Structure des points rationnels des groupes réductifs sur les corps quelconques

Benoit Loisel

24 octobre 2014

Résumé

Lobjectif de cet exposé est de pouvoir énoncer l'existence d'un système de Tits pour le groupe $G(k)$ des points rationnels d'un groupe réductif G défini sur un corps k quelconque. On veut également disposer de théorèmes de conjugaisons par les points rationnels. Je commencerai par attirer l'attention sur des questions de corps de définition et des critères galoisiens, puis je donnerai des théorèmes de conjugaison sur k. Enfin, je parlerai de déploiement des groupes réductifs, et donnerai un système de Tits pour les points rationnels.

1 Questions de corps de définition

1.1 Sous-variétés k-fermées et définies sur k

On considère l/k une extension de corps quelconque.

1.1.1 Définition. Si $X = \mathrm{Spec}(A)$ est un k-schéma affine représenté par une k-algèbre, on peut toujours le considérer comme un l-schéma affine par extension des scalaires et on note $X_l = \mathrm{Spec}(A \otimes_k l)$.

Soit $X = \mathrm{Spec}(A)$ est un l-schéma affine représenté par une l-algèbre A. Une k-structure sur A est une sous-k-algèbre A_k qui vérifie l'égalité $A = A_k \otimes_k l$. On dit alors que $X_k = \mathrm{Spec}(A_k)$ est une k-forme de X et que X est défini sur k lorsque cela existe.

Sous cette condition, si Z est un sous-schéma fermé de X, on dispose de l'idéal $J = \mathcal{J}(Z) \subset A$ qui le caractérise. On note $J_k = J \cap A_k$. On dit que Z est k-fermé lorsque $J = \sqrt{J_k A}$ et que Z est défini sur k lorsque $J = J_k A$.

1.1.2 Proposition. *Si V est une l-variété définie sur k et si Z est une sous-variété k-fermée de V, alors on a équivalence entre :*
(i) Z est définie sur k,
(ii) $k[Z] \otimes_k l$ est réduite,
(iii) $k(Z) \otimes_k l$ est réduite.

1.1.3 Remarque. Lorsque k est parfait, les notions « être k-fermé » et « être défini sur k » coïncident.

Action du groupe de Galois :
On suppose désormais que l'extension l/k est galoisienne et on note $\Gamma = \mathrm{Gal}(l/k)$ son groupe de Galois.

Si R est une k-algèbre, alors on peut définir une action continue et semi-linéaire de Γ sur la l-algèbre $R \otimes_k l$ par la formule suivante sur les tenseurs simples :

$$\gamma \cdot (f \otimes \lambda) = f \otimes \gamma(\lambda) \quad \forall \gamma \in \Gamma \, \forall f \in R \forall \lambda \in l$$

Notons également $\gamma_R : R \otimes_k l \to R \otimes_k l$ l'image de γ ainsi définie.

Réciproquement, si Γ ait continument et semi-linéairement sur une l-algèbre B alors la sous-k-algèbre notée B^Γ des points fixes de B sous l'action de Γ est une k-structure de B.

En particulier, lorsque V est une k-variété représentée par une k-algèbre A et R est une k-algèbre quelconque (on prend $R = k$ si l'on s'intéresse par exemple aux points rationnels de V), alors Γ agit sur les points $V(R)$ par l'action naturelle :

$$\gamma \cdot g = \gamma_R \circ g \circ \gamma_A^{-1}$$

Cette action fait également sens sur les sous-l-algèbres de $A \otimes_k l$ et on a un premier critère galoisien :

1.1.4 Proposition. *Soit X une variété définie sur k et Y une sous-variété fermée de X. Alors Y est définie sur k si et seulement si Y est définie sur l et Y est stable par l'action de Γ.*

1.2 Radical unipotent

Dans toute la suite, G désignera un groupe algébrique affine connexe et défini sur k.

1.2.1 Définition. On appelle radical unipotent de G et on note $\mathcal{R}_u(G_{\overline{k}})$, ou plus simplement $\mathcal{R}_u(G)$, le plus grand sous-groupe distingué fermé connexe unipotent dans $G_{\overline{k}}$. C'est une notion « géométrique », c'est-à-dire qu'elle est définie après extension des scalaires à la clôture algébrique $\overline{k}$ du corps de base.

On dit que G est réductif lorsque $\mathcal{R}_u(G)$ est trivial.

1.2.2 Proposition. *En général, $\mathcal{R}_u(G)$ est défini sur une extension finie purement inséparable de k.*

Démonstration. Notons p la caractéristique de k, définissons k_p la clôture parfaite de k et $\Gamma = \mathrm{Gal}(\overline{k}/k_p)$. En faisant agir Γ, on remarque que le radical unipotent $\mathcal{R}_u(G)$ est toujours k-fermé et défini sur k_p par le critère galoisien. Donc $\mathcal{R}_u(G)$ est défini sur k lorsque k est parfait. On peut donc supposer que k est imparfait de caractéristique $p > 0$. Notons $J = \mathcal{J}(\mathcal{R}_u(G)_{k_p})$, c'est un idéal de l'algèbre noethérienne $k[G] \otimes_k k_p$, donc J est engendré par un nombre fini d'éléments que l'on peut prendre de la forme $f \otimes \lambda$. Chaque λ appartient à un sous-corps $k^{p^{-n}}$ de k_p pour un certain $n \in \mathbb{N}$, donc $\mathcal{R}_u(G)$ est défini sur un certain $k^{p^{-N}}$ pour un $N \in \mathbb{N}$ assez grand. $\square$

1.2.3 Remarque. On ne peut pas dire mieux en général. Certains exemples peuvent se construire en utilisant la restriction de Weil.

1.3 Tores et poids

Tores :

1.3.1 Définition. On appelle tore un groupe algébrique diagonalisable connexe ou, de manière équivalente, un groupe algébrique isomorphe à un produit fini de $\mathbb{G}_m$ lorsqu'on passe à la clôture algébrique.

Étant donné un tore T, on appelle $X^*(T) = \mathrm{Hom}_{gr-alg}(T, \mathbb{G}_m)$ son groupe des caractères et $X_*(T) = \mathrm{Hom}_{gr-alg}(\mathbb{G}_m, T)$ son groupe des cocaractères.

1.3.2 Remarque. On peut interpréter $X^*(T)$ et $X_*(T)$ comme des $\mathbb{Z}$-modules qui sont en dualité par un certain crochet de dualité.

1.3.3 Définition. Un tore T est dit déployé sur k si son groupe des caractères définis sur k, noté $X^*(G)_k$, engendre $\overline{k}[G]$ comme $\overline{k}$-module, c'est-à-dire qu'il a « beaucoup » de caractères définis sur k. À l'inverse, T est dit anisotrope sur k si $X^*(G)_k$ est trivial.

1.3.4 Exemple. Si $k = \mathbb{R}$, alors $\mathbb{G}_{m,\mathbb{R}}$ est déployé sur $\mathbb{R}$ alors que $SO(2)_\mathbb{R}$ est anisotrope sur $\mathbb{R}$. On peut remarquer que ces deux tores sont deux $\mathbb{R}$-formes du même tore $\mathbb{G}_{m,\mathbb{C}}$.

1.3.5 Théorème. *Un tore défini sur k se déploie toujours sur une extension finie séparable de k.*

Poids :

1.3.6 Définition. Si T est un tore de G, il opère par conjugaison sur G et en différentiant cette action, on obtient une action appelée action adjointe de T sur l'algèbre de Lie $\mathfrak{g}$ de G. On la note $\mathrm{Ad} : S \to gl(\mathfrak{g})$.

Sous cette action, l'algèbre de Lie $\mathfrak{g}$ se décompose en somme directe d'espaces propres $\mathfrak{g} = \bigoplus_{\alpha \in X^*(T)} \mathfrak{g}_\alpha$, où $\mathfrak{g}_\alpha = \{X \in \mathfrak{g}\,,\ \forall t \in T\ \mathrm{Ad}(t)(X) = \alpha(t)X\}$

On appelle poids de G sous l'action de T tout caractère non nul $\alpha \in X^*(T) \setminus \{0\}$ tels que l'espace propre associé $\mathfrak{g}_\alpha$ est non nul et on note $\Phi(G,T)$ l'ensemble des poids.

On peut énoncer un second critère galoisien qui fait intervenir l'existence de tores maximaux.

1.3.7 Proposition. *Si T est un tore maximal de G défini sur k et si H est un sous-groupe connexe fermé dans G et normalisé par T, alors on a équivalence entre*

(i) H est défini sur k.

(ii) H est k-fermé.

(iii) $(H \cap T)^\circ$ est k-fermé et $\Phi(H,T)$ est Γ-invariant.

2 Conjugaisons rationnelles

2.1 Ce qui a lieu dans le cadre algébriquement clos

Par définition un sous-groupe de Borel est un sous-groupe de G qui est connexe résoluble et maximal pour ces propriétés. Ces groupes sont caractérisés par le fait qu'ils sont minimaux parmi les sous groupes fermés P de G pour lesquels la variété quotient G/P est propre. Ces groupes P sont appelés sous-groupes paraboliques.

Par définition, un tore maximal est toujours inclus dans un sous-groupe de Borel et les sous-groupes de Borel contiennent des tores maximaux de G. En faisant agir B sur la variété propre G/B et avec un théorème de point fixe, on peut en déduire le fait que les sous-groupes de Borel sont deux à deux conjugués, et qu'il en est donc de même pour les tores maximaux. Ce résultat est utile notamment pour affirmer que l'ensemble des poids $\Phi(G,T)$ est défini à isomorphisme près et ne dépend pas du choix d'un tore maximal T de G.

Lorsqu'on veut obtenir des résultats pour les points rationnels, il est naturel de s'intéresser aux tores déployés sur k maximaux, ce sont ceux pour lesquels on a une chance qu'il y ait suffisamment de caractères définis sur k pour décrire le groupe. On espère alors obtenir un théorème de conjugaison par les points rationnels pour ces tores.

On veut donc travailler avec des sous-groupes fermés de G définis sur k et établir des théorèmes de conjugaison par $G(k)$ pour ces sous-groupes. Un théorème de densité de $G(k)$ dans G est une bonne raison de croire qu'il y aura alors suffisamment de points rationnels pour conjuguer.

2.2 Unirationnalité et densité

2.2.1 Définition. On dit que V est unirationnelle sur k si $k(V)$ est un sous-corps d'une extension purement transcendante de k.

On a en ligne de mire la proposition suivante :

2.2.2 Proposition. *Soit V une k-variété irréductible. On suppose que k est infini et que V est unirationnelle sur k. Alors $V(k)$ est dense dans V.*

2.2.3 Remarque. Lorsque k est parfait, G est unirationnel sur k.

2.2.4 Lemme. *Les tores définis sur k sont unirationnels sur k. Ils sont en fait rationnels sur k.*

2.2.5 Théorème (dû à Grothendieck)**.** *Lorsque G est de plus réductif, il est unirationnel sur k.*

Ce théroème repose sur l'utilisation d'éléments réguliers et sur un autre théorème également dû à Grothendieck et également par Rosenlicht dans le cas des corps parfaits :

2.2.6 Théorème (dû à Rosenlicht et Grothendieck)**.** *G contient un tore maximal qui est défini sur k.*

On a donc le corollaire qui nous intéresse, à savoir

2.2.7 Corollaire. *Les points rationnels $G(k)$ forment une partie dense de G.*

2.3 Le cas des corps finis

Dans toute la suite, on supposera désormais de plus que G est réductif.

On note $k = \mathbb{F}_q$ et F_q le morphisme de Frobenius. Le cas des corps finis est le seul cas dans lequel on n'a pas la densité des points rationnels. En utilisant une application séparable $f : g \mapsto F_q(g)g^{-1}$, on parvient à construire des sous-groupes de Borel et des tores Galois stables qui auront le bon goût d'être défini sur $\mathbb{F}_q$. Par des résultats dûs à S. Lang, G admet des sous-groupes de Cartan, de Borel et des tores maximaux définis sur k. Les sous-groupes de Borel définis sur k sont de plus deux à deux $G(k)$-conjugués, ainsi que les tores maximaux définis sur k.

2.4 Sous-groupes paraboliques définis sur k

Dans toute la suite, on supposera désormais de plus que G est réductif.

2.4.1 Définition. Un sous-groupe P de G est dit parabolique s'il est fermé et tel que la variété G/P est propre.

2.4.2 Exemple. Un exemple qui servira de fil rouge aux différentes définitions est celui de $G = GL_n$. Un sous-groupe de matrices triangulaires supérieures $P = \begin{pmatrix} \boxed{*} & & * \\ & \ddots & \\ 0 & & \boxed{*} \end{pmatrix}$ est un sous-groupe parabolique de G. De plus, son radical unipotent est décrit par $\mathcal{R}_u(P) = \begin{pmatrix} \boxed{\mathrm{id}} & & * \\ & \ddots & \\ 0 & & \boxed{\mathrm{id}} \end{pmatrix}$.

Lorsque H est un sous-groupe fermé de G, on veut pouvoir scinder la projection $H \to H/\mathcal{R}_u(H)$. Ceci est par exemple possible lorsque H est un sous-groupe parabolique d'un groupe réductif G, pour une raison qui est que les groupes réductifs et leurs sous-groupes paraboliques se comprennent bien grâce aux racines (c'est-à-dire aux poids définis par un tore maximal). On obtient ce qui s'appelle une décomposition de Levi et on peut alors voir H comme produit semi-direct $H = L \ltimes \mathcal{R}_u(H)$ d'un certain sous-groupe L qu'on appelle facteur de Levi par le radical unipotent de H.

2.4.3 Exemple. $L = \begin{pmatrix} \boxed{*} & & 0 \\ & \ddots & \\ 0 & & \boxed{*} \end{pmatrix}$ est un facteur de Levi du sous-groupe parabolique $P = \begin{pmatrix} \boxed{*} & & * \\ & \ddots & \\ 0 & & \boxed{*} \end{pmatrix}$

On se demande alors ce qu'il en est sur le corps de base. Les résultats qui suivent découlent de l'existence d'un tore maximal défini sur k et normalisant certains sous-groupes.

2.4.4 Proposition (Borel-Tits). *Si P est un sous-groupe parabolique défini sur k, alors son radical unipotent $\mathcal{R}_u(P)$ est défini sur k et il existe un facteur de Levi de P qui est défini sur k. De plus, les facteurs de Levi de P sont deux à deux conjugués par les éléments de $\mathcal{R}_u(P)(k)$ et l'action est simplement transitive.*

Ceci est un premier théorème de conjugaison par les points rationnels.

2.4.5 Définition. Deux sous-groupes paraboliques P et P' sont dit opposés si $L = P \cap P'$ est un sous-groupe de Levi commun à P et P'.

2.4.6 Proposition. *Lorsque P et P' sont définis sur k et opposés, $L = P \cap P'$ est défini sur k.*

2.4.7 Remarque. Dans le cas de deux sous-groupes de Borel opposés $B \cap B'$ est un tore maximal commun à B et B'.

2.4.8 Proposition. *Si P est un sous-groupe parabolique défini sur k et L un sous-groupe de Levi défini sur k de P, alors il existe un unique sous-groupe parabolique P' opposé à P par rapport à L qui de plus est défini sur k.*

2.4.9 Proposition (Description des facteurs de Levi des sous-groupes paraboliques)**.** *Les centralisateurs dans G des tores k-déployés sont des facteurs de Levi des sous-groupes paraboliques définis sur k et ce sont les seuls. De plus, un sous-groupe parabolique défini sur k est minimal (parmi ceux définis sur k) si et seulement si ses sous-groupes de Levi sont des centralisateurs de tores k-déployés maximaux.*

2.4.10 Exemple. Pour le tore k-déployé $S = \begin{pmatrix} \boxed{*\mathrm{id}} & & 0 \\ & \ddots & \\ 0 & & \boxed{*\mathrm{id}} \end{pmatrix}$ des matrices scalaires par blocs, on a $\mathcal{Z}_G(S) = \begin{pmatrix} \boxed{*} & & 0 \\ & \ddots & \\ 0 & & \boxed{*} \end{pmatrix}$.

2.5 Théorèmes de conjugaison sur k

2.5.1 Théorème. *On suppose que le corps k est infini.*

(1) Les sous-groupes paraboliques définis sur k minimaux de G sont conjugués par des éléments de $G(k)$.

(2) Les tores k-déployés maximaux de G sont conjugués par des éléments de $G(k)$.

Remarquons que ces théorèmes de conjugaison ont déjà été énoncé dans le cas des corps finis.

Démonstration.

(1) Soit P et Q deux sous-groupes paraboliques définis sur k minimaux. Notons $M(P,Q) = \{g \in G\,,\, P \text{ et } {}^gQ \text{ sont opposés}\}$ où ${}^gQ = gQg^{-1}$. C'est un ouvert dense de G car la condition d'être opposé est générique, quels que soient P et Q. Comme G est réductif et k est infini, $G(k)$ est Zariski-dense dans G. Ainsi, il existe un point rationnel $g \in G(k) \cap M(P,P) \cap M(Q,P)$ car c'est une intersection finie d'ouverts denses (non vides) avec une partie dense.

Soit $L_1 = P \cap {}^gP$ et $L_2 = P \cap {}^gQ$. Ce sont deux sous-groupes de Levi définis sur k de P, ils sont conjugués par un élément $x \in \mathcal{R}_u(P)(k)$, disons $L_2 = {}^xL_1$. Alors $P \cap {}^gQ = L_2 = P \cap {}^{xg}P$. Par unicité du sous-groupe parabolique opposé contenant un sous-groupe de Levi donné, on a ${}^{xg}P = {}^gQ$. Ce qui conclut.

(2) Soit S et S' deux tores k-déployés maximaux. Soit $L = \mathcal{Z}_G(S)$ et $L' = \mathcal{Z}_G(S')$, ce sont des sous-groupes de Levi défini sur k de deux sous-groupes paraboliques définis sur k contenant chacun l'un d'eux, notés respectivement P et P', qui sont des sous-groupes paraboliques minimaux car S et S' sont des tores k-déployés maximaux. Par (1), il existe $g \in G(k)$ tel que ${}^gP' = P$. On

sait alors que ${}^{g}L'$ et L sont deux sous groupes de Levi définis sur k de P, donc qu'ils sont $\mathcal{R}_u(P)(k)$-conjugués par un éléments x ; mettons ${}^{xg}L' = L$. Soit $S'' = {}^{y}S'$ avec $y = xg \in G(k)$. Le centre de L' contient S' par définition donc le centre de L contient S'' par conjugaison et contient aussi S par définition. Or, le centre de $\mathcal{Z}_G(S)$ admet un unique plus grand sous-tore k-déployé (par commutativité) donc par maximalité $S = S''$. Ce qui conclut. $\square$

3 Déploiement des groupes réductifs

3.0.2 Définition et théorème. Soit T un tore maximal défini sur k de G et $\alpha \in \Phi(G,T)$ une racine. L'unique sous-groupe fermé normalisé par T défini sur k de G, noté U_α tel que $\mathrm{Lie}(U_\alpha) = \mathfrak{g}_(\alpha) = \bigoplus_{\beta \in \mathbb{R}_+^* \alpha} \mathfrak{g}_\beta$ est appelé groupe radiciel à un paramètre.

Ces groupes existent toujours lorsque $k = \overline{k}$, sont de dimension 1 et sont caractérisés par l'existence d'un isomorphisme $\theta_\alpha : \mathbb{G}_a \to U_\alpha$ satisfaisant $\forall t \in T,\ \forall x \in \mathbb{G}_a,\ t\theta_\alpha(x)t^{-1} = \theta_\alpha(\alpha(t)x)$. Cet isomorphisme est unique à multiplication par une constante de $\overline{k}$ près.

3.0.3 Remarque. Lorsque le corps k n'est pas de caractéristique nulle, il n'est pas évident de pouvoir relever l'espace propre $\mathfrak{g}_\alpha$ de l'algèbre de Lie en un sous-groupe de G. Néanmoins, U_α peut être défini en considérant la partie unipotente d'un sous-groupe de Borel d'un sous-groupe $G_\alpha = \mathcal{Z}_G((\ker\alpha)^\circ)$ de G.

3.0.4 Définition. On dit que G est déployé sur k s'il existe un tore maximal T de G qui est k-déployé, si les groupes radiciels à un paramètre U_α sont définis sur k et s'il existe des isomorphismes $\theta_\alpha : \mathbb{G}_a \to U_\alpha$ définis sur k pour tout $\alpha \in \Phi(G,T)$.

Le couple $(T, (\theta_\alpha)_{\alpha \in \Phi(G,T)})$ est appelé une donnée de déploiement pour G.

3.0.5 Théorème (Cartier)**.** *Si G admet un tore maximal T qui est k-déployé. Alors G est déployé sur k.*

En particulier, comme un tore défini sur k se déploie sur une extension finie séparable de k, les groupes réductifs se déploient eux aussi sur des extensions finies séparables du corps de base.

3.0.6 Exemple (Contre-exemple)*.* Soit $G = SL_n(\mathbb{C})$ que l'on considère comme groupe sur $\mathbb{R}$. C'est un groupe réductif. Les matrices diagonales à coefficients réels forment un tore $\mathbb{R}$-déployé maximal qui n'est pas un tore maximal. Par conjugaison des tores $\mathbb{R}$-déployés maximaux, ce groupe ne peut pas être déployé sur $\mathbb{R}$. Ses groupes radiciels à un paramètre sont de dimension 2.

4 Donnée combinatoire : système de Tits des points rationnels d'un groupe réductif

4.0.7 Définition. On dit qu'un groupe réductif est isotrope sur k s'il admet un tore k-déployé maximal non trivial, et qu'il est anisotrope sur k dans le cas contraire.

On suppose désormais, de plus, que G est isotrope et que S est un tore k-déployé maximal de G.

4.0.8 Définition. On appelle k-racines, et on note ${}_k\Phi$, l'ensemble $\Phi(G, S) \subset X^*(S)_k$.

On appelle groupe de Weyl relatif à k de G le quotient ${}_kW = \mathcal{N}_G(S)/\mathcal{Z}_G(S)$.

On note ${}_k\Delta$ une base du système de racines ${}_k\Phi$.

4.0.9 Théorème. *Soit P un sous-groupe parabolique défini sur k minimal de G contenant $\mathcal{Z}_G(S)$. Soit $N = \mathcal{N}_G(S)$. On définit $R = \{s_\alpha\,,\ \alpha \in {}_k\Delta\}$ et ${}_k\mathcal{T} = (G(k), P(k), N(k), R)$. Alors ${}_k\mathcal{T}$ est un système de Tits.*

Table des matières

Références

[Bor91] Armand Borel. *Linear algebraic groups.* Graduate texts in mathematics 126. Springer, 2nd edition, 1991.

[Spr98] T.A. Springer. *Linear algebraic groups.* Progress in Mathematics. Birkhäuser Boston, 2nd edition, 1998.

[Tit65] Armand Borel ; Jacques Tits. Groupes réductifs. *Publications Mathématiques de L'IHÉS*, 27, 1965.