Introduction au Domaine de Recherche

À propos des groupes algébriques semi-simples

Alexandre Lourdeaux

26 octobre 2015

Introduction

Dans cet IDR, on va s'intéresser aux groupes algébriques affines semi-simples sur un corps quelconque.

Un groupe algébrique est une variété algébrique munie d'une loi de groupe compatible à la structure de variété. Dans l'idée, un groupe algébrique est le lieu des zéros d'une famille de polynômes sur lequel on définit une loi de groupe à l'aide de formules polynomiales.

La famille des groupes algébriques se divise essentiellement en deux grandes sous-familles. D'une part, la sous-famille des groupes algébriques affines : ce sont les sous-groupes des groupes linéaires GL_n. D'autre part, les variétés abéliennes : ce sont les groupes dont les variétés sous-jacentes sont projectives, non-affines ; elles généralisent les courbes elliptiques en dimension supérieure.

Les groupes algébriques affines semi-simples généralisent les groupes classiques comme $\mathrm{SL}_n(k)$, $\mathrm{SO}(q)$ ou encore Sp_n sur un corps quelconque. Le problème est alors de les classifier.

Ce qui aide à la compréhension de la structure d'un groupe semi-simple G donné, est avant tout l'existence de sous-groupes particuliers (tores déployés, sous-groupes de Borel et paraboliques) qui permettent de décrire G combinatoirement, profitant de ce que l'on connaît déjà sur les systèmes de racines issus de l'étude des algèbres de Lie semi-simples complexes.

L'objectif de ce texte est de présenter les groupes algébriques en termes de foncteurs en groupes, d'exposer l'étude combinatoire des groupes semi-simples sur un corps séparablement clos, puis d'introduire l'aspect cohomologique de la classification des groupes semi-simples.

1 Groupes algébriques affines

Soit k un corps tout à fait quelconque.

1.1 Schémas en groupes affines

En toute généralité, un *k-schéma en groupes* est un k-schéma $G \to k$ sur lequel sont définies des opérations

$$\begin{array}{rccc l}
\mu : & G \times_k G & \to & G \otimes_k A & \text{(multiplication)}, \\
\imath : & G & \to & G & \text{(inverse)}, \\
\epsilon : & k & \to & G & \text{(unité/neutre)},
\end{array}$$

vérifiant les axiomes de groupes habituels.

Cependant, comme on ne s'intéresse qu'aux groupes affines, pour nous G est un k-schéma affine $\mathrm{Spec}(A) \to k$ caractérisé par une k-algèbre A. Dans ce cas, les opérations μ, $\imath$ et ϵ correspondent de manière univoque à des opérations

$$\begin{array}{rccc l}
c : & A & \to & A \otimes_k A & \text{(co-multiplication)}, \\
i : & A & \to & A & \text{(co-inverse)}, \\
u : & A & \to & k & \text{(co-unité / co-neutre)},
\end{array}$$

vérifiant les relations duales des axiomes de groupes :

$$\begin{tikzcd}
A \otimes_k A \otimes_k A & A \otimes_k A \arrow[l, "c \otimes \mathrm{id}_A"'] \, , \\
A \otimes_k A \arrow[u, "\mathrm{id}_A \otimes c"] & A \arrow[l, "c"] \arrow[u, "c"']
\end{tikzcd}
\qquad
\begin{tikzcd}
k \otimes_k A & A \otimes_k A \arrow[l, "u \otimes \mathrm{id}_A"'] \, , \\
A \arrow[u, equal] \arrow[r, equal] & A \arrow[u, "c"']
\end{tikzcd}$$

$$\begin{tikzcd}
A & A \otimes_k A \arrow[l, "m_A(i \otimes \mathrm{id}_A)"'] \\
k \arrow[u] & A \arrow[l, "u"] \arrow[u, "c"']
\end{tikzcd}$$

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

Définition 1.1. Une algèbre munie de telles opérations est appelée *k-algèbre de Hopf.*

Inversement, une k-algèbre de Hopf A détermine uniquement des opérations μ, $\imath$, et ϵ sur $\mathrm{Spec}(A)$ en en faisant un k-schéma en groupes affine.

Une manière plus systématique et plus claire pour manipuler un k-schéma en groupes affine G est de regarder son foncteur des points, car alors une définition ou propriété algébrique sur G est vérifiée si, et seulement si, elle l'est sur toute une famille de groupes abstraits.

D'abord notons $m_R : R \otimes_k R \to R$ la multiplication de la k-algèbre R.

Proposition 1.2. - *Soit* $G = \operatorname{Spec}(A)$ *est un* k*-schéma en groupes affine.*
Alors pour toute k*-algèbre* R*, l'expression*

$$f \cdot g := m_R \circ (f \otimes g) \circ c$$

pour tous $f,\ g \in \operatorname{Hom}_{Alg_k}(A, R)$*, définit une loi de groupe sur* $\operatorname{Hom}(A, R)$ *faisant de* $R \mapsto \operatorname{Hom}(A, R)$ *un foncteur en groupes* $Alg_k \to Grp$.

- Inversement, tout foncteur $Alg_k \to Grp$ *représentable et représenté par une* k*-algèbre* A*, détermine de manière unique des opérations sur* A *faisant de* A *une algèbre de Hopf et de* $G = \operatorname{Spec}(A)$ *un* k*-schéma en groupes affine.*

En résumé, un k-schéma en groupes affine G peut être identifié à un foncteur $G : Alg_k \to Grp$ et caractérisé par une algèbre de Hopf.

Notation 1.3. L'algèbre de Hopf du schéma en groupes affine G est notée $k[G]$.

Remarque. Si A est une k-algèbre de type fini : $A = k[t_1, ..., t_n]/I$, alors pour toute k-algèbre R, l'algèbre $\operatorname{Hom}(A, R)$ est canoniquement isomorphe à $\{(x_1, ..., x_n) \in R^n \,|\, \forall P \in I\ P(x_1, ..., x_n) = 0\}$, de sorte que se donner une structure de k-schéma en groupes affine sur $\operatorname{Spec}(A)$ revient à se donner des structures de groupes compatibles sur chacune des « réalisations » de I comme ensemble de zéros.

Parmi la multitude des schémas en groupes affines, on s'intéresse à ceux qui sont « gentils ».

Définition 1.4. On appelle *k-groupe* (sous-entendu *algébrique affine)* un k-schéma en groupes affine G tel que $k[G]$ soit une algèbre de type fini sur k et tel que $k[G] \otimes_k \bar{k}$ soit une algèbre réduite (sans élément nilpotent non nul).

En faisant un parallèle avec les groupes de Lie réels/complexes, la condition « de type fini » correspond à « de dimension finie » de G et la condition « algèbre réduite » à la lissité de G.

Exemples. Voici une série de groupes basiques et utiles (les opérations d'algèbre de Hopf ne sont pas expliciter).

$\diamond$ Le groupe trivial $\mathbf{1} = \mathbf{1}_k$ est le k-groupe de foncteur $R \mapsto \{1\}$. On a $k[\mathbf{1}] = k$.

$\diamond$ Le groupe additif $\mathbf{G}_a = \mathbf{G}_{a,k}$ est le k-groupe de foncteur $R \mapsto (R, +)$. On a $k[\mathbf{G}_a] = k[t]$.

$\diamond$ Le groupe multiplicatif $\mathbf{G}_m = \mathbf{G}_{m,k}$ est le k-groupe de foncteur $R \mapsto (R^\times, \cdot)$. On a $k[\mathbf{G}_m] = k[t, t^{-1}]$.

$\diamond$ Pour n premier à la caractéristique de k (pour respecter la condition de lissité, le groupe des racines n-ièmes de l'unité $\mu_n = \mu_{n,k}$ est le k-groupe de foncteur $R \mapsto \{x \in R \,|\, x^n = 1\}$. On a $k[\mu_n] = k[t]/(t^n - 1)$.

$\diamond$ Pour un k-espace vectoriel V, le groupe général linéaire de V $\mathbf{GL}(V)$ est le k-groupe de foncteur $R \mapsto \mathrm{GL}(V \otimes_k R)$, le groupes d'automorphismes du R-module $V \otimes_k R$. En particulier, pour $V = k^n$, on a le groupe général linéaire $\mathbf{GL}_n = \mathbf{GL}_{n,k}$. On a $k[\mathbf{GL}_n] = k[X_{ij},\, 1 \leqslant i,\, j \leqslant n]_{(\det((X_{ij})_{i,j}))}$.

$\diamond$ Pour un k-espace vectoriel V et q un forme quadratique non-dégénérée sur V, le groupe orthogonal $\mathbf{O}(V, q)$ est le k-groupe de foncteur $R \mapsto \mathrm{O}(V \otimes_k R, q \otimes \mathrm{id}_R)$

$\diamond$ Pour un k-espace vectoriel V et b une forme bilinéaire alternée non-dégénérée sur V, le groupe $\mathbf{Sp}(V, b)$ est le k-groupe de foncteur $R \mapsto \mathrm{Sp}(V \otimes_k R, b_R)$.

Morphismes de groupes algébriques.

Définition 1.5. Un morphisme du k-groupe G dans le k-groupe H est une transformation naturelle du foncteur G vers le foncteur H, c'est-à-dire la donnée de morphismes de groupes $G(R) \to H(R)$ pour toute k-algèbre R, fonctoriels en R.

Tout morphisme f d'un groupe G dans un groupe H détermine uniquement un morphisme d'algèbres de Hopf $f^* : k[H] \to k[G]$ et, inversement, tout morphisme d'algèbres de Hopf $k[H] \to k[G]$ détermine uniquement un morphisme $G \to H$.

Définition 1.6. Soit $f : G \to H$ un morphisme de k-groupes.
Lorsque f^* est surjective, on dit que f est une *immersion fermée.*

Une immersion fermée $f : G \to H$ permet de voir G comme un sous-k-groupe de H.

Extension des scalaires. Il est connu que pour un polynôme $P \in k[t]$ (non-constant), P n'est pas nécessairement scindé ou même n'a pas de racine sur k, tandis que si L est une extension de k, P ne peut que se simplifier lorsqu'il est vu comme polynôme sur L : un nouvelle racine apparaît ou les degrés des facteurs irréductibles de P diminuent, le cas extrême étant la décomposition en facteurs de degré 1 sur la clôture algébrique $\bar{k}$ de k.

De même, les variétés et les groupes algébriques sur k ont tendance à se simplifier et à se ressembler sur une extension de k, donc étudier ces objets sur une extension de k peut constituer une première étape dans leur étude.

Définition 1.7. Soit L/k une extension de corps.

Si G est un k-groupe, alors on définit le L-groupe G_L comme le L-schéma en groupes affine de foncteur

$$\begin{cases} Alg_L & \longrightarrow & Grp \\ R & \longmapsto & G(R) \end{cases}$$

et d'algèbre de Hopf

$$L[G_L] = k[G] \otimes_k L.$$

On dit que G_L est obtenu à partir de G par *extension des scalaires* de k à L.

De cette façon, si on se demande si G et H sont des k-groupes isomorphes, on peut d'abord regarder si G_L et H_L sont des L-groupes isomorphes. Les choses étant plus simples sur un corps algébriquement clos, il vaut mieux commencer à classifier une famille de groupes donnée sur un corps algébriquement clos.

1.2 Groupes semi-simples

Un k-groupe G est dit *connexe* s'il l'est en tant que schéma, c'est-à-dire si $\mathrm{Spec}(k[G])$ muni de la topologie de Zariski est connexe. Cela équivaut au fait que $k[G] \otimes_k \bar{k}$ est intègre.

Définition 1.8. Un k-groupe G est dit *semi-simple* s'il est connexe et si $G_{\bar{k}}$ est connexe et ne possède aucun sous-groupe connexe, résoluble et distingué autre que $\mathbf{1}_{\bar{k}}$.

Tores maximaux et déployés. L'existence de tores maximaux déployés ou de tores déployés maximaux est la première étape pour étudier la combinatoire des groupes semi-simples.

Définition 1.9. Un *k-tore* est un k-groupe T tel que $T_{\bar{k}}$ soit isomorphe à un produit de groupes multiplicatifs $\mathbf{G}_{m,\bar{k}} \times \ldots \times \mathbf{G}_{m,\bar{k}}$, et un k-tore est dit *déployé* s'il est déjà isomorphe sur k à un produit de groupes multiplicatifs.

Remarque. Le groupe $(\mathbf{G}_m)^n = \mathbf{G}_m \times ... \times \mathbf{G}_m$ est isomorphe au k-groupe $\mathbf{D}_n$ des matrices diagonales, de foncteur $R \mapsto \{diag(a_1, ..., a_n) \in \mathcal{M}_n(R) \,|\, a_i \neq 0\}$.

Pour un tore déployé $T \simeq \mathbf{D}_n$, le *groupe des caractères* de T est le groupe constitué des morphismes $T \to \mathbf{G}_m$ et que l'on note T^*. Il est isomorphe à $\mathbb{Z}^n$, engendré par les caractères diagonaux $\chi_i : diag(a_1, ..., a_n) \mapsto a_i$.

Proposition 1.10. *- Dans un k-groupe connexe G, tout tore est contenu dans un tore maximal (pour l'inclusion) de G et deux tores maximaux de G sont conjugués.*

- Tous les tores deviennent déployés sur la clôture séparable $k_s \subseteq \bar{k}$ de k.

Définition 1.11. Un groupe semi-simple est dit *déployé* lorsque ses tores maximaux le sont.

En particulier, un groupe semi-simple est déployé sur la clôture séparable de k.

La propriété de déploiement sur la clôture séparable de k est particulièrement utile car cela permet d'expliciter la combinatoire des groupes semi-simples sur k_s et ensuite de pouvoir dire des choses sur les groupes semi-simples sur k grâce au procédé de *descente galoisienne* (pour lequel on a besoin d'une extension galoisienne, alors que pour un corps imparfait, $\bar{k}/k$ n'est pas galoisienne).

2 Combinatoire des groupes semi-simples

On va décrire la classification des groupes semi-simples sur un corps séparablement clos.

Soit k un corps séparablement clos et G un k-groupe semi-simple.

Soit T un tore maximal de G. Il est déployé : $T \simeq \mathbf{D}_n$.

La remarque fondamentale à faire sur T est la suivante : T est commutatif et diagonalisable, donc pour toute représentation linéaire V de T (c'est-à-dire un morphisme $T \to \mathbf{GL}(V)$ avec V espace vectoriel de dimension finie), les éléments de T agissent par des automorphismes de V diagonalisables et qui commutent deux-à-deux, donc simultanément diagonalisables ; ainsi l'espace V se décompose en *espaces de poids* :

$$V = \bigoplus_{\alpha \in T^*} V_\alpha$$

avec $V_\alpha = \{v \in V \mid \forall t \in T,\, t \cdot v = \alpha(t)v\}$.

Sans expliquer la construction, on indique qu'il est possible (comme en géométrie différentielle) de définir l'algèbre de Lie d'un groupe algébrique H. On la note $\mathrm{Lie}(H)$ et elle est de dimension finie sur k. Pour une immersion fermée $H_1 \hookrightarrow H_2$, $\mathrm{Lie}(H_1)$ s'identifie naturellement à une sous-algèbre de Lie de $\mathrm{Lie}(H_2)$, et en différentiant l'action par conjugaison de H sur lui-même, on obtient la *représentation adjointe* $H \to \mathbf{GL}(\mathrm{Lie}(H))$ de H.

Dans le cas présent, cela donne une représentation $T \to \mathbf{GL}(\mathrm{Lie}(G))$, d'où une décomposition

$$\mathrm{Lie}(G) = \bigoplus_{\alpha \in T^*} \mathrm{Lie}(G)_\alpha.$$

L'espace $\mathrm{Lie}(G)$ étant de dimension finie, l'ensemble des α pour lesquels $\mathrm{Lie}(G)_\alpha \neq 0$ est fini. Ces α non nuls sont appelés *racines* de G relativement à T et leur ensemble est noté $R = R(G,T)$.

Proposition 2.1. *L'ensemble R est un système de racines réduit dans $T^* \otimes_{\mathbb{Z}} \mathbb{R}$*

La notion de système de racines provient de l'étude des algèbres de Lie semi-simples complexes et sont définis comme suit :

Définition 2.2. Soit V un $\mathbb{R}$-espace vectoriel de dimension finie.

Un *système de racines* R de V est un ensemble $R \subseteq V$ vérifiant :

1. R est fini ;
2. $0 \notin R$;
3. V est engendré par R ;
4. pour tout $\alpha \in R$, il existe une réflexion s_α de V telle que $s_\alpha(\alpha) = -\alpha$ et $s_\alpha(R) = R$;
5. pour tous α et $\beta \in R$, $s_\alpha(\beta) - \beta \in \mathbb{Z}\alpha$.

Le système R est dit *réduit* si $\forall \alpha \in R$, $\mathbb{R}\alpha \cap R = \{\alpha, -\alpha\}$, et *irréductible* s'il n'existe pas de partition $R = R_1 \sqcup R_2$ avec R_1 et R_2 non vides tels que $V = \mathrm{Vect}(R_1) \oplus \mathrm{Vect}(R_2)$ et R_i est un système de racines de $\mathrm{Vect}(R_i)$ $(i = 1, 2)$.

Le groupe d'automorphismes de V engendré par les s_α est fini, donc on peut définir un produit scalaire $(;)$ sur V invariant par tous les s_α. Ce produit scalaire permet de définir le *réseaux des poids*

$$\Lambda = \{x \in V \mid \forall \alpha \in R,\ (\alpha, x) \geqslant)\}.$$

On a aussi le *réseau des racines* $\Lambda_r = \mathbb{Z}R$.

Il est alors possible de montrer que dans l'espace vectoriel $V = T^* \otimes \mathbb{R}$, on a les inclusions $\Lambda_r \subseteq T^* \subseteq \Lambda$. Lorsque la première inégalité est une égalité, le groupe semi-simple G est dit *adjoint* ; lorsque la deuxième inégalité est une égalité, G est dit *simplement connexe*.

On connaît tout des systèmes de racines : tout système de racines est somme directe d'un nombre fini de systèmes irréductibles, lesquels sont répertoriés en quatre familles infinies, complétées par cinq cas exceptionnels : il y a les systèmes de type A_n ($n \geqslant 1$), B_n ($n \geqslant 1$), C_n ($n \geqslant 1$), D_n ($n \geqslant 3$), E_6, E_7, E_8, F_4 et G_2.

Note. Les indices désignent la dimension de l'espace vectoriel engendré par le système de racines.

Le résultat important sur la classification des groupes semi-simples sur un corps séparablement clos est le suivant :

Théorème 2.3. *Soit G et G' des groupes semi-simples et $T \subseteq G$, $T' \subseteq G'$ des tores maximaux.*

Un isomorphisme $G \tilde{\to} G'$ envoyant T sur T' détermine un isomorphisme $T^* \otimes \mathbb{R} \tilde{\to} T'^* \otimes \mathbb{R}$ transformant $R(G,T)$ en $R(G',T')$ et T^* en T'^*.

Inversement, un tel isomorphisme détermine un isomorphisme de groupe $G \tilde{\to} G'$ envoyant T sur T'.

De cette façon, le couple (G,T) est entièrement déterminé par la donnée de $R(G,T)$ et du réseau $T^* \subseteq R(G,T) \otimes \mathbb{R}$.

Dans le cas de groupes semi-simples adjoints ou simplement connexe, le système de racines $R(G,T)$ détermine entièrement le groupe G, vu que dans ces cas $T^* \subseteq T^* \otimes \mathbb{R}$ est entièrement déterminé par $R(G,T)$ (T^* est le réseau des racines ou des poids de $R(G,T)$) :

Corollaire 2.4. *Soient G et G' deux groupes semi-simples tous les deux simplement connexes ou tous les deux adjoints ; soient T un tore maximal de G et T' de G'.*

Alors G et G' sont isomorphes si, et seulement si, les systèmes de racines $R(G,T)$ et $R(G',T')$ le sont.

Exemples. - Les groupes semi-simples simplement connexes de système de racines A_n sont isomorphes à $\mathbf{SL}_{n+1}$.

- Les groupes semi-simples simplement connexes de système de racines C_n sont isomorphes à $\mathbf{Sp}_{2n}$.

3 Étude cohomologique

Pour étudier un k-groupe G, il est intéressant de commencer par regarder le groupe G_L obtenu par extension des scalaires de k à L. Idéalement on prend $L = \bar{k}$. Cependant, comme on aimerait utiliser les résultats obtenus sur L pour pouvoir dire des choses sur k, il vaut beaucoup mieux prendre $L = k_s$, la clôture séparable de k, car alors l'extension k_s/k est galoisienne (infinie *a priori*) pour laquelle on dispose de la théorie de Galois : notamment $k_s^{\mathrm{Gal}(k_s/k)} = k$.

L'ensemble H^1 de cohomologie non-abélienne prend en compte les structures de l'extension galoisienne k_s/k ainsi que du groupe G sur k_s, donnant un objet synthétisant ce problème de « descente » de structure.

Le groupe $\mathrm{Gal}(k_s/k)$ est naturellement muni d'une topologie : comme $k_s = \bigcup_{L/k \text{ gal. finies}} L$, on voit que $\mathrm{Gal}(k_s/k)$ s'identifie au sous-groupe de $\prod_{L/k \text{ gal. finie}} \mathrm{Gal}(L/k)$ constitué des éléments $(f^L)_L$ tels que, pour toutes extensions finies galoisiennes $L \subseteq M$ de k, la restriction $(f^M)_{/L}$ soit égale à f^L ; alors en munissant le groupe fini $\mathrm{Gal}(L/k)$ de la topologie discrète pour toute L/k galoisienne finie, et le produit $\prod \mathrm{Gal}(L/k)$ de la topologie produit, le groupe $\mathrm{Gal}(k_s/k)$ hérite naturellement d'une topologie.

On va noter Γ le groupe de Galois $\mathrm{Gal}(k_s/k)$. Il est implicitement toujours muni de la topologie ci-dessus.

3.1 Cohomologie galoisienne non abélienne

Un Γ-groupe est un groupe A sur lequel Γ agît continûment (à gauche) par automorphismes, A étant muni de la topologie discrète.

Un cocycle est une application continue

$$\alpha : \left\{ \begin{array}{ccc} \Gamma & \longrightarrow & A \\ \sigma & \longmapsto & \alpha_\sigma \end{array} \right.$$

vérifiant, pour tous σ, $\tau \in \Gamma$,

$$\alpha_{\sigma\tau} = \alpha_\sigma \cdot \sigma(\alpha_\tau).$$

L'ensemble des cocycles est noté $Z^1(k, A)$ et on définit dessus la relation d'équivalence « être cohomologue » comme suit : deux cocycles α et α' sont dits cohomologues s'il existe un élément a de A tel que pour tout $\sigma \in \Gamma$,

$$\alpha'_\sigma = a \cdot \alpha_\sigma \cdot \sigma(a)^{-1}.$$

On note alors $H^1(k,A)$ l'ensemble $Z^1(k,A)$ quotienté par la relation « être cohomologue » . Lorsque A est abélien, $H^1(k,A)$ est naturellement un groupe, de neutre la classe du cocycle trivial $\sigma \mapsto 1$. Mais en général $H^1(k,A)$ n'est pas un groupe ; cependant on en fait un ensemble pointé en distinguant la classe de $\sigma \mapsto 1$: l'intérêt est de pouvoir parler de « noyau » pour des applications $H^1(k,B) \to H^1(k,A)$ (B étant un autre Γ-groupe) et de pouvoir parler de suites exactes en cohomologie associées à des suites exactes de Γ-groupes comme dans les théories cohomologiques habituelles.

Pour un k-groupe algébrique G, on s'intéresse à l'ensemble $H^1(k, G(k_s))$, noté plus simplement $H^1(k,G)$.

Classification des formes. On va relier la construction qui précède aux groupes algébriques et par là justifier la définition des cocycles et de la relation « être cohomologue » .

Informellement, un *k-objet* est un « objet » défini sur k qui possède une certaine structure algébrique. L'intérêt est qu'un k-objet X donne canoniquement un L-objet X_L de la même famille algébrique pour toute extension L de k, et plus généralement, donne canoniquement un R-objet X_R de la même famille pour toute k-algèbre R. Essentiellement, un k-objet est un k-espace vectoriel, une k-algèbre, une k-variété algébrique ou encore un couple (V,b) constitué d'un k-espace vectoriel et d'une forme bilinéaire (symétrique, alternée,...) sur V.

Le lien avec les groupes algébriques se fait grâce au théorème ci-dessous et grâce à la remarque suivante : le foncteur $R \mapsto \mathrm{Aut}(X_R)$, qui à une k-algèbre R associe le groupe des automorphismes de X_R relativement à sa structure algébrique, est un k-schéma en groupes affine qui est un k-groupe dans la plupart des applications. Par exemple, pour V un k-espace vectoriel, on a le groupe $\mathbf{GL}(V)$; pour une forme quadratique q sur k^n on a le groupe $\mathbf{O}_n(q)$; etc.

On fixe X.

Une *forme* de X est un autre k-objet Y pour lequel $X_{k_s} \simeq Y_{k_s}$. On va noter Y_s au lieu de Y_{k_s}.

Pour tout k-objet Y, chaque $\sigma \in \Gamma$ induit un isomorphisme $\sigma_Y : Y_s \to Y_s$, σ en agissant sur les nouveaux scalaires.

En particulier, le groupe $\mathrm{Aut}(X_s)$ est un Γ-groupe pour $\sigma(f) := \sigma_X \circ f \circ \sigma_X^{-1}$, et tout isomorphisme $f : X_s \xrightarrow{\sim} Y_s$ avec une forme Y de X permet de définir un cocycle

$$\sigma \mapsto f^{-1} \circ \sigma_Y \circ f \circ \sigma_X^{-1} \in \mathrm{Aut}(X_s).$$

On vérifie que ce cocycle est cohomologue à celui défini par un autre isomorphisme $f' : X_s \xrightarrow{\sim} Y_s$. Ainsi on a une application

$$\phi : \{\text{classes d'iso. des formes de } X\} \to H^1\left(k, \operatorname{Aut}(X_s)\right)$$

envoyant la classe d'isomorphisme de X sur la classe de cohomologie du cocycle trivial.

Théorème 3.1. *L'application ϕ est une bijection.*

L'idée générale est, d'une part : si Y et Y' sont des formes de X déjà isomorphes sur k, alors Y_s et Y'_s sont isomorphes sur k_s et même Γ-isomorphes, tandis que si Y et Y' ne sont pas isomorphes sur k, alors Y_s et Y'_s sont isomorphes sur k_s mais pas Γ-isomorphes ; et d'autre part : toute classe de Γ-structure sur X_s provient d'une forme de X définie sur k.

La construction de l'inverse de ϕ consiste à se donner un cocycle α, puis modifier l'action de Γ sur X_L à l'aide α, de sorte que le résultat $X_{s,\alpha}$ soit isomorphe à X_s et que le cocycle associé à $X_{s,\alpha}$ soit α. Grâce à la nouvelle Γ-action, l'ensemble des points fixes est (potentiellement) différent de X. Alors il reste à vérifier que l'ensemble des points fixes donne un k-objet Y tel qu'un isomorphisme $X_s \xrightarrow{\sim} Y_s$ définisse un cocycle cohomologue à α.

Ce dernier point s'appelle la *descente galoisienne*.

Exemples. $\diamond$ Une forme quadratique q sur k^n induit une forme quadratique triviale q_s sur k_s^n (c'est-à-dire de matrice $diag(1, ..., 1)$ dans une certaine base) et alors l'ensemble $H^1(k, \mathrm{O}_n(q_s))$ classifie les formes quadratiques sur k à équivalence près.

$\diamond$ Les formes de $\mathbf{SL}_n$ sont les $\mathbf{SL}_1(A)$ pour A algèbre centrale simple de degré $n+1$.

Conjecture de Serre. L'ensemble $H^1(k, G)$ peut aussi s'interpréter comme l'ensemble des classes d'équivalence des espaces principaux homogènes sur G et un tel espace à un k-point rationnel si, et seulement si, il est dans la classe triviale (c'est-à-dire la classe de G où G opère par translation). Par ailleurs, pour certains corps, ce dernier résultat est valable pour tout espace homogène sur G. En particulier, pour ces corps, $H^1(k, G) = 0$ assure l'existence d'un point rationnel sur tout espace homogène. Il semble alors légitime de chercher des cas pour lesquels $H^1(k, G) = 1$.

La conjecture II de Serre affirme que $H^1(k, G)$ est nul pour k parfait de dimension cohomologique au plus 2, et G semi-simple simplement connexe. Bien que ce résultat soit prouvé pour un grand nombre de corps, il ne l'est pas complètement.

3.2 Invariants cohomologiques

Pour un Γ-groupe A, l'ensemble $H^1(k, A)$ est juste un ensemble pointé, et le but des invariants cohomologiques est de l'étudier via son comportement dans un groupe.

Un Γ-*module* est un Γ-groupe commutatif.

Pour un Γ-module M, $H^1(k, M)$ est un groupe et fait en réalité partie d'une famille $(H^d(k, M))_{d \geqslant 0}$ de groupes abéliens.

Définition 3.2. Soient G un k-groupe algébrique affine et M un Γ-module.

Un invariant cohomologique de degré d de G à coefficients dans M est un morphisme du foncteur $H^1(*, G)$ vers le foncteur $H^d(*, M)$: pour toutes extensions $K \subseteq L$ de k, le diagramme suivant est commutatif

$$\begin{tikzcd} H^1(K, G) \arrow[r] \arrow[d] & H^d(K, M) \arrow[d] \\ H^1(L, G) \arrow[r] & H^d(L, M) \end{tikzcd} .$$

Étant donnée d et M, $H^d(k, M)$ est un groupe, donc l'ensemble $\mathrm{Inv}^d(G, M)$ des invariants cohomologiques de G de degré d

Bibliographie

[Bou68] N. Bourbaki : *Groupes et Algèbres de Lie, Chap. 4, 5 et 6.* Hermann, 1968.

[GS06] P. Gille et T. Szamuely : *Central Simple Algebra and Galois Cohomology*, volume 101 de *Cambridge studies in advanced mathematics.* Cambrigde University Press, 2006.

[Hum72] W. Humphreys : *Introduction to Lie Algebras and Representation Theory*, volume 9 de *GTM.* Springer-Verlag, 1972.

[Hum75] W. Humphreys : *Linear Algebraic Groups*, volume 21 de *GTM.* Springer-Verlag, 1975.

[KMRT98] M.-A. Knus, A. Merkurjev, M. Rost et J.-P. Tignol : *The Book of Involutions*, volume 44 de *Colloquium Publications.* American Mathematical Society, 1998.

[Ser94a] J.-P. Serre : *Cohomologie Galoisienne*, volume 5 de *Lecture Notes in Mathematics.* Springer-Verlag, cinquième édition, 1994.

[Ser94b] J.-P. Serre : Cohomologie galoisienne : progrès et problèmes. *Séminaire Bourbaki, exp. 783*, 1994.

[Spr98] T. Springer : *Linear Algebraic groups.* Birkhäuser, deuxième édition, 1998.

[Wat79] W. Waterhouse : *Introduction to Affine Group Schemes*, volume 66 de *GTM.* Springer-Verlag, 1979.