Groupes algébriques réductifs

Référence : Borel, *Linear Algebraic Groups*, Springer GTM 126.

1. Introduction. Il existe une notion de réductivité pour les algèbres de Lie, et on dit parfois qu'un groupe de Lie complexe G est *réductif* si son algèbre de Lie $\mathfrak{g}$ l'est. Par exemple, les groupes $\mathbb{G}_a = (\mathbb{C}, +)$ et $\mathbb{G}_m = (\mathbb{C}^\times, \cdot)$ ont tous deux pour algèbre de Lie l'algèbre commutative de dimension 1, et sont donc réductifs en ce sens. Nous allons nous intéresser aux groupes *algébriques*, et développer pour eux une notion de réductivité plus forte, pour laquelle seul $\mathbb{G}_m$ ci-dessus sera réductif.

La structure des groupes algébriques réductifs se décrit à l'aide de leurs tores maximaux T, leurs sous-groupes de Borel B, leurs normalisateurs N, et leur groupe de Weyl $W = N/T$. L'objectif principal de l'exposé est de présenter ces objets et un certain nombre de leurs propriétés principales qui permettent de démontrer que W est un groupe de Coxeter. Ces propriétés mènent au formalisme des BN-paires.

Comme nous sommes intéressés par la construction d'immeubles de groupes réductifs sur des corps non algébriquement clos, on donne les définitions et résultats de base dans ce cadre quand cela n'alourdit pas trop. À partir du § 9, on suppose que k est algébriquement clos.

2. Groupes algébriques. Fixons un corps k (ex : $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{F}_p$) et $\overline{k}$ une clôture algébrique. Un k-groupe algébrique est une variété algébrique affine lisse G munie d'un point $1 \in G(k)$ et d'un morphisme $m : G \times G \to G$ qui vérifie les axiomes habituels. *Variété algébrique affine* veut dire fermé d'un espace affine $\mathbb{A}^n_k$, défini par des polynômes $f_1, \dots, f_m \in k[x_1, \dots, x_n]$. *Lisse* veut dire que la matrice jacobienne $J = (\partial f_i / \partial x_j)_{i,j}$ est de rang maximum au point 1 (la lissité se propage alors à tout le groupe par homogénéité). Un théorème de Cartier dit que si k est de caractéristique 0, la condition de lissité est automatique ; donc on ne se stresse pas trop avec ça. Exemples :

• Le groupe $\mathrm{SL}_{2,k}$ est défini dans $\mathbb{A}^4$ muni de coordonnées a, b, c, d par l'équation $f = \det - 1$ où $\det := ad - bc$. La multiplication est donnée par la multiplication matricielle.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$$

• Le groupe $\mathrm{GL}_{2,k}$ est défini dans $\mathbb{A}^5$ en coordonnées a, b, c, d, x par l'équation $f = x \det - 1$.

- Le groupe $\mathrm{GL}_{n,k}$. Le groupe multiplicatif $\mathbb{G}_{m,k} = \mathrm{GL}_{1,k}$.
- Le groupe additif $\mathbb{G}_{a,k}$ i.e. la droite affine $\mathbb{A}^1_k$ munie de la loi d'addition.
- Les groupes finis.

3. Algèbres de fonctions. L'algèbre de fonctions de G est $k[G] := k[x_1, \dots, x_n]/(f_1, \dots, f_m)$. Elle est munie d'une application $m' : k[G] \to k[G] \otimes_k k[G]$ déduite de m, que l'on doit considérer comme une partie de la structure de $k[G]$ tout comme m fait partie de la structure de G. Exemples :

- $k[\mathrm{SL}_2] = k[a, b, c, d]/(\det -1)$ et

$$m' : \frac{k[A, B, C, D]}{(\det -1)} \longrightarrow \frac{k[a, b, c, d, e, f, g, h]}{(\det_1 - 1, \det_2 - 1)}$$

est donnée par $A \mapsto ae + bg$, $B \mapsto af + bh$, $C \mapsto ce + dg$, $D \mapsto cf + dh$.

- $k[\mathrm{GL}_2] = k[a, b, c, d, x]/(x \det -1) = k[a, b, c, d, 1/\det]$.
- $k[\mathbb{G}_m] = k[t, 1/t]$ et $k[\mathbb{G}_a] = k[t]$.

Le Nullstellensatz (théorème des zéros) de Hilbert permet de démontrer que le foncteur $G \mapsto k[G]$ est une équivalence de catégories, c'est-à-dire qu'on peut reconstruire le groupe G à partir de l'algèbre $A := k[G]$, et que pour toute paire de k-groupes algébriques G, H l'application naturelle $\mathrm{Hom}(G, H) \to \mathrm{Hom}(k[H], k[G])$ est bijective. (Un peu de détail : dans le cas simple où k est algébriquement clos, le Nullstellensatz affirme que les idéaux maximaux de $k[x_1, \dots, x_n]$ sont de la forme $\mathfrak{m}_a := (x_1 - a_1, \dots, x_n - a_n)$ pour un certain $a = (a_1, \dots, a_n) \in k^n$. Les idéaux maximaux de $k[x_1, \dots, x_n]/(f_1, \dots, f_m)$ sont les $\mathfrak{m}_a$ avec a zéro commun des f_i. On retrouve donc G comme l'ensemble des idéaux maximaux de $A = k[G]$.)

4. Points rationnels. Pour toute extension de corps K/k, l'ensemble

$$G(K) = \{x \in K^n ; f_1(x) = \cdots = f_m(x) = 0\}$$

des points K-rationnels de G est un groupe abstrait. Tout morphisme de k-groupes algébriques $f : G \to H$ induit un morphisme de groupes abstraits $f(K) : G(K) \to H(K)$. On dit que f est *injectif*, resp. *surjectif* si $f(\overline{k}) : G(\overline{k}) \to H(\overline{k})$ est injectif, resp. surjectif. Exemples :

- On a un morphisme injectif de groupes abstraits $\mathbb{R} \hookrightarrow \mathbb{R}^\times$ mais il n'existe aucun morphisme non trivial $\mathbb{G}_{a,\mathbb{R}} \to \mathbb{G}_{m,\mathbb{R}}$ car il n'existe pas de polynôme $P \in \mathbb{R}[t]$ tel que $P(X + Y) = P(X)P(Y)$.

- Le morphisme $f : \mathbb{G}_{m,\mathbb{Q}} \to \mathbb{G}_{m,\mathbb{Q}}$, $f(x) = x^3$ est non injectif mais surjectif. Le morphisme induit sur les groupes de points $\mathbb{Q}$-rationnels est tout le contraire : injectif mais non surjectif. Noter que le noyau de f est le sous-groupe algébrique de $\mathbb{G}_{m,\mathbb{Q}}$ d'équation $x^3 - 1$.

On voit donc que les groupes de points rationnels reflètent assez mal les propriétés des groupes algébriques et des morphismes entre eux.

5. Formes. Soit M un k-groupe algébrique. On dit que le k-groupe algébrique G est une *forme* de M s'il existe un isomorphisme $G_{\overline{k}} \simeq M_{\overline{k}}$. Exemples :

- Pour $k = \mathbb{R}$, les formes de $\mathbb{G}_m$ sont $\mathbb{G}_{m,\mathbb{R}}$ et $G = \{x^2 + y^2 = 1\} \subset \mathbb{A}^2_{\mathbb{R}}$, dont les groupes de points $\mathbb{R}$-rationnels sur $\mathbb{R}^\times$ et le cercle S^1. Plus généralement, soit k quelconque de caractéristique $\neq 2$. Pour $d \in k$, soit $T_d \subset \mathbb{A}^2$ le groupe algébrique défini par l'équation $x^2 - dy^2 = 1$, avec multiplication $(x_1, y_1) \star (x_2, y_2) = (x_1 x_2 + d y_1 y_2, x_1 y_2 + x_2 y_1)$. Sur $\overline{k}$, on a un isomorphisme $(T_d)_{\overline{k}} \xrightarrow{\sim} \mathbb{G}_{m,\overline{k}}$, $(x, y) \mapsto$

$x+\sqrt{d}y$. On peut vérifier que $T_d \simeq T_e$ sont isomorphes ssi d/e est un carré. On obtient ainsi toutes les formes de $\mathbb{G}_{m,k}$.

• Les formes de PGL_2 sur un corps k sont les groupes $G = U/\mathbb{G}_m$ où U est le groupe des éléments inversibles d'une algèbre de quaternions.

• Pour $k=\mathbb{R}$, les formes de SL_2 sont $\mathrm{SL}_{2,\mathbb{R}}$ et SU_2. Plus généralement, sur un corps k quelconque, on peut fabriquer des formes de SL_2 comme groupes unitaires de quaternions de norme 1 définis sur une extension quadratique ℓ/k, et je pense qu'on obtient ainsi toutes les formes.

6. Représentations. Une représentation linéaire de G dans un k-espace vectoriel V de dimension finie est un morphisme de groupes algébriques $\rho : G \to \mathrm{GL}(V)$, où $\mathrm{GL}(V)$ est vu comme un groupe algébrique isomorphe à $\mathrm{GL}_{n,k}$. Trois résultats fondamentaux (admis car avoir le résultat sans la preuve suffit bien pour la suite) dûs à Chevalley découlent de l'existence de certaines représentations :

6.1. Il existe une représentation *fidèle* i.e. telle que ρ est injectif (c'est alors automatiquement une immersion fermée). Ainsi tout k-groupe algébrique est sous-groupe fermé de $\mathrm{GL}_{n,k}$ pour un n, et réciproquement.

6.2. Si H est un sous-groupe algébrique fermé de G, il existe une représentation fidèle V telle que H est le stabilisateur d'une droite. On réalise ainsi le quotient G/H comme une orbite de G agissant dans l'espace projectif $\mathbb{P}(V)$ et on déduit que G/H est une variété algébrique.

6.3. Si de plus H est distingué dans G, alors G/H est affine, c'est un groupe algébrique et $G \to G/H$ est un morphisme de groupes algébriques. Exemple : le groupe PGL_n quotient de GL_n par son centre est un groupe algébrique affine ; ceci se voit directement car $\mathrm{GL}(V)$ agit sur $\mathrm{End}(V)$ par conjugaison avec noyau égal au centre, induisant une immersion fermée $\mathrm{PGL}(V) \hookrightarrow \mathrm{GL}(\mathrm{End}(V)) \simeq \mathrm{GL}_{n^2}$.

7. Tores. On dit que G est un *tore* s'il existe un isomorphisme $G_{\overline{k}} \simeq (\mathbb{G}_m^n)_{\overline{k}}$ pour un certain $n \geqslant 0$. Soit $X(G) = \mathrm{Hom}(G, \mathbb{G}_m)$ le *groupe des caractères* de G. Par exemple, si $G = \mathbb{G}_{m,k}^n$ on a $X(G) \simeq \mathbb{Z}^n$ composé des morphismes $\chi_m : (t_1,\dots,t_n) \mapsto t_1^{m_1}\dots t_n^{m_n}$, $m \in \mathbb{Z}^n$. Pour chaque représentation linéaire V de G et chaque caractère $\chi : G \to \mathbb{G}_m$, notons $V_\chi = \{v \in V, g\cdot v = \chi(g)v, \forall g \in G\}$ le χ-espace propre de G ; si $V_\chi \neq 0$ on dit que χ est un *poids* de G dans V. Propriété fondamentale des tores :

7.1. Théorème de diagonalisabilité des tores : toute représentation linéaire de dimension finie V d'un tore G est diagonalisable, c'est-à-dire que l'application canonique $\oplus_{\chi\in X(G)} V_\chi \to V$ est un isomorphisme. En particulier V est semi-simple.

Preuve dans le cas $G = \mathbb{G}_{m,k}$ (le cas général n'est pas plus difficile). Une action de $\mathbb{G}_{m,k}$ sur V est donnée (après choix d'une base) par une matrice $M \in \mathrm{GL}_n(k[t,1/t])$. Écrivons $M = \sum_{i\in\mathbb{Z}} t^i M_i$ où $M_i \in \mathrm{GL}_n(k)$ et la somme est finie. L'identité d'action dit que $\sum_i t_1^i t_2^i M_i = (\sum_i t_1^i M_i)(\sum_j t_2^j M_j) = \sum_{i,j} t_1^i t_2^j M_i M_j$. Autrement dit $M_i^2 = M_i$ et $M_iM_j = 0$ si $i \neq j$ i.e. les M_i sont les projecteurs orthogonaux d'une décomposition en somme directe $V = \oplus V_i$. Pour tout vecteur $v \in V_i = M_iV$, on a $Mv = \sum_j t^j M_j v = t^i M_i v = t^i v$. Donc si on pose $\chi(t) = t^i$, on a $t\cdot v = \chi(t)v$ pour tout $v \in V_i$, c'est-à-dire $V_i = V_\chi$.

7.2. Exemple : soit G un groupe algébrique et $T \subset G$ un tore. On considère la représentation adjointe $T \subset G \to \mathrm{GL}(\mathfrak{g})$ et on note $\Phi = \Phi(G,T)$ l'ensemble des poids *non nuls* de T dans $\mathfrak{g}$, appelés *racines*. On a donc une décomposition $\mathfrak{g} = \mathfrak{g}_0 \oplus (\oplus_{\alpha\in\Phi}\mathfrak{g}_\alpha)$. Par exemple, lorsque $G = \mathrm{GL}_n$ et $T = D_n$ est le tore standard composé des matrices diagonales, une matrice $g = (g_{ij})$ est vecteur propre pour $\alpha \in X(T)$ si et seulement si $tgt^{-1} = \alpha(t)g$ i.e. $(c_ic_j^{-1}g_{ij}) = (g_{ij})$, pour tout $t = \mathrm{diag}(c_1,\dots,c_n) \in T$. On voit donc que $\mathfrak{g}_0$ est la sous-algèbre des matrices diagonales, et que les racines sont les $n(n-1)$ caractères α_{ij}, $i \neq j$, définis par $\alpha_{ij}(t) = t_it_j^{-1}$, avec pour espace propre $\mathfrak{g}_{\alpha_{ij}}$ égal à la droite vectorielle kE_{ij}.

Une autre propriété importante, que l'on laisse en exercice, est le fait que si $k = \overline{k}$ alors le foncteur groupe de caractères $G \mapsto X(G)$ est une équivalence de la catégorie des tores avec la catégorie des $\mathbb{Z}$-modules libres de type fini. En particulier si T est un tore de dimension n, alors $\mathrm{Aut}(T) \simeq \mathrm{GL}_n(\mathbb{Z})$ qui est discret. Corollaire immédiat :

7.3. Théorème de rigidité des tores : toute action d'un groupe algébrique connexe sur un tore est triviale.

8. Groupes unipotents. On dit que G est *unipotent* si toute représentation linéaire non nulle possède un vecteur fixe non nul : $V \neq 0 \Rightarrow V^G \neq 0$. Aucun tore non nul n'est unipotent. Exemples :

- $\mathbb{G}_{a,k}$ est unipotent.

En effet, soit V une représentation non nulle de $\mathbb{G}_a$, donnée (après choix d'une base) par un morphisme $\mathbb{G}_{a,k} \to \mathrm{GL}_{n,k}$. On a $k[\mathbb{G}_a] = k[t]$ et le morphisme est donc donné par une matrice $M \in \mathrm{GL}_n(k[t])$. On peut écrire $M = \sum_{i \geqslant 0} t^i M_i$ où $M_i \in \mathrm{GL}_n(k)$ et la somme est finie. L'identité d'action s'écrit $\sum_{i \geqslant 0} (t_1 + t_2)^i M_i = (\sum_{i \geqslant 0} t_1^i M_i)(\sum_{j \geqslant 0} t_2^j M_j)$, où t_1, t_2 sont deux indéterminées. Ceci s'écrit $\sum_{i,j \geqslant 0} \binom{i+j}{i} t_1^i t_2^j M_{i+j} = \sum_{i,j \geqslant 0} t_1^i t_2^j M_i M_j$ c'est-à-dire $\binom{i+j}{i} M_{i+j} = M_i M_j$ pour tous i, j. En caractéristique 0 on déduit que $M_i = (1/i!) M_1^i$ donc M_1 est nilpotent et $M = \exp(tM_1)$. Notons r l'indice de nilpotence de M_1, on voit que $W :=$ image de M_1^{r-1} est une sous-représentation non nulle composée de vecteurs fixes. En caractéristique p, il faut adapter le calcul mais on arrive facilement au même résultat.

- Tout sous-groupe du groupe $\mathbb{U}_{n,k}$ des matrices triangulaires unipotentes (i.e. à éléments diagonaux égaux à 1) est unipotent.

Réciproquement, en partant d'une représentation fidèle et en raisonnant par récurrence, on montre que tout groupe unipotent est isomorphe à un sous-groupe de $\mathbb{U}_{n,k}$.

9. Groupes résolubles. On dit que G est *résoluble* s'il admet une suite de composition $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = 1$ dont les quotients G_i / G_{i+1} sont commutatifs. Exemples :

- Tout tore est résoluble. Plus généralement tout groupe algébrique commutatif est résoluble.
- Tout groupe algébrique unipotent est résoluble.

9.1. Théorème du point fixe de Borel ($k = \overline{k}$) : un groupe résoluble connexe agissant sur une variété (éventuellement singulière, non connexe) projective non vide X possède un point fixe.

Preuve par récurrence sur $d = \dim(G)$. On peut supposer $d > 0$. Le groupe dérivé $N = (G, G)$ est résoluble, connexe (admis, pas trop difficile, l'idée est qu'il est engendré par un groupe connexe) et inclus dans le noyau de $G \to G/G_1$ donc de dimension $< d$. Par récurrence, la variété de points fixes $F = X^N$ qui est projective car fermée dans X, est non vide. De plus elle est G-stable car N est distingué. Soit $x \in F$ tel que l'orbite $G \cdot x$ est de dimension minimale ; elle est nécessairement fermée donc projective. Le stabilisateur G_x contient N donc est distingué. On a un isomorphisme $G/G_x \xrightarrow{\sim} G \cdot x$ avec G/G_x affine (cf 6.3) lisse connexe et $G \cdot x$ projective, donc $G \cdot x = \{x\}$ et $x \in X^G$.

9.2. Corollaire (Lie-Kolchin) ($k = \overline{k}$) : si $G \to \mathrm{GL}(V)$ est une représentation d'un groupe résoluble connexe, alors G laisse un drapeau complet de V invariant, i.e. G est trigonalisable.

Preuve : G agit sur la variété des drapeaux, qui est projective.

On en déduit assez facilement que si $k = \overline{k}$, tout groupe G résoluble connexe est produit semi-direct $U \rtimes T$ d'un groupe unipotent connexe par un tore.

Lorsque $k \neq \overline{k}$, on notera que le $\mathbb{R}$-groupe $S^1 \simeq \{ \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right); a^2 + b^2 = 1 \}$ n'est pas trigonalisable.

10. Radicaux, groupes semi-simples et réductifs. Si G est un k-groupe algébrique, il existe un unique sous-groupe algébrique résoluble distingué connexe maximal appelé *radical de G* et noté

$R_k(G)$ ou $R(G)$. De même il existe un unique sous-groupe algébrique unipotent distingué connexe maximal appelé *radical unipotent de* G et noté $R_{u,k}(G)$ ou $R_u(G)$.

Preuve. Si R_1, R_2 sont deux sous-groupes résolubles distingués connexes (RDC) de G, alors le sous-groupe R_1R_2 est distingué et connexe. Or les sous-groupes, quotients et extensions de groupes résolubles sont résolubles donc R_1R_2 est résoluble comme image de $f : R_1 \rtimes R_2 \to G$, $(r_1, r_2) \mapsto r_1r_2$. Il s'ensuit qu'un sous-groupe RDC de dimension maximale contient tous les sous-groupes RDC. Raisonnement mot pour mot identique pour le radical unipotent.

On dit que G est *semi-simple* si $R(G) = 1$ et *réductif* si $R_u(G) = 1$. Attention : ces notions ne sont pas stables par passage à un sous-groupe. Exemples :

• SL_n est semi-simple. En effet, si R est un sous-groupe résoluble connexe, il est trigonalisable par 9.2. S'il est distingué, il est donc triangulaire. Par le même argument il est anti-triangulaire, donc diagonal. Si une matrice diagonale a deux coefficients diagonaux distincts, alors la conjugaison par une matrice unipotente produit un coefficient non diagonal non nul comme montre le calcul $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}a&0\\0&b\end{smallmatrix}\right)\left(\begin{smallmatrix}1&-1\\0&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}a&b-a\\0&b\end{smallmatrix}\right)$. Ainsi les éléments de R sont des homothéties, donc des racines n-èmes de l'unité. Comme R est connexe, $R = 1$.

• GL_n est réductif, avec $R(G) = Z(G) \simeq \mathbb{G}_m$ le sous-groupe des matrices d'homothétie. En effet, le même raisonnement que pour SL_n montre que tout sous-groupe unipotent connexe distingué est trivial, et que $R(G) \subset Z(G)$ donc lui est égal.

Exercice : le radical R d'un groupe réductif est un tore central. Indices : R est résoluble donc produit semi-direct $U \rtimes T$, montrer que $U = 1$ puis faire agir G sur $R = T$ par conjugaison et conclure par rigidité des tores.

Comme $G/R(G)$ est semi-simple et $G/R_u(G)$ réductif, tout groupe algébrique est extension de fini, unipotent, tore, semi-simple.

11. Borels et paraboliques. Soit G un groupe algébrique connexe. On appelle *sous-groupe de Borel* un sous-groupe résoluble connexe maximal (mais non nécessairement distingué).

• Le Borel standard de GL_n : c'est le sous-groupe des matrices triangulaires supérieures. Il est visiblement résoluble connexe, et maximal par Lie-Kolchin.

11.1. Théorème de conjugaison des Borels ($k = \overline{k}$) : si B est un Borel, alors tous les Borels sont conjugués à B et G/B est une variété projective.

Idée de preuve. Soit R un Borel de dimension maximale. Par 6.2, on peut choisir une représentation fidèle V de G telle que R est le stabilisateur d'une droite V_1. Le théorème de Lie-Kolchin 9.2 appliqué à la représentation V/V_1 montre que R laisse invariant un drapeau $\mathscr{D} = (V_1 \subset V_2 \subset \cdots \subset V)$. Notons $\mathscr{F}(V)$ la variété des drapeaux de V ; c'est une variété projective. Comme $R \subset \mathrm{Stab}(\mathscr{D}) \subset \mathrm{Stab}(V_1) = R$ on voit que R est égal au stabilisateur de $\mathscr{D}$ dans $\mathscr{F}(V)$ de sorte que G/R s'identifie à l'orbite de $\mathscr{D}$. Du fait que R est choisi de dimension maximale, on montre que l'orbite G/R est de dimension minimale, donc fermée. Il s'ensuit que G/R est projective. En faisant agir B sur G/R naturellement et utilisant le théorème du point fixe, on trouve qu'il existe $x \in G$ tel que $BxR \subset xR$ d'où $x^{-1}Bx = R$ par maximalité.

On dit qu'un sous-groupe $P \subset G$ est *parabolique* s'il contient un Borel. Il revient au même de dire que G/P est projective : on voit un sens à l'aide du morphisme surjectif $G/B \twoheadrightarrow G/P$ et l'autre sens en utilisant le théorème du point fixe de Borel pour B agissant sur G/P. Un théorème de Chevalley montre que les paraboliques (en particulier les Borels) sont connexes et égaux à leur propre normalisateur.

11.2. Théorème sur la variété des Borels : soit $\mathscr{B}$ l'ensemble des Borels de G et $B_0 \in \mathscr{B}$. Alors l'action de G par conjugaison induit un isomorphisme $G/B_0 \xrightarrow{\sim} \mathscr{B}$, $g \mapsto gB_0g^{-1}$. En particulier $\mathscr{B}$ est une variété projective lisse connexe.

12. Tores maximaux, groupe de Weyl. Soit G un groupe algébrique connexe. On appelle *tore maximal* tout sous-groupe $T \subset G$ qui est... un tore, maximal.

12.1. Théorème de conjugaison des tores maximaux ($k = \overline{k}$) : tous les tores maximaux sont tores maximaux d'un Borel. Ils sont tous conjugués.

Preuve. Lorsque G est résoluble, une étude des groupes résolubles plus poussée que ce que nous avons fait permet d'obtenir le résultat ; voir Borel, th. 10.6. Le cas général s'y ramène car tout tore est par définition inclus dans un Borel. On conclut avec le cas résoluble et le théorème de conjugaison des Borels (11.1).

Si G est réductif, on appelle *rang de* G la dimension d'un tore maximal et *rang semi-simple* le rang de $G/R_u(G)$. Par conjugaison, ces entiers ne dépendent pas du choix du tore maximal. Si $G = \mathrm{GL}_n$, le rang est n et le rang semi-simple est $n-1$.

12.2. Théorème de réductivité des centralisateurs de tores ($k = \overline{k}$) : sous les hypothèses ci-dessus, le centralisateur $Z(T)$ est connexe réductif, et l'inclusion $T \hookrightarrow Z(T)$ est une égalité ssi T est maximal.

Preuve. C'est un théorème difficile. Le point clé est que $R(Z(T)) = R(G) \cap Z(T)$. Voir Borel, 13.17, cor. 2.

• Exemple. Soit $D_n \subset \mathrm{GL}_n$ le sous-groupe des matrices diagonales, qui est de dimension n. Tout tore T de GL_n est conjugué à un sous-tore de D_n. Regardons le cas d'un tore de codimension 1. Si $g = (g_{ij})$ centralise T, alors pour tout $t = \mathrm{diag}(c_1, \dots, c_n) \in T$ et tous $i \neq j$ on a $c_i c_j^{-1} g_{ij} = g_{ij}$. Si une racine $\alpha = \alpha_{rs}$ s'annule sur T, on voit que les matrices $A_{rs} := \mathrm{I}_n + E_{rs}$ et A_{sr} centralisent T, dans ce cas l'inclusion $T \subset \ker(\alpha)$ est une égalité pour raison de dimension et $Z(T) = \langle D_n, A_{rs}, A_{sr} \rangle$. Si aucune racine ne s'annule sur T, alors $Z(T) = D_n$.

Soit $N(T)$ le normalisateur de T dans G, qui agit sur T par conjugaison. Par rigidité des tores (7.3), la composante neutre $N(T)^\circ$ agit trivialement ce qui montre que $N(T)^\circ = Z(T)$. On voit alors que $W(T) := N(T)/Z(T) = N(T)/N(T)^\circ$ est un groupe fini que l'on appelle le *groupe de Weyl de* T *dans* G. Dans le cas où T est maximal, on a $W(T) := N(T)/T$ et par conjugaison des tores maximaux, ce groupe ne dépend pas de T à conjugaison près. On l'appelle le groupe de Weyl de G. On notera que W agit sur T par conjugaison, fidèlement à cause du fait que $Z(T) = T$.

12.3. Théorème ($k = \overline{k}$) : si T est un tore maximal et W son groupe de Weyl, alors W agit (par conjugaison) simplement transitivement sur $\mathscr{B}^T := \{\text{points fixes de } T \text{ sur } \mathscr{B}\} = \{\text{Borels contenant } T\}$. En particulier cet ensemble est fini, de cardinal $|W|$.

Preuve. L'action de T sur $\mathscr{B}$ est par conjugaison. Si un Borel B contient T, il est point fixe. Réciproquement si $B \in \mathscr{B}^T$ alors $T \subset N_G(B) = B$ d'après le théorème de Chevalley cité en 11.1. L'action de $N_G(T)$ sur $\mathscr{B}$ se factorise bien en une action de W, car T normalise les Borels qui le contiennent donc agit trivialement. Transitivité : soient $B_1, B_2 \in \mathscr{B}^T$ alors $B_2 = gB_1g^{-1}$ pour un $g \in G$. Alors T et gTg^{-1} sont des tores maximaux de B_2 donc sont B_2-conjugués. De $gTg^{-1} = bTb^{-1}$, $b \in B_2$, on tire que $n := g^{-1}b \in N_G(T)$ et $B_1 = nb^{-1}B_2bn^{-1} = nB_2n^{-1}$. Stabilisateurs : supposons que $nBn^{-1} = B$ avec $n \in N_G(T)$. Alors $n \in N_G(B) = B$ par le théorème de Chevalley. On écrit $B = U \rtimes T$ et on a un isomorphisme $\alpha : T \hookrightarrow B \twoheadrightarrow B/U$. Comme B/U est commutatif, pour tout $t \in T$ on a $[\alpha(n), \alpha(t)] = 1$ donc $[n, t] = 1$ puisque α est injectif. Ceci signifie que $n \in Z_G(T)$ qui est égal à T par 12.2.

13. Groupes réductifs de rang semi-simple 1. C'est la clé pour le théorème de structure sur les groupes réductifs qui vient ensuite. Soient G connexe réductif, T tore maximal, $W = W(T)$.

13.1. Théorème ($k = \overline{k}$) : Les conditions suivantes sont équivalentes (Borel, prop. 13.13) :
(i) le rang semi-simple de G est égal à 1,
(ii) $\mathrm{card}(W) = 2$.

Preuve. On se contente de montrer que (i) $\Rightarrow$ (ii). Soit $\pi : G \to G' = G/R(G)$ le quotient.

Le groupe $T' = \pi(T)$ est (quotient d'un tore donc) un tore. De plus $\ker(\pi) = R(G)$ est un tore (exercice dans le § 10) donc $\pi^{-1}(T')$ est un tore contenant T, donc égal à T. Le même argument montre que T' est maximal. Notons $N = N_G(T)$ et $N' = N_{G'}(T')$. De ce qui précède on déduit sans difficulté que π induit un isomorphisme $W = N/T \xrightarrow{\sim} W' = N'/T'$.

Comme G' est de rang semi-simple 1, on a $T' \simeq \mathbb{G}_m$ donc $W \simeq W' \hookrightarrow \mathrm{Aut}(T) = \mathrm{Aut}(\mathbb{G}_m) = \mathbb{Z}/2\mathbb{Z}$.

Remplaçant G par G' et T par $T' = \mathbb{G}_m$, il ne reste qu'à montrer que $2 \leqslant \mathrm{card}(W) = \mathrm{card}(\mathscr{B}^T)$, cf 12.3. Soit V un espace vectoriel avec action de T tel que $Y := \mathscr{B}$ se plonge dans $\mathbb{P}(V)$, voir 6.2. Comme G n'est pas résoluble, on a $\dim \mathscr{B} \geqslant 1$. Il suffit donc de montrer l'énoncé général suivant : dans un espace projectif avec action d'un tore T, pour tout $d \geqslant 0$, le tore T possède au moins $d+1$ points fixes dans toute sous-variété stable $Y \subset \mathbb{P}(V)$ de dimension d. On fait une récurrence sur d. Comme T est connexe il laisse stables les composantes irréductibles de Y donc on peut supposer Y irréductible. Si $d = 0$ alors Y est un point et l'assertion est claire. Si $d \geqslant 1$, quitte à remplacer V par l'intersection des hyperplans contenant Y (qui forment une famille T-stable) on peut supposer que Y n'est pas inclus dans un hyperplan. Soit $e_1, \dots, e_n$ une base de V qui diagonalise l'action de $T = \mathbb{G}_m$ i.e. si $v = \sum a_i e_i$, on a $t \cdot v = \sum t^{m_i} a_i e_i$ pour certains poids m_i. Quitte à renuméroter les e_i on peut supposer $m_1 = \dots = m_r < m_{r+1} \leqslant \dots \leqslant m_n$. Soit $H \subset \mathbb{P}(V)$ l'hyperplan $\{a_1 = 0\}$. Par choix de V il existe $x = [v] \in Y \smallsetminus H$, et on a $t \cdot x = [t \cdot v] = [\sum t^{m_i - m_1} a_i e_i]$. Le point limite $0 \cdot x = [\sum_{i=1}^r a_i e_i]$ appartient à Y (qui est fermée) et pas à H (visiblement) et est T-fixe. Par ailleurs $Y \cap H$ est non vide (toute sous-variété projective de dimension $\geqslant 1$ rencontre l'hyperplan H) et de dimension $d-1$ donc, par récurrence, contient d autres points fixes. On a terminé.

Soit B un Borel contenant T. En travaillant un peu plus, on peut montrer que (i)-(ii) sont aussi équivalentes à dire que G/B est isomorphe à $\mathbb{P}^1$ (on montre que c'est de dimension 1 ; projectif lisse ; rationnel car contenant l'orbite d'un tore $\mathbb{G}_m$, cqfd). L'action de G dessus fournit un morphisme $G \to \mathrm{PGL}_2$ qui permet de montrer que $\Phi(G,T) = \{\alpha, -\alpha\}$.

14. Groupes réductifs quelconques. Soit G connexe réductif, $T \subset G$ un tore maximal, $\Phi \subset X$ l'ensemble des racines, W le groupe de Weyl, et $\alpha \in \Phi$. On rappelle que la représentation adjointe vue comme représentation de T possède une décomposition $\mathfrak{g} = \mathfrak{g}_0 \oplus (\oplus_{\alpha\in\Phi} \mathfrak{g}_\alpha)$. Nous espérons que ce qui a été exposé précédemment rend plausibles les résultats de structure suivants (il reste du travail !).

14.1. Théorème : Soit $T_\alpha = (\ker \alpha)^\circ$ et $G_\alpha = Z_G(T_\alpha)$. Alors G_α est un groupe connexe réductif de rang semi-simple égal à 1. Les sous-groupes $W(G_\alpha, T) \subset W$ engendrent W.

- Pour $G = \mathrm{GL}_n$, les G_α ont été décrits en 12.2.

14.2. Théorème : 1) Il existe un unique sous-groupe $U_\alpha \subset G$ d'algèbre de Lie égale à $\mathfrak{g}_\alpha$, isomorphe à $\mathbb{G}_a$, normalisé par T. L'action de T par conjugaison est donnée par $t \cdot x = \alpha(t)x$.
2) Il existe un unique morphisme de groupes $\varphi_\alpha : \mathrm{SL}_2 \to G_\alpha$ qui envoie le tore diagonal D dans T, et les sous-groupes $U_\pm$ (unipotent supérieur et inférieur) isomorphiquement dans $U_{\pm\alpha}$.

Introduisons $X^\vee = \mathrm{Hom}(\mathbb{G}_m, T)$, le groupe des *sous-groupes à un paramètre* de T. Puisque $\mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m) = \mathbb{Z}$, on a une dualité parfaite $X \times X^\vee \to \mathbb{Z}$, $\langle \chi, \lambda \rangle := \chi \circ \lambda$. À l'aide de φ_α, on peut définir un sous-groupe à un paramètre particulier $\alpha^\vee : \mathbb{G}_m \to T$, $\alpha^\vee(c) = \varphi_\alpha(\mathrm{diag}(c, 1/c))$. On note $\Phi^\vee \subset X^\vee$ l'ensemble des $\alpha^\vee$. On vérifie que les endomorphismes $s_\alpha : X \to X$, $s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha$ sont des réflexions d'hyperplan fixe l'orthogonal de $\alpha^\vee$.

On appelle *donnée radicielle (abstraite)* un quadruplet $R = (X, \Phi, X^\vee, \Phi^\vee)$ dans laquelle :
- X et $X^\vee$ sont des $\mathbb{Z}$-modules libres de rang fini munis d'une dualité parfaite $\langle -, - \rangle : X \times X^\vee \to \mathbb{Z}$,
- $\Phi \subset X \smallsetminus \{0\}$ et $\Phi^\vee \subset X^\vee \smallsetminus \{0\}$ sont des sous-ensembles finis stables par négation,

et telle que :
- il existe une bijection $\Phi \to \Phi^\vee$, $\alpha \mapsto \alpha^\vee$, telle que $\langle \alpha, \alpha^\vee \rangle = 2$,
- Φ (resp. $\Phi^\vee$) est stable par les s_α (resp. par les $s_{\alpha^\vee}$).

On dit que cette donnée est *réduite* si $\mathbb{Q}\alpha \cap \Phi = \{\pm\alpha\}$ pour tout α.

14.3. Théorème : Le quadruplet $R = (X, \Phi, X^\vee, \Phi^\vee)$ est une donnée radicielle réduite. Réciproquement, toute donnée radicielle réduite détermine une unique paire (G, T) composée d'un groupe réductif avec tore maximal, unique à conjugaison torale près.

Ce théorème est en fait valable sur un corps de base k quelconque (et même sur un anneau de base quelconque).

Si on note S l'ensemble formé par les éléments d'ordre 2 des groupes $W(G_\alpha, T)$, la paire (W, S) est un groupe de Coxeter. Sa « représentation canonique » (comme groupe de Coxeter) est l'espace vectoriel réel $V := X \otimes_{\mathbb{Z}} \mathbb{R}$ où les éléments de S sont les réflexions s_α. On dispose de même de réflexions $s_{\alpha^\vee} : X^\vee \to X^\vee$, $s_{\alpha^\vee}(\lambda) = \lambda - \langle \lambda, \alpha \rangle \alpha^\vee$ dans $V^\vee := X^\vee \otimes_{\mathbb{Z}} \mathbb{R}$.)