $X \otimes_{\mathbb{Z}} \mathbb{R}$ engendré par R, R est un système de racines dans V. Les systèmes de racines sont employés pour la classification des algèbres de Lie semi-simples et aussi pour les groupes semi-simples.

On associe au couple (G, T) la donnée radicielle $\Psi(G, T) = (X, X^\vee, R, R^\vee)$ avec $X = \widehat{T}(F) = \mathrm{Hom}_{F-gr}(T, \mathbb{G}_{m,F})$, $X^\vee = \mathrm{Hom}_{F-gr}(\mathbb{G}_{m,F}, T)$, R désignant l'ensemble des racines de la représentation adjointe restreinte à T, c'est-à-dire l'ensemble des caractères α de T tels que l'espace propre

$$\mathfrak{g}_\alpha : \left\{ x \in \mathfrak{g} \mid Ad(t).x = \alpha(t)\, x \ \ \forall t \in T \right\}$$

soit non nul. Pour $\alpha \in R$, on pose

$$T_\alpha := \ker\bigl(T \xrightarrow{\alpha} \mathbb{G}_m\bigr)^0,$$

et $G_\alpha = D\bigl(Z_G(T_\alpha)\bigr)$. Le k–groupe $Z_G(T_\alpha)$ est réductif et son centre contient le tore T_α de codimension un dans T. Son algèbre de Lie contient $\mathfrak{g}_\alpha$, donc $T \subsetneq Z_G(T_\alpha)$ et le k–groupe G_α est semi-simple de rang un. D'après le théorème 19.1, on sait alors que G_α est isomorphe à SL_2 ou PSL_2. On dispose donc d'un morphisme $\alpha^\vee : \mathrm{SL}_2 \to G$ d'image G_α dont la restriction au tore standard $\mathbb{G}_m \subset \mathrm{SL}_2$ produit un cocaractère $\alpha^\vee : \mathbb{G}_m \to T$ qui satisfait $\langle \alpha^\vee, \alpha \rangle = 2$.

Le morphisme $\alpha^\vee$ définit en outre un morphisme $U_\alpha : \mathbb{G}_a \to G$ suivant

$$U_\alpha(x) = \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix}.$$

Un point important est que l'espace propre $\mathfrak{g}_\alpha$ ci-dessus est de dimension 1, engendré par $\mathfrak{u}_\alpha = U_{\alpha,*}(\mathrm{Lie}(\mathbb{G}_a))$. On dispose aussi l'élément

$$n_\alpha \ := \ \alpha^\vee \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in N_G(T)(F) \tag{19.4}$$

qui induit la réflexion s_α sur X.

De plus, la donnée radicielle $\Psi(G, T)$ est réduite. En termes de l'algèbre de Lie, on a la décomposition en espaces propres

$$\mathfrak{g} = \mathfrak{t} \oplus \bigoplus_{\alpha \in R} k\mathfrak{u}_\alpha,$$

où $\mathfrak{t} = \mathrm{Lie}(T)$ est l'espace propre pour le caractère nul de T. Le fait correspondant du point de vue groupes est que le groupe G est engendré (au sens Zariski) par T et les sous–groupes radiciels $(U_\alpha)_{\alpha \in R}$.

19.5. **Exemple.** $G = \mathrm{GL}_n$ de tore maximal diagonal $\mathbb{G}_m^n$ et d'algèbre de Lie $\mathfrak{g}l_n = M_n(F)$. La représentation adjointe est $Ad(A).X = A\,X\,A^{-1}$.

On a $X = \mathbb{Z}^n$ de base $(\lambda_i)_{i=1,\dots,n}$, $X^\vee = \mathbb{Z}^n$ et les racines sont les $(\alpha_{i,j} = \lambda_i \lambda_j^{-1})_{i,j=1,\dots,n, i\neq j}$ de vecteurs propres associés respectifs les matrices élémentaires $e_{i,j}$. Le morphisme $\alpha_{1,2}^\vee : \mathrm{SL}_2 \to \mathrm{GL}_n$ est donné par

$$\begin{bmatrix} * & * \\ * & * \end{bmatrix} \mapsto \begin{bmatrix} * & * & 0 & \cdots & & 0 \\ * & * & 0 & \cdots & & 0 \\ 0 & 0 & 1 & 0 & & 0 \\ & & .... & 1 & & \\ & & .... & & & \\ 0 & & \cdots & & 0 & 1 \end{bmatrix}$$

Pour d'autres exemples, voir [Mi, §17].

19.6. **Lemme.**

$$Z(G) = \bigcap_{\alpha \in R} \ker\big(T \xrightarrow{\alpha} \mathbb{G}_m\big).$$

Démonstration. Le centre $Z(G)$ de G est inclus dans T et dans $\ker(Ad)$, d'où l'inclusion

$$Z(G) \subset T \cap \ker(Ad) = \bigcap_{\alpha \in R} \ker(\alpha).$$

Il y a fait égalité puisque le groupe de droite commute avec T et tous les G_α donc avec tout G. □

Les propriétés suivantes de G se reflètent donc dans la donnée radicielle $\Psi(G, T)$.

19.7. **Corollaire.** *(a) G est un tore si et seulement si $R = \emptyset$.*

(b) G est semi-simple si et seulement si R engendre $X \otimes_{\mathbb{Z}} \mathbb{Q}$.

(c) G est adjoint si et seulement si R engendre X.

Démonstration. (a) En en effet, $T = Z(G)$ ssi $R = \emptyset$.

(b) G est semi-simple si et seulement si $Z(G)$ est fini. si et seulement si R engendre un sous–réseau d'indice fini de X, alors $Z(G)$ est fini.

(c) Dire que $Z(G) = 1$ est équivalent au fait que R engendre $X = \widehat{T}$. □

Si G est semi-simple, G est engendré par les sous–groupes de rang un $(G_\alpha)_{\alpha \in R}$ ou encore par les sous–groupes radiciels $(U_\alpha)_{\alpha \in R}$.

19.8. **Définition.** [SGA3, XXI] Un morphisme de donnnées radicielles $f : (X, R, X^\vee, R^\vee) \to (X', R', X'^\vee, R'^\vee)$ est la donnée d'une application $\mathbb{Z}$-linéaire $f : X \to X'$ telle que f induit une bijection de R sur R' et $f^\vee$ induit une bijection de $R'^\vee$ sur $R^\vee$

On dit que f est une isogénie si f est injectif de conoyau fini.

Une isogénie $\lambda : G' \to G$ donne lieu à une isogénie de données radicielles $\Psi(G,T) \to \Psi(G',T')$ où $T' = \lambda^{-1}(T)$. En outre $\widehat{\ker(\lambda)} = X/X'$.

En particulier, si $R^\vee$ engendre $X^\vee$, alors la donnée radicielle $\Psi(G,T)$ n'admet pas d'isogénie propre, donc G est simplement connexe.

19.3. **Théorèmes fondamentaux.**

19.9. **Théorème.** *(théorème d'unicité,* [Sp, th. 9.6.5]*)*
Deux groupes réductifs G/F et G'/F ayant des données radicielles isomorphes sont isomorphes.

19.10. **Théorème.** *(théorème d'existence,* [Sp, th. 10.1.1]*)*
Soit $\Psi = (X, X^\vee, R, R^\vee)$ une donnée radicielle réduite. Il existe un F–groupe réductif G/F muni d'un F–tore maximal T tel que $\Psi(G,T)$ est isomorphe à Ψ.

Un tel groupe G/F est appelé le groupe de Chevalley de la donnée radicielle Ψ.

La classification est donc indépendante de la caractéristique. Un point remarquable dans ce dictionnaire est que les groupes de Chevalley sont définis sur le corps premier (i.e. $\mathbb{Q}$ ou $\mathbf{F}_p$).

A posteriori, le lien entre groupes adjoints, algèbres de Lie et données radicielles réduites peut s'exprimer dans le dictionnaire suivant.

19.11. **Théorème.** *On suppose* $\mathrm{car}(F) = 0$*. Alors il y a une correspondance bijective entre*

$$\Big\{ F\text{-algèbres de Lie semi-simples} \Big\}$$

$$< -- > \Big\{ F\text{-groupes adjoints} \Big\}$$

$$< -- > \Big\{ \text{données radicielles réduites } (X, R, X^\vee, R^\vee) \text{ telles que } R \text{ engendre } X \Big\}$$

On associe à un F–groupe G son algèbre de Lie. Réciproquement, on associe à une algèbre de Lie semi-simple $\mathcal{L}$ le F–groupe algébrique $\mathrm{Aut}_{F-alg.\,de\,Lie}(\mathcal{L})^0$, i.e. la composante connexe du groupe des automorphismes de l'algèbre de Lie $\mathcal{L}$ qui est un sous–groupe de $\mathrm{GL}(\mathcal{L})$.

On peut associer directement à une donnée radicielle (ou plutôt une algèbre de Lie) une algèbre de Lie définie par générateurs et relations, voir [H1, §18.1].

19.12. **Remarque.** Attention, en caractéristique positive, il y a de nouvelle algèbres de Lie semi-simples, voir l'exposé d'O. Mathieu à ce sujet [Mt].

19.4. **A propos du revêtement universel.** Soit G/F un groupe semi-simple.

On associe alors à la donnée radicielle $\Psi(G,T) = (X, R, X^\vee, R^\vee)$ la donnée radicielle $\Psi' = (X', R, Y'^\vee, R^\vee)$ où $X'^\vee$ est le sous–réseau de $X^\vee$ engendré par $R^\vee$. Le morphisme de données radicielles $\Psi(G,T) \to \Psi'$ est alors une isogénie. Le théorème d'existence produit un groupe de Chevalley (G', T') et on construit alors une isogénie $G' \to G$ dont le noyau est le groupe fondamental de G.

L'esquisse de démonstration ci-dessus indique comment le théorème d'existence permet de construire le revêtement universel de G. En outre $R^\vee$ engendre $X^\vee$ si et seulement si G est semi-simple simplement connexe. A notre

20. Groupes résolubles déployés

20.1. **Définition.** Soit G un k–groupe algébrique. On dit que G est résoluble (resp. unipotent) k–déployé si G admet une suite de compositions dont les quotients successifs sont des $\mathbb{G}_a$ ou des $\mathbb{G}_m$ (resp. $\mathbb{G}_a$).

20.2. **Théorème.** *(Théorème de point fixe de Borel-Rosenlicht)*
Soit G un k–groupe algébrique résoluble k–déployé. Soit X une variété propre munie d'une action de G. Si satisfaisant $X(k) \neq \emptyset$, alors $X^G(k) \neq \emptyset$.

La forme générale ci-dessus est due à Rosenlicht, le cas d'un corps algébriquement clos est le théorème de point fixe de Borel.

Démonstration. La remarque cruciale est que la variété des points fixes X^G est propre puisque c'est une sous-variété fermée.

On procède par récurrence sur le nombre de facteurs. Dans le cas d'un facteur, on a $G = \mathbb{G}_a$ ou $G = \mathbb{G}_m$. Soit $x \in X(k)$ et considérons le morphisme $f : G \to X, g \mapsto g.x$. Le critère valuatif de propreté indique que f se prolonge de façon unique en un morphisme $\widetilde{f} : \mathbb{P}^1_k \to X$. Ainsi $\widetilde{f}$ est $G(k)$–équivariant et on constate alors que le point $\widetilde{f}(\infty) \in X(k)$ est fixe par G.

Pour le cas général, on a une suite exacte de k–groupes algébriques $1 \to H \to G \to G/H \to 1$ où H est résoluble k–déployé et $G/H = \mathbb{G}_a$ ou $\mathbb{G}_m$. L'hypothèse de récurrence permet de supposer que $X^H(k) \neq \emptyset$. Mais G/H agit sur la k–variété propre X^H et $X^G = (X^H)^{G/H}$. Le premier cas permet de conclure que $X^G(k) \neq \emptyset$. □

Une première application est la suivante.

20.3. **Théorème.** *(théorème de Lie-Kolchin) Soit G/k un k–groupe résoluble k-déployé. Alors il existe un entier n tel que $G \subset B_n$ où $B_n \subset \mathrm{GL}_n$ désigne le k–groupe des matrices inversibles triangulaires supérieures.*

On dit que G est trigonalisable.

Démonstration. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire fidèle. Le théorème 20.2 montre qu'il existe une droite $D \subset V$ qui est G–stable. On obtient donc un morphisme $G \to \mathrm{GL}(V/D)$. Par récurrence on voit que G stabilise un drapeau

$$0 \subsetneq V_1 \subsetneq V_2 \subsetneq \cdots V_{n-1} \subsetneq V$$

En choisissant une base de V, on a affaire au drapeau standard $0 \subsetneq k \subsetneq k^2 \subsetneq \cdots k^{n-1} \subsetneq k^n$. Ainsi $G \subset B_n$. □

20.4. **Proposition.** *Soit G/k un k–groupe résoluble k-déployé.*

(1) *On a une suite exacte canonique*

$$1 \to R_u(G) \to G \to T \to 1,$$

où T est un k–tore déployé et $R_u(G)$ est un k–groupe unipotent k–déployé.

(2) *$D(G)$ est un k–groupe unipotent lisse connexe.*

Démonstration. (1) Construisons tout d'abord une telle suite exacte avec un plongement de G dans le groupe B_n. On a $B_n = R_u(B_n) \rtimes \mathbb{G}_m^n$ et l'image du composé $G \to B_n \to \mathbb{G}_m^n$ est un sous–groupe multiplicatif de $\mathbb{G}_n^n$ qui est connexe puisque G est connexe. On a donc une suite exacte

$$1 \to R_u(B_n) \cap G \to G \to T \to 1,$$

où T est un k–tore déployé. Pour allons montrer par récurrence sur $\dim(G)$ que $R_u(B_n) \cap G$ est unipotent k–déployé. Soit $1 \to H \to G \to G/H \to 1$ une suite exacte de k–groupes où H est k–résoluble déployé et $G/H = \mathbb{G}_m$ ou $\mathbb{G}_a$. Si $G/H = \mathbb{G}_m$, on a $R_u(B_n) \cap H = R_u(B_n) \cap G$ et $R_u(B_n) \cap G$ est unipotent k–déployé selon l'hypothèse de récurrence. Si $G/H = \mathbb{G}_a$, on forme le diagramme commutatif

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & & \\
 & R_u(B_n) \cap H \arrow[r] \arrow[d] & R_u(B_n) \cap G \arrow[d] & & \\
1 \arrow[r] & H \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & \mathbb{G}_a \arrow[r] & 1. \\
 & T_H \arrow[r] \arrow[d] & T \arrow[d] & & \\
 & 1 & 1 & &
\end{tikzcd}$$

Il définit un morphisme de $\mathbb{G}_a$ dans le k–tore $\mathrm{coker}(T_H \to T)$, celui ci est trivial et une chasse au diagramme produit la suite exacte de k–groupes

$$1 \to R_u(B_n) \cap H \to R_u(B_n) \cap G \to \mathbb{G}_a \to 1.$$

Ainsi $R_u(B_n) \cap G$ est unipotent k–déployé. Cette suite est canonique puisque $R_u(B_n) \cap G$ est le plus grand sous–groupe unipotent de G.

(2) $D(G)$ est un k–groupe lisse connexe d'après le théorème général 13.3. Vu que $D(G)$ est un sous–groupe de $R_u(B_n)$, il est unipotent.

$\square$

20.5. **Remarque.** Le groupe $D(G)$ est en fait unipotent k–déployé [DG, IV.4.3.11].

20.6. **Lemme.** [8] *Soit G un k–groupe unipotent. Si $G \times_k k_s$ est trigonalisable, alors G est trigonalisable.*

Démonstration. Si $G \times_k k_s$ est trigonalisable, il existe une extension galoisienne finie K/k telle que $G \times_k K$ est trigonalisable. Il existe un entier n tel que $G \times_k K$ se plonge dans $R_u(B_{n,K})$. On considère le composé

$$G \to R_{K/k}(G) \to R_{K/k}(R_u(B_{n,K}))$$

où $R_{K/k}(G)$ est la restriction des scalaires de K à k de G. Le point est que $R_{K/k}(R_u(B_{n,K}))$ est un sous–groupe trigonalisable de $\mathrm{GL}(K^n)$. Par suite, G est trigonalisable. $\square$

20.7. **Proposition.** *On suppose que* $\mathrm{car}(k) = 0$*. Alors tout k–groupe unipotent est k–déployé.*

Démonstration: Le point ici est que $\mathbb{G}_{a,k}$ n'admet pas de sous–groupe propre non trivial. Le groupe G est $\overline{k}$-déployé donc $\overline{k}$–trigonalisable d'après le théorème de Lie-Kolchin. Le lemme indique que G est k–trigonalisable, i.e. G admet un plongement dans $R_u(B_n)$ pour un certain n. La trace sur G d'une suite de composition de $R_u(B_n)$ à quotients $\mathbb{G}_a$ est une suite de composition de G à quotients 1 ou $\mathbb{G}_a$. Le groupe G est donc k–déployé. $\square$

Plus généralement, on a la

20.8. **Proposition.** *(voir (*[SGA3, XVII.4.1.3]*) ou* [DG, IV.2.3.9]*) On suppose k parfait. Soit U un k–groupe unipotent lisse connexe. Alors U est un k–groupe unipotent k–déployé.*

20.9. **Remarque.** (a) Ceci est faux sans l'hypothèse de perfection sur k.

(b) Si $\mathrm{car}(k) = 0$, tout groupe k–unipotent est déployé.

Nous admettons le résultat suivant.

20.10. **Théorème.** *Soit $1 \to U \to G \to S \to 1$ une suite exacte de k–groupes affines où S est un k–groupe de type multiplicatif et U un groupe unipotent k–déployé. Alors cette suite est scindée et deux scindages $S \to G$ sont conjugués par un élément de $U(k)$.*

[8] On sait en fait que tout k–groupe unipotent est trigonalisable, mais c'est plus cher [SGA3, XVII.3].

Pour le cas G connexe, nous renvoyons à [Sp, §14.4]; pour le cas général, nous renvoyons à [SGA3, théorème XVII.6.1.1]. Revenant à la proposition 20.4, ceci entraîne qu'un k–groupe résoluble déployé G est le produit semi-direct d'un k–tore déployé et de son sous–groupe unipotent maximal $R_u(G)$; en outre les k–tores maximaux de G sont conjugués par $R_u(G)(k)$.

Ce résultat est à mettre en regard avec le suivant.

20.11. **Théorème.** *(Mostow,* [Mo, th. 7.1]*) On suppose* $\mathrm{car}(k) = 0$*. Soit* $1 \to U \to G' \to G \to 1$ *une suite exacte de k–groupes affines où G est un k–groupe réductif (ou même seulement linéairement réductif) et U un k–groupe unipotent déployé. Alors cette suite est scindée et deux scindages $G \to G'$ sont conjugués par un élément de $U(k)$.*

21. Groupes résolubles, radicaux

21.1. **Définition.** Soit G un k–groupe algébrique. On dit que G est résoluble s'il admet une suite de compositions dont les quotients successifs sont commutatifs.

Tout sous–groupe fermé et tout quotient d'un groupe résoluble est résoluble; toute extension de groupes résolubles est résoluble.

Il est assez délicat de voir en caractéristique positive que cette définition est de nature géométrique, c'est-à-dire que $G \times_k \overline{k}$ résoluble entraîne G résoluble [DG, IV.4.2.7] (en particulier, un k–groupe unipotent est résoluble). Cependant, si G est lisse, le point précédent est immédiat avec le lemme suivant.

21.2. **Lemme.** *Soit G/k un groupe algébrique linéaire. Alors les assertions suivantes sont équivalentes:*

(1) *G est résoluble;*
(2) *$D^n(G) = 1$ pour $n >> 0$.*

□

21.3. **Proposition.** *On suppose que k est un corps parfait. Soit G un k–groupe algébrique linéaire.*

(1) *Il existe un unique sous–groupe fermé $R(G)$ de G qui soit connexe, lisse, résoluble, distingué, et maximal pour cette propriété.*
(2) *Il existe un unique sous–groupe fermé $R_u(G)$ de G qui soit connexe, lisse unipotent, distingué, et maximal pour cette propriété.*

Démonstration. On peut supposer k algébriquement clos.

(1) On définit alors le sous–groupe fermé

$$R(G) = \Big(\bigcap_H H \Big)^0$$

où l'intersection est prise sur les sous-groupes connexes lisses résolubles maximaux de G. Alors $R(G)$ est résoluble et distingué. Il est connexe et réduit donc lisse suivant le théorème de Cartier 1.7. Il contient tout sous–groupe ayant les mêmes propriétés.

(2) Dans le cas unipotent, la définition de $R_u(G)$ est la même si ce n'est que H parcourt les sous-groupes connexes lisses unipotents et maximaux de G. □

Le k–groupe $R_u(G)$ (resp. $R_u(G)$) est le radical (resp. radical unipotent) de G. Le k–groupe $R_u(G)$ est un groupe unipotent k–déployé (Prop. 20.8) et c'est un k–groupe unipotent maximal lisse connexe de $R(G)$. Il faut prendre garde que ces objets ne sont pas définis si k n'est pas parfait.

21.4. **Lemme.** *On suppose que k est un corps parfait. Soit G un k–groupe algébrique linéaire connexe.*

(1) *$G/R_u(G)$ est réductif. En particulier, G est réductif si et seulement si $R(G) = 1$.*
(2) *$G/R(G)$ est semi–simple. En particulier, G est semi-simple si et seulement si $R(G) = 1$.*
(3) *$R(G)/R_u(G) \xrightarrow{\sim} Z(G/R_u(G))^0$. En particulier, $R_u(G)$ est le radical unipotent de $R(G)$.*

Démonstration. On peut supposer k algébriquement clos.

(1) On vérifie la définition (7.3). Soit U un k-groupe unipotent lisse connexe et distingué de $G/R_u(G)$. Si $\pi : G \to G/R_u(G)$ désigne le morphisme quotient, alors $\pi^{-1}(U)$ est un k–groupe unipotent lisse, connexe et distingué de G contenant $R_u(G)$, donc $R(G) = \pi^{-1}(U)$ et $U = 1$. Le groupe G est donc réductif.

(2) Selon la définition (11.3), c'est-à-dire que l'on doit vérifier que $G/R(G)$ est réductif de centre connexe trivial. Le même raisonnement que ci-dessus indique que $G/R(G)$ est réductif. Soit S un k-tore central de $G/R_u(G)$. Si $\pi : G \to G/R(G)$ désigne le morphisme quotient, alors $\pi^{-1}(S)$ est un k–groupe résoluble lisse, connexe et distingué de G contenant $R(G)$, donc $R(G) = \pi^{-1}(S)$ et $S = 1$. Le groupe G est donc semi-simple.

(3) Le diagramme commutatif

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R_u(G) & \longrightarrow & G & \longrightarrow & G_{red} & \longrightarrow & 1 \\ & & \downarrow & & \| & & \downarrow & & \\ 1 & \longrightarrow & R(G) & \longrightarrow & G & \longrightarrow & G_{ss} & \longrightarrow & 1 \end{array}$$

produit un isomorphisme de groupes résolubles connexes $R(G)/R_u(G) \cong \ker(G_{red} \to G_{ss})$. Le k–groupe $H := \ker(G_{red} \to G_{ss})$ est réductif et résoluble, ainsi $D(G) = D^2(G) = \cdots = D^\infty(G) = 1$ et $H \xrightarrow{\sim} \mathrm{corad}(G)$ (proposition 13.5). Le k–groupe H est donc un k–tore algébrique qui est central dans G_{red} par "rigidité" (lemme 11.1). Il est maximal pour cette propriété, c'est donc le centre connexe de G. □

Le groupe $R(G) \times_k k_s$ est donc résoluble déployé. D'après la proposition 20.4 (appliquée à $G \times_k k_s$), on a on a une suite exacte

$$0 \to R_u(G) \to R(G) \to T \to 1$$

où T est un k–tore algébrique. En outre cette suite est scindée (th. 20.10).

Un complément L de $R_u(G)$ dans G s'appelle un sous–groupe de Levi. Il y en a toujours en caractéristique nulle et ils sont alors tous conjugués par $R_u(G)(k)$ suivant le théorème de Mostow.

22. Sous–groupes paraboliques

22.1. **Définition.** Soit G/k un k–groupe algébrique linéaire. Un k-sous–groupe fermé P lisse est un k–sous–groupe parabolique si la variété quotient G/P est projective.

On sait qu'une k-varieté $X \times_k \overline{k}$ est projective (resp. quasi projective) si et seulement si $X \times_k \overline{k}$ est projective [EGA4, 9.1.5]. Par suite, un k-sous–groupe P est parabolique si et seulement si $P \times_k \overline{k}$ est un $\overline{k}$–sous–groupe parabolique de $G \times_k \overline{k}$.

Par construction, un espace homogène G/P est une variété quasi–projective. Ainsi P est un k–sous–groupe parabolique si et seulement si la variété G/P est propre.

22.1. **Exemples.** Pour le groupe linéaire, les quotients GL_n/P sont les grassmaniennes et plus généralement les variétés de drapeaux. C'est pourquoi les les variétés G/P sont appelées variétés de drapeaux généralisées.

22.2. **Lemme.** *Soit P un k–sous–groupe parabolique de G.*

(1) *Soit $P^\sharp$ un k-sous–groupe fermé lisse de G satisfaisant $P \subset P^\sharp \subset G$. Alors P est un k–sous–groupe parabolique de $P^\sharp$ et $P^\sharp$ est un k-sous–groupe parabolique de G.*
(2) *Les k–sous–groupes paraboliques de Q de G qui sont inclus dans P sont les k-sous–groupes paraboliques de P.*

Démonstration (1) Suivant [DG, III.3.2.5], le morphisme $P^\sharp/P \to G/P$ est une immersion fermée. Par suite $P^\sharp/P$ est projective. Le morphisme $G/P \to G/P^\sharp$ est surjectif, donc $G/P^\sharp$ est propre. On conclut que $P^\sharp$ est un k-sous–groupe parabolique de G.

(2) Soit $Q \subset P$ un k-sous–groupe parabolique de G. Les fibres du morphismes $G/Q \to G/P$ sont projectives, donc P/Q est projective. Par suite, Q est un k–sous-groupe parabolique de P. Réciproquement, soit Q un k-sous–groupe parabolique de P. Alors les fibres géométriques du morphisme $G/Q \to G/P$ sont propres, donc G/Q est propre. On conclut que Q est un k–sous–groupe parabolique de G. □

Le théorème de point fixe s'applique.

22.3. **Lemme.** *On suppose k algébriquement clos. Soit $H \subset G$ un sous–groupe k–résoluble déployé. Soit P un k–sous–groupe parabolique de G. Alors il existe $g \in G(k)$ tel que*

$$H \subset gPg^{-1}.$$

Démonstration. Le k–groupe résoluble déployé H admet un point fixe sur la k-varieté propre G/P (20.2). Soit $[gP] \in (G/P)^H(k)$ un point. Alors $H \subset gPg^{-1}$. □

Ceci s'applique à a situation suivante.

22.4. **Lemme.** *Soit $1 \to H \to G' \to G \to 1$ une suite exacte de k–groupes algébriques linéaires où l'on suppose H k–résoluble déployé.*

(1) *Soit P' un k-sous–groupe parabolique de G'. Alors $H \subset P'$.*
(2) *Le morphisme quotient $\pi : G' \to G$ induit une correspondance bijective entre les k–sous–groupes paraboliques de G' et ceux de G.*

Démonstration (1) On peut supposer ici k algébriquement clos. Le lemme précédent montre qu'il existe $g \in G(k)$ tel que $H \subset gPg^{-1}$, d'où $H \subset P$.
(2) Si P' un k-sous–groupe parabolique de G', il est clair que $\pi(P')$ est un k-sous–groupe parabolique de G. De plus (1) indique que $P' = \pi^{-1}(\pi(P'))$. □

22.5. **Théorème.** *(théorème de Borel) On suppose k algébriquement clos. Soit G un groupe algébrique linéaire connexe. Soit B un sous–groupe de Borel de G (i.e. k–résoluble déployé maximal).*

(1) *Si P est un k-sous–groupe parabolique de G, alors il existe $g \in G(k)$ tel que $B \subset gPg^{-1}$.*
(2) *B est un sous–groupe parabolique de G.*

Démonstration. (1) C'est un cas particulier du lemme 22.3.

(2) Soit $P \subset G$ un sous-groupe parabolique minimal (connexe) de G. On va montrer que P est résoluble déployé ce qui suivant (1) implique que P est un sous–groupe de Borel. On a une suite exacte

$$1 \to R(P) \to P \to H \to 1.$$

Le lemme 21.4 indique que H est semi-simple et le lemme 22.4 montre que H H n'admet pas de sous k–groupe parabolique propre. On raisonne par l'absurde en supposant que H admet une represéntation linéaire V non triviale que l'on suppose de degré minimal. On fait agir H sur l'espace projectif $\mathbb{P}(V)$. Le lemme de l'orbite fermée ([Po, 10.4], [DG, II.5.3.3]) montre qu'il existe $x \in \mathbb{P}(V)(k)$ tel que $H.x$ est fermée. Alors H/H_x est une variété projective et $H_{x,red}$ est un k–sous–groupe parabolique de H, donc $H_{x,red} = H_x = H$. Le point x est donc fixe par H et il existe une droite $D \subset V$ stable par H. Par suite, on a un morphisme $H \to \mathrm{GL}(V/D)$ qui est trivial puisque $\dim(V.D) < \dim(V)$. La représentation $\rho : H \to \mathrm{GL}(V)$ est donc à valeurs dans le groupe

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

Le groupe $H/\ker(\rho)$ est semi-simple et résoluble, il est donc trivial (lemme 21.4). La représentation ρ est donc triviale, contradiction. $\square$

22.6. **Corollaire.** *(théorème de Borel) On suppose k algébriquement clos. Les sous–groupes de Borel de G sont conjugués par $G(k)$.*

22.7. **Remarque.** La démonstration classique procède par l'application du lemme de l'orbite fermée à la variété des drapeaux maximaux.

23. Systèmes de Tits et sous–groupes paraboliques standards

L'étude des sous–groupes paraboliques d'un k–groupe algébrique peut être menée avec les groupes abstraits de k–points, au moyen du formalisme des (B, N)-paires appelées aussi systèmes de Tits. La référence est Bourbaki [BAC2, IV.2]

23.1. Systèmes de Tits.

23.1. **Définition.** On appelle système de Tits un quadruplet (G, B, N, S) où G est un groupe,B et N deux sous–groupes et S une partie de $W := N/B \cap B$ satisfaisant aux axiomes suivants :

(T1) L'ensemble $B \cup N$ engendre G et $B \cap N$ est un sous–groupe distingué de N.

(T2) L'ensemble S engendre le groupe W et se compose d'éléments d'ordre 2.

(T3) On a $sBw \subset BwB \cup BswB$ pour $s \in S$ et $w \in W$.

(T4) Pour tout $s \in S$, on a $sBs \not\subset B$.

On fixe un système de Tits (G, B, N, S). Le groupe W est appelé le groupe de Weyl du système de Tits. La notation BwB signifie BnB où n est un relevé (quelconque) de w dans N. Ces axiomes donnent un cadre général pour les deux résultats fondamentaux suivants.

23.2. **Théorème.** *Alors on a une décomposition en doubles classes*

$$G = \bigsqcup_{w \in W} BwB.$$

Si $X \subset S$, on note W_X le sous–groupe de W engendré par S et $G_X = \bigsqcup_{w \in W_X} BwB$.

23.3. **Théorème.** (1) *Pour toute partie X de S, l'ensemble G_X est un sous–groupe de G et il est engendré par B et X.*
(2) *L'application $X \mapsto G_X$ est une bijection de $\mathcal{P}(S)$ sur l'ensemble des sous–groupes de G contenant B.*

En particulier, si W est fini, il y a un nombre fini de sous–groupes de G contenant B.

23.4. **Définition.** On dit qu'un sous–groupe P de G est parabolique s'il contient un conjugué de B.

23.5. **Théorème.** (1) *Tout groupe parabolique est son propre normalisateur.*
(2) *Soient P_1 et P_2 deux sous–groupes paraboliques de G. Alors $P_1 \cap P_2$ contient un conjugué de T.*

23.2. **Groupes de Chevalley.** Soit $(X, X^\vee, R, R^\vee)$ une donnée radicielle réduite et (G, T) le k–groupe réductif de Chevalley associé par le théorème d'existence, i.e. tel que $\Psi(G, T) = (X, X^\vee, R, R^\vee)$. On note $N = N_G(T)$ et $W = N_G(T)/T$ le groupe de Weyl qui est un k-groupe fini constant. Le groupe W agit sur $(X, X^\vee, R, R^\vee)$.

La théorie des systèmes de racines indique qu'il existe une "base" Δ de R, c'est-à-dire que tout élément β de R s'écrit de façon unique

$$\beta = \sum_{\alpha \in \Delta} m_\alpha \, \alpha,$$

où les m_α sont des entiers tous ≥ 0 ou tous ≤ 0. La racine β est dite positive (par rapport à Δ) si $m_\alpha \geq 0$ pour tout $\alpha \in \Delta$.

Le groupe W agit de façon simplement transitive sur les "bases" de $(X, X^\vee, R, R^\vee)$. Si $\alpha \in \Delta$, on dispose des sous-groupes $U_{\pm\alpha}$ et de $s_\alpha \in W$ (19.4). Mentionnons les étapes principales de la construction d'un système de Tits associé à (G, T) et Δ.

23.6. **Proposition.** [Sp, 8.2.4] *Le sous–groupe B de G engendré par T et les U_α ($\alpha \in R_+$) est un sous–groupe de Borel de G.*

23.7. **Théorème.** [Sp, 8.2.8] *Le groupe de Weyl W est engendré par les s_α pour $\alpha \in \Delta$.*

Alors $T = N_G(T) \cap B$ et on considère le quadruplet $(G(k), B(k), N(k), S)$ où $S = (s_\alpha)_{\alpha \in \Delta}$ engendre W.

23.8. **Théorème.** *(*[Bo, 14.15, 21.15]*) $(G(k), B(k), N(k), S)$ est un système de Tits.*

Ceci donne lieu à une série d'applications.

23.9. **Théorème.** *(décomposition de Bruhat) Soit $(n_w)_{w \in W}$ une section (ensembliste) de $N_G(T)(k) \to W$. On a la décomposition*

$$G(k) = \bigsqcup_{w \in W} B(k)\, n_w \, B(k).$$

Si $I \subset \Delta$, on note $[I] \subset R$ le sous–ensemble de racines qui sont combinaisons linéaires d'éléments de I.

• $T_I = \Big(\bigcap_{\alpha \in I} \ker(\alpha) \Big)^0 \ \subset \ T$;
• $L_I = C_G(T_I) \ \subset \ G$;
• $U_I \subset U$ le sopus–groupe de $R_u(B)$ engendré par les U_α, $\alpha \in R_+ \setminus I$.
• $P_I = U_I \rtimes L_I$.

23.10. **Théorème.** *(paraboliques standard,* [Sp, 8.4.3]*) Les k–sous-groupes paraboliques de G contenant B sont les $(P_I)_{I \subset \Delta}$. Ils satisfont*

$$P_I = N_G(P_I) = N_G(U_I).$$

Le groupe $P_I(k)$ est le sous–groupe parabolique associé à la partie I de Δ. Les P_I donnent donc lieu à des classes de conjugaison géométriques distinctes. Si k est algébriquement clos, il y a donc une correspondance bijective entre les classes de conjugaison de k–sous–groupes paraboliques de G et les $\mathcal{P}(\Delta)$.

L'algèbre de Lie de P_I est

$$\mathfrak{p}_I := \mathfrak{t} \oplus \bigoplus_{\alpha \in [I]} \mathfrak{u}_\alpha$$

où $[I] \subset R$ est le sous-ensemble engendré par $I \subset \Delta$. En particulier $P_\Delta = G$ et $P_\emptyset = B$. De plus, on peut retrouver l'indice I avec

$$T_I = Z(L_I)^0.$$

On peut définir de la même façon les k-sous–groupes paraboliques $P_I^- = U_I^- \rtimes L_I$ où U_I^- est le sous–groupe de G engendré par les $U_{-\alpha}$ pour $\alpha \in I$.

23.11. **Remarque.** L_I est l'unique sous–groupe de Levi de P_I qui contient T (see [Sp, 8.4.4]).

24. Retour au cas général

Soit G/k un k–groupe réductif. Un point technique important est le suivant.

24.1. **Proposition.** *(existence d'une décomposition de Levi,* [Sp, 16.1.1], [SGA3, XXVI.2.3]*)*

Un k–groupe parabolique P d'un k–groupe G admet une décomposition $R_u(P) \rtimes L$ où $R_u(P)$ est unipotent k–déployé et L réductif. De plus, tout les sous–groupes de Levi L de P sont conjugués sous $R_u(P)(k)$.

En caractéristique nulle, c'est un cas particulier du théorème de Mostow 20.11).

24.1. **Intersection de sous–groupes paraboliques.**

24.2. **Proposition.** *Soient P, Q deux k-sous–groupes paraboliques de G.*

(1) *$P \cap Q$ contient un k–tore maximal.*
(2) *$(P \cap Q).R_u(P)$ est un k-sous–groupe parabolique de G. Il est égal à P si et seulement si Q contient un sous–groupe de Levi de P.*

Démonstration (1) : cas k est algébriquement clos : le Théorème 22.5 nous ramène à montrer que deux sous–groupes de Borel B and B' contiennent un tore maximal. On a $B' = gBg^{-1}$ pour un élément $g \in G(k)$. Soit $T \subset B$ un tore maximal de B. La décomposition de Bruhat (23.10) produit un élément $n \in N_G(T)(k)$ tel que $g \in B(k)nB(k)$. On écrit alors $g = b_1 n b_2$ pour obtenir $b_1 T b_1^{-1} \subset B \cap B'$.

(1) : k est de caractéristique nulle : posant[9] $H := (P \cap Q)^0$ Le groupe $H := H/R_u(H)$ est réductif de rang $rang(G)$. Il admet un k–tore maximal T de rang $rang(G)$, celui-ci se relève à $(P \cap Q)^0$ (suivant le th. 20.10 ou 20.11).

Nous renvoyons à [SGA3, XXVI.11] pour la démonstration du cas général.
(2) On peut supposer k algébriquement clos. Soit (B, T) un couple de Killing. La première assertion permet de supposer que $T \subset P \cap Q$ et que $B \subset P$. Alors $P = P_I$ est un sous–groupe parabolique standard. On considère le sous–système de racines $\Phi(Q, T) \subset \Phi(G, T)$. Puisque Q est un sous–groupe parabolique, on sait que $\Phi(Q, T)$ est un sous-système parabolique, c'est-à-dire $\Phi(G, T) = \Phi(Q, T) \cup -\Phi(Q, T)$. Alors tout sous–groupe de Borel B' de $P \cap Q$ contenant T contient au moins un des U_α, $U_{-\alpha}$ pour tout $\alpha \in [I]$. Par suite, le groupe k-résoluble $B'.R_u(P)$ contient T et un des U_α, $U_{-\alpha}$ pour chaque $\alpha \in \Phi(G, T)$. Sa dimension étant plus grande ou égale à celle d'un sous–groupe de Borel, c'est un sous–groupe de Borel. Le lemme 22.2 indique que alors que $(P \cap Q).R_u(P)$ est parabolique. La seconde assertion est évidente. □

24.2. **Groupes paraboliques opposés.**

24.3. **Définition.** Deux k–sous–groupes paraboliques P et Q de G sont opposés si $P \cap Q$ est un sous–groupe de Levi commun à P et à Q.

Dans le cas d'un groupe de Chevalley, le groupe P_I^- est l'unique sous–groupe parabolique qui est opposé à P_I et contient L_I (ou même T suivant la remarque 23.11). On peut formaliser ceci avec le lemme suivant.

24.4. **Lemme.** *Soit P un k-sous–groupe parabolique de G. Il y a une correspondance entre les k-sous–groupes paraboliques opposés de P, les sous-groupes de Levi de P et les tores maximaux de P.*

En particulier, il existe toujours un sous–groupe parabolique opposé à P.

[9] Il est connu que $P \cap Q$ est connexe.

24.5. **Lemme.** [BoT, 4.10] *Soient P, P' deux k-sous–groupes paraboliques. Alors les conditions suivantes sont équvalentes :*

(1) *P et P' sont opposés;*
(2) *Les classes de conjugaison gémométriques de P and P' sont opposées*[10] *et P, P' contiennent des sous–groupes de Borel opposés;*
(3) *$(P \cap P').R_u(P) = P$, $(P \cap P').R_u(P') = P'$, et P, P' contiennent des sous–groupes de Borel opposés.*
(4) *$P \cap R_u(P') = 1$ and $P' \cap R_u(P) = 1$.*

On utilise seulement dans la suite l'implication (1) $\Longrightarrow$ (4). Pour la démontrer, on peut supposer que $k = \overline{k}$ et que $P = P_I$, $P' = P_I^-$ sont des k–sous–groupes paraboliques standards d'un k–groupe de Chevalley. Alors $P_I \cap U_I^- = 1$.

25. Le théorème de Borel-Tits

On décompose ce résultat en deux parties.

25.1. **Théorème.** *Soit G un k–groupe réductif et soit P un k–sous–groupe parabolique.*

(1) *La fibration $G \to G/P$ est localement triviale pour la topologie de Zariski.*
(2) *La k–variété G/P est k-rationnelle.*
(3) *L'application $G(k) \to (G/P)(k)$ est surjective et l'application $H^1(k, P) \to H^1(k, G)$ est injective.*

Démonstration (pour k infini). (1) Soit P' un k–sous–groupe parabolique opposé à P. Le lemme 24.5 montre que $R_u(P') \cap P = 1$. Ainsi le morphisme $R_u(P') \to G/P$ est un monomorphisme, il existe donc un ouvert dense sur lequel c'est une immersion [DG, I.3.4.7]. Pour des raisons de dimension, c'est une immersion ouverte[11]. Puisque $G(k)$ est Zariski dense dans G, on peut recouvrir G/P par les ouverts trivialisants $gR_u(P')$ ($g \in G(k)$). On conclut que la fibration $G \to G/P$ est triviale pour la topologie de Zariski.
(2) Nous venons de voir que $R_u(P')$ est birationnellemnt isomorphe à G/P. Comme k-variété, $R_u(P')$ est k–isomorphe à un espace affine. La variété G/P est donc une variété k-rationnelle.
(3) Par suite l'application $G(k) \to (G/P)(k)$ est surjective. La suite exacte longue d'ensembles pointés

$$1 \to P(k) \to G(k) \to (G/P)(k) \to H^1(k, P) \to H^1(k, G),$$

montre que la flèche $H^1(k, P) \to H^1(k, G)$ a un noyau trivial. Pour obtenir l'injeectivité, on utilise la technique de "torsion" [S1, §I.5.3]. Celle-ci ramène à voir que les flèches $H^1(k, {}_zP) \to H^1(k, {}_zG)$ ont un noyau trivial pour tout

[10] c'est-à-dire il existe $g \in G(\overline{k})$ tel que ${}^g\big(P \times_k \overline{k}\big)$ et $P' \times_k \overline{k}$ sont opposés.

[11] En fait $R_u(P') \to G/P$ est une immersion ouverte [SGA3, XXVI.4.3.2]. En effet, c'est un monomorphisme étale.

$[z] \in H^1(k,P)$. Ceci est vrai puisque ${}_zP$ est un k-sous–groupe parabolique de ${}_zG$. $\square$

Ceci nous permet de raffiner le lemme 22.5.

25.2. **Corollaire.** *Soit $H \subset G$ un sous–groupe k–résoluble déployé. Soit P un k–sous–groupe parabolique de G. Alors il existe $g \in G(k)$ tel que*

$$H \subset gPg^{-1}.$$

Démonstration. Le théorème de point fixe 20.2 indique que $(G/P)^H(k) \neq \emptyset$. Soit x un tel point. Le théorème 25.1 montre que $x = [gP]$ avec $g \in G(k)$. Par suite $H \subset gPg^{-1}$. $\square$

25.3. **Théorème.** *Soit G un k–groupe réductif et soient P, Q deux k-sous–groupes paraboliques de G.*

(1) *Si P et Q sont des k–sous–groupes paraboliques minimaux, alors P et Q sont conjugués sous $G(k)$.*
(2) *Si $P \times_k \overline{k}$ et $Q \times_k \overline{k}$ sont conjugués sous $G(\overline{k})$, alors P et Q sont conjugués sous $G(k)$.*

Proof. (1) On suppose donc que P, Q sont des k–sous–groupes paraboliques de G. D'après le corollaire 25.2, quitte à remplacer P par un conjugué, on peut supooser que $R_u(Q) \subset P$, d'où

$$(*) \qquad (P \cap Q).R_u(Q) \subset P \cap Q.$$

Maintenant, la proposition 24.2.2 énonce que le groupe de gauche est un k-sous–groupe parabolique de Q et de G. La minimalité de P et Q permet de conclure que $(P \cap Q).R_u(P) = P = Q$.

(2) Quitte à conjuguer P par $G(k)$, le même argument nous permet de supposer que $R_u(Q) \subset P$ et ainsi l'inclusion $(*)$ ci-dessus vaut. Pour montrer que $P = Q$, il est loisible d'étendre les scalaires à $\overline{k}$. Puisque $(P \cap Q).R_u(Q)$ est un k–sous–groupe parabolique, il contient un couple de Killing (B,T). Ainsi $P = P_I$ et $Q = P_J$ sont des sous–groupes paraboliques standards G qui sont conjugués sous $G(\overline{k})$. On conclut que $P = Q$. $\square$

25.4. **Corollaire.** *Soit P un k-sous–groupe parabolique minimal de G. Alors la classe de conjugaison géométrique de P est auto-opposée.*

26. Retour aux exemples

26.1. **Unicité dans le théorème de Wedderburn.** Soit A une k–algèbre simple centrale de degré d. Alors $A \otimes_k k_s \cong M_d(k_s)$, i.e. A est une k–forme de $M_d(k)$. Le k-groupe $\mathrm{GL}_1(A)$ est donc une k-forme de GL_d. Si $A = M_r(D)$ où D est une k–algèbre centrale à divisions, le k-sous–groupe

$$P = \begin{pmatrix} D & * & . & . & * \\ 0 & D & * & . & * \\ . & . & . & . & . \\ 0 & . & 0 & D & * \\ 0 & . & 0 & 0 & D \end{pmatrix} \subset \mathrm{GL}_r(D) = \mathrm{GL}_1(A)$$

est un k-sous–groupe parabolique minimal de $\mathrm{GL}_1(A)$ et $P/R_u(P) = \mathrm{GL}_1(D)^r$. L'algèbre D est donc "codée" par P. Le théorème de Borel-Tits permet donc de comprendre l'unicité dans le théorème de Wedderburn.

26.2. **Groupes spéciaux orthogonaux.** Soit $q = q_0 \perp \nu\mathbb{H}$ où q_0 est une forme quadratique aniostrope. Soit $P \subset SO(q)$ le sous–groupe de $SO(q)$ qui stabilise V_0, l'espace vectoriel sous–jacent à q_0. Alors P est un k-sous–groupe parabolique minimal de $SO(q)$ et $P/R(P) = SO(q_0)$. Le théorème de Borel-Tits montre que la classe de similitude de q_0 est "codée" dans $SO(q_0)$, obtenant ainsi une version faible du théorème de Witt.

Tores déployés maximaux, k–groupes irréductibles et anisotropes

27. Restriction des scalaires à la Weil II

27.1. **Théorème.** *(voir* [V, §3.12]*) Soit L/k une extension finie séparable de corps. Soit Y une L–variété affine (resp. quasi–projective). Alors le foncteur*

$$\begin{array}{ccc} \Big\{k\text{–algèbres}\Big\} & \longrightarrow & \mathcal{E}ns \\ R & \mapsto & Y(R \otimes_k L) \end{array}$$

est représentable par une k–variété affine (resp. quasi–projective) notée $R_{L/k}(Y)$.

La variété $R_{L/k}(Y)$ est la restriction à la Weil de L à k de Y/L. On a donc une bijection

$$\mathrm{Hom}_k(X, R_{L/k}(Y)) \xrightarrow{\sim} \mathrm{Hom}_L(X_L, Y)$$

pour toute k–variété X. On a donc $R_{L/k}(Y)(k) = X(L)$. En particulier, en prenant $X = R_{L/k}(Y)$ et l'identité, on obtient un L–morphisme canonique $p : R_{L/k}(Y) \times_k L \to Y$. Ceci généralise le §3.4 où nous avions considéré uniquement le cas où $Y = Y_0 \times_k L$ est défini sur k.

Si G/L est un L–groupe algébrique, $R_{L/k}(G)$ est un k–groupe algébrique. Si $k \subset L \subset k_s$, on s'intéresse au composé

$$H^1(k, R_{L/k}(G)) \overset{Res}{\to} H^1(L, R_{L/k}(G) \times_k L) \overset{p_*}{\to} H^1(L, G).$$

27.2. **Lemme.** *(lemme de Shapiro) L'application $H^1(k, R_{L/k}(G)) \to H^1(L, G)$ est une bijection.*

Ceci peut se faire avec des cocycles [KMRT, 29.6] mais il est plus éclairant d'établir une correspondance entre $R_{L/k}(G)$–espaces principaux homogènes et G–espaces principaux homogènes.

Pour la restriction des scalaires de Weil dans le langage des schémas, voir [BLR, §7.6].

28. Groupes paraboliques et tores

Soit G/k un groupe réductif.

28.1. Des tores vers les sous–groupes paraboliques.

28.1. **Proposition.** [Bo, §20.4] *Soit $S \subset G$ un k-tore déployé. Alors $Z_G(S)$ est le sous–groupe de Levi d'un k–sous–groupe parabolique de G.*

Esquisse de Démonstration. Soit T un k–tore maximal de G contenant S. Soit $\lambda : \mathbb{G}_m \to S$ tel que pour tout $\alpha \in \Phi(G, S)$, $\alpha \circ \lambda \neq 0$. On note $\Phi = \Phi(G \times_k k_s, T \times_k k_s)$ le système de racines absolu de G et on pose

$$\Psi := \Big\{\alpha \in \Phi(G \times_k k_s, T \times_k k_s) \mid \langle \lambda, \alpha \rangle > 0\Big\}.$$

Vu que $\Phi(Z_G(S) \times_k k_s, T \times_k k_s) = \Big\{\alpha \in \Phi(G \times_k k_s, T \times_k k_s) \mid \langle \lambda, \alpha \rangle = 0\Big\}$, on a

$$\Phi = \Phi(Z_G(S) \times_k k_s, T \times_k k_s) \sqcup \Psi \sqcup -\Psi.$$

On montre alors que le sous–groupe de $G \times_k k_s$ engendré par $Z_G(S)$ et les sous–groupes radiciels U_β pour $\beta \in \Psi$ est un k_s–sous–groupe parabolique qui se descend en un k–sous–groupe parabolique Q de G. Le k–groupe $Z_G(S)$ est alors un k–sous–groupe de Levi de Q. □

28.2. **Remarque.** Le k–sous–groupe parabolique Q construit dans la démonstration peut-être défini intrinsèquement en fonction du coractère $\lambda : \mathbb{G}_m \to G$, il s'agit du k–groupe parabolique $P(\lambda)$, voir [Sp, §13.4].

28.3. **Corollaire.** *Si G admet un k-tore déployé non central, alors G admet un k–sous–groupe parabolique propre.*

Le résultat suivant généralise le cas géométrique.

28.4. **Théorème.** *Les k-tores déployés maximaux de G sont conjugués sous $G(k)$.*

Etant donné un k-tore T, on note T_d le plugs grand k-tore déployé de T; son groupe des cocaractères est $(\widehat{T}^0)^{\Gamma_k}$.

Démonstration. Soient S, S' deux k-tores déployés maximaux. Soit P un k–sous–groupe parabolique minimal de G. Le corollaire 25.2 permet de supposer que S and S' sont des k-tores déployés maximaux de P. On note $\pi : P \to P/R(P)$. Les images $\pi(S)$ et $\pi(S')$ dans $P/R(P)$ sont des k–tores déployés maximaux du groupe semi-simple $P/R(P)$ qui ne possède aucun k–sous–groupe parabolique propre. Le corollaire 28.3 indique que $\pi(S) = \pi(S') = 1$. Ainsi S et S' sont des k–tores déployés maximaux de $R(P)$. On a une suite exacte

$$1 \to R_u(P) \to P \xrightarrow{p} T \to 1,$$

où T est un k–tore algébrique et qui est scindée (20.10). Ainsi $p(S)$ et $p(S')$ sont des k–tores déployés maximaux de T, i.e. $p(S) = p(S') = T_d$. En considérant l'image inverse par $T_d \to T$ de l'extension ci-dessus, on conclut que S et S' sont conjugués par un élément de $R_u(P)(k)$. □

28.2. **Des k–sous–groupes paraboliques vers les tores.**

28.5. **Proposition.** [Bo, 20.6] *Soient P un k–sous–groupe parabolique propre de G, L un sous–groupe de Levi et S le centre connexe de L. Alors*

(1) $L = Z_G(S) = Z_G(S_d)$;

(2) P est minimal si et seulement si S_d est un k-tore déployé maximal de G.

28.6. **Lemme.** *Soit $L \subset L'$ où L et L' sont des sous–groupes de Levi de k–sous–groupes paraboliques de G. Alors L est un sous–groupe de Levi d'un k–sous–groupe parabolique de L'.*

Démonstration. Soit P (resp. P') un k–sous–groupe parabolique de G dont L (resp. L') est un sous–groupe de Levi. On note $\pi : P \to P/R_u(P)$. On a l'inclusion

$$L \subset (P \cap P').R_u(P) \subset P$$

donc $(P \cap P').R_u(P) = P$. Ainsi L est un k–groupe de Levi du k–sous–groupe parabolique $\big(P \cap P'.R_u(P')\big)/R_u(P')$ de $P'/R_u(P') \cong L'$. $\square$

Démonstration. On note $\pi : P \to P/R_u(P)$.

(1) L'égalité $L = Z_G(S)$ se vérifie après extension des scalaires sur le cas des groupes de Levi standards.

On a $L = Z_G(S) \subset Z_G(S_d) = L'$ ou L' est un k–sous–groupe de Levi d'un k–sous–groupe parabolique P' de G (proposition 28.1). D'après le lemme 28.6, L est le sous–groupe de Levi d'un k–sous–groupe parabolique propre Q' de L'. En quotientant par S_d, $Z_G(S)/S_d$ est un k–sous–groupe de Levi du k–sous–groupe parabolique propre Q'/S_d. de L'/S_d. Mais $Z(L/S_d)^0 = S/S_d$ est un k–tore anisotrope, i.e. tel que $(S/S_d)_d = 1$. On s'est donc ramené au cas $S_d = 1$, c'est-à-dire $L' = G$. Sans perte de généralité, on peut supposer aussi que G est adjoint.

On raisonne par l'absurde en supposant que P est un k–sous–groupe parabolique propre de G. Soit T un k–tore maximal de G contenant S. On note K/k une sous–extension galoisienne finie de k_s déployant T. Alors on a une décomposition Γ_k–équivariante

$$\Phi := \Phi(G \times_k K, T \times_k K) = \Phi(Z_G(S) \times_k K, T \times_k K) \sqcup \Psi \sqcup -\Psi$$

où $R_u(P)\times_k K$ est le sous-groupe de G engendré par les U_β pour β parcourant Ψ. Il existe un ordre sur Φ tel que $\Psi \subset \Phi^+$. L'ensemble Ψ est non vide et est permuté par Γ_k. On note Δ une base de Φ pour cet ordre et $I \subset \Delta$ le sous–ensemble de racines tel que $P \times_k K = P_I$. On a

$$\widehat{T}(K) = \oplus_{\alpha \in \Delta} \mathbb{Z}.\alpha$$

et

$$(\widehat{T/S})(K) = \oplus_{\alpha \in I} \mathbb{Z}.\alpha \subset (\widehat{T})(K).$$

Soit $\beta \in \Psi$. Alors $\beta = \sum_{\alpha \in \Delta} m_\alpha \alpha$ avec $m_\alpha \geq 0$ et il existe une racine $\underline{\alpha} \in \Delta \setminus I$ telle que $m_{\underline{\alpha}} > 0$. Nous prétendons que la restriction à S du k–caractère

$$\gamma := \sum_{\sigma \in \mathrm{Gal}(K/k)} \sigma(\beta) \in \widehat{T}(k)$$

est non nulle. En effet, les $\sigma(\beta)$ appartiennent à Φ_+ et le coefficient de γ en $\underline{\alpha}$ est > 0. Ainsi le tore S admet un caractère non trivial et satisfait donc $S_d \neq 1$. Contradiction.

(2) Soit S'_d un k–tore déployé contenant S_d. Alors on a une inclusion $Z_G(S'_d) \subset Z_G(S_d)$ et le lemme 28.3 indique que $Z_G(S'_d)$ est un k–sous–groupe de Levi d'un k–sous–groupe parabolique de $Z_G(S_d)$.

Si P est minimal, alors $Z_G(S'_d) = Z_G(S_d)$, d'où $S_d = S'_d$ en prenant le centre connexe.

Si P n'est pas minimal, alors $Z_G(S_d)$ admet un k–sous–parabolique propre dont un sous–groupe de Levi s'écrit $Z_{Z_G(S_d)}(S'_d)$ avec $S_d \subsetneq S'_d$. □

Dans la démonstration des propositions 28.1 et 28.5, nous avons utilisé le système de racines relatif $\Phi(G,S)$ à partir d'un k–tore déployé maximal S de G. On peut définir aussi une donnée radicielle relative $(\widehat{S}, R, (\widehat{S})^0, R^\vee)$. Avec quelques modifications mineures, la théorie absolue se généralise. En particulier, on dispose alors de k–sous–groupes paraboliques standards et de la décomposition de Bruhat généralisée par rapport à un k–sous–groupe parabolique minimal P.

28.3. **Réductibilité et isotropie.**

28.7. **Définition.** [12] Soit H un k–groupe algébrique linéaire connexe. On dit que H est réductible si H admet un k-sous–groupe parabolique propre.

On dit que H est isotrope si H admet un k–tore déployé non trivial.

Les notions opposées sont respectivement "irréductible" et "anisotrope". Le k–tore $\mathbb{G}_m$ est isotrope mais irréductible. Les deux notions sont stables sous des isogénies et aussi par extension par un k–groupe unipotent déployé. Les propositions 28.1 et 28.5 donnent lieu aux caractérisations suivantes.

28.8. **Corollaire.** *Soit G un k–groupe réductif.*

(1) *Si G est réductible, alors il est isotrope.*
(2) *Si G est semi-simple, alors réductible $\Longleftrightarrow$ isotrope.*
(3) *G est anisotrope si et seulement si son groupe adjoint G_{ad} est anisotrope et son centre connexe $Z(G)^0$ est anisotrope.*

29. Début de la classification

29.1. **Groupe d'automorphismes des groupes semi-simples.** On fixe un k–groupe de Chevalley G/k muni d'un k–tore déployé T. On note G_{ad} le groupe adjoint de G et T_{ad} son image de T dans G_{ad}. On note Δ une base du système de racines $\Phi(G,T)$ et B le sous–groupe de Borel associé.

29.1. **Proposition.** [Sp, 2.12] *Le foncteur $R \to \mathrm{Aut}_{R-gr}(G \times_k R)$ est représentable par un k–groupe algébrique* $\mathrm{Aut}(G)$. *Il a les propriétés suivantes :*

(1) *Le quotient* $\mathrm{Out}(G) := \mathrm{Aut}(G)/G_{ad}$ *est un k–groupe constant fini.*
(2) *On a une suite exacte de k–groupes algébriques*

$$1 \to T_{ad} \to \mathrm{Aut}(G,B,T) \to \mathrm{Out}(G) \to 1.$$

(3) *On a un isomorphisme* $\mathrm{Aut}\Big(G,B,T,(\mathfrak{u}_\alpha)_{\alpha\in\Delta}\Big) \xrightarrow{\sim} \mathrm{Out}(G)$, *la suite exacte ci-dessus est donc scindée.*

[12] Il existe une définition relative. Si H agit sur un k–groupe algébrique linéaire connexe G, on dit que cette action est réductible, si H normalise un k–sous–groupe parabolique propre Q de G. Ainsi H est réductible si H agit sur lui-même par automorphismes intérieurs de façon réductible.

(4) *Il y a un morphisme naturel* $\mathrm{Out}(G_0) \hookrightarrow \mathrm{Aut}(\Delta)$*, où* Δ *est le diagramme de Dynkin. C'est un isomorphisme si* G *est simplement connexe ou adjoint.*

29.2. **Exemple.** Le groupe SL_n ($n \geq 3$). Il y a alors une suite exacte $1 \to \mathrm{PGL}_n \to \mathrm{Aut}(\mathrm{SL}_n) \to \mathbb{Z}/2\mathbb{Z} \to 1$. La théorie des groupes de Lie compacts nous dit que l'involution de Cartan $X \to {}^tX^{-1}$ définit un scindage de cette suite exacte. Mais celui-ci ne normalise pas le sous–groupe de Borel des matrices triangulaires supérieures. Le scindage donné par la propositon est le conjugué de l'involution de Cartan par la matrice antidiagonale standard.

Par descente galoisienne, les k-formes de G (à isomorphisme près) correspondent à l'ensemble $H^1(k, \mathrm{Aut}(G))$. Pour cette raison, on ne peut éviter les groupes non connexes.

29.2. **Groupes quasi-déployés.** On rappelle la

29.3. **Définition.** Un k–groupe réductif H est quasi-déployé s'il admet un sous–groupe de Borel Q, c'est-à-dire tel que $Q \times_k \overline{k}$ est un sous-groupe de Borel de $H \times_k \overline{k}$.

29.4. **Proposition.** (1) *Les* k*–formes quasi-déployée de* G *sont classifiées par* $H^1(k, \mathrm{Aut}(G, B, T)) \xrightarrow{\sim} H^1(k, \mathrm{Out}(G))$.

(2) *Une* k*-forme de* G *est une* k*–forme intérieure d'une unique* k*–forme quasi-déployée de* G*.*

Démonstration. (1) Notons $H^1_{qd}(k, \mathrm{Aut}(G)) \subset H^1(k, \mathrm{Aut}(G))$ le sous–ensemble des k-formes quasi-déployées de G. La première étape est de voir que

$$\mathrm{Im}\Big(H^1(k, \mathrm{Aut}(G, B, T)) \to H^1(k, \mathrm{Aut}(G))\Big) = H^1_{qd}(k, \mathrm{Aut}(G)).$$

En effet, si $z \in Z^1(k, \mathrm{Aut}(G, B, T))$, alors le k–groupe tordu ${}_zB$ est un sous–groupe de Borel de ${}_zG$; le groupe ${}_zG$ est donc quasi-déployé. Dans l'autre sens, on se donne un cocycle $z \in Z^1(k, \mathrm{Aut}(G))$ tel que $G' := {}_zG$ est quasi-déployé. Il admet un k–sous–groupe de Borel B'. Soit $T' \subset B'$ un k–tore maximal de B'. Alors $(B' \times_k k_s, T' \times_k k_s)$ est un couple de Killing de $G \times_k k_s \overset{\phi}{\xrightarrow{\sim}} G' \times_k k_s$. Par suite, il existe $g \in G(k_s)$ tel que $\phi^{-1}(T', B') = g(B, T)g^{-1}$. Puisque $z_\sigma = \phi^{-1}\, \sigma(\phi)$, on vérifie que $z' = g^{-1}\, z_\sigma\, \sigma(g)$ normalise (B, T). En d'autres mots, $[z]$ provient de $H^1(k, \mathrm{Aut}(G, B, T))$.

La seconde étape est de montrer que $H^1(k, \mathrm{Aut}(G, B, T)) \cong H^1(k, \mathrm{Out}(G))$. On note ρ le scindage de $\mathrm{Out}(G) \to \mathrm{Aut}(G, B, T)$ donné dans la proposition 29.1.(3). L'application associée $\rho_* : H^1(k, \mathrm{Out}(G)) \to H^1(k, \mathrm{Aut}(G, B, T))$ fournit un scindage de $p_* : H^1(k, \mathrm{Aut}(G, B, T)) \cong H^1(k, \mathrm{Out}(G))$ qui est donc scindé surjectif. Pour l'injectivité, il suffit de démontrer que $p_*^{-1}\big([\rho(a)]\big) = [a]$ pour tout $[a] \in H^1(k, \mathrm{Out}(G))$. Cela passe par la suite exacte

$$1 \to T/C(G) \to \mathrm{Aut}(G, B, T) \xrightarrow{p} \mathrm{Out}(G) \to 1.$$

Etant donné $[a] \in H^1(k, \mathrm{Out}(G))$, on tord cette suite exacte par $\rho(a)$

$$1 \to {}_{\rho(a)}(T/C(G)) \to {}_{\rho(a)}\mathrm{Aut}(G,B,T) \to {}_a\mathrm{Out}(G) \to 1.$$

Par "torsion", il y a une bijection entre $p_*^{-1}\big([a]\big)$ et

$$\mathrm{Im}\Big(H^1(k, {}_{\rho(a)}(T/C(G))) \to H^1(k, {}_{\rho(a)}\mathrm{Aut}(G,B,T))\Big).$$

Le point est que le groupe des caractères de $T/C(G)$ est le réseau des racines, i.e. $(\widehat{T/C(G)}) = \oplus_{\alpha\in\Delta}\mathbb{Z}\,\alpha$. L'action de $\rho(a)$ sur ce réseau est une action de "permutation" sur les racines (29.1.(4)). Par suite le module galoisien des caractères de ${}_{\rho(a)}(T/C(G))$ est un Γ_k-module de permutation, d'où ${}_\rho(a)(T/C(G))$ est un k–tore induit. Selon le lemme de Shapiro et le théorème 90 de Hilbert, la cohomologie galoisienne des k–tores induits est triviale, d'où $H^1(k, {}_{\rho(a)}(T/C(G))) = 0$ et $p_*^{-1}([a]) = \{[\rho(a)]\}$.

Enfin, puisque l'application $H^1(k, \mathrm{Aut}(G,B,T)) \cong H^1(k, \mathrm{Out}(G))$ factorise par $H^1(k, \mathrm{Aut}(G)) \cong H^1(k, \mathrm{Out}(G))$, il suit que $H^1(k, \mathrm{Aut}(G,B,T))$ s'injecte dans $H^1(k, \mathrm{Aut}(G))$. On conclut que

$$H^1(k, \mathrm{Aut}(G,B,T)) \cong H^1_{qd}(k, \mathrm{Aut}(G)) \cong H^1_{qd}(k, \mathrm{Aut}(G)).$$

(2) Soit $[z] \in H^1(k, \mathrm{Aut}(G))$ et posons $a = p_*(z) \in Z^1(k, \mathrm{Out}(G))$. La même technique de torsion montre qu'il existe $z' \in Z^1(k, {}_{\rho(a)}G)$ tel que ${}_zG$ est isomorphe à ${}_{z'}\big({}_{\rho(a)}G\big)$. L'unicité du groupe quasi-déployé ${}_{\rho(a)}G$ est une conséquence de (1). □

Si la forme quasi-déployée sous–jacente à une k–forme M de G est déployée, on dit que M est une forme interiéure. Le morphisme $\mathrm{Out}(G) \to \mathrm{Aut}(\Delta)$ donne lieu à une application

$$H^1(k, \mathrm{Out}(G)) \to H^1(k, \mathrm{Aut}(\Delta)) = \mathrm{Hom}_{ct}(\Gamma_k, \mathrm{Aut}(\Delta))/\text{conjugaison}\ .$$

En d'autres mots, on attache à une k-forme de G une action du groupe de Galois Γ_k sur Δ à conjugaison près par $\mathrm{Aut}(\Delta)$. C'est l'action étoile (star action) de Γ_k sur Δ.

30. Cohomologie galoisienne, suite

30.1. **La décomposition de Witt-Tits.**

30.1. **Théorème.** *Soit H un k–groupe algébrique linéaire dont la composante neutre H^0 est un k–groupe de Chevalley. On note Δ_H le diagramme de Dynkin de H et P_I les sous–groupes paraboliques standards de H.*

(1) *Soit $I \subset \Delta_H$. On note $H^1(k, N_H(P_I))_{irr}$ l'ensemble des classes $[z]$ telles que le k–groupe ${}_zP_I$ est irréductible. Alors l'application $H^1\big(k, N_H(P_I)\big)_{irr} \to H^1(k, H)$ est injective.*

(2) *Soient P_{I_1}, ... , P_{I_l} des représentants des $H(k_s)$-classes de conjugaisons de k–sous–groupes paraboliques de H. Alors nous avons la décomposition*

$$\bigsqcup_{j=1,\dots,l} H^1\big(k, N_H(P_{I_j})\big)_{irr} \;\cong\; H^1(k,H).$$

La démonstration est fondée sur l'article de Bruhat-Tits [BT3, section 3].

Démonstration. (1) On se donne deux cocycles $z, z' \in Z^1(k, \mathrm{N}_H(P_I))_{irr}$ ayant même image dans $H^1(k,H)$. Il existe $h \in H(k_s)$ tel que $z'_\sigma = h^{-1}\, z_\sigma\, \sigma(h)$ pour tout $\sigma \in \Gamma_k$. On considère une trivialisation $\phi : H \times_k k_s \cong {}_zH \times_k k_s$ (resp. ϕ') satisfaisant $\phi^{-1}\sigma(\phi) = z_\sigma$ pour tout $\sigma \in \Gamma_k$; on a $(\phi')^{-1} \circ \phi = \mathrm{Int}(h)$. Alors $\phi(P_I)$ (resp. $\phi'(P_I)$) definit un k–sous–groupe parabolique minimal de ${}_zH^0$ (resp. ${}_{z'}H^0$). Puisque $\mathrm{Int}(h)$ produit un k-isomorphisme ${}_zH^0 \cong {}_{z'}H^0$, on voit que $\phi(P_I)$ et $\phi(hP_Ih^{-1})$ sont deux k-sous–groupes paraboliques minimaux de ${}_zH^0$. Le théorème de Borel-Tits énonce que $\phi(P_I)$ et $\phi(hP_Ih^{-1})$ sont conjugués sous ${}_zH^0(k)$. Il existe $g \in H^0(k_s)$ tel que

$$\phi(hP_Ih^{-1}) = \phi(gP_Ig^{-1}) \ \text{ et } \ z_\sigma\sigma(g)z_\sigma^{-1} = g \ \ \forall \sigma \in \mathrm{Gal}(k_s/k).$$

Par suite $n := g^{-1}h \in N_H(P_I)(k_s)$ et la relation $z_\sigma\, \sigma(g)\, z_\sigma^{-1}$ entraîne que

$$z'_\sigma = h^{-1}\, z_\sigma\, \sigma(h) = n^{-1} z_\sigma\, \sigma(n)$$

pour tout $\sigma \in \Gamma_k$. On conclut que $[z] = [z'] \in H^1(k, N_H(P_I))$.

(2)*Deuxième étape : injectivité:* Soient $I, I' \subset \Delta$ figurant dans la liste des I_j et des cocycles $z \in Z^1(k, N_H(P_I))_{irr}$, $z' \in Z^1(k, N_H(P_{I'}))_{irr}$ ayant même image dans $H^1(F,H)$. Alors il existe $h \in H(k_s)$ tel que $z'_\sigma = h^{-1}\, z_\sigma\, \sigma(h)$ pour tout $\sigma \in \Gamma_k$. Alors $\phi(P_I)$ (resp. $\phi'(P_{I'})$) definit un k-sous–groupe parabolique minimal de ${}_zH^0$ (resp. ${}_{z'}H^0$). L'argument ci-dessus indique que $\phi(P_I)$ and $\phi(hP_{I'}h^{-1})$ sont conjugués sous ${}_zH^0(k)$. Ainsi P_I et $P_{I'}$ sont conjugués sous $H(k_s)$ et $I = I'$. L'assertion (1) montre alors que $[z] = [z'] \in H^1(k, N_H(P_I))$.

Troisième étape : surjectivité: Soit $z \in Z^1(k,H)$. On note $\phi : H \times_k k_s \cong {}_zH \times_k k_s$ une trivialisation. Soit P un k–sous–groupe parabolique minimal de ${}_zH^0$. Alors il existe I figurant dans la liste des I_j tel que $P = hP_Ih^{-1}$ avec $h \in H(k_s)$. Ceci signifie que $z_\sigma\, \sigma(h)\, P_I \sigma(h)^{-1}\, z_\sigma^{-1} = hP_Ih^{-1}$ pour tout $\sigma \in \Gamma_k$, d'où

$$h^{-1}\, z_\sigma\, \sigma(h)\, P_I\, \sigma(h)^{-1}\, z_\sigma^{-1}\, h = P_I.$$

Par suite, $h^{-1}\, z_\sigma\, \sigma(h) \in N_H(P_I)(k_s)$. On conclut que

$$[z] \in \mathrm{Im}\Big(H^1(k, N_H(P_I))_{irr} \to H^1(k,H) \Big).$$

□

On peut être plus précis avec le lemme suivant.

30.2. **Lemme.** *Soit $M = R_u(M) \rtimes L$ un k–groupe algébrique linéaire équipé d'une décomposition de Levi où $R_u(M)$ est un k–groupe unipotent déployé. On a alors des bijections naturelles*

$$H^1(k, L) \cong H^1(k, M) \cong H^1(k, M/R_u(M)).$$

30.3. **Lemme.** *Soit U un k–groupe unipotent déployé. Alors toute k–forme de U est unipotent k–déployé.*

En caractéristique nulle (resp. caractéristique libre), cela résulte du lemme 20.7 (resp. la combinaison de [SGA3, XVII.4.1.1 et 4.1.3]).

Démonstration. Il suffit détablir la seconde bijection. La flèche $H^1(k, M) \cong H^1(k, M/R_u(M))$ est scindée, donc surjective. Pour l'injectivité, il faut montrer que $p^{-1}(p([z])) = \{[z]\}$ pour tout $[z] \in H^1(k, M)$. Suivant la technique éprouvée de torsion, on a une suite exacte

$$1 \to {}_zR_u(M) \to {}_zM \overset{zp}{\to} {}_z(M/R_u(M)) \to 1$$

et il revient au même de montrer que ${}_zp_* : H^1(k, {}_zM) \to H^1\bigl(k, {}_z(M/R_u(M))\bigr)$ a un noyau trivial. Le lemme 30.3 montre que ${}_zR_u(M)$ est unipotent k–déployé. Vu que $H^1(k, \mathbb{G}_a) = 0$, on a $H^1\bigl(k, {}_zR_u(M)\bigr) = 1$ par dévissage. on conclut que $\ker({}_zp_*) = 1$. □

30.2. **Classification.** On considère le cas $H = \mathrm{Aut}(G)$ où G désigne toujours un groupe semi-simple de Chevelley. Pour $I \subset \Delta$, on a besoin de décrire le normalisateur $N_G(P_I)$ et ses sous–groupes de Levi. Selon [Sp, 16.3.9.(4)], on définit le k–groupe des I-automorphismes de G par

$$\mathrm{Aut}_I(G) = \mathrm{Aut}(G, P_I, L_I).$$

On a alors une suite exacte

$$1 \to L_I/Z(G) \to \mathrm{Aut}_I(G) \to \mathrm{Out}_I(G) \to 1,$$

où $\mathrm{Out}_I(G) = \mathrm{Out}(G) \cap \mathrm{Aut}(\Delta, I)$. On a aussi

$$\mathrm{Aut}(G, P_I) = U_I \rtimes \mathrm{Aut}_I(G).$$

La décomposition de Witt-Tits prend alors la forme suivante

$$\bigsqcup_{[I] \subset \Delta/\,\mathrm{Out}(G)} H^1(k, \mathrm{Aut}_I(G))_{irr} \;\; \cong \;\; H^1(k, \mathrm{Aut}(G)).$$

On note que l'orbite $\mathrm{Out}(G)\,.I \subset \Delta$ est "codée" dans la décomposition de Witt-Tits, ce qui est un peu moins précis que l'indice de Tits défini cidessous. Revenons sur nos exemples favoris.

30.4. **Exemple. Le théorème de Wedderburn.** Soit A une k–algèbre simple centrale de degré d de classe $[A] \in H^1(k, \mathrm{PGL}_d)$. Alors il existe un unique indice $I \subset \{1, ..., d-1\}$ tel que $[A]$ provienne d'un (unique) $[z] \in H^1(k, L_I)_{irr}$. Un tel L_I est de la forme $\Bigl(\mathrm{GL}_{m_1} \times \cdots \mathrm{GL}_{m_r}\Bigr)/\mathbb{G}_m$ avec $m_1 + .. + m_r = d$. On peut voir à la main (ou ci-dessus avec la notion d'indices éligibles) que les m_i sont égaux. Ainsi L_I est le quotient de $(\mathrm{GL}_m)^r$ par le sous–groupe diagonal $\mathbb{G}_m$. Par torsion galoisienne, il vient

$$ {}_zL_I \cong \mathrm{GL}_1(D)^r/\mathbb{G}_m $$

pour une unique k–algèbre simple centrale D. Puisque ${}_zL_I$ est irréductible, on conclut que D est une algèbre à divisions.

30.5. **Exemple. Le théorème de Witt.** En rang pair, il s'agit du cas du groupe orthogonal $O(2n)$ de la forme quadratique hyperbolique $\sum_{i=1,\dots,n} X_iY_i$. L'ensemble $H^1(k, O(2n))$ classifie les formes quadratiques non dégénérées de rang $2n$. Dans la décomposition, on garde uniquement les sous–groupes paraboliques standards dont un supplément de Levi est $O(2) \times \mathbb{G}_m^{n-1}$, $O(4) \times \mathbb{G}_m^{n-2}$, $\cdots$ $O(2n-2) \times \mathbb{G}_m$, $O(2n)$ (les autres ont des contributions nulles). Alors la décomposition s'écrit

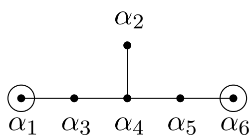
$$ \bigsqcup_{i=1,\dots,n} H^1(k, O(2i))_{irr} \;\cong\; H^1(k, O(n)). $$

ce qui est exactement le théorème de Witt.

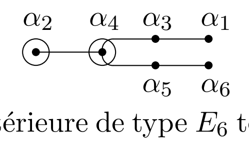
La décomposition de Witt-Tits ramène la classification des groupes semi-simples à celle d'objets irréductibles. Dans une certaine mesure, pour $[z] \in H^1(k, \mathrm{Aut}_I(H))_{irr}$, le k–groupe ${}_zG$ peut être recomposé par son *noyau anisotrope* ${}_zD(L_I)$ qui est un k–groupe semi-simple anisotrope [T1].

30.3. **Indices de Tits.** Si $z \in Z^1(k, G)$, le premier invariant de la k-forme ${}_zG$ de G est sa forme quasi–déployée. La classe de conjugaison géométrique d'un k–sous–groupe parabolique minimal de ${}_zG$ définit un sous–ensemble $I \subset \Delta$. C'est l'indice de Tits de ${}_zG$.

Donnons un exemple de telle donnée. Le diagramme



signifie que l'on a affaire à une k-forme intérieure d'un groupe de type E_6 dont la classe de conjugaison géométrique des k–sous–groupes paraboliques minimaux est $I = \{\alpha_1, \alpha_6\}$. Le diagramme



correspond à une forme extérieure de type E_6 tel que la classe de conjugaison géométrique d'un k–sous–groupe parabolique minimal est $\{\alpha_2, \alpha_4\}$.

Il y a une condition supplémentaire liée à l'action du groupe de Weil sur le système de racines $\Phi = \Phi(G, T)$.

30.6. **Définition.** On dit qu'un sous–ensemble $I \subset \Delta$ est éligible si il est auto–opposé et si pour tout $J \subset \Delta$ la propriété suivante vaut:

$$(*) \qquad J = w\, I \text{ pour } w \in W \text{ si et seulement si } I = J.$$

Enonçons maintenant notre observation.

30.7. **Proposition.** *Soit $I \subset \Delta$ l'indice de Witt-Tits de la k-forme ${}_zG$ de G. Alors I est éligible.*

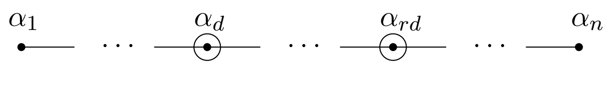
Démonstration. Il est commode de supposer G adjoint. La décomposition de Witt-Tits permet de supposer que le cocycle z est à valeurs dans $\mathrm{Aut}_I(G)$. On considère une trivialisation $\phi : G \times_k k_s \cong {}_zG \times_k k_s$ satisfaisant $\phi^{-1}\sigma(\phi) = z_\sigma$ pour tout $\sigma \in \Gamma_k$. Le k-groupe tordu ${}_zP_I$ est un k–sous–groupe parabolique minimal de ${}_zG$, il est donc de type I.

On a déjà vu que I est auto-opposé. Soit $J \subset \Delta$ tel que $J = w\, I$ pour un certain $w \in W$. Soit $n_w \in N_G(T)(k)$ un relèvement de w. Alors $n_w.L_J = L_I$. En d'autres mots, L_I est un sous–groupe de Levi de P_I et de $Q := n_w P_J n_w^{-1}$. Alors $\phi(Q)$ définit un k–sous–groupe parabolique de ${}_zG$, qui a la même dimension que P_I. Le théorème de Borel-Tits permet d'affirmer que $\phi(P_I)$ et $\phi(Q)$ sont conjugués sous ${}_zG(k)$. Il existe $g \in G(k_s)$ tel que $\phi(Q) = \phi(gP_Ig^{-1})$. Il résulte que $P_I \times_k k_s$ et $Q \times_k k_s$ sont $G(k_s)$-conjugués, d'où $I = J$. □

30.8. **Remarque.** En termes géométriques, les indices W-éligibles sont ceux des groupes paraboliques dont la classe de conjugaison géométrique est déterminée par celle de leur groupe de Levi.

La liste de tous les indices de Tits possibles (pour toutes les formes, pour tous les corps) a été déterminée par Tits [T1]; ces tables figurent aussi à la fin du livre de Springer [Sp].

Nous n'avons pas de tables pour les indices éligibles, on ne peut donc pas comparer ces deux notions. Dans le cas de A_n, les indices éligibles sont précisèment les indices symétriques, c'est-à-dire de la forme



References

[BP] E. Bayer-Fluckiger, R. Parimala, *Galois cohomology of linear algebraic groups over fields of cohomological dimension* ≤ 2, Inventiones Mathematicae **122** (1995), 195-229.

[B] A. Borel, *Introduction aux groupes arithmétiques*, Hermann.

[Bo] A. Borel, *Linear algebraic groups*, second edition, Springer.

[BS] A. Borel et J.-P. Serre, *Théorèmes de finitude en cohomologie galoisienne*, Comment. Math. Helv. 39 (1964), 111–164.

[BSp] A. Borel and T. Springer, *Rationality properties of linear algebraic groups, II*, Tohoku Math. Jour. **20** (1968), 443-497.

[BoT] A. Borel and J. Tits, *Groupes réductifs*, Pub. Math. IHES **27**, (1965), 55–152.

[BoT2] A. Borel and J. Tits, *Eléments unipotents et sous-groupes paraboliques des groupes réductifs, I*, Invent. Math. **12** (1971), 95–104.

[BLR] S. Bosch, W. Lütkebohmert et M. Raynaud, *Néron Models*, Ergebnisse der Mathematik und ihrer Grenzgebiete **21** (1990) Springer-Verlag.

[BAC] N. Bourbaki, *Algèbre commutative*, chapitres 5 à 7, Masson, 1985 ; réimpression inchangée, Springer, 2007.

[BAC2] N. Bourbaki, *Groupes et algèbres de Lie*, chapitres 4 à 6, Masson, 1981.

[BK] M. Borovoi, B. Kunyavskiĭ, *Arithmetical birational invariants of linear algebraic groups over two dimensional geometric fields*, J. Algebra 276 (2004), 292-339.

[BT2] F. Bruhat et J. Tits, *Groupes réductifs sur un corps local II*, Publ. Math. IHES **60** (1984).

[BT3] F. Bruhat, J. Tits, *Groupes algébriques sur un corps local III. Compléments et application à la cohomologie galoisienne*, J. Fac. Sci. Univ. Tokyo **34** (1987), 671–698.

[Ca] R. W. Carter, *Lie algebras of finite and affine type*, Cambridge Studies in Advanced Mathematics **96** (2005), Cambridge University Press. def-red

[CGR] V. Chernousov, P. Gille, Z. Reichstein, *Resolving G-torsors by abelian base extensions*, J. Algebra **296** (2006), 561–581.

[CT] J–L. Colliot–Thélène, *Lectures on linear algebraic groups*, Morningside center, Beijing (2007), http://www.math.u-psud.fr/ colliot/liste-cours-exposes.html

[CTS1] J–L. Colliot–Thélène et J.–J. Sansuc, *La R–équivalence sur les tores*, Ann. Scient. ENS, vol. **10** (1977), 175–230.

[CTS2] J–L. Colliot–Thélène et J.–J. Sansuc, *Principal homogeneous spaces under flasque tori : applications*, J. of Alg. **106** (1987), 148–205.

[CTS3] J–L. Colliot–Thélène et J.–J. Sansuc, *The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group)*, in Proceedings of the International Colloquium on Algebraic groups and Homogeneous Spaces (Mumbai 2004), ed. V. Mehta, TIFR Mumbai, Narosa Publishing House (2007), 113–186.

[CR] C. W. Curtis and I. Reiner, *Methods of representation theory. Vol. I. With applications to finite groups and orders*, Pure and Applied Mathematics, John Wiley and Sons, Inc., New York, 1981.

[DG] M. Demazure et P. Gabriel, *Groupes algébriques*, Masson (1970).

[EGA4] A. Grothendieck (avec la collaboration de J. Dieudonné), *Eléments de Géométrie Algébrique IV*, Publications mathématiques de l'I.H.É.S. no 20, 24, 28 and 32 (1964 - 1967).

[EM] S. Endo, T. Miyata, *On a classification of function field of algebraic tori*, Nagoya Math. J. **56** (1974), 85–104.

[FH] W. Fulton et J. Harris, *Representation theory. A first course*, Graduate Texts in Mathematics **129** (1991), Springer.

[GS] P. Gille, T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics **101** (2006), Cambridge University Press.

[Ha] D. Harari, *Cours fondamental de géométrie algébrique, Orsay, 2007/2008*, http://www.math.u-psud.fr/ harari/enseignement/geoalg/

[H1] J. Humphreys, *Introduction to Lie algebras and representation theory*, Springer (1972).

[H2] J. Humphreys, *Linear algebraic groups*, Springer (1975).

[H3] J. Humphreys, *Conjugacy Classes in Semisimple Algebraic Groups*, AMS, 1995.

[Km] T. Kambayashi, *On the absence of nontrivial separable forms of the affine plane*, J. Algebra **35** (1975), 449–456.

[K1] M. Kneser, *Galoiskohomologie halbeinfacher algebraischer Gruppen über p-adischen Körper*, I, Math. Zeit. **88** (1965), 555-563; II, Math. Zeit. **89** (1965), 250-272.

[K2] M. Kneser, *Lectures on the Galois cohomology of the classical groups*, Tata Institute.

[KMRT] M. Knus, A.S. Merkurjev, M. Rost, J.-P. Tignol, *The Book of Involutions*, AMS Colloquium Publications, Vol. 44, 1998, 593 pp.

[KT] M. Knus, A.S., J.-P. Tignol, *Quartic exercises* Int. J. Math. Math. Sci. **68** (2003), 4263–4323.

[Ko] R. Kottwitz, *Rational conjugacy classes in reductive groups*, AMS, 1995.

[Ku] B. Kunyavskiĭ, *Tores algébriques de dimension 3*, traduction anglaise dans Selecta Math. Soviet. **21** (1990), 1–21.

[KS] B. Kunyavskiĭ, A. Skorobogatov, *Weak approximation in algebraic groups and homogeneous spaces*, Contemp. Math. 131 (1992), Part 3, 447-451.

[J] J. Jahnel, *The Brauer-Severi Variety Associated with a Central Simple Algebra: A Survey*, prépublication (2000), serveur LAGRS.

[La] T. Y. Lam, *Introduction to quadratic forms over fields*, AMS (2005).

[Lg] S. Lang, *Algebraic groups over finite fields*, American J. of Math. **78** (1956), 555-563.

[Mt] O. Mathieu, *Classification des algèbres de Lie simple*, Séminaire Bourbaki No. 858 (Vol. 1998/99), Astérisque **266** (2000).

[Mi] J. S Milne, *Algebraic groups and arithmetic groups*, page personnelle de l'auteur.

[Mo] G. D. Mostow, *Fully reducible subgroups of algebraic groups*, American Journal of Mathematics **78** (1956), 200–221.

[N] Ngô Bao Châu, *Groupes algébriques et schémas en groupes*, notes de cours, http://www.math.u-psud.fr/ ngo/GR.html

[Oo] F. Oort, *Algebraic group schemes in characteristic zero are reduced*, Invent. Math. **2** (1966), 79–80.

[PR] V.P. Platonov, A.S. Rapinchuk, *Algebraic groups and number theory*, Academic Press, 1994.

[Po] P. Polo, *Notes de cours de M2 (2006 et 2007): Groupes algébriques et groupes de Lie I*, http://www.math.jussieu.fr/ polo/M2/

[R] M.S. Raghunathan, *Tori in quasi-split groups*, J. Ramanujan Math. Soc. **19** (2004), 281-287.

[Sa] D. J. Saltman, *Retract rational fields and cyclic Galois extensions*, Israel J. Math. **47** (1984), 165–215.

[Sc] R. Scharlau, *Quadratic and Hermitian forms*, Springer.

[SB] G. Schwarz et M. Brion, *Théorie des invariants et géométrie des variétés quotients*, Hermann (2000).

[Sz] E. Szabó, *Severi-Brauer varieties*, preprint.

[SGA1] *Séminaire de Géométrie algébrique de l'I.H.É.S., Revêtements étales et groupe fondamental, dirigé par A. Grothendieck*, Lecture Notes in Math. 224. Springer (1971).

[SGA3] *Séminaire de Géométrie algébrique de l'I.H.É.S., 1963-1964, schémas en groupes, dirigé par M. Demazure et A. Grothendieck*, Lecture Notes in Math. 151-153. Springer (1970).

[S1] J.-P. Serre, *Cohomologie galoisienne*, LN 5, 5-ième édition, Springer, 1997.

[S2] J.-P. Serre, *Groupes algébriques et corps de classes*, 2-ième édition, Hermann.

[Sh] I. R. Shafarevich, On some infinite-dimensional groups, Rend. Mat. e Appl. **25** (1966), 208–212.

[Sp] T.A. Springer, *Linear Algebraic Groups*, second edition (1998), Birkäuser.

[St] R. Steinberg, *Regular conjugacy classes in algebraic groups*, Pub. Math. IHES **25** (1965), 49–80.

[Ta] K.-I. Tahara, On the finite subgroups of $GL_3(\mathbb{Z})$, Nagoya Math. J. **41** (1971), 169–209.

[TY] P. Tauvel et R.W.T. Yu, *Lie algebras and algebraic groups*, Springer (2006).

[T1] J. Tits, *Classification of algebraic semisimple groups*, Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), 33–62 Amer. Math. Soc. (1966).

[T2] J. Tits, *Représentations linéaires irréductibles d'un groupe rductif sur un corps quelconque*, J. reine ang. Math. 247 (1971), 196-220.

[T3] J. Tits, *Lecture on algebraic groups*, rédigé par A. Winter, Yale university Press (1967).

[T4] J. Tits, *Reductive groups over local fields*, Proceedings of Symposia in Pure Mathematics (Corvallis). Vol. 33, part 1 (1979), 29-69, AMS.

[T5] J. Tits, *Strongly inner anisotropic forms of simple algebraic groups*, Journal of. Algebra **131** (1990), 648-677.

[V] V.I. Voskresenskiĭ, *Algebraic Groups and their birational invariants*, AMS, 1998.

[Wa] W. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics **66** (1979), Springer.

[W] A. Weil, *Foundations of Algebraic Geometry*, American Mathematical Society (1962).

UMR 8552 du CNRS, DMA, Ecole Normale Supérieure, F-75005 Paris, France
E-mail address: `Philippe.Gille@ens.fr`