Le Théorème de simplicité de Tits

— Exposé de maîtrise —

Barbara Gris & Jérémy Boussier

sous la direction de Philippe Gille

Table des matières

Introduction

Nous nous intéressons ici au théorème de simplicité de Tits (voir [7]), dans le cadre du formalisme des systèmes de Tits (ou (B,N) paires). Pour cela, nous commençons par étudier la notion de système de Coxeter qui est étroitement liée à celle de système de Tits. Dans une deuxième partie, nous démontrons ce théorème de simplicité. Enfin, nous en présentons une application importante : la simplicité du groupe $\mathrm{PSL}_\mathrm{n}(\mathbf{K})$ (quotient de $\mathrm{SL}_\mathrm{n}(\mathbf{K})$ par son centre), où $\mathbf{K}$ est un corps commutatif.

Nous tenons à remercier chaleureusement Philippe Gille pour nous avoir proposé ce sujet et pour l'aide précieuse qu'il nous a apportée.

1 Systèmes de Coxeter

1.1 Définitions

Soient $(W,\times)$ un groupe et $S \subset W$ un système de générateurs de W dont les éléments sont d'ordre 2 et tel que $S = S^{-1}$. On note T l'ensemble des conjugués des éléments de S dans W.

Définition 1.1 Soit $w \in W$, on appelle *longueur* de w (par rapport à S), et l'on note $l_S(w)$ ou simplement $l(w)$, le plus petit entier $q \geq 0$ tel que w est le produit d'une suite de q éléments de S. On appelle *décomposition réduite* de w (par rapport à S) toute suite $\mathbf{s} = (s_1, \ldots, s_q)$ d'éléments de S telle que $w = (s_1 \ldots, s_q)$ et $q = l(w)$.

Proposition 1.2 *Soient w et w' dans W. On a la relation*

$$\left| l(w) - l(w') \right| \leq l(ww'^{-1}).$$

Définition 1.3 Pour s, s' dans S, on note $m(s,s')$ l'ordre de ss'. On note I l'ensemble des couples (s,s') tels que $m(s,s')$ est fini. On dit que (W,S) est un *système de Coxeter* si l'ensemble générateur S et les relations $(ss')^{m(s,s')} = 1$ pour s et s' dans I forment une présentation du groupe W, *i.e.* pour tout groupe G et toute application f de S dans G telle que pour tout $(s,s') \in I$, $(f(s)f(s'))^{m(s,s')} = 1$, il existe un (unique) homomorphisme g de W dans G prolongeant f.

Remarque 1.4 En notant $\mathfrak{S}_n$ le groupe symétrique d'ordre n, s_i la transposition $(i, i+1)$ pour $1 \leq i \leq n-1$ et $S = \{s_1, \ldots, s_{n-1}\}$, on peut montrer que $(\mathfrak{S}_n, S)$ est un système de Coxeter (voir [3]).

Définition 1.5 Un système de Coxeter (W,S) est dit *irréductible* s'il n'existe pas de partition de S en deux ensembles S' et S'' non vides tels que tout élément de S' commute avec tout élément de S''.

1.2 Le groupe diédral

Définition 1.6 On appelle *groupe diédral* tout groupe engendré par deux éléments d'ordre 2 distincts.

Le groupe diédral d'ordre $2m$ est le produit semi-direct du groupe multiplicatif $M = \{1, -1\}$ par $\mathbf{Z}/m\mathbf{Z}$ pour l'action de passage à l'opposé, on le note $\mathbf{D}_m$. La loi de groupe dans $\mathbf{D}_m$ est donnée par la formule

$$(\epsilon, x).(\epsilon', x') = (\epsilon\epsilon', \epsilon' x + x').$$

On pose $\rho = (-1, \bar{0})$, $\rho' = (-1, \bar{1})$ et $\pi = (1, \bar{1})$. Alors ρ et ρ' sont d'ordre 2 et $\mathbf{D}_m$ est le groupe diédral engendré par $\{\rho, \rho'\}$.

Proposition 1.7 *Soit W un groupe diédral engendré par $S = \{s, s'\}$. Soit $p = ss'$ et soit m son ordre. Alors il existe un unique isomorphisme ϕ de $\mathbf{D}_m$ sur W tel que $\phi(\rho) = s$ et $\phi(\rho') = s'$.*

Proposition 1.8 *Tout groupe diédral est un groupe de Coxeter.*

Démonstration Soit D un groupe diédral, notons $\{\rho, \rho'\}$ son ensemble générateur et $m \geq 2$ l'ordre de $\rho\rho'$. Soit W un groupe de présentation défini par un ensemble de générateurs $S = \{s, s'\}$ et les relations $\{s^2 = 1, s'^2 = 1, (ss')^m = 1\}$. En particulier, W est un système de Coxeter. Or, d'après la proposition précédente, il existe un unique isomorphisme ϕ de D sur W tel que $\phi(\rho) = s$ et $\phi(\rho') = s'$. Ainsi, D est isomorphe à un groupe de Coxeter ; par transport de structure, D est un groupe de Coxeter.

□

1.3 Quelques propriétés

Proposition 1.9 *Soit $(P_s)_{s \in S}$ une famille de parties de W satisfaisant les conditions suivantes :*

(A) *Pour tout $s \in S$, $1 \in P_s$.*

(B) *Pour tout $s \in S$, les ensembles P_s et sP_s sont disjoints.*

(C) *Pour tout $(s, s') \in S^2$, pour tout $w \in W$, si $w \in P_s$ et $ws' \notin P_s$, alors $sw = ws'$.*

Alors (W, S) est un système de Coxeter et P_s se compose des éléments w de W tels que $l(sw) > l(w)$.

Proposition 1.10 *Pour toute suite $\mathbf{s} = (s_1, \ldots, s_q)$, on note $\Phi(\mathbf{s})$ la suite $(t_1, \ldots, t_q)$ d'éléments de T telle que pour tout $1 \leq j \leq q$, $t_j = (s_1, \ldots, s_{j-1}) s_j (s_1, \ldots, s_{j-1})^{-1}$. Pour tout élément $t \in T$, on note $n(\mathbf{s}, t)$ le nombre d'entiers j tels que $1 \leq j \leq q$ et $t_j = t$. Pour $w \in W$ et $t \in T$, le nombre $(-1)^{n(\mathbf{s},t)}$ a la même valeur $\eta(w, t)$ pour toutes les suites $\mathbf{s} = (s_1, \ldots, s_q)$ d'éléments de S telles que $w = s_1 \ldots s_q$. Pour $w \in W$, on note T_w l'ensemble des éléments t tels que $\eta(w, t) = -1$.*

Proposition 1.11 *Une décomposition $\mathbf{s}$ est réduite si et seulement si les t_j sont distincts.*

Proposition 1.12 *Pour toute partie X de S on note W_X le sous-groupe de W engendré par X. Pour $w \in W$ il existe $S_w \subset S$ telle que pour toute décomposition réduite $(s_1, \ldots, s_q)$ de w on a $S_w = \{s_1, \ldots, s_q\}$. De plus, pour toute partie X de S, le sous-groupe W_X de W se compose des éléments w de W tels que $S_w \subset X$.*

Proposition 1.13 *La fonction qui à $X \subset S$ associe W_X est injective.*

DÉFINITION 1.14 On désigne sous le nom de *condition d'échange* l'assertion suivante :

Soient $w \in W$ et $s \in S$ tels que $l(sw) \leq l(w)$. Pour toute décomposition réduite $(s_1, \ldots, s_q)$ de w, il existe un entier j tel que $1 \leq j \leq q$ et $ss_1 \ldots s_{j-1} = s_1 \ldots s_j$.

THÉORÈME 1.15 *Pour que (W, S) soit un système de Coxeter, il faut et il suffit qu'il satisfasse la condition d'échange.*

2 Le théorème de Tits

2.1 Systèmes de Tits

Définition 2.1 On appelle *système de Tits* un quadruplet (G, B, N, S) où G est un groupe, B et N deux sous-groupes de G et S une partie de $N/(B \cap N)$ satisfaisant les axiomes suivants :

(T$_1$) L'ensemble $B \cup N$ engendre G et $B \cap N$ est un sous-groupe distingué de N.

(T$_2$) L'ensemble S engendre le groupe $W = N/(B \cap N)$ et se compose d'éléments d'ordre 2.

(T$_3$) Pour tous $s \in S$ et $w \in W$, $sBw \subset BwB \cup BswB$.

(T$_4$) Pour tout $s \in S$, on a $sBs \not\subset B$.

Le groupe $W = N/(B \cap N)$ est appelé le groupe de Weyl du système de Tits (G, B, N, S).

Dans toute la suite, (G, B, N, S) désigne un système de Tits. On pose $T = B \cap N$.

On fait opérer le groupe $B \times B$ sur G par la loi $(b, b').g = bgb^{-1}$ pour b,b' dans B et g dans G. Les doubles classes de G suivant B sont les orbites de $B \times B$ dans G, *i.e.* les ensembles BgB pour g dans G. L'ensemble quotient correspondant est noté $B\backslash G/B$. Par double classe, on entend une double classe de G suivant B. Pour tout $w \in W$, on pose $\mathrm{C}(w) = BwB$.

Proposition 2.2 *Pour tout $s \in S$, $w \in W$, on a les égalités suivantes, qui nous seront utiles pour la suite :*

$$\mathrm{C}(w^{-1}) = \mathrm{C}(w)^{-1} \tag{2.1}$$

$$\mathrm{C}(s).\mathrm{C}(w) \subset \mathrm{C}(w) \cup \mathrm{C}(sw) \tag{2.2}$$

$$\mathrm{C}(w).\mathrm{C}(s) \subset \mathrm{C}(w) \cup \mathrm{C}(ws) \tag{2.3}$$

$$\mathrm{C}(s).\mathrm{C}(w) = \begin{cases} \mathrm{C}(sw) & si \quad \mathrm{C}(w) \not\subset \mathrm{C}(s).\mathrm{C}(w) \ ; \\ \mathrm{C}(w) \cup \mathrm{C}(sw) & si \quad \mathrm{C}(w) \subset \mathrm{C}(s).\mathrm{C}(w). \end{cases} \tag{2.4}$$

$$\mathrm{C}(s).\mathrm{C}(s) = B \cup \mathrm{C}(s) \tag{2.5}$$

$$\mathrm{C}(s).\mathrm{C}(s).\mathrm{C}(w) = \mathrm{C}(w) \cup \mathrm{C}(sw) \tag{2.6}$$

Lemme 2.3 *Soient $s_1, \ldots, s_q \in S$ et soit $w \in W$. On a*

$$\mathrm{C}(s_1 \ldots s_q).\mathrm{C}(w) \subset \bigcup_{(i_1,\ldots,i_p)} \mathrm{C}(s_{i_1} \ldots s_{i_p} w),$$

où $(i_1, \ldots, i_p)$ décrit l'ensemble des suites strictement croissantes d'entiers de l'intervalle $[\![1, q]\!]$.

2.2 Relation avec les systèmes de Coxeter

Théorème 2.4 *On a $G = BWB$. L'application*

$$\phi : \begin{cases} W & \longrightarrow & B\backslash G/B \ ; \\ w & \longmapsto & \mathrm{C}(w) \end{cases}$$

est une bijection.

Démonstration La double classe BWB est stable par passage à l'inverse, et par le lemme 2.3, elle est stable par produit. Comme elle contient B et N (car $W = N/(B \cap N)$), elle est donc égale à G.

Montrons que si $w \neq w'$, alors $\mathrm{C}(w) \neq \mathrm{C}(w')$. Pour cela, montrons par récurrence sur $q \in \mathbf{N}$ que

$$\text{Pour tout } w \neq w' \text{ tels que } l_S(w) \geq l_S(w') = q, \text{ on a } \mathrm{C}(w) \neq \mathrm{C}(w').$$

Cette assertion est évidente pour $q = 0$, car alors $w' = 1$ et $w \neq 1$, donc $\mathrm{C}(w') = B \neq \mathrm{C}(w)$. Supposons que $q \geq 1$ et que w, w' vérifient $w \neq w'$ et $l_S(w) \geq l_S(w') = q$. Soit $s \in S$ tel que sw' soit de longueur $q - 1$. On a donc

$$l_S(w) > l_S(sw'),$$

ce qui donne $w \neq sw'$. Donc par la proposition 1.2, on a

$$l_S(sw) \geq l_S(w) - 1 \geq l_S(sw') = q - 1.$$

En outre, $sw \neq sw'$.
Donc, par hypothèse de récurrence, on a $\mathrm{C}(sw')$ distinct de $\mathrm{C}(w)$ et de $\mathrm{C}(sw)$. De la formule (2.2), on déduit que $\mathrm{C}(sw') \cap \mathrm{C}(s).\mathrm{C}(w) = \varnothing$. Comme $\mathrm{C}(sw') \subset \mathrm{C}(s).\mathrm{C}(w')$, on a bien $\mathrm{C}(w) \neq \mathrm{C}(w')$, ce qui conclut la preuve. □

Théorème 2.5 *Le couple* (W, S) *est un système de Coxeter. De plus, pour* $s \in S$ *et* $w \in W$, *les relations* $\mathrm{C}(sw) = \mathrm{C}(s).\mathrm{C}(w)$ *et* $l_S(sw) > l_S(w)$ *sont équivalentes.*

Démonstration Pour tout $s \in S$, on note P_s l'ensemble des éléments $w \in W$ tels que $\mathrm{C}(s).\mathrm{C}(w) = \mathrm{C}(sw)$. Vérifions que les P_s satisfont les conditions (A), (B) et (C) de la proposition 1.9.

La condition (A) est évidente.

Vérifions (B). Si $w \in P_s \cap sP_s$, alors w et sw qui appartiendraient à P_s, d'où

$$\mathrm{C}(s).\mathrm{C}(w) = \mathrm{C}(sw), \quad \mathrm{C}(s).\mathrm{C}(sw) = \mathrm{C}(w).$$

On aurait alors $\mathrm{C}(s).\mathrm{C}(s).\mathrm{C}(w) = \mathrm{C}(w)$, et d'après la formule (2.6), ceci entraînerait $\mathrm{C}(w) = \mathrm{C}(sw)$, en contradiction avec le théorème 2.4.

Vérifions (C). Soient $(s, s') \in S^2$, $w \in W$, et $w' = ws'$. On suppose que $w \in P_s$ et $w' \notin P_s$. On a alors $\mathrm{C}(sw) = \mathrm{C}(s).\mathrm{C}(w)$, *i.e.*

$$\mathrm{C}(sw) = \mathrm{C}(s)w's'B. \tag{2.7}$$

D'après (2.3), on a $\mathrm{C}(w').\mathrm{C}(s') \subset \mathrm{C}(w') \cup \mathrm{C}(w's')$, *i.e.*

$$\mathrm{C}(w')s'B \subset \mathrm{C}(ws') \cup \mathrm{C}(w). \tag{2.8}$$

De plus, de $w' \notin P_s$, on déduit que $\mathrm{C}(w') \subset \mathrm{C}(s).\mathrm{C}(w')$ d'après (2.4), *i.e.* $\mathrm{C}(w') \subset \mathrm{C}(s)w'B$. Donc la double classe $\mathrm{C}(s)w'$ rencontre $\mathrm{C}(w')$, et donc $\mathrm{C}(s)w's'B$ rencontre $\mathrm{C}(w')s'B$. Par (2.7), $\mathrm{C}(sw)$ rencontre $\mathrm{C}(w')s'B$, et par (2.8), $\mathrm{C}(sw)$ est égale à l'une des doubles classes $\mathrm{C}(ws')$ et $\mathrm{C}(w)$. Comme $sw \neq w$, le théorème 2.4 permet de conclure que $sw = ws'$. □

Corollaire 2.6 *Soient* $w_1, \ldots, w_q \in W$ *et* $w = w_1 \ldots w_q$. *Alors*

$$l_S(w) = l_S(w_1) + \ldots + l_S(w_q) \quad \Longrightarrow \quad \mathrm{C}(w) = \mathrm{C}(w_1) \ldots \mathrm{C}(w_q).$$

Démonstration En prenant les décompositions réduites des w_i, on se ramène au cas d'une décomposition réduite, et tous les w_i sont dans S. Si $u = w_2 \dots w_q$, alors $l_S(w_1 u) > l_S(u)$, d'où $\mathrm{C}(w) = \mathrm{C}(w_1).\mathrm{C}(u)$ d'après le théorème. La formule s'en déduit par récurrence sur q. □

Corollaire 2.7 *Soit $w \in W$ et T_w la partie de W associée à w par le procédé de la proposition 1.10. Si $t \in T_w$, alors*

$$\mathrm{C}(t) \subset \mathrm{C}(w).\mathrm{C}(w^{-1}).$$

Démonstration Si $t \in T_w$, il existe par définition des éléments $w', w'' \in W$ et $s \in S$ tels que

$$w = w'sw'', \quad l_S(w) = l_S(w') + l_S(w'') + 1 \quad \text{et} \quad t = w'sw'^{-1}.$$

Par le corollaire 2.6, on a

$$\mathrm{C}(w).\mathrm{C}(w^{-1}) = \mathrm{C}(w').\mathrm{C}(s).\mathrm{C}(w'').\mathrm{C}(w''^{-1}).\mathrm{C}(s).\mathrm{C}(w'^{-1}),$$

d'où

$$\mathrm{C}(w').\mathrm{C}(s).\mathrm{C}(s).\mathrm{C}(w'^{-1}) \subset \mathrm{C}(w).\mathrm{C}(w^{-1}).$$

Or, d'après (2.5), on a $\mathrm{C}(s) \subset \mathrm{C}(s).\mathrm{C}(s)$. Donc

$$\mathrm{C}(t) \subset \mathrm{C}(w').\mathrm{C}(s).\mathrm{C}(s).\mathrm{C}(w'^{-1}) \subset \mathrm{C}(w).\mathrm{C}(w^{-1}),$$

ce qui conclut la preuve. □

Corollaire 2.8 *Soit $w \in W$ et H_w le sous-groupe de G engendré par $\mathrm{C}(w).\mathrm{C}(w^{-1})$. Alors*

1. *Pour toute décomposition réduite $(s_1, \dots, s_q)$ de w,*

$$\mathrm{C}(s_j) \subset H_w \quad \textit{pour } 1 \leq j \leq q.$$

2. *Le groupe H_w contient $\mathrm{C}(w)$ et est engendré par $\mathrm{C}(w)$.*

Démonstration Démontrons 1 par récurrence sur $j \geq 1$. Le cas $j = 1$ est trivial. On suppose la propriété vraie pour tout $k < j$. Soit

$$t = (s_1 \dots s_{j-1}) s_j (s_1 \dots s_{j-1})^{-1}.$$

On a $t \in T_w$ d'après la proposition 1.11, donc d'après le corollaire 2.7, $\mathrm{C}(t) \in H_w$, *i.e.* $\mathrm{C}(s_j) \in H_w$.

Comme $\mathrm{C}(w) = \mathrm{C}(s_1) \dots \mathrm{C}(s_q)$ d'après le corollaire 2.6, on a $\mathrm{C}(w) \in H_w$. De plus, $\mathrm{C}(w^{-1}) = \mathrm{C}(w)^{-1}$, ce qui donne 2. □

2.3 Sous-groupes de G contenant B

Pour toute partie X de S, on note W_X le sous-groupe de W engendré par X et G_X la réunion BW_XB des doubles classes $\mathrm{C}(w)$ pour $w \in W_X$.

Théorème 2.9 *On a les assertions suivantes :*

1. *Pour toute partie X de S, l'ensemble G_X est un sous-groupe de G engendré par $\bigcup_{s \in X} \mathrm{C}(s)$.*

2. *L'application $X \mapsto G_X$ est une bijection croissante de l'ensemble des parties de S dans l'ensemble des sous-groupes de G contenant B.*
3. *Soit $(X_i)_{i\in I}$ une famille de parties de S. Si $X = \bigcap_{i\in I} X_i$, on a $G_X = \bigcap_{i\in I} G_{X_i}$.*

Corollaire 2.10 *S est uniquement déterminé par (G, B, N).*

Démonstration Montrons que S est l'ensemble des $w \in W$ tels que $w \neq 1$ et que $B \cup \mathrm{C}(w)$ soit un sous-groupe de G. Ces éléments sont exactement ceux pour lesquels il existe $X \subset S$ tel que $W_X = \{1, w\}$. Comme $w \neq 1$, on a $w \in S$. □

Remarque 2.11 On peut donc se permettre de dire de façon abusive que (G, B, N) est un système de Tits.

Proposition 2.12 *Soient X une partie de S et $g \in G$. Alors*

$$gBg^{-1} \subset G_X \implies g \in G_X.$$

Démonstration Soit $w \in X$ tel que $g \in \mathrm{C}(w)$. Comme B est un sous-groupe de G_X, l'hypothèse $gBg^{-1} \subset G_X$ entraîne $\mathrm{C}(w).\mathrm{C}(w^{-1}) \subset G_X$, d'où $\mathrm{C}(w) \subset G_X$ d'après le corollaire 2.8. On a donc $g \in G_X$. □

2.4 Sous-groupes paraboliques

Définition 2.13 On dit qu'un sous-groupe de G est *parabolique* s'il contient un conjugué de B.

Proposition 2.14 *Soit P un sous-groupe de G.*

1. *Pour que P soit parabolique, il faut et il suffit qu'il existe une partie X de S telle que P soit conjugué de G_X.*
2. *Soient $X, X' \subset S$ et $g, g' \in G$ tels que $P = gG_Xg^{-1} = g'G_{X'}g'^{-1}$. Alors $X = X'$ et $g'g^{-1} \in P$.*

Définition 2.15 Si le sous-groupe parabolique P est conjugué de G_X, avec $X \subset S$, on dit que X est le *type* de P.

Théorème 2.16

1. *Soient P_1 et P_2 deux sous-groupes paraboliques de G dont l'intersection est parabolique et soit $g \in G$ tel que $gP_1g^{-1} \subset P_2$. Alors $g \in P_2$ et $P_1 \subset P_2$.*
2. *Deux sous-groupes paraboliques distincts dont l'intersection est parabolique ne sont pas conjugués.*
3. *Soient Q_1 et Q_2 deux sous-groupes paraboliques de G contenus dans un sous-groupe Q de G. Tout $g \in G$ tel que $gQ_1g^{-1} = Q_2$ appartient à Q*

Démonstration Montrons 1. Quitte à conjuguer $Q = P_1 \cap P_2$, on peut supposer $B \subset Q$. D'où $B \subset P_1$ et $B \subset P_2$. D'où $P_i = G_{X_i}$ avec $X_i \subset S$. Par hypothèses, $gBg^{-1} \subset gP_1g^{-1} \subset P_2 = G_{X_2}$. D'après la proposition 2.12, on a $g \in P_2$. L'assertion 2 découle immédiatement de 1. Sous les hypothèses du 3, on a $gQ_1g^{-1} \subset Q$, d'où $g \in Q$ d'après 1. □

Corollaire 2.17 *Tout sous-groupe parabolique est son propre normalisateur.*

Démonstration Ceci résulte du 3 du théorème précédent, en prenant $Q = Q_1 = Q_2$. □

2.5 Le théorème de simplicité de Tits

Lemme 2.18 *Soit H un sous-groupe distingué de G. Il existe une partie X de S telle que $BH = G_X$ et tout élément de X commute à tout élément de $S \setminus X$.*

Démonstration Puisque BH est un sous-groupe de G contenant B, il existe une unique partie X de S telle que $BH = G_X$. Soient $s_1 \in X$ et $s_2 \in S \setminus X$, n_1 et n_2 des représentants respectifs de s_1 et s_2 dans N. On a $n_1 \in G_X = BH$, donc il existe $b \in B$ tel que $bn_1 \in H$. Soit $h = n_2 b n_1 n_2^{-1}$. L'élément $h \in H$ car H est distingué dans G. De plus, $h \in \mathrm{C}(s_2).\mathrm{C}(s_1).\mathrm{C}(s_2)$.

Si $l_S(s_2 s_1 s_2) = 3$, le corollaire 2.6 entraîne $\mathrm{C}(s_2 s_1 s_2) = \mathrm{C}(s_2).\mathrm{C}(s_1).\mathrm{C}(s_2)$. Donc $H \cap \mathrm{C}(s_2 s_1 s_2) \neq \varnothing$. D'où $G_X \cap \mathrm{C}(s_2 s_1 s_2) \neq \varnothing$, et $s_2 s_1 s_2 \in W_X$. D'après la proposition 1.12, comme $(s_2 s_1 s_2)$ est une décomposition réduite, on a $s_2 \in X$, ce qui contredit l'hypothèse.

On a donc $l_S(s_2 s_1 s_2) \leq 2$. Si $l_S(s_1 s_2) = 1$, on a $s_1 s_2 \in S$, donc $(s_1 s_2)^2 = 1$, et s_1 et s_2 commutent. Si $l_S(s_1 s_2) = 2$, par la condition d'échange (théorème 1.15), on a encore s_1 et s_2 qui commutent. □

Théorème 2.19 (Théorème de simplicité de Tits) *Soit Z l'intersection des conjugués de B, soit U un sous-groupe de B et soit G_1 le sous-groupe engendré par les conjugués de U dans G. On suppose que :*

1. *U est distingué dans B et $B = UT$.*
2. *Pour tout sous-groupe distingué V de U distinct de U, le groupe des commutateurs de U/V est distinct de U/V.*
3. *G_1 est égal à son groupe des commutateurs.*
4. *Le système de Coxeter (W, S) est irréductible.*

Alors tout sous-groupe H de G normalisé par G_1 est contenu dans Z ou contient G_1.

Remarque 2.20 Si U est résoluble, alors 2 est immédiatement vérifié. En effet, si par l'absurde il existe V distingué tel que le groupe dérivé de U/V est lui-même, alors U/V n'est pas résoluble, ce qui est impossible.

Démonstration Montrons d'abord que $G = G_1 T$. Le groupe $G_1 T$ contient B, donc est parabolique, et ainsi est son propre normalisateur, d'après le corollaire 2.17. Comme N normalise G_1 (car G_1 est distingué dans G) et T (car (G, B, N, S) est un système de Tits), il normalise $G_1 T$, donc $N \subset G_1 T$. Puisque $B \cup N$ engendre G, on a bien $G = G_1 T$.

On pose

$$G' = G_1 H, \quad B' = B \cap G, \quad N' = N \cap G',$$
$$T' = T \cap G' = B' \cap N' \quad \text{et} \quad W' = N'/T'.$$

On a $G = G'T$ puisque G' contient G_1, d'où $N = N'T$. L'injection de N' dans N définit donc, par passage au quotient, un isomorphisme ψ de W' dans W. On pose S' l'image réciproque de S par cet isomorphisme.

Montrons que (G', B', N', S') est un système de Tits. Comme U est distingué dans B,

$TU = UT$, et donc comme $G = BNB$, il vient $G = UNU$. Comme U est un sous-groupe de G', on en déduit $G' = UN'U$, d'où (T_1). La condition (T_2) est trivialement vérifiée grâce à l'isomorphisme ψ. Vérifions (T_3). Soit $w \in W$ et w' son image réciproque par ψ. On a $BwB = BwTB'$. Or $BwT = BwTw^{-1}w = Bw$ car T sous-groupe distingué de N. D'où $BwB = Bw'B'$, et $G' \cap BwB = B'w'B'$. L'axiome (T_3) est alors vérifié, et l'axiome (T_4) découle de $B = B'T$.

Soit H un sous-groupe de G normalisé par G_1. Il est donc distingué dans G'. Par le lemme 2.18 appliqué à (G', B', N', S'), il existe une partie X' de S' telle que $B'H = G_{X'}$, et tout élément de $S' \setminus X'$ commute à tout élément de X'. Par l'hypothèse 4, seuls deux cas sont possibles :

- Si $X' = \varnothing$, alors $B'H = B'$, et $H \subset B' \subset B$. Soit $g \in G$. On peut écrire $g = g_1 t$ avec $g_1 \in G_1$, $t \in T$. Comme G_1 normalise H, $H \subset g_1 H g_1^{-1} \subset g_1 B g_1^{-1}$. Donc $H \subset gBg^{-1}$, et ce pour tout $g \in G$. Par définition de Z, on a $H \subset Z$.
- Si $X' = S'$, alors $B'H = G'$. Comme $G = G'T$, $G = B'HT = HB'T = HB$. Le groupe B normalisant U, tout conjugué de U est de la forme hUh^{-1} avec $h \in H$. Comme H est normalisé par U, un tel sous-groupe est contenu dans UH, d'où $G_1 \subset UH$ par définition. Ainsi, $UH = G_1 H$. On a donc

$$U/(U \cap H) = UH/H = G_1 H/H = G_1/(G_1 \cap H).$$

  D'après l'hypothèse 3, $G_1/(G_1 \cap H)$ est égal à son groupe dérivé. D'après l'hypothèse 2, $U/(U \cap H)$ est donc réduit à l'élément neutre. D'où $G_1 \cap H = G_1$, et $G_1 \subset H$.

$\square$

Corollaire 2.21 *Sous les hypothèses du théorème 2.19, le groupe $G_1/(G_1 \cap Z)$ est simple non commutatif, ou réduit à l'élément neutre.*

Démonstration Le théorème 2.19 montre que $G_1/(G_1 \cap Z)$ est simple ou réduit à l'élément neutre ; d'autre part l'hypothèse 3 entraîne qu'il est égal à son groupe des commutateurs ; d'où le corollaire. $\square$

3 Le cas de $\mathrm{GL_n}(\mathbf{K})$

3.1 Système de Tits

Dans toute la suite, on désigne par $G = \mathrm{GL_n}(\mathbf{K})$ le groupe linéaire de dimension n sur un corps $\mathbf{K}$ commutatif. On pose également

- B le groupe des matrices triangulaires supérieures de G ;
- N le groupe des matrices monomiales (dont chaque ligne et chaque colonne possède un unique élément non nul) ;
- $T = B \cap N$ l'ensemble des matrices diagonales ;
- $W = N/T$ l'ensemble des matrices de permutation, isomorphe à $\mathfrak{S}_n$;
- S l'ensemble des transpositions de la forme $(i, i+1)$ ou $i \in [\![1, n-1]\!]$.

On remarque que $N = T \rtimes W$.

Commençons par montrer un lemme :

Proposition 3.1 (Décomposition de Bruhat de G) *Le groupe G se décompose de la façon suivante :*

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

Démonstration Montrons que cette union est disjointe. Soient $w, w' \in W$, $b_1, b_2, b_3, b_4 \in B$ tels que $b_1 w b_2 = b_3 w' b_4$. Alors $w b_2 b_4^{-1} w'^{-1} = b_1^{-1} b_3$, d'où

$$w_1 b w_2 \in B$$

si $w_1 = w$, $w_2 = w'^{-1}$ et $b = b_2 b_4^{-1}$. Soit $b(t)$ la matrice obtenue à partir de b en multipliant les éléments non diagonaux par t. On a alors $w_1 b(t) w_2 \in B$ car w_1 et w_2 sont des matrices de permutation. En particulier, si $t = 0$, $b(0)$ est diagonale et donc $w_1 w_2 \in B \cap W$, d'où $w_1 w_2 = \mathrm{I}_n$, et $w = w'$.

Montrons que G est bien la réunion de ces doubles classes. Cela revient donc à montrer que l'on peut, à partir d'une matrice inversible de G, se ramener à une matrice de permutation à l'aide des opérations suivantes :

- $L_i \leftarrow L_i + \lambda L_j$ si $\lambda \in \mathbf{K}$ et $i < j$;
- $C_i \leftarrow C_i + \lambda C_j$ si $\lambda \in \mathbf{K}$ et $j < i$;
- $L_i \leftarrow \lambda L_i$ si $\lambda \in \mathbf{K}^*$;
- $C_i \leftarrow \lambda C_i$ si $\lambda \in \mathbf{K}^*$.

Soit $M = (a_{i,j})_{i,j \in [\![1,n]\!]} \in G$. Soit j minimal tel que $a_{n,j} \neq 0$. Avec les opérations décrites ci-dessus, on peut faire en sorte que la ligne n et la colonne j n'aient que des coefficients nuls à l'exception de $a_{n,j}$, que l'on peut rendre égal à 1. On procède de même de la ligne $n-1$ à la ligne 1. On obtient bien une matrice de permutation. □

Proposition 3.2 *Le quadruplet (G, B, N, S) forme un système de Tits.*

Démonstration L'axiome (T_1) est vérifié : $B \cup N$ engendre G par la proposition 3.1, et les matrices diagonales commutent aux matrices monomiales, donc T est distingué dans N. Il est bien connu que S engendre $\mathfrak{S}_n$, donc le quadruplet vérifie l'axiome (T_2).

Montrons que (T_3) est vérifié, *i.e.* que si $s_j = (j, j+1)$, et $w \in W$, $s_j B w \subset BwB \cup Bs_j wB$, ou encore

$$s_j B \subset BB' \cup Bs_j B',$$

où $B' = wBw^{-1}$. Soit (e_i) la base canonique de $\mathbf{K}^n$, et G_j le sous-groupe de G formé des éléments laissant fixes les e_i pour $i \neq j, j+1$ et laissant stable le plan engendré par e_j et e_{j+1} ; ce groupe est isomorphe à $\mathrm{GL}_2(\mathbf{K})$. On vérifie que $G_jB = BG_j$. Comme $s_j \in G_j$, on a $s_jB \subset BG_j$. Il suffit donc de montrer que

$$G_j \subset (B \cap G_j)(B' \cap G_j) \cup (B \cap G_j)s_j(B' \cap G_j).$$

Si on identifie G_j à $\mathrm{GL}_2(\mathbf{K})$, alors le groupe $B \cap G_j$ s'identifie au sous-groupe triangulaire supérieur B_2 de $\mathrm{GL}_2(\mathbf{K})$; le groupe $B' \cap G_j$ s'identifie à B_2 lorsque $w(j) < w(j+1)$, et au sous-groupe triangulaire inférieur B_2^- sinon.
Dans le premier cas, la formule à démontrer s'écrit

$$\mathrm{GL}_2(\mathbf{K}) = B_2 \cup B_2 s B_2, \qquad \text{où} \quad s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Elle résulte de la décomposition de Bruhat (proposition 3.1) par exemple.
Dans le second cas, la formule à démontrer est

$$\mathrm{GL}_2(\mathbf{K}) = B_2 B_2^- \cup B_2 s B_2^-,$$

qui résulte de la première par multiplication à droite par s, puisque $B_2^- = sB_2s$.

Vérifions l'axiome (T_4). Soit $s = s_j \in S$. Soit b la matrice telle que $b(e_i) = e_i$ pour tout $i \neq j, j+1$, et tel que sa restriction à (e_j, e_{j+1}) soit

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

Alors $b \in B$, mais $sbs^{-1} \notin B$. D'où l'axiome (T_4) est vérifié. □

THÉORÈME 3.3 *Le couple (W, S) forme un système de Coxeter.*

DÉMONSTRATION C'est une conséquence immédiate de la proposition précédente, et démontre la remarque 1.4. □

3.2 Simplicité de $\mathrm{PSL_n}(\mathbf{K})$

Dans ce paragraphe, on montre certaines propriétés de $\mathrm{SL_n}(\mathbf{K})$, et ce grâce au théorème de simplicité de Tits. Soit U l'ensemble des matrices unipotentes, *i.e.* triangulaires et dont tous les éléments de la diagonale sont 1, qui est un sous-groupe de B.

LEMME 3.4 *Le sous-groupe G_1 engendré par les conjugués de U dans G est* $\mathrm{SL_n}(\mathbf{K})$.

DÉMONSTRATION Tout les éléments de G_1 sont dans $\mathrm{SL_n}(\mathbf{K})$ car ils sont de déterminant 1. Réciproquement, $\mathrm{SL_n}(\mathbf{K})$ est engendré par les transvections. Soit $T_{i,j}(\lambda)$ une transvection. Si $i < j$, $T_{i,j}(\lambda) \in U$. Sinon, si

$$J = \begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix},$$

alors $JT_{i,j}(\lambda)J^{-1} = T_{j,i}(\lambda) \in U$, ce qui conclut la preuve. □

Lemme 3.5 *Deux transvections sont toujours conjuguées dans* $\mathrm{GL_n}(\mathbf{K})$.

Démonstration Soient u et v deux transvections. Comme elles ont la même matrice dans deux bases différentes, elles sont conjuguées dans $\mathrm{GL_n}(\mathbf{K})$. □

Proposition 3.6 *Si $n \geq 3$ ou si $n = 2$ et* $\mathrm{card}(\mathbf{K}) \geq 4$, $\mathrm{SL_n}(\mathbf{K})$ *est égal à son groupe des commutateurs (i.e. son groupe dérivé).*

Démonstration Soit D le groupe dérivé de $\mathrm{SL_n}(\mathbf{K})$. Il suffit de montrer que D contient une transvection $[u, v]$. En effet, si c'est le cas, soit t une transvection. Par le lemme 3.5, soit $w \in \mathrm{GL_n}(\mathbf{K})$ tel que $w[u, v]w^{-1} = t$. Alors

$$t = w[u, v]w^{-1} = [wuw^{-1}, wvw^{-1}].$$

Le groupe $\mathrm{SL_n}(\mathbf{K})$ étant conjugué dans $\mathrm{GL_n}(\mathbf{K})$, on a donc $t \in D$. Comme les transvections engendrent $\mathrm{SL_n}(\mathbf{K})$, $D = \mathrm{SL_n}(\mathbf{K})$.
Montrons donc que D contient une transvection.

- Si $\mathbf{K}$ est de cardinal au moins 4, soit $\lambda \neq 0, 1, -1$. Soient

$$s = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \quad s' = \begin{pmatrix} \mathrm{I}_{n-2} & 0 \\ 0 & s \end{pmatrix} \quad \text{et} \quad t' = \begin{pmatrix} \mathrm{I}_{n-2} & 0 \\ 0 & t \end{pmatrix}.$$

  Alors $[s', t']$ est une transvection car $\lambda^2 - 1 \neq 0$.
- Si $\mathbf{K}$ est de cardinal 2 ou 3 et $n \geq 3$, on prend

$$s = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

  On a alors $[s, t]$ est bien une transvection, et on généralise à $n \geq 3$ de la même façon qu'au point précédent.

□

Dans toute la suite, on se place dans le cas $n \geq 3$ ou $n = 2$ et $\mathrm{card}(\mathbf{K}) \geq 4$.

Proposition 3.7 *Avec les notations précédentes, les hypothèses du théorème 2.19 sont vérifiées.*

Démonstration L'hypothèse 1 est vérifiée : U est distingué dans B car c'est le noyau de l'homomorphisme qui à toute matrice associe ses coefficients diagonaux. De plus, $B = UT$ de manière évidente.

Le groupe U est résoluble, donc la propriété 2 est vérifiée. En effet, si G_m est l'ensemble des matrices triangulaires supérieures, de diagonale 1, dont toutes les diagonales $\{i = j + k\}$, $k \in [\![1, m]\!]$ sont nulles, en posant $G_{-1} = U$, $G_n = \{\mathrm{I}_n\}$, et pour tout i, G_{i+1} est distingué dans G_i et G_i/G_{i+1} est abélien.

La propriété 3 est vérifiée grâce à la proposition 3.6.

Le système de Coxeter (W, S) est irréductible. En effet, si S' et S'' forment une partition de S et tous les éléments de S' commutent à tous ceux de S'', supposons S' non vide. Soit $(j, j + 1) \in S'$. Alors $(j - 1, j)$ et $(j + 1, j + 2)$ ne sont pas dans S'' car ne commutent pas à $(j, j + 1)$. Donc ils appartiennent à S'. De proche en proche, on obtient donc $S' = S$. □

Lemme 3.8 *Si Z est l'intersection des conjugués de B, alors $Z = D$ l'ensemble des matrices scalaires.*

Démonstration Un élément de Z est trigonalisable dans toute base, donc tout vecteur est vecteur propre, et cet élément est diagonal. □

Théorème 3.9 *Tout sous-groupe distingué propre de $\mathrm{SL_n}(\mathbf{K})$ est sous-groupe de Z.*

Démonstration C'est exactement le théorème de Tits (théorème 2.19). □

Corollaire 3.10 *Le groupe $\mathrm{PSL_n}(\mathbf{K}) = \mathrm{SL_n}(\mathbf{K})/(D \cap \mathrm{SL_n}(\mathbf{K}))$ est simple.*

Démonstration C'est une conséquence directe du corollaire 2.21. Ceci avait déjà été prouvé par Iwasawa (voir [4]). □

Conclusion

Le théorème de Tits permet de montrer la plupart des résultats de simplicité connus. Notamment, $\mathrm{PSL_n}(\mathbf{K})$ est simple dans le cas d'un corps commutatif. Il existe des corps gauche (*i.e.* des corps non commutatifs), comme par exemple l'algèbre des quaternions. Platonov a montré dans [6] qu'il existe $\mathbf{K}$ un corps et D un corps gauche de centre $\mathbf{K}$ tels que le théorème de simplicité est faux, *i.e.* tels que $\mathrm{SL}_n(D)$ a un sous-groupe propre non central. En fait, $G_1 \subsetneq \mathrm{SL}_n(D)$ donc le théorème ne s'applique pas. L'étude du groupe $\mathrm{SL}_n(D)/G_1$ constitue un sujet actuel de recherche.

Bibliographie

[1] Nicolas Bourbaki, *Éléments de mathématique, groupes et algèbres de Lie*, chap. IV à VI, Hermann, 1968, § 1–2, pp. 9–32

[2] David Harari, *Cours d'algèbre, groupes et géométrie*, `http://www.math.u-psud.fr/~harari/exposes/geom.pdf`, 2010

[3] James E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge Studies in advanced mathematics, 1990, chap 1, pp. 3–28

[4] K. Iwasawa, *Über die Struktur der endlichen Gruppen, deren echte Untergruppen sämtlich nilpotent sind*, Proc. Phys. Math. Soc. Japan, 23, 1941

[5] Daniel Perrin, *Cours d'algèbre*, Ellipses, 1996, § 4

[6] V. P. Platonov, *The Tannaka-Artin Problem and reduced K-theory*, Math. USSR Izv. 10 21, 1976, pp. 227–261

[7] Jacques Tits, *Algebraic and abstract simple groups*, Annals of maths, 1964, pp. 313-329