ENS DE LYON

Rapport de stage de Master 1

(B,N)-paires et groupes finis de type Lie

Auteur :
Bruno Laurent

Directeur de stage :
M. Michaël Bulois

27 mai 2013 - 7 juillet 2013

Institut Camille Jordan - Saint-Étienne

Table des matières

Remerciements

Je tiens à remercier tout particulièrement Monsieur Michaël Bulois et à lui adresser toute ma reconnaissance pour avoir accepté d'encadrer mon stage de Master 1 et s'être montré si disponible. Ses précieux conseils m'ont permis de comprendre un peu mieux ces objets passionants que sont les groupes algébriques et les groupes finis de type Lie, et de découvrir la notion de (B,N)-paire.

Je remercie également tous les membres du site stéphanois de l'Institut Camille Jordan. Grâce à leur accueil chaleureux, j'ai passé six excellentes semaines au sein du laboratoire.

Je remercie enfin Messieurs Alexis Tchoudjem et Emmanuel Grenier pour m'avoir aidé à trouver un stage intéressant.

Introduction

La notion de groupe muni d'une (B,N)-paire a été introduite par Jacques Tits en 1962 dans [9], dans le but de donner une interprétation géométrique de certains groupes simples, grâce à la théorie des immeubles. Le premier objectif de mon stage a été de me familiariser avec cette notion et avec quelques-unes de ses conséquences combinatoires, en particulier la décomposition de Bruhat et sa version forte quand la (B,N)-paire est scindée. En revanche, je n'ai pas du tout abordé l'aspect « théorie des immeubles ».

Les groupes auxquels Jacques Tits s'est intéressé sont des groupes finis de type Lie. Ceux-ci sont des analogues algébriques des groupes de Lie, définis non pas sur $\mathbf{R}$ ou $\mathbf{C}$ mais sur des corps finis [1]. Cependant, en géométrie algébrique, et en particulier en théorie des groupes algébriques, on se place souvent sur un corps algébriquement clos, notamment pour disposer du théorème des zéros de Hilbert et de plusieurs résultats de connexité. Le second objectif de mon stage a donc été de comprendre comment, partant du cas où le corps est fini, on peut se ramener au cas algébriquement clos. Cela se fait grâce à la notion de structure $\mathbf{F}_q$-rationnelle, et les groupes finis de type Lie apparaissent alors naturellement.

Bien qu'ils paraissent très différents, les deux objectifs se rejoignent. En effet, les résultats obtenus sur les (B,N)-paires permettent de donner une structure commune aux groupes finis de type Lie et d'accéder à certaines informations sur ces groupes. C'est ainsi que, dans ce rapport, on apporte tous les outils nécessaires au calcul de leur cardinal grâce aux (B,N)-paires.

Au cours de mon stage, j'ai dû étudier, vérifier et mettre en perspective plusieurs résultats présentés par Meinolf Geck dans [3]. J'ai notamment été amené à compléter certaines démonstrations, par exemple en énonçant et démontrant la proposition 3.1.10 sur le produit de variétés munies d'une structure $\mathbf{F}_q$-rationnelle ; cette proposition est utilisée dans une étape cruciale de la démonstration du théorème 3.2.3. J'ai également énoncé et démontré la proposition 1.2.12, même si elle n'est pas vraiment utilisée ensuite.

La première section de ce rapport traite des groupes munis d'une (B,N)-paire. Après avoir introduit la notion de (B,N)-paire, on présente quelques résultats divers. Le but principal, qui fait l'objet des trois premières sous-sections, est d'arriver à la décomposition de Bruhat (théorème 1.1.8) et à une version forte de celle-ci (théorème 1.2.13), et surtout d'expliquer comment cette décomposition se comporte sous l'action d'un automorphisme de groupe (théorème 1.3.4). La quatrième sous-section, indépendante, établit un lien combinatoire entre les séries de Hilbert d'un groupe de Weyl et le système de racines correspondant (théorème 1.4.8) ; cela permettra d'effectuer plus efficacement les calculs de la sous-section 3.3.

Dans la deuxième section, on étudie deux exemples de groupes munis d'une (B,N)-paire : le groupe général linéaire et le groupe symplectique. Il s'agit de deux cas particuliers d'un résultat général sur les groupes algébriques réductifs, énoncé en fin de section (théorème 2.3.1).

La troisième section est consacrée aux structures $\mathbf{F}_q$-rationnelles et aux groupes finis de type Lie. Dans la première sous-section, on introduit la notion de structure $\mathbf{F}_q$-rationnelle sur une variété affine et on explique pourquoi cela correspond bien à l'idée intuitive de « variété affine sur $\mathbf{F}_q$ ». Dans la sous-section suivante, on s'intéresse au cas où la variété affine est un groupe algébrique. On y montre entre autres le théorème de Lang-Steinberg (théorème 3.2.4). Dans la dernière sous-section, on définit enfin les groupes finis de type Lie et on explique comment utiliser les théorèmes 1.3.4, 2.3.1 et 3.2.4 pour les munir d'une (B,N)-paire et calculer leur cardinal (théorème 3.3.4). Pour illustrer la formule obtenue, on traite les exemples du groupe général linéaire et du groupe symplectique, en utilisant les séries de Hilbert de la fin de la première section.

Enfin, une annexe regroupe quelques définitions et résultats sur les groupes algébriques, qui peuvent faciliter la compréhension des deuxième et troisième sections. Cette annexe détaille également certains calculs laissés de côté dans le corps du rapport.

1. En outre, ces groupes sont d'un intérêt tout particulier puisque tout groupe fini simple est soit un groupe alterné, soit un groupe sporadique, soit un groupe fini de type Lie (voir par exemple [2, p. 1]).

1 (B,N)-paires

Dans cette section, on commence par présenter quelques propriétés élémentaires des (B,N)-paires, dont la décomposition de Bruhat (théorème 1.1.8) et le lien avec les groupes de Coxeter (théorème 1.1.19). Ensuite, on étudie le cas où le groupe de Weyl de la (B,N)-paire est fini et introduit la notion de (B,N)-paire scindée, ce qui conduit à une version forte de la décomposition de Bruhat (théorème 1.2.13). Puis, on montre comment, à partir d'un groupe G muni d'une (B,N)-paire scindée et d'un automorphisme φ, on peut obtenir une (B,N)-paire scindée pour le sous-groupe des points fixes G^φ (théorème 1.3.4). Enfin, on définit les séries de Hilbert et on donne un moyen de les calculer quand le groupe de Weyl est un groupe de réflexion fini (théorème 1.4.8). Les références principales utilisées sont [1], [3] et [4] pour les trois premières sous-sections, et [1] et [2] pour la dernière sous-section.

1.1 Généralités

Définition 1.1.1 : *Soit G un groupe, B et N deux sous-groupes de G, $H := B \cap N$ et $W := N/H$. On dit que B et N constituent une* **(B,N)-paire** *pour G si :*

(BN1) *on a $G = \langle B, N\rangle$;*

(BN2) *on a $H \trianglelefteq N$ et W est engendré (comme groupe) par un ensemble S (non vide) d'éléments d'ordre 2 ;*

(BN3) *pour tout $s \in S$ et tout représentant $n_s \in N$ de s, on a $n_s B n_s \neq B$;*

(BN4) *pour tous $s \in S$ et $n \in N$, on a $n_s B n \subseteq B n_s n B \cup B n B$;*

(BN5) *on a $\bigcap_{n\in N} nBn^{-1} = H$.*

H est appelé le **sous-groupe de Cartan** *et W est appelé le* **groupe de Weyl**. *Les sous-ensembles $C(w) := Bn_wB$ pour $w \in W$ et $n_w \in N$ un représentant de w sont appelés les* **cellules de Bruhat**.

Remarques 1.1.2 :

• Comme on a $H \leq B$, les conditions (BN3) et (BN4) et la définition des $C(w)$ ne dépendent pas des représentants choisis. De plus, pour vérifier (BN4), il suffit de montrer que pour tous $s \in S$ et $w \in W$, on a $n_s B n_w \subseteq B n_s n_w B \cup B n_w B$.

• Bourbaki appelle (G, B, N) un **système de Tits**. La proposition 1.1.13 justifiera que l'on ne mentionne pas S dans le triplet (G, B, N).

• Les cellules de Bruhat sont des orbites pour l'action de $B \times B$ sur G définie par $\forall (b, b') \in B \times B, \forall g \in G, (b, b') \cdot g := bgb'^{-1}$. En particulier, deux cellules sont toujours soit disjointes soit égales, donc pour $g \in G$ et $w \in W$, si $g \in C(w)$ alors $BgB = C(w)$.

Exemple 1.1.3 : Soit $n \geq 3$. Soit $G := \mathfrak{S}_n$ agissant sur $\{1, \dots, n\}$, $B := \mathrm{Fix}_G(n) = \mathfrak{S}_{n-1}$ et $N := \mathrm{Stab}_G(\{n-1, n\}) = \mathfrak{S}_{n-2} \cdot \langle \tau\rangle$ avec τ la transposition échangeant $n-1$ et n. Alors on a déjà $G = \langle B, N\rangle$, $H = \mathfrak{S}_{n-2} \trianglelefteq N$ et $W = \langle \overline{\tau}\rangle \simeq \mathbf{Z}/2\mathbf{Z}$ (on pose donc $S := \{\overline{\tau}\}$). On a $n \geq 3$ donc $\tau B \tau = \mathrm{Fix}_G(n-1) \neq B$. De plus, on a $\tau B \subseteq B\tau B$ et pour $b \in B$, on a $\tau b \tau = b \in B$ si $b \in H$ et, avec σ la transposition échangeant $n-1$ et $b^{-1}(n-1)$, $\tau b \tau = (\tau b \tau \sigma \tau)\tau\sigma \in B\tau B$ sinon, donc $\tau B \tau \subseteq B \cup B\tau B$. Enfin, $\bigcap_{n\in N} nBn^{-1} = B \cap \tau B \tau = \mathrm{Fix}_G(n-1, n) = H$. Par conséquent, B et N constituent une (B,N)-paire pour G.

Exemple 1.1.4 : Soit $\mathbf{K}$ un corps commutatif muni d'une valuation discrète v, A son anneau de valuation et $t \in A$ une uniformisante. Soit $G := \mathrm{SL}_2(\mathbf{K})$, $B := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(A) \,\middle|\, v(c) \geq 1 \right\}$ et $N := \left\{ \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix} \,\middle|\, a \in \mathbf{K}^\times \right\} \cup \left\{ \begin{pmatrix} 0 & b \\ -\frac{1}{b} & 0 \end{pmatrix} \,\middle|\, b \in \mathbf{K}^\times \right\}$ l'ensemble des matrices monomiales de G. On vérifie très facilement que B et N sont des sous-groupes de G. Démontrons qu'ils constituent une (B,N)-paire pour G, dont le groupe de Weyl est le groupe diédral infini $(\mathbf{Z}/2\mathbf{Z}) * (\mathbf{Z}/2\mathbf{Z})$ (où $*$ désigne le produit libre).

B contient les matrices triangulaires supérieures de $\mathrm{SL}_2(A)$ et N contient $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ donc $\langle B, N\rangle$ contient toutes les matrices élémentaires à coefficients dans A. Pour $M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \in G$, on peut choisir le coefficient non nul m_{ij} dont la valuation est minimale et effectuer des opérations élémentaires sur les lignes et les colonnes pour annuler les autres coefficients sur la ligne i et ceux sur la ligne j. Comme $v(m_{ij})$ est minimale, cela revient à multiplier par des matrices élémentaires à coefficients dans A (donc par des éléments de $\langle B, N\rangle$). On obtient ainsi une matrice monomiale, nécessairement de déterminant 1, donc dans N. Donc $M \in \langle B, N\rangle$. Donc $G = \langle B, N\rangle$. On a $H = \left\{ \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix} \,\middle|\, a \in A^\times \right\}$ et on vérifie facilement $H \trianglelefteq N$. Avec $n_1 := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in N$ et $n_2 := \begin{pmatrix} 0 & t \\ -\frac{1}{t} & 0 \end{pmatrix} \in N$, on a $W = \langle n_1 H, n_2 H\rangle$, $n_1 H$ et $n_2 H$ sont d'ordre 2 et $W \simeq \langle n_1 H\rangle * \langle n_2 H\rangle$ (voir calculs en annexe).

On a $n_1 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} n_1 = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$ et $n_2 \begin{pmatrix} 1 & t^2 \\ 0 & 1 \end{pmatrix} n_2 = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$ donc $n_1 B n_1 \neq B$ et $n_2 B n_2 \neq B$.
La vérification de (BN4) est un peu fastidieuse mais n'est pas difficile (voir calculs en annexe).
Enfin, on a $\forall m \in \mathbf{Z}, \forall M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in B, (n_1 n_2)^m M (n_1 n_2)^{-m} = \begin{pmatrix} a & bt^{2m} \\ \frac{c}{t^{2m}} & d \end{pmatrix}$ donc $H \subseteq \bigcap_{n \in \mathbf{N}} nBn^{-1} \subseteq \bigcap_{m \in \mathbf{Z}} (n_1 n_2)^m B (n_1 n_2)^{-m} = H$.

Les groupes algébriques réductifs sont des exemples importants de groupes munis d'une (B,N)-paire et font l'objet de la section 2.

Pour $w \in W$, on note $l(w)$ la plus petite longueur des expressions de w comme mot sur S, avec la convention $l(1) = 0$. Une expression de w de longueur $l(w)$ est dite **réduite**. Remarquons que si $s_1 \cdots s_p$ (avec les s_i dans S) est une expression réduite alors $s_2 \cdots s_p$ et $s_1 \cdots s_{p-1}$ sont réduites.

Comme les éléments de S sont d'ordre 2, en prenant une expression réduite de w et en passant à l'inverse, on obtient $l(w^{-1}) = l(w)$. On a aussi $\forall w \in W \setminus \{1\}, \exists s \in S, l(sw) = l(w) - 1$, car il suffit de prendre pour s le premier terme d'une expression réduite de w ; on a également $\forall w \in W \setminus \{1\}, \exists s \in S, l(ws) = l(w) - 1$. Cela servira régulièrement dans des raisonnements par récurrence.

En considérant des expressions réduites, on a $\forall w \in W, \forall s \in S, l(w) - 1 \leq l(sw) \leq l(w) + 1$ et $l(w) - 1 \leq l(ws) \leq l(w) + 1$ (mais on n'a pas nécessairement $l(sw) = l(ws)$).

Les lemmes suivants énoncent des faits élémentaires et découlent directement de la définition de (B,N)-paire.

Lemme 1.1.5 : *Les représentants des éléments de W vérifient :*
- $\forall s \in S, n_s H = n_s^{-1} H$ *donc* $n_s B = n_s^{-1} B$ *et* $B n_s = B n_s^{-1}$;
- $\forall w \in W, \forall w' \in W, n_{ww'} H = n_w n_{w'} H$ *donc* $n_{ww'} B = n_w n_{w'} B$ *et* $B n_{ww'} = B n_w n_{w'}$.

Démonstration : On a $H \trianglelefteq N$ donc $H = s^2 = n_s H n_s H = n_s H n_s$ et $n_{ww'} H = ww' = n_w H n_{w'} H = n_w n_{w'} H$. □

Remarques 1.1.6 :
- En revanche, il n'existe pas nécessairement de choix de représentants tels que l'on ait $\forall w \in W$, $\forall w' \in W, n_{ww'} = n_w n_{w'}$. En effet, avec les notations de l'exemple 1.1.4, quel que soit le représentant n de $n_1 H$, on a $n^3 = -n \neq n$ (si $\mathbf{K}$ n'est pas de caractéristique 2) mais $(n_1 H)^3 = n_1 H$.
- En utilisant (BN4), on déduit $\forall s \in S, \forall w \in W, C(s)C(w) \subseteq C(sw) \cup C(w)$.

Lemme 1.1.7 : (BN4') *Pour tous $s \in S$ et $n \in N$, on a $nBn_s \subseteq Bnn_sB \cup BnB$.*

Démonstration : D'après (BN4), on a $n_s B n^{-1} \subseteq B n_s n^{-1} B \cup B n^{-1} B$ donc il suffit de passer à l'inverse. □

L'action de $B \times B$ sur G induit une partition de G en $(B \times B)$-orbites. Le théorème suivant donne une forme plus précise de cette partition.

Théorème 1.1.8 (Décomposition de Bruhat) : *Soit G un groupe muni d'une (B,N)-paire, de groupe de* Weyl *W. Alors on a $G = \bigsqcup_{w \in W} C(w)$.*

Démonstration :
- BNB n'est pas vide et est stable par passage à l'inverse. De plus, pour tous $(b_1, n_1, b_1') \in B \times N \times B$ et $(b_2, n_2, b_2') \in B \times N \times B$, on a $b_1' b_2 \in B$ donc, d'après (BN4), $n_1 b_1' b_2 n_2 \in n_1 B n_2 \subseteq B n_1 n_2 B \cup B n_2 B \subseteq BNB$. Donc $b_1 n_1 b_1' b_2 n_2 b_2' \in BNB$, donc BNB est stable par multiplication. Donc BNB est un sous-groupe de G. Comme on a $G = \langle B, N \rangle$ et $H \leq B$, on a donc $G = BNB = \bigcup_{n \in N} BnB = \bigcup_{w \in W} Bn_wB$.
- Soit $w \in W$ et $w' \in W$ tels que $C(w) = C(w')$; quitte à échanger w et w', on peut supposer $l(w) \leq l(w')$. Démontrons par récurrence sur $l(w)$ que l'on a $w = w'$, ce qui montrera que la réunion du point précédent est une réunion disjointe. Si $l(w) = 0$ alors $w = 1$ donc $C(w') = C(1) = B$ donc $n_{w'} \in B$ or on a déjà $n_{w'} \in N$ donc $n_{w'} \in B \cap N = H$ donc $w' = 1 = w$. Supposons $l(w) \geq 1$ et supposons que le résultat est démontré au rang $l(w) - 1$. Soit $s \in S$ tel que $l(sw) = l(w) - 1$. Alors on a $n_s n_{sw} B = n_{ssw} B = n_w B \subseteq C(w) = C(w')$

donc $n_{sw}B \subseteq n_s^{-1}C(w') = n_sC(w')$ donc $C(sw) \subseteq C(s)C(w') \subseteq C(sw') \cup C(w')$ donc $C(sw) = C(sw')$ ou $C(sw) = C(w')$. Or on a $l(sw) = l(w) - 1 \leq l(w') - 1 \leq l(sw')$ et $l(sw) < l(w')$ donc, par hypothèse de récurrence, $sw = sw'$ ou $sw = w'$. Pour raison de longueur, on a $sw \neq w'$, donc $sw = sw'$ donc $w = w'$. □

Les lemmes suivants précisent le comportement des cellules de BRUHAT vis-à-vis de la multiplication.

Lemme 1.1.9 : *Soit $s \in S$ et $w \in W$. Alors $l(sw) = l(w)+1$ ou $l(sw) = l(w)-1$. De plus, on a respectivement $C(s)C(w) = C(sw)$ et $C(s)C(w) = C(sw) \cup C(w)$.*

Démonstration :

• Premier cas, $l(sw) \geq l(w)$: Démontrons $C(s)C(w) = C(sw)$ par récurrence sur $l(w)$. Si on a $l(w) = 0$ alors $w = 1$ donc $C(s)C(w) = C(s)B = C(s)$. Supposons $l(w) \geq 1$ et supposons que le résultat est démontré jusqu'au rang $l(w)-1$. Soit $t \in S$ tel que $l(wt) = l(w)-1$. D'après (BN4), on a déjà $C(s)C(w) \subseteq C(sw) \cup C(w)$. Raisonnons par l'absurde et supposons $C(s)C(w) \cap C(w) \neq \emptyset$. Alors on a $n_sBn_w \cap C(w) \neq \emptyset$ donc $n_sBn_{wt} \cap C(w)n_t \neq \emptyset$ donc $C(s)C(wt) \cap C(w)n_t \neq \emptyset$. Or on a $l(swt) \geq l(sw) - 1 \geq l(w) - 1 = l(wt)$ donc, par hypothèse de récurrence, $C(s)C(wt) = C(swt)$ donc $C(swt) \cap C(w)n_t \neq \emptyset$. Donc, d'après (BN4'), $C(swt) \cap C(wt) \neq \emptyset$ ou $C(swt) \cap C(w) \neq \emptyset$ donc $swt = wt$ ou $swt = w$ donc $swt = w$ donc $l(sw) = l(wt) = l(w) - 1$, ce qui contredit $l(sw) \geq l(w)$. Par conséquent, on a $C(s)C(w) \cap C(w) = \emptyset$ donc $C(s)C(w) \subseteq C(sw)$; l'inclusion réciproque est évidente.

• Deuxième cas, $l(sw) \leq l(w)$: D'après (BN4), on a $n_sBn_s \subseteq B \cup C(s)$. Or d'après (BN3), on a $n_sBn_s \neq B$ donc $n_sBn_s \subsetneq B$ (sinon $B \subseteq n_s^{-1}Bn_s^{-1} = n_sBn_s \subseteq B$ donc $n_sBn_s = B$) donc $n_sBn_s \cap C(s) \neq \emptyset$ donc $n_sB \cap Bn_sBn_s \neq \emptyset$ donc $C(s)C(w) \cap C(s)C(sw) \neq \emptyset$ or $l(ssw) = l(w) \geq l(sw)$ donc, d'après le premier cas, $C(s)C(sw) = C(ssw) = C(w)$, donc $C(s)C(w) \cap C(w) \neq \emptyset$ donc $C(w) \subseteq C(s)C(w)$ (car tout élément de $C(w)$ est dans la $(B \times B)$-orbite d'un élément de $C(s)C(w) \cap C(w)$). De plus, on a évidemment $C(sw) \subseteq C(s)C(w)$, donc $C(sw) \cup C(w) \subseteq C(s)C(w)$ et, d'après (BN4), il y a égalité.

• On sait déjà $l(w) - 1 \leq l(sw) \leq l(w) + 1$. D'après ce que l'on vient de montrer, on ne peut pas avoir $l(sw) = l(w)$ sinon on aurait $C(sw) = C(sw) \cup C(w)$, ce qui contredirait le fait que les cellules $C(sw)$ et $C(w)$ sont disjointes et non vides. □

Remarque 1.1.10 : En particulier, si $s_1 \cdots s_p$ est une expression réduite alors on a $C(s_1 \cdots s_p) = C(s_1) \cdots C(s_p)$.

Lemme 1.1.11 : *Soit $p \in \mathbf{N}^*$, $s_1 \in S, \ldots, s_p \in S$ et $w \in W$. Alors on a la généralisation de (BN4) suivante :*

$$C(s_1 \cdots s_p)C(w) \subseteq \bigcup_{r=0}^{p} \bigcup_{1 \leq i_1 < \cdots < i_r \leq p} C(s_{i_1} \cdots s_{i_r} w).$$

Démonstration : Pour $p = 1$, il s'agit simplement de (BN4). Le cas général s'obtient par une récurrence immédiate sur p en utilisant $C(s_1 \cdots s_p) \subseteq C(s_1)C(s_2 \cdots s_p)$. □

Lemme 1.1.12 : *Soit P un sous-groupe de G et $w \in W$. Si on a $C(w)C(w^{-1}) \subseteq P$ alors on a $C(w) \subseteq P$.*

Démonstration : Si $l(w) = 0$ alors $C(w) = C(w^{-1}) = C(w)C(w^{-1}) = B$ donc $C(w) \subseteq K$. On suppose désormais $l(w) \geq 1$. Soit $s_1 \cdots s_p$ une expression réduite de w. On a déjà $B \subseteq C(w)C(w^{-1})$ donc $B \subseteq P$. Soit $j \in \{1, \ldots, p\}$ et supposons $C(s_1 \cdots s_{j-1}) \subseteq P$ (avec $C(s_1 \cdots s_{j-1}) = B$ pour $j = 1$). D'après le lemme 1.1.9, on a $C(s_j) \subseteq B \cup C(s_j) = C(s_j)C(s_j)$ donc $C(s_1 \cdots s_j) \subseteq C(s_1 \cdots s_{j-1})C(s_j) \subseteq C(s_1 \cdots s_{j-1})C(s_j)C(s_j) \subseteq C(s_1 \cdots s_{j-1})C(s_j)C(s_{j+1} \cdots s_p)C(s_p \cdots s_{j+1})C(s_j)C(s_{j-1} \cdots s_1)C(s_1 \cdots s_{j-1}) = C(w)C(w^{-1})C(s_1 \cdots s_{j-1})$. P étant stable par multiplication, on a donc $C(s_1 \cdots s_j) \subseteq P$. Par itération, on en déduit le résultat. □

De ces lemmes, on déduit une caractérisation de S et une propriété des sous-groupes de G contenant B.

Proposition 1.1.13 : *On a $S = \{w \in W | w \neq 1$ et $B \cup C(w) \leq G\}$.*

Démonstration :

• Soit $s \in S$. Alors $B \cup C(s)$ est non vide et stable par passage à l'inverse car $s = s^{-1}$. De plus, on a $(B \cup C(s))(B \cup C(s)) = BB \cup BC(s) \cup C(s)B \cup C(s)C(s) \subseteq B \cup C(s) \cup C(s) \cup (C(ss) \cup C(s)) = B \cup C(s)$. Donc $B \cup C(s)$ est un sous-groupe de G.

• Soit $w \in W \setminus \{1\}$ tel que $B \cup C(w)$ est un sous-groupe de G. Soit $s \in S$ avec $l(sw) = l(w) - 1$. Alors, d'après le lemme 1.1.9 on a $C(s)C(w) = C(sw) \cup C(w)$ donc $C(s)C(w) \cap C(w) \neq \emptyset$ donc $n_s \in C(w)C(w^{-1}) = C(w)C(w) \subseteq B \cup C(w)$ car $B \cup C(w)$ est un sous-groupe de G donc est stable par produit. Or, d'après (BN3),

$n_s \notin B$ donc $n_s \in C(w)$ donc on a $C(s) = C(w)$ donc, d'après la décomposition de BRUHAT (théorème 1.1.8), $w = s \in S$. □

Proposition 1.1.14 : *Si P est un sous-groupe de G contenant B alors P est égal à son normalisateur.*

Démonstration : Soit $g \in N_G(P)$. Alors $gBg^{-1} \subseteq gPg^{-1} = P$ donc avec $w \in W$ tel que $g \in C(w)$, on a $C(w)C(w^{-1}) = BgBg^{-1}B \subseteq BPB = P$ donc, d'après le lemme 1.1.12, $C(w) \subseteq P$ donc $g \in P$. □

Enfin, deux propriétés des expressions réduites permettent d'établir le lien avec les groupes de COXETER.

Proposition 1.1.15 (Condition d'échange) : *Soit $w \in W$, $s_1 \cdots s_p$ une expression réduite de w et $s \in S$. Si $l(sw) = l(w) - 1$ alors il existe $i \in \{1, \ldots, p\}$ tel que l'on a $sw = s_1 \cdots \hat{s}_i \cdots s_p$.*

Démonstration : D'après le lemme 1.1.9, on a $C(s)C(w) = C(sw) \cup C(w)$ donc $n_s B n_w \cap C(w) \neq \emptyset$ donc $n_s \in C(w)C(w^{-1})$. Donc, d'après le lemme 1.1.11, il existe des indices $1 \leq i_1 < \ldots < i_r \leq p$ tels que l'on a $n_s \in C(s_{i_1} \ldots s_{i_r} w^{-1})$ donc $C(s) = C(s_{i_1} \ldots s_{i_r} w^{-1})$ donc $s = s_{i_1} \ldots s_{i_r} w^{-1}$. On conclut en utilisant $l(sw) = l(w) - 1$. □

Remarques 1.1.16 :
- En particulier, si $l(sw) = l(w) - 1$ alors il existe une expression réduite de w qui commence par s.
- Par passage à l'inverse, on a une propriété analogue si $l(ws) = l(w) - 1$.

Proposition 1.1.17 (Condition de simplification) : *Soit $p \geq 2$ et $s_1 \in S, \ldots, s_p \in S$. Si $s_1 \cdots s_p$ n'est pas une expression réduite alors il existe des indices i et j avec $i < j$ et $s_1 \cdots s_p = s_1 \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_p$.*

Démonstration : Soit $j \geq 2$ maximal tel que $s_1 \cdots s_{j-1}$ soit une expression réduite. Alors $l(s_1 \cdots s_{j-1} s_j) = l(s_1 \cdots s_{j-1}) - 1$ donc, d'après la condition d'échange 1.1.15, il existe $i \in \{1, \ldots, j-1\}$ tel que $s_1 \cdots s_{j-1} s_j = s_1 \cdots \hat{s}_i \cdots s_{j-1}$. □

Remarque 1.1.18 : En particulier, pour $w \in W$, de toute expression de w on peut obtenir une expression réduite de w en supprimant un nombre pair de termes.

Théorème 1.1.19 : *Soit G un groupe muni d'une (B,N)-paire, de groupe de* WEYL *W engendré par S. Alors W est un groupe de* COXETER *par rapport à S.*

Démonstration :

• Pour $s \in S$ et $s' \in S$, on note $m(s, s') \in \mathbf{N}^* \cup \{+\infty\}$ l'ordre de ss'. Pour $s \in S$, on choisit un symbole t_s et on considère le groupe libre F sur $\{t_s | s \in S\}$. Il existe un unique morphisme de groupes surjectif $e : F \longrightarrow W$ vérifiant $\forall s \in S, e(t_s) = s$ (donné par $e(t_{s_1} \cdots t_{s_n}) = s_1 \cdots s_n$) ; il suffit alors de montrer que $\ker e$ est le sous-groupe distingué engendré par les $(t_s t_{s'})^{m(s,s')}$ pour $m(s, s') < +\infty$, que l'on notera K. Soit $\tilde{w} = t_{s_1} \cdots t_{s_n} \in \ker e$. D'après la condition de simplification 1.1.17, n est pair. Démontrons $\tilde{w} \in K$ par récurrence sur $m := \dfrac{n}{2}$.

• Si $m = 0$ alors il n'y a rien à montrer. Si $m = 1$ alors $s_1 s_2 = 1$ donc $\tilde{w} = t_{s_1}^2 \in K$. Supposons $m \geq 2$ et supposons que le résultat est démontré jusqu'au rang $m - 1$. On a $s_1 \cdots s_n = 1$ donc $s_1 \cdots s_{m+1} = s_n \cdots s_{m+2}$ or le membre de droite est de longueur au plus $m - 1$ donc $s_1 \cdots s_{m+1}$ n'est pas une expression réduite donc, d'après la condition de simplification 1.1.17, il existe des indices $1 \leq i < j \leq m + 1$ tels que $s_1 \cdots s_{m+1} = s_1 \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_{m+1}$ donc $s_{i+1} \cdots s_j = s_i \cdots s_{j-1}$ $(*)$ donc, en passant à l'inverse, $s_j \cdots s_{i+1} = s_{j-1} \cdots s_i$, d'où $(t_{s_{j-1}}^{-1} \cdots t_{s_{i+1}}^{-1} t_{s_i})(t_{s_{i+1}} \cdots t_{s_j}) \in \ker e$. De plus, $s_1 \cdots s_n = s_1 \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_n$ donc $t_{s_1} \cdots \hat{t}_{s_i} \cdots \hat{t}_{s_j} \cdots t_{s_n} \in \ker e$ donc, par hypothèse de récurrence, $t_{s_1} \cdots \hat{t}_{s_i} \cdots \hat{t}_{s_j} \cdots t_{s_n} \in K$. Si $i > 1$ ou $j < m + 1$ alors $l((t_{s_{j-1}}^{-1} \cdots t_{s_{i+1}}^{-1} t_{s_i})(t_{s_{i+1}} \cdots t_{s_j})) = 2(j - i) \leq 2m - 2$ donc, par hypothèse de récurrence, $\tilde{w} = [t_{s_1} \cdots t_{s_i}][(t_{s_i}^{-1} t_{s_{i+1}} \cdots t_{s_{j-1}})(t_{s_{j-1}}^{-1} \cdots t_{s_{i+1}}^{-1} t_{s_i})][(t_{s_{i+1}} \cdots t_{s_j})(t_{s_{j+1}} \cdots t_{s_n})] =$
$[t_{s_1} \cdots \hat{t}_{s_i} \cdots t_{s_{j-1}}][(t_{s_{j-1}}^{-1} \cdots t_{s_{i+1}}^{-1} t_{s_i})(t_{s_{i+1}} \cdots t_{s_j})][t_{s_1} \cdots \hat{t}_{s_i} \cdots t_{s_{j-1}}]^{-1}[t_{s_1} \cdots \hat{t}_{s_i} \cdots \hat{t}_{s_j} \cdots t_{s_n}] \in K$.

• On suppose désormais $i = 1$ et $j = m+1$; alors $(*)$ s'écrit $s_2 \cdots s_{m+1} = s_1 \cdots s_m$. On a $s_2 \cdots s_n s_1 = 1$ donc, comme précédemment, il existe des indices $2 \leq i' < j' \leq m + 2$ tels que $s_2 \cdots s_{m+2} = s_2 \cdots \hat{s}_{i'} \cdots \hat{s}_{j'} \cdots s_{m+2}$. Si $i' > 2$ ou $j' < m + 2$ alors, en utilisant $\tilde{w} = t_{s_i}[t_{s_2} \cdots t_{s_n} t_{s_1}] t_{s_1}^{-1}$, le raisonnement du point précédent donne $\tilde{w} \in K$. On suppose désormais $i' = 2$ et $j' = m + 2$; alors $(*)$ s'écrit $s_3 \cdots s_{m+2} = s_2 \cdots s_{m+1}$ donc on a $1 = s_1 \cdots s_n = s_1 \hat{s}_2 \cdots \hat{s}_{m+2} \cdots s_n$ donc, par hypothèse de récurrence, $t_{s_1} \hat{t}_{s_2} \cdots \hat{t}_{s_{m+2}} \cdots t_{s_n} \in K$. Or on a l'écriture $\tilde{w} = t_{s_1} t_{s_3} [t_{s_3}^{-1} (t_{s_2} \cdots t_{s_{m+1}})(t_{s_{m+2}} t_{s_{m+1}}^{-1} \cdots t_{s_4}^{-1})] t_{s_3}^{-1} t_{s_1}^{-1} [t_{s_1} \hat{t}_{s_2} \cdots \hat{t}_{s_{m+2}} \cdots t_{s_n}]$ donc il suffit de montrer que l'on a $\tilde{w}' := t_{s_3}^{-1} (t_{s_2} \cdots t_{s_{m+1}})(t_{s_{m+2}} t_{s_{m+1}}^{-1} \cdots t_{s_4}^{-1}) \in K$. Or $s_3 \cdots s_{m+2} = s_2 \cdots s_{m+1}$ donc $s_3 (s_2 \cdots s_{m+1})(s_{m+2} \cdots s_4) =$

1 et le membre de gauche a $2m$ termes donc, par le même raisonnement que précédemment, on obtient $\tilde{w}' \in K$ si on peut utiliser l'hypothèse de récurrence et, sinon, $(*)$ s'écrit $s_2 \cdots s_{m+1} = s_3(s_2 \cdots s_m)$. Dans ce dernier cas, en combinant avec $s_2 \cdots s_{m+1} = s_1 \cdots s_m$, on obtient $s_1 = s_3$.

• En utilisant successivement $s_3 \cdots s_n s_1 s_2 = 1, \ldots, s_n s_1 \cdots s_{n-1} = 1$, le raisonnement du point précédent donne $\tilde{w} \in K$ ou $s_1 = s_3 = \cdots = s_{n-1}$ et $s_2 = s_4 = \cdots s_n$. Dans ce dernier cas, on a $\tilde{w} = (t_{s_1} t_{s_2})^m$ et nécessairement $m(s_1, s_2)$ divise m, donc $\tilde{w} \in K$. □

Remarque 1.1.20 : On vient même de démontrer que, plus généralement, si W est un groupe (quelconque) engendré par un ensemble S d'éléments d'ordre 2 et si W vérifie la condition de simplification 1.1.17, alors W est un groupe de Coxeter par rapport à S. On peut aussi montrer que, réciproquement, tout groupe de Coxeter vérifie la condition de simplification (voir par exemple [4, p. 117]).

1.2 Groupe de Weyl fini et (B,N)-paires scindées

Dans cette sous-section, on fixe un groupe G muni d'une (B,N)-paire, de groupe de Weyl W et on s'intéresse au cas où W est fini. En ajoutant l'hypothèse supplémentaire que la (B,N)-paire est scindée, on obtiendra une version forte de la décomposition de Bruhat (théorème 1.2.13).

Proposition 1.2.1 : *Si W est fini alors il existe un unique élément $w_0 \in W$ de longueur maximale. De plus, w_0 est d'ordre 2, vérifie $\forall w \in W, l(ww_0) = l(w_0 w) = l(w_0) - l(w)$ et est caractérisé par $\forall s \in S, l(sw) < l(w)$.*

Démonstration :

• W est fini donc on a au moins l'existence d'un $w_0 \in W$ de longueur maximale. Démontrons $\forall w \in W, l(ww_0) = l(w_0) - l(w)$ par récurrence sur $l(w)$. Si $l(w) = 0$ alors $w = 1$ donc il n'y a rien à faire. Supposons $p := l(w) - 1 \geq 0$ et supposons que le résultat est démontré au rang p. Soit $s_1 \cdots s_p s$ une expression réduite de w ; on pose $q := l(s_1 \cdots s_p w_0)$. L'expression $s_1 \cdots s_p$ est réduite donc, par hypothèse de récurrence, on a $q = l(w_0) - p$. Soit $t_1 \cdots t_q$ une expression réduite de $s_1 \cdots s_p w_0$. Alors on a $w_0 = s_p \cdots s_1 t_1 \cdots t_q$ et il s'agit d'une expression réduite (car de longueur $l(w_0)$). Comme on a $l(sw_0) < l(w_0)$ par définition de w_0, la condition d'échange 1.1.15 donne l'existence d'un indice $1 \leq i \leq p$ ou d'un indice $1 \leq j \leq q$ vérifiant $sw_0 = s_p \cdots \hat{s_i} \cdots s_1 t_1 \cdots t_q$ ou $sw_0 = s_p \cdots s_1 t_1 \cdots \hat{t_j} \cdots t_q$. Le premier cas est impossible (sinon, en remplaçant w_0 par son expression réduite et en simplifiant par $t_1 \cdots t_q$ on obtiendrait $l(w) = l(w^{-1}) = l(ss_p \cdots s_1) = l(s_p \cdots \hat{s_i} \cdots s_1) \leq p - 1 = l(w) - 2$), donc $l(ww_0) = l(t_1 \cdots \hat{t_j} \cdots t_q) = q - 1 = l(w_0) - p - 1 = l(w_0) - l(w)$.

• En prenant $w = w_0$, on obtient $w_0^2 = 1$ (et $w_0 \neq 1$ car les éléments de S sont de longueur 1). En utilisant le résultat du premier point et en passant à l'inverse, on obtient donc $l(w_0 w) = l(w^{-1} w_0) = l(w_0) - l(w^{-1}) = l(w_0) - l(w)$.

• Soit $w \in W$ vérifiant $\forall s \in S, l(sw) < l(w)$. Alors on a $\forall s \in S, l(sww_0) = l(w_0) - l(sw) > l(w_0) - l(w) = l(ww_0)$ donc $ww_0 = 1$ donc $w = w_0$. En particulier, w_0 est l'unique élément de longueur maximale. □

Remarque 1.2.2 : D'après la remarque 1.1.20, comme on a seulement utilisé la condition d'échange 1.1.15, cette proposition est même valable pour n'importe quel groupe de Coxeter fini.

Pour $w \in W$ et $K \leq G$ normalisé par H, on définit les sous-groupes $K^w := n_w^{-1} K n_w$ et $K_w := K \cap K^{w_0 w}$. Les lemmes suivants donnent quelques propriétés des B^w et B_w.

Lemme 1.2.3 : *Soit $w \in W$ et $s \in S$. Si $l(sw) = l(w) + 1$ alors $n_s B n_s \cap B n_w B n_w^{-1} \subseteq B$.*

Démonstration : D'après (BN4), on a $n_s B n_s \subseteq B \cup B n_s B$ donc $n_s B n_s \cap B n_w B n_w^{-1} \subseteq B \cup (B n_s B \cap B n_w B n_w^{-1})$. Supposons $n_s B n_s \cap B n_w B n_w^{-1} \nsubseteq B$. Alors $B n_s B \cap B n_w B n_w^{-1} \neq \emptyset$ donc $B n_s B n_w \cap B n_w B \neq \emptyset$ or, d'après (BN4), on a $B n_s B n_w \subseteq B n_s n_w B \sqcup B n_w B$ donc $B n_s B n_w \nsubseteq B n_s n_w B$, ce qui contredit le lemme 1.1.9. □

Lemme 1.2.4 : *Soit $w \in W$ et $w' \in W$. Si $l(ww') = l(w) + l(w')$ alors $B \cap B^{ww'} \subseteq B \cap B^{w'}$. De plus, on a $B \cap B^{w_0} = H$.*

Démonstration :

• Démontrons l'inclusion par récurrence sur $l(w)$. Si $l(w) = 0$ alors $w = 1$ et il n'y a rien à faire. Si $l(w) = 1$ alors $w \in S$ donc, d'après le lemme 1.2.3, $n_{w'}(B \cap B^{ww'}) n_{w'}^{-1} = n_{w'} B n_{w'}^{-1} \cap n_w^{-1} B n_w \subseteq B$. Supposons $l(w) \geq 2$ et supposons que le résultat est démontré au rang $l(w) - 1$. Soit $s \in S$ tel que $l(ws) = l(w) - 1$; on pose $y := ws$ et $y' := sw'$. Alors $ww' = yy'$ donc $l(yy') = l(ww') = l(w) + l(w') = l(y) + l(w') + 1 \geq l(y) + l(y') \geq l(yy')$ donc $l(yy') = l(y) + l(y')$ donc, par hypothèse de récurrence et d'après le cas de la longueur 1, $B \cap B^{ww'} = B \cap B^{yy'} \subseteq B \cap B^{y'} = B \cap B^{sw'} \subseteq B \cap B^{w'}$.

• Si $w_0 = xy$ alors, d'après la proposition 1.2.1, $l(x)+l(y) = l(x)+l(x^{-1}w_0) = l(x)+l(w_0)-l(x^{-1}) = l(w_0)$ donc $B \cap B^{w_0} \subseteq B^y$. Donc, d'après (BN5), $B \cap B^{w_0} \subseteq \bigcap_{y\in W} B^y = H$. De plus, on a $H \trianglelefteq N$ et $H \subseteq B$ donc $H \subseteq B^{w_0}$. □

Lemme 1.2.5 : *Soit $w \in W$ et $s \in S$ tels que $l(ws) = l(w)+1$. Alors on a $B = B_sB_{w_0s} = B_{w_0s}B_s$, $H \subsetneq B_s \subseteq B_{w_0w}$ et $B_{ws} = B_s(B_w)^s = (B_w)^sB_s$.*

Démonstration :
• On pose $y := w_0s$. Alors $l(sy^{-1}) = l(ys) = l(y)+1 = l(y^{-1})+1$ donc, d'après le lemme 1.1.9, $n_sBn_y^{-1} \subseteq Bn_sn_y^{-1}B$ donc $B \subseteq n_s^{-1}Bn_sn_y^{-1}Bn_y = B^sB^y$. On a déjà $(B\cap B^s)(B\cap B^y) \subseteq B$. Soit $b \in B$; soit $b' \in B^s$ et $b'' \in B^y$ tels que $b = b'b''$. Alors, d'après le lemme 1.2.3, $b' = bb''^{-1} \in B^s \cap BB^y \subseteq B$ donc $b' \in B$ donc $b'' \in B$ aussi. Donc $B = (B\cap B^s)(B\cap B^y) = B_{w_0s}B_{w_0y} = B_{w_0s}B_s$. En passant à l'inverse, on obtient $B = B_sB_{w_0s}$.
• On a déjà $H \subseteq B_s$. Si $H = B_s$ alors $B_s = H \leq B_{w_0s}$ donc $B = B_{w_0s} = B\cap B^s$ donc $B_s \subseteq B$, ce qui contredit (BN3).
• D'après la proposition 1.2.1, si $w_0 = yws$ avec $y \in W$, $w \in W$ et $s \in S$ tels que $l(ws) = l(w)+1$ alors $l(w_0) = l(y)+l(w)+1$ donc $l(yw) = l(w_0s) = l(w_0)-1 = l(y)+l(w)$ donc, d'après le lemme 1.2.4, $B_s = B\cap B^{w_0s} = B\cap B^{yw} \subseteq B\cap B^w = B_{w_0w}$.
• D'après la proposition 1.2.1, $l(w_0wss) = l(w_0)-l(w) = l(w_0)-l(ws)+1 = l(w_0ws)+1$ donc $B_s \subseteq B_{w_0w_0ws} = B_{ws}$. Donc $B_{ws} = B_{ws}\cap B = B_{ws}\cap B_sB_{w_0s} = B_s(B_{ws}\cap B_{w_0s})$. Il reste à montrer $B_{ws}\cap B_{w_0s} = (B_w)^s$. On a $B_{ws}\cap B_{w_0s} = B\cap B^{w_0ws}\cap B^s = n_s^{-1}(B_s\cap B^{w_0w}\cap B)n_s = n_s^{-1}(B_s\cap B_w)n_s$ or, d'après le lemme 1.2.4, $B_w = B\cap B^{w_0w} = B\cap B^{w_0wss} \subseteq B\cap B^s \subseteq B^s$ donc $B_{ws}\cap B_{w_0s} = n_s^{-1}B_wn_s = (B_w)^s$. En passant à l'inverse, on obtient aussi $B_{ws} = (B_w)^sB^s$. □

Lemme 1.2.6 : *Soit $w \in W$ et $s \in S$ tels que $l(sw) = l(w)+1$. Alors on a $B_{sw} = B_w(B_s)^w = (B_s)^wB_w$.*

Démonstration : Démontrons le résultat par récurrence sur $l(w)$. Si $l(w) = 0$ alors $w = 1$ donc $B_{sw} = B_s = H(B_s)^w$ et, d'après le lemme 1.2.4, on a $H = B\cap B^{w_0} = B_w$. Supposons $l(w) \geq 1$ et supposons que le résultat est démontré au rang $l(w)-1$. Soit $t \in S$ tel que $l(wt) = l(w)-1$; on pose $y := wt$. Alors $l(syt) = l(sw) = l(w)+1 = l(y)+2$ donc $l(syt) = l(sy)+1$ donc, d'après le lemme 1.2.5, $B_{sw} = B_{syt} = (B_{sy})^tB_t$ donc, par hypothèse de récurrence, $B_{sw} = ((B_s)^yB_y)^tB_t = (B_s)^{yt}(B_y)^tB_t$ or $l(yt) = l(y)+1$ donc, d'après le lemme 1.2.5, $B_{sw} = (B_s)^{yt}B_{yt}$. En passant à l'inverse, on obtient aussi $B_{sw} = B_{yt}(B_s)^{yt}$. □

Lemme 1.2.7 : *On a $\forall w \in W, B = B_wB_{w_0w} = B_{w_0w}B_w$.*

Démonstration : Démontrons le résultat par récurrence sur $l(w)$. Si $l(w) = 0$ alors on a $B = B_{w_0} = HB_{w_0} = B_wB_{w_0}$ et $B = B_{w_0w}B_w$. Supposons $l(w) \geq 1$ et supposons que le résultat est démontré au rang $l(w)-1$. Soit $s \in S$ tel que $l(sw) = l(w)-1$; on pose $y := sw$. Alors $l(sy) = l(y)+1$ donc, d'après le lemme 1.2.6, on a $B_wB_{w_0w} = B_y(B_s)^yB_{w_0w}$ or $B_{w_0w} = B\cap B^w = (B^{w^{-1}}\cap B)^w = (B_{w_0w})^w$ donc $B_wB_{w_0w} = B_y(B_s)^y(B_{w_0(sy)^{-1}})^{sy} = B_y(B_s(B_{w_0(sy)^{-1}})^s)^y$ or, d'après la proposition 1.2.1, $l(w_0w^{-1}s) = l(w_0)-l(w^{-1}s) = l(w_0)-l(sw) = l(w_0)-l(w)+1 = l(w_0)-l(w^{-1})+1 = l(w_0w^{-1})+1$ donc, d'après le lemme 1.2.5 et par hypothèse de récurrence, $B_wB_{w_0w} = B_y(B_{w_0(sy)^{-1}s})^y = B_y(B_{w_0y^{-1}})^y = B_y(B\cap B^{y^{-1}})^y = B_yB_{w_0y} = B$. En passant à l'inverse, on obtient aussi $B = B_{w_0w}B_w$. □

On introduit maintenant la notion de (B,N)-paire scindée, qui permet d'avoir une version forte de la décomposition de Bruhat.

Définition 1.2.8 : *Soit G un groupe muni d'une (B,N)-paire et U un sous-groupe de G. On dit que la (B,N)-paire est* **scindée** *(par U) si on a $U \trianglelefteq B$, $B = UH$, $U\cap H = \{1\}$ et $\forall n \in N, n^{-1}Un \cap B \subseteq U$.*

Remarques 1.2.9 :
• Comme on a $U \trianglelefteq B$ et $H \leq B$, pour $w \in W$, $n_wUn_w^{-1}$ ne dépend que de w et pas de n_w.
• On a $B = U \rtimes H$ et, dans le cas où B est fini, $|B| = |U||H|$.

Exemple 1.2.10 : En reprenant l'exemple 1.1.3, la (B,N)-paire est scindée si et seulement si $n = 3$, $n = 4$ ou $n = 5$. En effet, si $n = 3$ alors il suffit de prendre $U = B$, si $n = 4$ alors il suffit de prendre $U = \mathfrak{A}_3$, si $n = 5$ alors il suffit de prendre pour U le sous-groupe de B engendré par les doubles transpositions et si $n \geq 6$ alors $B = \mathfrak{S}_{n-1}$ n'a pas de sous-groupe distingué d'ordre $\dfrac{|B|}{|H|} = n-1$.

Toutefois, les exemples de (B,N)-paires scindées sont assez nombreux. En particulier, toutes les (B,N)-paires construites dans la section 2 seront scindées.

Les deux propositions suivantes expliquent comment, à partir d'une (B,N)-paire scindée pour un groupe G, on peut construire une (B,N)-paire scindée pour certains sous-groupes et quotients de G.

Proposition 1.2.11 : *Soit G un groupe muni d'une (B,N)-paire scindée par un sous-groupe U et G' un sous-groupe distingué de G contenant U. On pose $B' := B \cap G'$, $N' := N \cap G'$, $H' := H \cap G'$ et $W' := N'/H'$. Alors B' et N' constituent une (B,N)-paire scindée par U pour G' et on a $W' \simeq W$.*

Démonstration :

• On a $G = BNB = UHNHU = UNU$ donc $G' = UN'U \subseteq B'N'B'$ donc $G' = \langle B', N' \rangle$.

• On a $H \trianglelefteq N$ et $G' \trianglelefteq G$ donc $B' \cap N' = H' \trianglelefteq N'$. La restriction $N' \longrightarrow\!\!\!\!\!\rightarrow W$ de la projection canonique a pour noyau H' et induit donc un morphisme de groupes injectif $\alpha : \left| \begin{array}{ccc} W' & \longrightarrow & W \\ nH' & \longmapsto & nH \end{array} \right.$. On a $G' \trianglelefteq G$ donc $G'H$ est un sous-groupe contenant $UH = B$ donc, d'après la proposition 1.1.14, $G'H$ est égal à son normalisateur, or $G'H$ est normalisé par N, donc N est un sous-groupe de $G'H$ donc $\langle B, N \rangle$ est un sous-groupe de $G'H$ donc $G = G'H$ donc $N = G'H \cap N = N'H$, donc α est surjectif donc est un isomorphisme. Donc W' est engendré par $S' := \alpha^{-1}(S)$.

• De même, $B = B'H$ donc, pour $s \in S$ et n_s un représentant dans N' (qui existe d'après le point précédent), on a $n_sBn_s = n_sB'Hn_s = n_sB'n_sH$ or $n_sBn_s \neq B$ donc $n'_sB'n'_s \neq B'$.

• Pour $n \in N'$, on a $n_sB'n = n_sBn \cap G' \subseteq (Bn_snB \cup BnB) \cap G' = (B'Hn_snB \cup B'HnB) \cap G' = (B'n_snB \cup B'nB) \cap G' = B'n_snB' \cup B'nB'$.

• On a $\bigcap_{n \in N'} nB'n = (\bigcap_{n \in N'} nBn) \cap G' = (\bigcap_{n \in N} nBn) \cap G' = H \cap G' = H'$.

• On a bien $U \trianglelefteq B'$, $U \cap H' \subseteq U \cap H = \{1\}$ et $\forall n \in N', n^{-1}Un \cap B' = (n^{-1}Un \cap B) \cap G' \subseteq U \cap G' = U$. □

Proposition 1.2.12 : *Soit G un groupe muni d'une (B,N)-paire et D un sous-groupe distingué contenu dans H. On pose $\widetilde{B} := B/D$, $\widetilde{N} := N/D$, $\widetilde{H} := H/D$ et $\widetilde{W} := \widetilde{N}/\widetilde{H}$. Alors $\widetilde{B}$ et $\widetilde{N}$ constituent une (B,N)-paire pour $\widetilde{G}$ et on a $\widetilde{W} \simeq W$. Si de plus la (B,N)-paire de G est scindée par un sous-groupe U alors, avec $\widetilde{U} := UD/D$, la (B,N)-paire de $\widetilde{G}$ est scindée par $\widetilde{U}$.*

Démonstration :

• On a $G = \langle B, N \rangle$ donc, par passage au quotient, $\widetilde{G} = \langle \widetilde{B}, \widetilde{N} \rangle$.

• Soit $\pi : G \longrightarrow\!\!\!\!\!\rightarrow \widetilde{G}$ la projection canonique, qui induit une bijection entre les sous-groupes de G contenant D et les sous-groupes de $\widetilde{G}$. Alors $\widetilde{H} = \widetilde{B} \cap \widetilde{N}$. On a $D \leq H \trianglelefteq N$ donc, par passage au quotient, $\widetilde{H} \trianglelefteq \widetilde{N}$. D'après le troisième théorème d'isomorphisme de Noether, on a $\widetilde{W} \simeq W$ et, pour $s \in S$, si $n_s \in N$ est un représentant de s alors n_sD est un représentant dans $\widetilde{N}$ de $s \in \widetilde{W}$.

• On a $n_sD \cdot \widetilde{B} \cdot n_sD = \{n_sD \cdot bD \cdot n_sD | b \in B\} = \{n_sbn_sD | b \in B\} = \pi(n_sBn_s)$ donc si $n_sD \cdot \widetilde{B} \cdot n_sD = \widetilde{B}$ alors $n_sBn_s = n_sBn_sD = \pi^{-1}(\pi(n_sBn_s)) = \pi^{-1}(\widetilde{B}) = B$, ce qui contredit (BN3).

• De même, pour $n \in N$, on a $n_sD \cdot \widetilde{B} \cdot nD = \pi(n_sBn) \subseteq \widetilde{B} \cdot n_sDnD \cdot \widetilde{B} \cup \widetilde{B} \cdot nD \cdot \widetilde{B}$.

• On a $\bigcap_{n \in N} nD \cdot \widetilde{B} \cdot (nD)^{-1} = \bigcap_{n \in N} \pi(nBn^{-1}) = \pi(\pi^{-1}(\bigcap_{n \in N} \pi(nBn^{-1}))) = \pi(\bigcap_{n \in N} \pi^{-1}(\pi(nBn^{-1}))) = \pi(\bigcap_{n \in N} nBn^{-1}D) = \pi(\bigcap_{n \in N} nBn^{-1}) = \pi(H) = \widetilde{H}$.

• UD est un sous-groupe distingué de B contenant D donc $\widetilde{U}$ est un sous-groupe distingué de $\widetilde{B}$. On a $\widetilde{B} = \pi(B) = \pi(UH) = \pi(U)\pi(H) = \widetilde{U}\widetilde{H}$. De plus $\widetilde{U} \cap \widetilde{H} = \pi(UD) \cap \pi(H) = \pi(UD \cap H)$ car UD et H sont des sous-groupes contenant D, donc $\widetilde{U} \cap \widetilde{H} = \pi(D) = \{1\}$. Enfin, pour $n \in N$, $(nD)^{-1} \cdot \widetilde{U} \cdot nD \cap \widetilde{B} = \pi(n^{-1}Un \cap B) \subseteq \pi(U) = \widetilde{U}$. □

On énonce enfin le théorème qui est l'objectif de cette sous-section.

Théorème 1.2.13 (Décomposition de Bruhat, version forte) : *Soit G un groupe muni d'une (B,N)-paire scindée dont le groupe de Weyl est fini. Alors on a $G = \bigsqcup_{w \in W} Bn_wU_w$ avec unicité de l'écriture (c'est-à-dire que, pour $g \in Bn_wU_w$, il existe des uniques $b \in B$ et $u \in U_w$ tels que $g = bn_wu$). De plus, on a $\forall w \in W \setminus \{1\}, U_w \neq \{1\}$.*

Démonstration :

• Soit $w \in W$. Démontrons $B_w = U_w H$. On a déjà $B_w = B \cap B^{w_0 w} = UH \cap n_{w_0 w}^{-1} U n_{w_0 w} n_{w_0 w}^{-1} H n_{w_0 w} = UH \cap U^{w_0 w} H \supseteq U_w H$. Soit $g \in B_w$; on vient de montrer $g \in UH \cap U^{w_0 w} H$ donc il existe $u \in U$ et $h \in H$ tels que $g = uh$ et il existe $u' \in U$ et $h' \in H$ tels que $g = n_{w_0 w}^{-1} u' n_{w_0 w} h'$. Alors $n_{w_0 w}^{-1} u' n_{w_0 w} = g h'^{-1} \in U^{w_0 w} \cap B \subseteq U$ or $B = U \rtimes H$, donc $n_{w_0 w}^{-1} u' n_{w_0 w} = u$ donc $u \in U_w$ donc $g \in U_w H$. Donc $B_w \subseteq U_w H$.

• On a déjà $U_w U_{w_0 w} \subseteq U$. Établissons l'inclusion réciproque. Soit $u \in U$. D'après le lemme 1.2.7, il existe $b_1 \in B_w$ et $b_2 \in B_{w_0 w}$ tels que $u = b_1 b_2$. D'après le point précédent, il existe $u_1 \in U_w$ et $h_1 \in H$ tels que $b_1 = u_1 h_1$ et il existe $u_2 \in U_{w 0 w}$ et $h_2 \in H$ tels que $b_2 = u_2 h_2$. Donc $u = u_1 h_1 u_2 h_2 = u_1 (h_1 u_2 h_1^{-1}) h_1 h_2$ or $B = U \rtimes H$ donc $h_1 h_2 = 1$ et $u = u_1 h_1 u_2 h_2 = u_1 (h_1 u_2 h_1^{-1})$. De plus, U est normalisé par H et H est normalisé par N donc $U_{w_0 w} = U \cap n_w^{-1} U n_w$ est normalisé par H, donc $h_1 u_2 h_1^{-1} \in U_{w_0 w}$ donc $u \in U_w U_{w_0 w}$.

• On a $n_w U_{w_0 w} n_w^{-1} = U_{w^{-1}} \subseteq U$ donc, d'après le point précédent, $C(w) = B n_w H U = B n_w U = B n_w U_{w_0 w} U_w = B n_w U_{w_0 w} n_w^{-1} n_w U_w = B n_w U_w$ donc, d'après la décomposition de Bruhat (théorème 1.1.8), on a $G = \bigsqcup_{w \in W} B n_w U_w$.

• Démontrons l'unicité de l'écriture. Soit $b \in B$, $b' \in B$, $u \in U_w$ et $u' \in U_w$ tels que $b n_w u = b' n_w u'$. Alors on a $b^{-1} b' = n_w u u'^{-1} n_w^{-1} \in B \cap n_w U_w n_w^{-1} \subseteq B \cap U^{w_0}$. Or, d'après le lemme 1.2.4, $B \cap U^{w_0} \subseteq B \cap B^{w_0} = H$ et $B \cap U^{w_0} \subseteq U$ donc $B \cap U^{w_0} = \{1\}$. Donc $b = b'$ donc $u = u'$.

• Supposons $w \neq 1$ et $U_w = \{1\}$. Alors, d'après le premier point, $B_w = H$. Soit $s \in S$ tel que $l(ws) = l(w) - 1$. Alors $l(wss) = l(ws) + 1$ donc, d'après le lemme 1.2.5, $H \subsetneq B_s \subseteq B_s (B_{ws})^s = B_{wss} = B_w$, ce qui est contradictoire. □

1.3 Automorphismes et points fixes

Dans cette section, on fixe un groupe G muni d'une (B,N)-paire scindée dont le groupe de Weyl est fini, ainsi qu'un automorphisme de groupe $\varphi : G \longrightarrow G$. On suppose que :

(BN$^\varphi$1) φ laisse stables N, H et U (donc B aussi) ;

(BN$^\varphi$2) pour $n \in N$, si on a $\varphi(nH) \subseteq nH$ alors nH contient un point fixe de φ.

L'objectif est de construire une (B,N)-paire pour le sous-groupe des points fixes G^φ.

Remarques 1.3.1 :

• D'après (BN$^\varphi$1), on a un automorphisme de groupe $\overline{\varphi} : \left| \begin{array}{ccc} W & \longrightarrow & W \\ nH & \longmapsto & \varphi(n)H \end{array} \right.$.

• Donc φ induit une permutation des cellules de Bruhat, avec $\forall w \in W, \varphi(C(w)) = C(\overline{\varphi}(w))$.

• Il découle directement de la définition et de $B = U \rtimes H$ que l'on a $H^\varphi = B^\varphi \cap N^\varphi$, $B^\varphi = U^\varphi H^\varphi$ et $U^\varphi \cap H^\varphi = \{1\}$.

On note $\overline{S}$ l'ensemble des orbites des éléments de S sous l'action de $\overline{\varphi}$ et, pour $J \in \overline{S}$, on pose $W_J := \langle J \rangle$ (qui est un sous-groupe de W). Les lemmes suivants expliquent l'effet de $\overline{\varphi}$ sur S, W et les W_J.

Lemme 1.3.2 : *On a $\overline{\varphi}(S) = S$ et $\forall w \in W, l(\overline{\varphi}(w)) = l(w)$.*

Démonstration : Soit $s \in S$. D'après la proposition 1.1.13, $B \cup B n_s B$ est un sous-groupe de G donc $B \cup B n_{\overline{\varphi}(s)} B = \varphi(B \cup B n_s B)$ aussi donc $\overline{\varphi}(s) \in S$. Donc $\overline{\varphi}$ induit une bijection de S, d'où l'égalité des longueurs. □

Lemme 1.3.3 : *Chaque W_J possède un unique élément w_J de longueur maximale et celui-ci vérifie $w_J^2 = 1$ et est caractérisé parmi les éléments de W_J par $\forall s \in J, l(s w_J) < l(w_J)$. De plus, on a $W_J^{\overline{\varphi}} = \{1, w_J\}$ et $W^{\overline{\varphi}} = \langle (w_J)_{J \in \overline{S}} \rangle$.*

Démonstration :

• On a $J \subseteq S$ et, d'après le théorème 1.1.19, W est un groupe de Coxeter par rapport à S, donc W_J est un groupe de Coxeter par rapport à J et la longueur dans W_J est égale à la longueur dans W. Donc, d'après la remarque 1.2.2, w_J est unique, vérifie $w_J^2 = 1$ et est caractérisé parmi les éléments de W_J par $\forall s \in J, l(s w_J) < l(w_J)$.

• D'après le lemme 1.3.2, on a $l(\overline{\varphi}(w_J)) = l(w_J)$ or $\varphi(w_J) \in W_J$ donc, par unicité de w_J, on a $w_J \in W_J^{\overline{\varphi}}$. Donc on a déjà $\{1, w_J\} \subseteq W_J^{\overline{\varphi}}$ et $\langle (w_J)_{J \in \overline{S}} \rangle \subseteq W^{\overline{\varphi}}$.

• Soit $w \in W^{\overline{\varphi}}$. Démontrons $w \in \langle (w_J)_{J \in \overline{S}} \rangle$. Si $w = 1$ alors il n'y a rien à faire. On suppose désormais $w \neq 1$. En raisonnant par récurrence sur la longueur, il suffit de montrer qu'il existe $J \in \overline{S}$ et $w' \in W^{\overline{\varphi}}$ tels que $w = w_J w'$ et $l(w) = l(w_J) + l(w')$. Soit $s \in S$ tel que $l(sw) = l(w) - 1$ et $J \in \overline{S}$ tel que $s \in J$. D'après le lemme 1.3.2, on a $\forall n \in \mathbf{N}, l(\overline{\varphi}^n(s) w) = l(\overline{\varphi}^n(sw)) = l(sw) = l(w) - 1$, c'est-à-dire $\forall t \in J, l(tw) = l(w) - 1$. Soit $y \in W_J$

de longueur maximale tel qu'il existe $w' \in W$ avec $w = yw'$ et $l(w) = l(y) + l(w')$. Soit $t \in J$ et $s_1 \cdots s_p$ et $t_1 \cdots t_q$ des expressions réduites de y et w'. D'après la condition d'échange 1.1.15, il existe un indice $1 \leq i \leq p$ ou un indice $1 \leq j \leq q$ tel que $tw = s_1 \cdots \hat{s}_i \cdots s_p t_1 \cdots t_q$ ou $tw = s_1 \cdots s_p t_1 \cdots \hat{t}_j \cdots t_q$. Le deuxième cas est impossible, sinon, pour raison de longueur, $ts_1 \cdots s_p t_1 \cdots \hat{t}_j \cdots t_q$ serait une expression de w et $ts_1 \cdots s_p \in W_J$ serait de longueur $p+1$, ce qui contredirait la définition de y. Donc, en simplifiant à droite par w', on obtient $ty = s_1 \cdots \hat{s}_i \cdots s_p$ donc $l(ty) < l(y)$. Donc, d'après les points précédents, on a $y = w_J$ et $w' = w_J w \in W^{\overline{\varphi}}$.

• Soit $w \in W_J^{\overline{\varphi}} \setminus \{1\}$. D'après le premier point, il existe $s \in J$ tel que $l(sw) = l(w) - 1$. Soit $w' \in W^{\overline{\varphi}}$ donné par le point précédent. On a donc $l(w) = l(w_J) + l(w')$ mais $w \in W_J$ et w_J est de longueur maximale dans W_J donc $w' = 1$ et $w = w_J$. Donc $W_J^{\overline{\varphi}} = \{1, w_J\}$. □

On en déduit comment construire une (B,N)-paire pour le sous-groupe des points fixes.

Théorème 1.3.4 : *Soit G un groupe muni d'une (B,N)-paire scindée dont le groupe de* Weyl *est fini et $\varphi : G \longrightarrow G$ un automorphisme de groupe vérifiant (BN$^\varphi$1) et (BN$^\varphi$2). On suppose de plus $\forall J \in \overline{S}, U_{w_J}^\varphi \neq \{1\}$. Alors B^φ et N^φ constituent une (B,N)-paire scindée par U^φ pour G^φ, de groupe de* Weyl *$W^{\overline{\varphi}}$ engendré par les w_J pour $J \in \overline{S}$.*

Démonstration :

• On a déjà $H^\varphi = B^\varphi \cap N^\varphi$ et $\langle B^\varphi, N^\varphi \rangle \subseteq G^\varphi$. Soit $g \in G^\varphi$. D'après la version forte de la décomposition de Bruhat (théorème 1.2.13), il existe des uniques éléments $b \in B$, $w \in W$ et $u \in U_w$ tels que $g = bn_w u$. Alors $\varphi(g) = \varphi(b) n_{\overline{\varphi}(w)} \varphi(u)$ donc, par unicité et comme $(U_w)^\varphi = (U^\varphi)_w$, on a $b \in B^\varphi$, $w \in W^{\overline{\varphi}}$ et $u \in U^\varphi$ donc $g \in \langle B^\varphi, N^\varphi \rangle$.

• On a bien $H^\varphi \trianglelefteq N^\varphi$. Soit le morphisme de groupes $\alpha : \left| \begin{array}{ccc} N^\varphi/H^\varphi & \longrightarrow & W \\ nH^\varphi & \longmapsto & nH \end{array} \right.$. Pour $n \in N^\varphi$, on a $\overline{\varphi}(nH) = nH$ donc α est à valeurs dans $W^{\overline{\varphi}}$. Soit $nH \in W^{\overline{\varphi}}$. Alors, d'après (BN$^\varphi$2), il existe $n' \in N^\varphi$ tel que $nH = n'H$ donc $nH = \alpha(n'H^\varphi)$. Donc $\alpha : N^\varphi/H^\varphi \longrightarrow W^{\overline{\varphi}}$ est surjectif. Pour n et n' dans N^φ, si $nH = n'H$ alors $nH^\varphi = \{h \in nH | \varphi(h) = h\} = \{h \in n'H | \varphi(h) = h\} = n'H^\varphi$, donc α est injectif. De plus, d'après le lemme 1.3.3, les w_J sont d'ordre 2 et engendrent $W^{\overline{\varphi}}$.

• Soit $J \in \overline{S}$ et supposons $n_{w_J} B^\varphi n_{w_J}^{-1} = B^\varphi$. Alors $n_{w_J} U_{w_J}^\varphi n_{w_J}^{-1} \subseteq B^\varphi$. Or, on a $U_{w_J} = U \cap n_{w_0 w_J}^{-1} U n_{w_0 w_J}$ donc $n_{w_J} U_{w_J} n_{w_J}^{-1} \subseteq U^{w_0}$ donc, d'après le lemme 1.2.4, $n_{w_J} U_{w_J}^\varphi n_{w_J}^{-1} \subseteq B^\varphi \cap (U^{w_0})^\varphi = H^\varphi \subseteq H$. Donc $U_{w_J}^\varphi \subseteq n_{w_J}^{-1} H n_{w_J} = H$ donc $U_{w_J}^\varphi \subseteq U \cap H = \{1\}$, ce qui est contradictoire.

• Soit $J \in \overline{S}$ et $w \in W^{\overline{\varphi}}$. D'après le lemme 1.1.11, la version forte de la décomposition de Bruhat (théorème 1.2.13) et le lemme 1.3.3, on a $n_{w_J} B^\varphi n_w \subseteq \bigcup_{w' \in W_J} (B n_{w'w} U_{w'w})^\varphi = \bigcup_{w' \in W_J^{\overline{\varphi}}} B^\varphi n_{w'w} U_{w'w}^\varphi = B^\varphi n_w U_w^\varphi \cup B^\varphi n_{w_J w} U_{w_J w}^\varphi \subseteq B^\varphi n_w B^\varphi \cup B^\varphi n_{w_J w} B^\varphi$.

• Le lemme 1.3.2 implique $w_0 \in W^{\overline{\varphi}}$. On a donc $H^\varphi \subseteq \bigcap_{n \in N^\varphi} n B^\varphi n^{-1} \subseteq B^\varphi \cap n_{w_0} B^\varphi n_{w_0}^{-1} = (B \cap B^{w_0})^\varphi$. Le lemme 1.2.4 donne $(B \cap B^{w_0})^\varphi = H^\varphi$, d'où $\bigcap_{n \in N^\varphi} n B^\varphi n^{-1} = H^\varphi$.

• On a bien $U^\varphi \trianglelefteq B^\varphi$, $B^\varphi = U^\varphi U^\varphi$, $U^\varphi \cap H^\varphi = \{1\}$ et $\forall n \in N^\varphi, n^{-1} U^\varphi n \cap B^\varphi = (n^{-1} U^n \cap B)^\varphi \subseteq U^\varphi$. □

1.4 Groupe de Weyl et systèmes de racines

Soit W le groupe de Weyl d'une (B,N)-paire (ou, plus généralement, un groupe de Coxeter). La série formelle $W(t) := \sum_{w \in W} t^{l(w)} \in \mathbf{Z}[[t]]$ est appelée la **série de Hilbert** associée à W. L'objectif de cette sous-section est de donner un moyen de calculer $W(t)$ dans le cas où W est un groupe de réflexion fini (théorème 1.4.8), ce qui servira à calculer l'ordre de certains groupes finis dans la section 3.

Définition 1.4.1 : *Soit $(V, \langle \cdot, \cdot \rangle)$ un espace euclidien et $\Phi \subseteq V \setminus \{0\}$ fini (non vide). Pour $x \in V \setminus \{0\}$, on pose $x^\vee := \frac{2}{\langle x, x \rangle} x$. On note, pour $\alpha \in \Phi$, $s_\alpha : \left| \begin{array}{ccc} V & \longrightarrow & V \\ x & \longmapsto & x - 2\langle \alpha^\vee, x \rangle \alpha \end{array} \right.$ la réflexion orthogonale par rapport à $\alpha^\perp$, W le groupe engendré par les s_α (appelé* **groupe de réflexion** *associé à Φ) et $\Phi^\vee := \{\alpha^\vee | \alpha \in \Phi\}$. On dit que Φ est un* **système de racines** *(réduit), que les éléments de Φ sont des* **racines** *et que les éléments de $\Phi^\vee$ sont des* **coracines** *si :*

(i) Φ est stable par W ;

(ii) Φ engendre V comme espace vectoriel ;

(iii) on a $\forall \alpha \in \Phi, \forall \lambda \in \mathbf{R}, \lambda\alpha \in \Phi \Leftrightarrow \lambda \in \{-1, 1\}$;

(iv) pour toutes racines α et β, $\langle \alpha^\vee, \beta \rangle$ est dans $\mathbf{Z}$.

Dans ce cas, on appelle **chambres de Weyl** *les composantes connexes de* $V \setminus \bigcup_{\alpha\in\Phi} \alpha^\perp$*, qui sont des cônes polyédraux convexes ouverts.*

Remarques 1.4.2 :

- Dans ce cas, W est fini car il agit fidèlement sur Φ.
- Comme W agit par homéomorphismes sur $V \setminus \bigcup_{\alpha\in\Phi} \alpha^\perp$, il permute les chambres de Weyl. On peut montrer que l'action de W sur les chambres est simplement transitive (voir par exemple [2, p. 22]).
- Un calcul élémentaire montre que $\Phi^\vee$ est aussi un système de racines, de groupe de réflexion W.

On fixe une chambre C_0, appelée **chambre fondamentale**. Soit $v \in C_0$; alors $v^\perp$ ne contient aucune racine (sinon v serait dans un $\alpha^\perp$). D'après la condition (ii), il y a un nombre pair de racines et $v^\perp$ découpe $V \setminus v^\perp$ en deux demi-espaces ouverts, chacun contenant une moitié de Φ. On note Φ^+ la moitié dans le demi-espace contenant v et Φ^- l'autre moitié, dont les éléments sont appelés respectivement **racines positives** et **racines négatives**. On note Δ l'ensemble des racines positives qui ne sont pas combinaisons $\mathbf{N}$-linéaires d'au moins deux racines positives. Les éléments de Δ sont appelés **racines simples** ; on les note $p_1, \dots, p_l$. Bien entendu, ces définitions dépendent de C_0 (mais pas de v).

Fait 1.4.3 : On peut montrer que Δ est une base de V vérifiant $\forall \alpha \in \Delta, \forall \beta \in \Delta, \langle \alpha, \beta \rangle \leq 0$, que toute racine positive est combinaison $\mathbf{N}$-linéaire de racines simples et que la chambre fondamentale est l'ensemble des vecteurs $x \in V$ vérifiant, pour $1 \leq i \leq l$, $\langle p_i, x \rangle > 0$. Pour $\alpha \in \Phi$, il existe donc une unique famille $(c_1, \dots, c_l) \in \mathbf{N}^l$ telle que $\alpha = \sum_{i=1}^{l} c_i p_i$ et alors $\mathrm{ht}(\alpha) := \sum_{i=1}^{l} c_i$ est appelée **hauteur** de α. De plus, $\Phi^{\vee +} := \{\alpha^\vee | \alpha \in \Phi^+\}$ est bien un ensemble de racines positives pour $\Phi^\vee$, dont l'ensemble des racines simples est $\Delta^\vee := \{\alpha^\vee | \alpha \in \Delta\}$. En outre, les s_α pour $\alpha \in \Delta$ engendrent W donc on peut définir une fonction de longueur l sur W par rapport à ce système de générateurs (donc on a aussi une série de Hilbert $W(t)$). Pour $w \in W$, $l(w)$ est aussi le nombre de racines positives envoyées par w sur des racines négatives. Enfin, en voyant w comme élément de $\mathrm{GL}(V)$, on a $\det(w) = (-1)^{l(w)}$ (voir par exemple [2, pp. 12-23]).

La famille $(p_1, \dots, p_l)$ est une base de V donc $(p_1^\vee, \dots, p_l^\vee)$ engendre V et est une base pour raison de cardinalité. Donc il existe une unique base $(q_1, \dots, q_l)$ vérifiant $\forall (i,j) \in \{1, \dots, l\}^2, \langle p_i^\vee, q_j \rangle = \delta_{ij}$. Les q_j sont appelés les **poids fondamentaux** (associés à Φ^+). On définit aussi le **réseau des poids** $Q := \{q \in V | \forall \alpha \in \Phi, \langle \alpha^\vee, q \rangle \in \mathbf{Z}\}$. On a l'inclusion $\Phi \subseteq Q$. D'après le fait 1.4.3, on a $Q = \{q \in V | \forall \alpha \in \Delta, \langle \alpha^\vee, q \rangle \in \mathbf{Z}\}$, qui est un groupe abélien pour l'addition. On en déduit que Q est l'ensemble des combinaisons $\mathbf{Z}$-linéaires des poids fondamentaux. De plus, W agit sur Q car pour $w \in W$, $q \in Q$ et $\alpha \in \Phi$, on a $w^{-1}(\alpha) \in \Phi$ et w préserve $\langle \cdot, \cdot \rangle$ donc $\alpha^\vee = w(w^{-1}(\alpha))^\vee = w(w^{-1}(\alpha)^\vee)$ donc $\langle \alpha^\vee, w(q) \rangle = \langle w^{-1}(\alpha)^\vee, q \rangle \in \mathbf{Z}$; par linéarité, il s'agit bien d'une action de groupe.

Pour simplifier l'écriture, on considère $e(Q)$ le groupe Q dont la loi est notée multiplicativement ; pour $q \in Q$, on note $e(q)$ l'élément de $e(Q)$ correspondant à q. Soit A la $\mathbf{Q}$-algèbre de $e(Q)$ [2]. L'action de W sur Q s'étend en une action linéaire sur A. Pour $a \in A$, on dit que a est **alterné** si on a $\forall w \in W, w(a) = \det(w)a$. On définit aussi $\theta := \sum_{w\in W} \det(w) w$, qui est un endomorphisme d'algèbre de A. Le but est maintenant d'établir la formule de Macdonald (proposition 1.4.7), qui est une idendité formelle dans $\mathrm{Frac}(A)[t]$ (ce qui a bien un sens car, les q_i formant une $\mathbf{Z}$-base de Q, A est un sous-anneau d'un corps de fractions rationnelles), et d'en déduire une formule dans $\mathbf{Q}(t)$ liant $W(t)$ et la hauteur des racines positives (théorème 1.4.8). Pour cela, on aura besoin de plusieurs lemmes intermédiaires portant sur $R := \frac{1}{2} \sum_{\alpha\in\Phi^+} \alpha$

Lemme 1.4.4 : *Soit* $\Omega \subseteq \Phi^+$*. Si* $R - \sum_{\alpha\in\Omega} \alpha$ *n'est pas dans un des hyperlans de réflexion alors il existe un unique* $w \in W$ *tel que* $R - \sum_{\alpha\in\Omega} \alpha = w(R)$*.*

Démonstration :

- On suppose que $R_\Omega := R - \sum_{\alpha\in\Omega} \alpha$ n'est pas dans un des hyperlans de réflexion. Ce vecteur est donc dans

2. Ici $\mathbf{Q}$ est bien sûr le corps des nombres rationnels.

une chambre de Weyl donc, d'après la remarque 1.4.2, il existe $w \in W$ tel que $w^{-1}(R_\Omega)$ soit dans la chambre fondamentale. Or, en développant la somme définissant R_Ω, chaque racine positive apparaît une fois et une seule, avec un coefficient $\frac{1}{2}$ ou $-\frac{1}{2}$, et w^{-1} permute les racines, donc il existe $\Omega' \subseteq \Phi^+$ tel que, avec $x := \sum_{\alpha \in \Omega'} \alpha$, on ait $w^{-1}(R_\Omega) = R - x$ (en outre, comme Ω' est obtenu après avoir développé la somme terme à terme, la donnée de w et de Ω' détermine Ω). Alors $R - x$ est dans la chambre fondamentale donc, d'après le fait 1.4.3, pour $1 \leq i \leq l$, on a $\langle p_i^\vee, R - x\rangle > 0$ or $\langle p_i^\vee, R - x\rangle = 1 - \langle p_i^\vee, x\rangle$ et $\langle p_i^\vee, x\rangle \in \mathbf{Z}$ donc $\langle p_i^\vee, x\rangle \leq 0$ donc $\langle p_i, x\rangle \leq 0$. De plus, x est somme de racines positives donc il existe $(\lambda_1, \ldots, \lambda_l) \in \mathbf{N}^l$ tel que $x = \lambda_1 p_1 + \cdots + \lambda_l p_l$, donc $\langle x, x\rangle = \lambda_1\langle p_1, x\rangle + \cdots \lambda_l\langle p_l, x\rangle \leq 0$, donc $x = 0$ (donc, en particulier, R est dans la chambre fondamentale).

• Si $w \in W$ et $w' \in W$ vérifient $w(R) = w'(R)$ alors $w^{-1}w'$ fixe R donc fixe la chambre fondamentale. Donc, par simple transitivité de l'action de W sur les chambres, $w^{-1}w'$ est trivial donc $w = w'$. □

Lemme 1.4.5 : *L'ensemble des éléménts alternés de A est $\theta(A)$.*

Démonstration :

• Soit $a \in A$ et $w \in W$. Alors $w(\theta(a)) = \sum_{w' \in W} \det(w)\det(ww')ww'(a) = \det(w)\theta(a)$ car $\det w \in \{-1, 1\}$. Donc $\theta(a)$ est alterné.

• Soit $a \in A$ alterné. Alors $\theta(a) = \sum_{w \in W} \det(w)w(a) = \sum_{w \in W} a = |W|a$ donc $a = \theta\left(\frac{1}{|W|}a\right) \in \theta(A)$. □

Lemme 1.4.6 : *On a* $\theta(e(R)) = e(-R)\prod_{\alpha \in \Phi^+}(e(\alpha) - 1)$.

Démonstration :

• Soit $a := e(-R)\prod_{\alpha \in \Phi^+}(e(\alpha) - 1)$. Pour $1 \leq i \leq l$, on a $s_{p_i}(R) = R - p_i$ car s_{p_i} permute $\Phi^+ \setminus \{p_i\}$ et envoie p_i sur $-p_i$ donc $s_{p_i}(a) = e(-s_{p_i}(R))\prod_{\alpha \in \Phi^+}(e(s_{p_i}(\alpha)) - 1) = e(p_i - R)\frac{e(-p_i) - 1}{e(p_i) - 1}\prod_{\alpha \in \Phi^+}(e(\alpha) - 1) = -a$. Donc, d'après le fait 1.4.3, a est alterné.

• Puisque a est alterné, on a les égalités suivantes :

$$\begin{aligned} a &= e(R)e(-2R)\prod_{\alpha \in \Phi^+}(e(\alpha) - 1) = e(R)\prod_{\alpha \in \Phi^+}e(-\alpha)\prod_{\alpha \in \Phi^+}(e(\alpha) - 1) = e(R)\prod_{\alpha \in \Phi^+}(1 - e(-\alpha)) \\ &= e(R)\sum_{\Omega \subseteq \Phi^+}(-1)^{|\Omega|}e\left(-\sum_{\alpha \in \Omega}\alpha\right) = \sum_{\Omega \subseteq \Phi^+}(-1)^{|\Omega|}e\left(R - \sum_{\alpha \in \Omega}\alpha\right) = \frac{1}{|W|}\sum_{\Omega \subseteq \Phi^+}(-1)^{|\Omega|}\theta\left(e\left(R - \sum_{\alpha \in \Omega}\alpha\right)\right). \end{aligned}$$

Si $R - \sum_{\alpha \in \Omega}\alpha$ est dans $\beta^\perp$ pour un certain $\beta \in \Phi^+$ alors, en développant θ, les contributions de w et ws_β pour $w \in W$ se compensent, donc $\theta\left(e\left(R - \sum_{\alpha \in \Omega}\alpha\right)\right) = 0$. Sinon, d'après le lemme 1.4.4, il existe un unique $w' \in W$ tel que $R - \sum_{\alpha \in \Omega}\alpha = w'(R)$ et, d'après le fait 1.4.3, on a $|\Omega| = l(w')$; de plus, pour tout $w' \in W$, $w'(R)$ est de la forme $R - \sum_{\alpha \in \Omega}\alpha$ pour un $\Omega \subseteq \Phi^+$; cet Ω vérifie les hypothèses du lemme 1.4.4 donc, avec les notations de la démonstration de ce lemme, Ω' est vide et Ω est unique. Par conséquent, on a $a = \frac{1}{|W|}\sum_{w' \in W}\det(w')\theta(e(w'(R))) = \frac{1}{|W|}\sum_{w' \in W}\det(w')\theta(w'(e(R))) = \frac{1}{|W|}\sum_{w' \in W}\theta(e(R)) = \theta(e(R))$. □

Proposition 1.4.7 (Formule de Macdonald) : *On a* $W(t) = \sum_{w \in W}\prod_{\alpha \in \Phi^+}\frac{1 - te(-w(\alpha))}{1 - e(-w(\alpha))}$.

Démonstration :

• Soit a comme dans la démonstration du lemme 1.4.6. L'élément a est alterné donc, pour $w \in W$, on a $\det(w)a = w(a) = w(R)\prod_{\alpha \in \Phi^+}(1 - e(-w(\alpha)))$ donc $\prod_{\alpha \in \Phi^+}(1 - e(-w(\alpha))) = e(-w(R))\det(w)a$.

• En utilisant le lemme 1.4.6 et un calcul effectué dans sa démonstration, on a donc

$$\begin{aligned} W(t) &= \frac{1}{a}\sum_{w'\in W} t^{l(w')}\theta(e(R)) = \frac{1}{a}\sum_{\Omega\subseteq\Phi^+} t^{|\Omega|}(-1)^{|\Omega|}\theta\left(e\left(R-\sum_{\alpha\in\Omega}\alpha\right)\right) \\ &= \frac{1}{a}\sum_{w\in W}\left(\det(w)e(w(R))\sum_{\Omega\subseteq\Phi^+} t^{|\Omega|}(-1)^{|\Omega|}e\left(w\left(-\sum_{\alpha\in\Omega}\alpha\right)\right)\right) \\ &= \frac{1}{a}\sum_{w\in W}\left(\det(w)e(w(R))\prod_{\alpha\in\Phi^+}(1-te(-w(\alpha)))\right) = \sum_{w\in W}\prod_{\alpha\in\Phi^+}\frac{1-te(-w(\alpha))}{1-e(-w(\alpha))}. \end{aligned}$$

□

La formule de MACDONALD est une identité dans $\mathrm{Frac}(A)[t]$, mais il existe une formule plus simple dans $\mathbf{Q}(t)$, ne faisant appel qu'à la hauteur des racines positives.

Théorème 1.4.8 : *Soit Φ un système de racines de groupe de réflexion W. On choisit un ensemble de racines positives Φ^+. Alors on a $W(t) = \prod_{\alpha\in\Phi^+}\frac{t^{\mathrm{ht}(\alpha)+1}-1}{t^{\mathrm{ht}(\alpha)}-1}$.*

Démonstration :

• On commence par prolonger la hauteur en un morphisme du sous-$\mathbf{Z}$-module P de V engendré par Δ dans $\mathbf{Z}$ et valant 1 sur chaque élément de Δ. On considère $e(P)$ le groupe P dont la loi est notée multiplicativement et B la $\mathbf{Q}$-algèbre de $e(P)$. On a donc un morphisme de groupes $\psi : \left|\begin{array}{ccc} e(P) & \longrightarrow & \langle t\rangle \\ e(p) & \longmapsto & t^{-\mathrm{ht}(p)}\end{array}\right.$. ψ se prolonge en un morphisme d'algèbres $\psi : B \longrightarrow \mathbf{Q}(t)$, puis en un morphisme d'algèbres $\psi : B[t] \longrightarrow \mathbf{Q}(t)$ en imposant $\psi(t) = t$, puis en un morphisme d'algèbres $\psi : \mathrm{Frac}(B)(t) \longrightarrow \mathbf{Q}(t)$.

• La formule de MACDONALD (proposition 1.4.7) est une identité dans $\mathrm{Frac}(A)[t]$, mais aussi dans $\mathrm{Frac}(B)(t)$. En appliquant ψ à cette formule, on obtient $\sum_{w\in W} t^{l(w)} = \sum_{w\in W}\prod_{\alpha\in\Phi^+}\frac{1-t^{1+\mathrm{ht}(w(\alpha))}}{1-t^{\mathrm{ht}(w(\alpha))}}$. Or, pour $w \neq 1$, il existe $\alpha \in \Phi^+$ telle que $\mathrm{ht}(w(\alpha)) = -1$ (sinon, en passant à l'opposé, aucune racine négative n'est envoyée dans Δ donc Δ est envoyé dans Φ^+ par w^{-1} donc, par $\mathbf{N}$-linéarité, aucun élément de Φ^+ n'est envoyé dans Φ^- donc, d'après le fait 1.4.3, $l(w^{-1}) = 0$, ce qui contredit $w \neq 1$) donc la contribution de w dans le membre de droite est nulle. □

Remarque 1.4.9 : En admettant la classification des systèmes de racines, on peut encore simplifier la formule. En effet, en notant k_j le nombre de racines positives de hauteur j (en particulier $k_1 = l$), on constate que l'on a $k_j \geq k_{j+1}$ donc les k_j forment une partition d'un entier. On peut donc considérer la partition duale $(m_1,\ldots,m_l)$, qui est définie par $m_i := |\{j | k_j \geq i\}|$. On a alors $W(t) = \prod_j\prod_{i=1}^{k_j}\frac{t^{j+1}-1}{t^j-1} = \prod_{i=1}^{k_1}\prod_{\substack{j\\ k_j\geq i}}\frac{t^{j+1}-1}{t^j-1}$ or $\prod_{\substack{j\\ k_j\geq i}}\frac{t^{j+1}-1}{t^j-1} = \frac{t^{m_i+1}-1}{t-1}$ car on a un produit télescopique, d'où $W(t) = \prod_{i=1}^{l}\frac{t^{m_i+1}-1}{t-1}$.

2 Groupes algébriques linéaires

Dans cette section, on présente une classe importante de groupes munis d'une (B,N)-paire : les groupes algébriques réductifs. On commence par traiter l'exemple du groupe général linéaire puis celui du groupe symplectique. Les références principales utilisées sont [3] et [5].

2.1 Groupe général linéaire

Soit $\mathbf{K}$ un corps commutatif, $n \in \mathbf{N}^*$ et $G := \mathrm{GL}_n(\mathbf{K})$. On note B le sous-groupe des matrices triangulaires supérieures inversibles, N le sous-groupe des matrices monomiales (c'est-à-dire ayant un unique coefficient non nul sur chaque ligne et chaque colonne), H le sous-groupe des matrices diagonales inversibles et U le sous-groupe des éléments de B dont tous les coefficients diagonaux valent 1. L'objectif de cette sous-section est de montrer

que B et N constituent une (B,N)-paire scindée par U pour G, d'interpréter la longueur des éléments du groupe de Weyl et de déterminer les U_w (proposition 2.1.3).

Remarque 2.1.1 : On a déjà $H = B \cap N \trianglelefteq N$, $B = UH$ et $H \cap U = \{I_n\}$. En identifiant $\mathfrak{S}_n$ au sous-groupe des matrices de permutation, on a $N = H \rtimes \mathfrak{S}_n$ et $N/H \simeq \mathfrak{S}_n$. De plus, les valeurs propres étant invariantes par conjugaison, on a $U \trianglelefteq B$.

On note E_{ij} les matrices élémentaires, $X_{ij} := I_n + \mathbf{K}E_{ij}$, $X_i := X_{i,i+1}$, $X_{-i} := X_{i+1,i}$, n_i la matrice de permutation de la transposition $(i, i+1)$ et $V_i := \{g \in U | g_{i,i+1} = 0\}$. Un calcul élémentaire montre que V_i est un sous-groupe de U.

Lemme 2.1.2 : *Pour $1 \leq i \leq n-1$, on a $X_i \cap V_i = \{I_n\}$ et $U = X_iV_i = V_iX_i$ avec unicité de l'écriture. De plus, on a $n_iX_in_i^{-1} = X_{-i} \subseteq \{I_n\} \cup X_in_iX_iH$ et $n_iV_in_i^{-1} = V_i$.*

Démonstration :

• L'égalité $X_i \cap V_i = \{I_n\}$ est évidente. Démontrons $U = X_iV_i$. On a déjà $X_iV_i \subseteq U$. Soit $g = I_n + \lambda E_{i,i+1} \in X_i$, $h = (h_{lm})_{1 \leq l,m \leq n} \in V_i$ et $M = (m_{lm}))_{1 \leq l,m \leq n} \in U_n$. Alors $gh = I_n + \sum_{\substack{1 \leq l,m \leq n \\ l \neq i}} h_{lm}E_{lm} + \sum_{m=i+1}^{n} (h_{im} + \lambda h_{i+1,m})E_{im}$ donc $M = gh$ si et seulement si, pour $1 \leq l, m \leq n$ et $l \neq i$ on a $h_{lm} = m_{lm}$, $\lambda = m_{i,i+1}$ et, pour $i+2 \leq m \leq n$, $h_{im} = m_{im} - m_{i,i+1}m_{i+1,m}$. Donc on a $U = X_iV_i$ avec unicité de l'écriture. En passant à l'inverse, on obtient $U = V_iX_i$.

• Les deux dernières égalités découlent du fait général $\forall w \in \mathfrak{S}_n, n_wE_{lm}n_w^{-1} = E_{w(l)w(m)}$, donc conjuguer par n_i revient à échanger les lignes i et $i+1$ et échanger les colonnes i et $i+1$. Pour l'inclusion, il suffit de considérer le bloc 2×2 des coefficients en positions (i,i), $(i,i+1)$, $(i+1,i)$ et $i+1,i+1$ et d'utiliser $\forall \lambda \in \mathbf{K}^\times, \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{\lambda} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & -\frac{1}{\lambda} \end{pmatrix}$. □

On déduit de ces lemmes le résultat annoncé au début de la sous-section.

Proposition 2.1.3 : *B et N constituent une (B,N)-paire scindée par U pour GL_n, de groupe de Weyl $W = \mathfrak{S}_n$ engendré par les transpositions élémentaires. De plus, pour $w \in W$, $l(w)$ est le nombre d'inversions de w[3] donc $w_0 := \prod_{i=1}^{\lfloor \frac{n+1}{2} \rfloor} (i, n+1-i)$ est de longueur maximale. Enfin, pour $w \in W$, on a $U_w = \langle \{X_{ij} | i < j, w(i) > w(j)\} \rangle$.*

Démonstration :

• Soit $g \in G$. Soit $b \in B$ tel que le nombre total de zéros au début des lignes de bg soit maximal. Supposons que deux débuts de lignes de bg aient le même nombre de zéros. Alors, en ajoutant à la première des deux lignes un certain multiple de la deuxième (donc en multipliant à gauche par un élément de B), on augmenterait le nombre total de zéros, ce qui contredirait la définition de b. Donc il existe $w \in W = \mathfrak{S}_n$ tel que $n_wbg \in B$. Donc $G = \langle B, N \rangle$.

• On a bien $H \trianglelefteq N$ et W est engendré par les transpositions élémentaires.

• D'après le lemme 2.1.2, on a $n_iBn_i = n_iBn_i^{-1} = n_iV_in_i^{-1}n_iX_in_i^{-1}n_iHn_i^{-1} = V_iX_{-i}H \neq B$.

• Soit $w \in W$. Si on a $w^{-1}(i) < w^{-1}(i+1)$ alors $n_w^{-1}X_in_w = X_{w^{-1}(i),w^{-1}(i+1)} \subseteq U$ donc, d'après le lemme 2.1.2, $n_iBn_w = n_iV_iX_iHn_w = V_in_in_wn_w^{-1}X_in_wH \subseteq V_in_in_wUH \subseteq Bn_in_wB$. Sinon, avec $w' := (i, i+1)w$, d'après le cas précédent, on a $n_iBn_{w'} \subseteq Bn_in_{w'}B = Bn_wB$ donc $n_iBn_w = n_iBn_in_{w'}$ or, d'après le point précédent et le lemme 2.1.2, on a $n_iBn_i = V_iX_{-i}H \subseteq V_iH \cup V_iX_in_iX_iH \subseteq B \cup Bn_iB$, donc $n_iBn_w \subseteq Bn_{w'} \cup Bn_iBn_{w'} = Bn_in_w \cup Bn_iBn_in_w \subseteq Bn_in_wB \cup Bn_wB$.

• Soit $n_0 = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$ la matrice de permutation de w_0. Alors $n_0Bn_0^{-1}$ est le sous-groupe des matrices triangulaires inférieures inversibles donc $H \subseteq \bigcap_{n \in N} nBn^{-1} \subseteq B \cap n_0Bn_0^{-1} = H$.

• On a déjà $B = U \rtimes H$. Les valeurs propres étant invariantes par conjugaison, on a $\forall n \in N, n^{-1}Un \cap B \subseteq U$.

• Démontrons que, pour $1 \leq i \leq n-1$ et $w \in \mathfrak{S}_n$, on a $l((i,i+1)w) > l(w) \Leftrightarrow w^{-1}(i) < w^{-1}(i+1)$. Si $w^{-1}(i) < w^{-1}(i+1)$ alors on a montré que l'on a $n_iBn_w \subseteq Bn_in_wB$ donc $Bn_iBBn_wB \subseteq Bn_in_wB$ donc,

3. On rappelle que le nombre d'inversions est le nombre de couples (i,j) avec $1 \leq i < j \leq n$ et $w(i) > w(j)$.

d'après le lemme 1.1.9, $l((i,i+1)w) > l(w)$. Si $w^{-1}(i) > w^{-1}(i+1)$ alors, en raisonnant avec $(i,i+1)w$ au lieu de w, on obtient $l(w) = l((i,i+1)(i,i+1)w) > l((i+1,i)w)$.

• Démontrons par récurrence que $l(w)$ est le nombre d'inversions de w. Si $l(w) = 0$ alors $w = 1$ n'a pas d'inversions. Supposons $l(w) \geq 1$ et supposons que le résultat est démontré au rang $l(w)-1$. Soit $s_1 \cdots s_p$ une expression réduite de w ; on pose $y := s_2 \cdots s_p$, i tel que $s_1 = (i,i+1)$, $j := y^{-1}(i)$ et $j' := y^{-1}(i+1)$. Alors, par hypothèse de récurrence, y possède $l(w)-1$ inversions. D'après le point précédent, on a $j < j'$. De plus, $w(j) = s_1(i) = i+1$ et $w(j') = i$, donc w possède exactement une inversion de plus que y.

• Démontrons par récurrence sur $l(w)$ que U_w est de la forme souhaitée. Si $l(w) = 0$ alors $w = 1$ donc $U_w = U \cap n_0^{-1} U n_0 = \{I_n\}$. Si $l(w) = 1$ alors il existe i tel que $w = (i,i+1)$ et un calcul élémentaire donne $U_w = X_i$. Supposons $l(w) \geq 2$ et supposons que le résultat est démontré au rang $l(w)-1$. Soit $y \in W$ et $s = (i,i+1)$ tels que $w = ys$ et $l(w) = l(y)+1$. Dans la démonstration du théorème 1.2.13, on a obtenu $\forall w \in W, B_w = U_w H$ donc, d'après le lemme 1.2.6, on a $U_w H = B_w = B_y(B_s)^y = U_y H (U_s H)^y = U_y H (U_s)^y H = U_y (U_s)^y H$ or $B = U \rtimes H$ donc $U_w = U_y (U_s)^y$. De plus, un calcul élémentaire donne $(U_s)^y = X_{y^{-1}(i),y^{-1}(i+1)}$. Il suffit alors d'utiliser le point précédent, l'hypothèse de récurrence et l'égalité $X_{\alpha\beta} X_{\gamma\delta} = I_n + \mathrm{Vect}(E_{\alpha\beta}, E_{\gamma\delta})$ pour tous α, β, γ et δ. □

Remarques 2.1.4 :

• En particulier, U_w est un espace affine de dimension $l(w)$.

• En utilisant les propositions 1.2.11 et 1.2.12, on obtient des (B,N)-paires scindées pour SL_n, PGL_n et PSL_n.

2.2 Groupe symplectique

Pour $m \in \mathbf{N}^*$, on pose $Q_m := \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$ et $J_{2m} := \left(\begin{array}{c|c} 0 & Q_m \\ \hline -Q_m & 0 \end{array}\right)$. Alors le groupe symplectique est $\mathrm{Sp}_{2m}(\mathbf{K}) := \{A \in \mathrm{GL}_{2m}(\mathbf{K}) \mid {}^tA J_{2m} A = J_{2m}\} \leq \mathrm{GL}_{2m}(\mathbf{K})$.

Pour $n \in \mathbf{N}^*$, on considère les sous-groupes de $\mathrm{GL}_n(\mathbf{K})$ définis dans la sous-section précédente. Pour éviter les confusions, on précise la taille : ces sous-groupes seront donc notés B_n, N_n, H_n et U_n. De plus, le sous-espace de $M_n(\mathbf{K})$ formé des matrices symétriques est noté S_n. On se place ici dans le cas $n = 2m$. On pose enfin $t := (m, m+1)$ et, pour $1 \leq i \leq m-1$, $s_i := (m-i, m-i+1)(m+i, m+i+1)$, et on définit alors $W'_{2m} := \langle t, s_1, \ldots, s_{m-1} \rangle \leq \mathfrak{S}_{2m}$. On a alors la proposition suivante.

Proposition 2.2.1 : *$B_{2m} \cap \mathrm{Sp}_{2m}$ et $N_{2m} \cap \mathrm{Sp}_{2m}$ constituent une (B,N)-paire scindée par $U_{2m} \cap \mathrm{Sp}_{2m}$ pour Sp_{2m}, de groupe de* Weyl *W'_{2m}.*

Démonstration :

• Soit $\varphi : \left|\begin{array}{ccc} \mathrm{GL}_{2m} & \longrightarrow & \mathrm{GL}_{2m} \\ A & \longmapsto & J_{2m}^{-1}\, {}^tA^{-1} J_{2m} \end{array}\right.$. Alors φ est un automorphisme de groupe (involutif) et on a $\mathrm{Sp}_{2m} = \mathrm{GL}_{2m}^{\varphi}$. Il suffit donc de vérifier que les hypothèses du théorème 1.3.4 sont remplies.

• On a bien une (B,N)-paire scindée pour GL_{2m}, de groupe de Weyl fini.

• Avec $M := \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) \in \mathrm{GL}_{2m}$, on a $J_{2m}^{-1} M J_{2m} = \left(\begin{array}{c|c} Q_m D Q_m & -Q_m C Q_m \\ \hline -Q_m B Q_m & Q_m A Q_m \end{array}\right)$. Donc un calcul élémentaire montre que φ laisse stables N_{2m}, H_{2m} et U_{2m}.

• Pour $w \in \mathfrak{S}_{2m}$ et n_w la matrice de permutation associée, on a ${}^t n_w^{-1} = n_w$ donc $\overline{\varphi}(w) = w_0^{-1} w w_0$. Donc les orbites de $\overline{\varphi}$ sur les transpositions élémentaires sont de la forme $\{(i,i+1), (2m-i, 2m-i+1)\}$ pour $1 \leq i \leq m-1$ et $\{(m,m+1)\}$. En utilisant le lemme 1.3.3, on obtient $W^{\overline{\varphi}} = W'_{2m}$. En particulier, pour vérifier (BNφ2), il suffit de montrer que t et les s_i ont chacun un représentant dans N^{φ}. Pour t, il suffit de prendre $\left(\begin{array}{c|cc|c} I_{m-1} & & & \\ \hline & 0 & 1 & \\ & -1 & 0 & \\ \hline & & & I_{m-1} \end{array}\right)$ et pour s_i, la matrice de permutation usuelle convient.

• Enfin, on a $U_t^{\varphi} = I_{2m} + \mathbf{K} E_{m,m+1} \neq \{I_{2m}\}$ et $U_{s_i}^{\varphi} = I_{2m} + \mathbf{K}(E_{m-i,m-i+1} - E_{m+i,m+i+1}) \neq \{I_{2m}\}$. □

Remarques 2.2.2 :

• En utilisant la proposition 1.2.12, on en déduit une (B,N)-paires scindée pour PSp_{2m}.

• On a $H_{2m} \cap \mathrm{Sp}_{2m} = \left\{ \mathrm{diag}\left(t_1, \ldots, t_m, \frac{1}{t_m}, \ldots, \frac{1}{t_1}\right) \mid (t_1, \ldots, t_m) \in (\mathbf{K}^{\times})^m \right\}$.

Proposition 2.2.3 : *Soit* $w_0 := \prod_{i=1}^{\lfloor \frac{n+1}{2} \rfloor} (i, n+1-i)$. *Alors* w_0 *est l'élément de plus grande longueur de* W'_{2m} *et il est de longueur* m^2.

Démonstration :

• On a $s_i \cdots s_1 t s_1 \cdots s_i = (m-i, m-i+1)$, donc $w_0 = t(s_1 t s_1) \cdots (s_{m-1} \cdots s_1 t s_1 \cdots s_{m-1}) \in W'_{2m}$. Cette expression de w_0 possède m^2 termes, donc il faut montrer qu'elle est réduite. Pour $\sigma \in W'_{2m}$, on note $\widetilde{l}(\sigma) := |\{i \leq m | \sigma(i) \geq m+1\}|$. On a $\forall \sigma \in W'_{2m}, \forall \tau \in W'_{2m}, \widetilde{l}(\sigma\tau) \leq \widetilde{l}(\sigma) + \widetilde{l}(\tau)$ or $\widetilde{l}(w_0) = m$, $\widetilde{l}(t) = 1$ et $\widetilde{l}(s_i) = 1$, donc il faut au moins m occurences de t dans toute expression de w_0. Donc si l'expression précédente de w_0, qui comporte m t et $m^2 - m$ s_i, n'était pas réduite alors, d'après la condition de simplification 1.1.17, on pourrait obtenir une expression réduite en supprimant certains s_i ; comme t possède 1 inversion et les s_i en possèdent 2, w_0 aurait au plus $m + 2(m^2 - m - 1) < \frac{2m(2m-1)}{2}$ inversions, ce qui est absurde.

• Donc on a déjà $l(tw_0) < l(w_0)$. Un calcul immédiat permet d'obtenir les relations $s_1 t s_1 t s_1 = t s_1 t$, $t s_i = s_i t$ pour $i \geq 2$, $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ et $s_i s_j = s_j s_i$ pour $|j-i| \geq 2$, donc on a $s_1 s_2 \cdots s_i \cdots s_2 s_1 = s_i \cdots s_2 s_1 s_2 \cdots s_i$ et (en « remontant » successivement les termes de la deuxième moitié vers la gauche et en utilisant la troisième relation) $s_i \cdots s_1 s_i \cdots s_2 = (s_{i-1} s_i)(s_{i-2} s_{i-1}) \cdots (s_1 s_2) s_1$. Donc, avec $y := t(s_1 t s_1) \cdots (s_{i-2} \cdots s_1 t s_1 \cdots s_{i-2})$ et $y' := (s_{i+1} \cdots s_1 t s_1 \cdots s_{i+1}) \cdots (s_{m-1} \cdots s_1 t s_1 \cdots s_{m-1})$, on a les égalités successives

$$\begin{aligned}
s_i w_0 &= y s_i (s_{i-1} \cdots s_1 t \underbrace{s_1 \cdots s_{i-1})(s_i s_{i-1} \cdots s_1}\, t s_1 \cdots s_{i-1} s_i) y' \\
&= y s_i s_{i-1} \cdots s_1 \underbrace{t s_i s_{i-1} \cdots}\, s_1 \underbrace{\cdots s_{i-1} s_i t}\, s_1 \cdots s_{i-1} s_i y' \\
&= y \underbrace{s_i \cdots s_1 s_i \cdots s_2}\, t s_1 t \underbrace{s_2 \cdots s_i s_1 \cdots s_i}\, y' \\
&= y s_{i-1} s_i s_{i-2} s_{i-1} \cdots s_1 s_2 \underbrace{s_1 t s_1 t s_1}\, s_2 s_1 \cdots s_{i-1} s_{i-2} s_i s_{i-1} y'
\end{aligned}$$

donc $l(s_i w_0) < l(w_0)$. Donc, d'après la proposition 1.2.1, w_0 est de longueur maximale. □

Remarque 2.2.4 : On peut montrer que, pour le groupe spécial orthogonal SO_n, $B_n \cap \mathrm{SO}_n$ et $N_n \cap \mathrm{SO}_n$ constituent une (B,N)-paire scindée par $U_n \cap \mathrm{SO}_n$ (voir par exemple [3, pp. 79-87]). Si n est impair alors le raisonnement est le même que pour le groupe symplectique. Toutefois, si n est pair alors on ne peut plus utiliser le théorème 1.3.4 (car l'hypothèse $\forall J \in \overline{S}, U_{w_J}^{\varphi} \neq \{1\}$ n'est plus satistaite) et il faut tout vérifier « à la main », ce qui, à défaut d'être très difficile, est long et fastidieux.

2.3 Groupes algébriques réductifs

Les exemples de GL_n, SL_n et Sp_{2m} sont des cas particuliers du théorème suivant, qui est un résultat classique en théorie des groupes algébriques (voir par exemple [5, pp. 170-176]).

Théorème 2.3.1 : *Soit* $\mathbf{K}$ *un corps algébriquement clos,* G *un groupe algébrique affine connexe réductif*[4]*,* H *un tore maximal,* B *un sous-groupe de* Borel *contenant* H*,* N *le normalisateur de* H *dans* G *et* U *le radical unipotent de* B*. Alors* B *et* N *constituent une (B,N)-paire scindée par* U *pour* G *; on appelle* **(B,N)-paire réductive** *toute (B,N)-paire de cette forme. De plus,* B *est le normalisateur de* U*,* U *est le groupe dérivé de* B*, le groupe dérivé* $[G,G]$ *de* G *est semi-simple et on a* $G = [G,G] \cdot H$*. Enfin,* W *est un groupe de réflexion fini qui ne dépend pas de la (B,N)-paire réductive choisie et, pour* $w \in W$*, on a* $\dim U_w = l(w)$.

3 Groupes finis de type Lie

Dans cette section, on commence par présenter les notions de structure $\mathbf{F}_q$-rationnelle et de morphisme de Frobenius. On étudie notamment le cas particulier des groupes algébriques. On définit ensuite les groupes finis de type Lie et on explique comment calculer leur cardinal (théorème 3.3.4). Enfin, on vérifie la formule obtenue sur les exemples bien connus de $\mathrm{GL}_n(\mathbf{F}_q)$ et $\mathrm{Sp}_{2m}(\mathbf{F}_q)$ (3.3.5 et 3.3.6). La référence principale utilisée est [3].

3.1 Structures $\mathbf{F}_q$-rationnelles

Soit p un nombre premier, q une puissance de p et $\overline{\mathbf{F}}_p := \bigcup_{n \in \mathbf{N}} \mathbf{F}_{p^{n!}}$ (qui est une clôture algébrique de $\mathbf{F}_p$).

4. Pour les définitions, on pourra se reporter à l'annexe A.1.

Définition 3.1.1 : *Soit (X, A) une variété algébrique affine sur $\overline{\mathbf{F}}_p$ et $F : X \longrightarrow X$ un morphisme. On dit que X possède une* **structure $\mathbf{F}_q$-rationnelle**, *de* **morphisme de Frobenius** *(géométrique) F, si :*

(i) $F^* : A \longrightarrow A$ est injectif et a pour image $A^q := \{f^q | f \in A\}$;

(ii) pour tout $f \in A$, il existe $m \in \mathbf{N}^*$ tel que l'on ait $(F^*)^m(f) = f^{q^m}$.

Alors $X^F := \{x \in X | F(x) = x\}$ est appelé l'ensemble des points **$\mathbf{F}_q$-rationnels** *de X, $\sigma : \left| \begin{array}{ccc} A & \longrightarrow & A \\ f & \longmapsto & (F^*)^{-1}(f^q) \end{array} \right.$ est appelé le* **morphisme de Frobenius arithmétique** *et on pose $A_0 := A^\sigma = \{f \in A | F^*(f) = f^q\}$.*

Remarques 3.1.2 :

• F^* est un morphisme de $\overline{\mathbf{F}}_p$-algèbres donc on a $\forall f \in A, F^* \circ \sigma(f) = \sigma \circ F^*(f) = f^q$.

• $\sigma : A \longrightarrow A$ est un automorphisme d'anneau. En effet, σ est bien un morphisme, est injectif (car pour $f \in A$ et $g \in A$, si $\sigma(f) = \sigma(g)$ alors $f^q = F^* \circ (\sigma(f)) = F^* \circ \sigma(g) = g^q$ donc $f = g$) et est surjectif (car pour $g \in A$, il existe $f \in A$ tel que $F^*(g) = f^q = F^* \circ \sigma(f)$ donc $g = \sigma(f)$ car F^* est injectif).

• Plus généralement, on dit que F est un **morphisme de Frobenius généralisé** s'il existe une itérée de F qui est un morphisme de Frobenius.

Exemple 3.1.3 : Soit $n \in \mathbf{N}^*$ et $F_q : \left| \begin{array}{ccc} \overline{\mathbf{F}}_p^n & \longrightarrow & \overline{\mathbf{F}}_p^n \\ (x_1, \ldots, x_n) & \longmapsto & (x_1^q, \ldots, x_n^q) \end{array} \right.$, qui est un morphisme bijectif. F_q est surjectif donc F_q^* est injectif. On a $A = \overline{\mathbf{F}}_p[X_1, \ldots, X_n]$ et, pour $1 \leq i \leq n$, $F_q^*(X_i) = X_i^q$ donc, pour raison de caractéristique, $F_q^*(A) = A^q$. Enfin, pour $f \in A$, il existe $m \in \mathbf{N}^*$ tel que $f \in \mathbf{F}_{q^m}[X_1, \ldots, X_n]$ et alors $(F_q^*)^m(f) = f^{q^m}$. Donc F_q est un morphisme de Frobenius, appelé **morphisme de Frobenius standard**. On a $F_q^* : \left| \begin{array}{ccc} A & \longrightarrow & A \\ \sum_\alpha \lambda_\alpha X^\alpha & \longmapsto & \sum_\alpha \lambda_\alpha X^{q\alpha} \end{array} \right.$ et $\sigma : \left| \begin{array}{ccc} A & \longrightarrow & A \\ \sum_\alpha \lambda_\alpha X^\alpha & \longmapsto & \sum_\alpha \lambda_\alpha^q X^\alpha \end{array} \right.$ (où α est un multi-indice).

Les deux lemmes suivants donnent des informations sur les liens entre les structures de $\overline{\mathbf{F}}_p$-algèbre et de $\mathbf{F}_q$-algèbre de A.

Lemme 3.1.4 : *Pour $f \in A$, $\mathrm{Vect}_{\overline{\mathbf{F}}_p}(\{\sigma^n(f) | n \in \mathbf{N}\})$ est un sous-$\overline{\mathbf{F}}_p$-espace vectoriel de A de dimension finie et possède une base formée d'éléments de A_0. Par conséquent, A peut-être engendrée comme $\overline{\mathbf{F}}_p$-algèbre par un nombre fini d'éléménts de A_0 et possède une $\overline{\mathbf{F}}_p$-base dénombrable formée d'éléments de A_0.*

Démonstration : Soit $m \in \mathbf{N}^*$ tel que $(F^*)^m = f^{q^m}$. Alors $(F^*)^m(\sigma^m(f)) = (F^* \circ \sigma)^m(f) = f^{q^m} = (F^*)^m(f)$ donc $\sigma^m(f) = f$. Donc on a déja $\dim_{\overline{\mathbf{F}}_p} \mathrm{Vect}_{\overline{\mathbf{F}}_p}(\{\sigma^n(f) | n \in \mathbf{N}\}) \leq m$. Le $\mathbf{F}_q$-espace vectoriel $\mathbf{F}_{q^m}$ est de dimension m ; soit $(\lambda_0, \ldots, \lambda_{m-1})$ une base. On pose $g_i := \sum_{j=0}^{m-1} \sigma^j(\lambda_i f)$. Alors $g_i \in A_0$ car $\sigma^m(\lambda_i f) = \lambda_i^{q^m} \sigma^m(f) = \lambda_i f$. De plus, $g_i = \sum_{j=0}^{m-1} \lambda_i^{q^j} \sigma^j(f)$ donc obtient un système linéaire d'inconnues les $\sigma^j(f)$, dont le déterminant est un déterminant de Vandermonde non nul (car les λ_i^q sont deux à deux distincts). Donc les g_i forment une famille $\overline{\mathbf{F}}_p$-génératrice. La deuxième partie du lemme découle du fait que A est une $\overline{\mathbf{F}}_p$-algèbre de type fini. □

Lemme 3.1.5 : *A_0 est une $\mathbf{F}_q$-algèbre de type fini et la multiplication $\overline{\mathbf{F}}_p \otimes_{\mathbf{F}_q} A_0 \longrightarrow A$ est un isomorphisme de $\overline{\mathbf{F}}_p$-algèbres.*

Démonstration : D'après le lemme 3.1.4, il existe $S \subseteq A_0$ fini engendrant A comme $\overline{\mathbf{F}}_p$-algèbre et alors il existe une $\overline{\mathbf{F}}_p$-base T de A formée de produits d'éléments de S. La multiplication est donc surjective et on a $\mathrm{Vect}_{\mathbf{F}_q}(T) \leq A_0$. Pour $f \in A_0$, il existe une famille presque nulle de $\lambda_t \in \overline{\mathbf{F}}_p$ telle que $f = \sum_{t \in T} \lambda_t t$ et alors $\sum_{t \in T} \lambda_t^q t = \sigma(f) = f = \sum_{t \in T} \lambda_t t$ donc $\lambda_t^q = \lambda_t$ donc $\lambda_t \in \mathbf{F}_q$. Donc $\mathrm{Vect}_{\mathbf{F}_q}(T) = A_0$ donc la multiplication est injective. □

Remarque 3.1.6 : Donc toute famille d'éléments de A_0 est $\overline{\mathbf{F}}_p$-libre si et seulement si elle est $\mathbf{F}_q$-libre.

Le théorème suivant montre que l'on peut se ramener au cas des fermés algébriques de $\overline{\mathbf{F}}_p^n$.

Théorème 3.1.7 : *Soit (X, A) une variété algébrique affine sur $\overline{\mathbf{F}}_p$ possédant une structure $\mathbf{F}_q$-rationnelle, de morphisme de* Frobenius *F. Alors il existe $n \in \mathbf{N}^*$ et une immersion fermée $\iota : X \hookrightarrow \overline{\mathbf{F}}_p^n$ telle que $F_q \circ \iota = \iota \circ F$ (où F_q est le morphisme de* Frobenius *standard de l'exemple 3.1.3). De plus, $\mathcal{I}(\iota(X))$ est engendré par des éléments de $\mathbf{F}_q[X_1, \ldots, X_n]$, F est bijectif, les X^{F^m} pour $m \in \mathbf{N}^*$ sont finis et on a $X = \bigcup_{m \in \mathbf{N}^*} X^{F^m}$.*

Démonstration :

• A_0 est une $\mathbf{F}_q$-algèbre de type fini donc il existe $n \in \mathbf{N}^*$ et un idéal I_0 de $\mathbf{F}_q[X_1, \ldots, X_n]$ tels que $A_0 \simeq \mathbf{F}_q[X_1, \ldots, X_n]/I_0$. Alors, d'après le lemme 3.1.5, avec I l'idéal engendré par I_0 dans $\overline{\mathbf{F}}_p[X_1, \ldots, X_n]$, on a des isomorphismes de $\overline{\mathbf{F}}_p$-algèbres $A \simeq \overline{\mathbf{F}}_p \otimes_{\mathbf{F}_q} (\mathbf{F}_q[X_1, \ldots, X_n]/I_0) \simeq (\overline{\mathbf{F}}_p \otimes_{\mathbf{F}_q} \mathbf{F}_q[X_1, \ldots, X_n])/(\overline{\mathbf{F}}_p \otimes_{\mathbf{F}_q} I_0) \simeq \overline{\mathbf{F}}_p[X_1, \ldots, X_n]/I$. Soit alors $\pi : \overline{\mathbf{F}}_p[X_1, \ldots, X_n] \twoheadrightarrow A$ la projection canonique. C'est un morphisme de $\overline{\mathbf{F}}_p$-algèbres donc il existe un unique morphisme de variétés $\iota : X \hookrightarrow \overline{\mathbf{F}}_p^n$ tel que $\pi = \iota^*$. π est surjectif donc ι est une immersion fermée et $\iota(X) = \mathcal{Z}(\ker \iota^*) = \mathcal{Z}(I)$ donc $\mathcal{I}(\iota(X)) = \sqrt{I} = I$, la dernière égalité découlant du fait que A est réduite.

• Soit $f \in \mathbf{F}_q[X_1, \ldots, X_n]$. La restriction de π à $\mathbf{F}_q[X_1, \ldots, X_n]$ est la projection canonique sur A_0 donc $(F_q \circ \iota)^*(f) = \pi(F_q^*(f)) = \pi(f^q) = \pi(f)^q = (F^* \circ \sigma)(\pi(f)) = F^*(\pi(f)) = (\iota \circ F)^*(f)$. Par $\overline{\mathbf{F}}_p$-linéarité, on en déduit $(F_q \circ \iota)^* = (\iota \circ F)^*$ donc $F_q \circ \iota = \iota \circ F$.

• $\iota \circ F$, étant égal à $F_q \circ \iota$, est injectif donc F est injectif. Soit $x \in X$. F_q est bijectif donc il existe $v \in \overline{\mathbf{F}}_p^n$ tel que $\iota(x) = F_q(v)$ or $\forall f \in I_0, f(v)^q = f(F_q(v)) = f(\iota(x)) = 0$ donc $v \in \mathcal{Z}(I_0) = \iota(X)$ donc il existe $y \in X$ tel que $v = \iota(y)$ et alors, comme ι est injectif, $x = F(y)$. Donc F est surjectif.

• Donc $\iota(X^F) \subseteq (\overline{\mathbf{F}}_p^n)^{F_q} = \mathbf{F}_q^n$ donc $|X^F| = |\iota(X^F)| \leq q^n$. Plus généralement, pour $m \in \mathbf{N}^*$, F^m munit X d'une structure $\mathbf{F}_{q^m}$-rationnelle donc X^{F^m} est également fini.

• Soit $x \in X$. Soit $m \in \mathbf{N}^*$ tel que $\iota(x) \in F_{q^m}^n$. Alors $\iota(F^m(x)) = F_q^m(\iota(x)) = \iota(x)$ donc $x \in X^{F^m}$. □

Remarques 3.1.8 :

• Plus généralement, si F est seulement un morphisme de Frobenius généralisé alors F est bijectif, les X^{F^m} pour $m \in \mathbf{N}^*$ sont finis et on a $X = \bigcup_{m \in \mathbf{N}^*} X^{F^m}$. En effet, avec $d \in \mathbf{N}^*$ tel que F^d soit un morphisme de Frobenius, F^d est bijectif donc F aussi et on a $X^{F^m} \subseteq X^{(F^d)^m}$.

• L'application ι étant un isomorphisme sur son image, on peut identifier X^F à un sous-ensemble de $\mathbf{F}_q^n$ défini par des équations polynomiales à coefficients dans $\mathbf{F}_q$. Les structures $\mathbf{F}_q$-rationnelles conviennent donc bien pour décrire la notion intuitive de « variété affine sur $\mathbf{F}_q$ ».

Corollaire 3.1.9 : *Soit (X, A) une variété algébrique affine sur $\overline{\mathbf{F}}_p$ possédant une structure $\mathbf{F}_q$-rationnelle, de morphisme de* Frobenius *F, et Y un fermé de X. Alors les assertions suivantes sont équivalentes :*

(i) Y est stable par F ;

(ii) on a $F(Y) = Y$;

(iii) $\mathcal{I}_A(Y)$ est engendré par des éléments de A_0 ;

(iv) il existe $S \subseteq A_0$ tel que l'on ait $Y = \mathcal{Z}_X(S)$.

Dans ce cas, Y est muni d'une structure $\mathbf{F}_q$-rationnelle, de morphisme de Frobenius *$F_{|Y} : Y \longrightarrow Y$.*

Démonstration :

• $(i) \Rightarrow (ii)$: On suppose (i) vraie. D'après le théorème 3.1.7 et comme Y est stable par F, on a $Y = \bigcup_{m \in \mathbf{N}^*} Y^{F^m}$ et les Y^{F^m} sont finis. Donc $F_{|Y^{F^m}} : Y^{F^m} \longrightarrow Y^{F^m}$, étant injectif, est également surjectif. Donc $F_{|Y} : Y \longrightarrow Y$ est surjectif, donc (ii) est vraie.

• $(ii) \Rightarrow (iii)$: On suppose (ii) vraie. Pour $f \in \mathcal{I}_A(Y)$, avec $g := \sigma(f)$, on a $g \circ F = F^*(g) = f^q$ donc, comme on a $F(Y) = Y$, $g_{|Y} = g_{|F(Y)} = g \circ F_{|Y} = 0$. Donc $\mathcal{I}_A(Y)$ est stable par σ. Soit $S \subseteq A$ engendrant $\mathcal{I}_A(Y)$ comme idéal. Alors, d'après le lemme 3.1.5, $\mathrm{Vect}_{\overline{\mathbf{F}}_p}(\{\sigma^i(s) | s \in S, i \in \mathbf{N}\}) \subseteq \mathcal{I}_A(Y)$ possède une base $\widetilde{S}$ formée d'éléments de A_0. On a $S \subseteq \mathrm{Vect}_{\overline{\mathbf{F}}_p}(\widetilde{S})$ donc $\mathcal{I}_A(Y) = (S) \subseteq (\mathrm{Vect}_{\overline{\mathbf{F}}_p}(\widetilde{S})) = (\mathrm{Vect}_{\overline{\mathbf{F}}_p}(\{\sigma^i(s) | s \in S, i \in \mathbf{N}\})) \subseteq \mathcal{I}_A(Y)$. Donc $\widetilde{S} \subseteq A_0$ engendre $\mathcal{I}_A(Y)$ comme idéal. Donc (iii) est vraie.

• $(iii) \Rightarrow (iv)$: On suppose (iii) vraie. Avec les notations du point précédent, on a $Y = \mathcal{Z}(\mathcal{I}_A(Y)) = \mathcal{Z}(\widetilde{S})$. Donc (iv) est vraie.

• $(iv) \Rightarrow (i)$: On suppose (iv) vraie. Soit $y \in Y$. Alors on a $\forall f \in S, f(F(y)) = F^*(f)(y) = f^q(y) = 0$ donc $F(y) \in \mathcal{Z}(S) = Y$. Donc (i) est vraie. □

La proposition suivante précise comment on peut munir un produit de variétés d'une structure $\mathbf{F}_q$-rationnelle.

Proposition 3.1.10 : *Soit (X, A) et (X', A') deux variétés algébriques affines sur $\overline{\mathbf{F}}_p$ munies d'une structure $\mathbf{F}_q$-rationnelle, de morphismes de* FROBENIUS *F et F'. Alors $F \times F'$ munit $(X \times X', A \otimes_{\overline{\mathbf{F}}_p} A')$ d'une structure $\mathbf{F}_q$-rationnelle. De plus, on a $(A \otimes_{\overline{\mathbf{F}}_p} A')_0 = A_0 \otimes_{\mathbf{F}_q} A'_0$.*

Démonstration :

- $F \times F'$ est bien un morphisme de FROBENIUS car on a $(F \times F')^* = F^* \otimes F'^*$.
- Démontrons qu'il suffit de traiter le cas des sous-variétés de $\overline{\mathbf{F}}_p^n$. Soit $\iota : X \hookrightarrow \overline{\mathbf{F}}_p^m$ et $\iota' : X' \hookrightarrow \overline{\mathbf{F}}_p^n$ les immersions fermées données par le théorème 3.1.7. Alors $\iota \times \iota' : X \times X' \hookrightarrow \overline{\mathbf{F}}_p^m \times \overline{\mathbf{F}}_p^n$ est une immersion fermée qui commute avec les morphismes de FROBENIUS. Notons B et B' les algèbres des fonctions régulières de $\iota(X)$ et $\iota'(X')$. Alors, pour $f \in A$, on a les équivalences $f \in A_0 \Leftrightarrow F^*(f) = f^q \Leftrightarrow F^* \circ \iota^*((\iota^*)^{-1}(f)) = \iota^*((\iota^*)^{-1}(f^q)) \Leftrightarrow F_q^*((\iota^*)^{-1}(f)) = (\iota^*)^{-1}(f)^q \Leftrightarrow (\iota^*)^{-1}(f) \in B_0$. Donc $\iota^* : B_0 \longrightarrow A_0$ est un isomorphisme de $\mathbf{F}_q$-algèbres. Donc on a des isomorphismes de $\mathbf{F}_q$-algèbres $A_0 \otimes_{\mathbf{F}_q} A'_0 \simeq B_0 \otimes_{\mathbf{F}_q} B'_0$ et $(A \otimes_{\overline{\mathbf{F}}_p} A')_0 \simeq (B \otimes_{\overline{\mathbf{F}}_p} B')_0$.
- On suppose désormais que X et X' sont des sous-variétés de $\overline{\mathbf{F}}_p^m$ et $\overline{\mathbf{F}}_p^n$ stables par les morphismes de FROBENIUS standard de l'exemple 3.1.3. D'après le corollaire 3.1.9, il existe un idéal $I_0 \subseteq \mathbf{F}_q[X_1, \dots, X_m]$ tel que, avec $I \subseteq \overline{\mathbf{F}}_p[X_1, \dots, X_m]$ l'idéal engendré par I_0, on ait un isomorphisme de $\overline{\mathbf{F}}_p$-algèbres $A \simeq \overline{\mathbf{F}}_p[X_1, \dots, X_m]/I$. De plus, la multiplication $\overline{\mathbf{F}}_p \otimes_{\mathbf{F}_q} \mathbf{F}_q[X_1, \dots, X_m] \longrightarrow \overline{\mathbf{F}}_p[X_1, \dots, X_m]$ est un isomorphisme de $\overline{\mathbf{F}}_p$-algèbres tel que l'image de l'idéal $\overline{\mathbf{F}}_p \otimes_{\mathbf{F}_q} I_0$ est l'idéal I. Par passage au quotient, on en déduit $(\overline{\mathbf{F}}_p \otimes_{\mathbf{F}_q} \mathbf{F}_q[X_1, \dots, X_m])/(\overline{\mathbf{F}}_p \otimes_{\mathbf{F}_q} I_0) \simeq \overline{\mathbf{F}}_p[X_1, \dots, X_m]/I$. Comme $\left| \begin{array}{ccc} \overline{\mathbf{F}}_p \otimes_{\mathbf{F}_q} (\mathbf{F}_q[X_1, \dots, X_m]/I_0) & \longrightarrow & (\overline{\mathbf{F}}_p \otimes_{\mathbf{F}_q} \mathbf{F}_q[X_1, \dots, X_m])/(\overline{\mathbf{F}}_p \otimes_{\mathbf{F}_q} I_0) \\ \sum_i \lambda_i \otimes (P_i \bmod I_0) & \longmapsto & \sum_i \lambda_i \otimes P_i \bmod \overline{\mathbf{F}}_p \otimes_{\mathbf{F}_q} I_0 \end{array} \right.$ est aussi un isomorphisme, $\mu : \left| \begin{array}{ccc} \overline{\mathbf{F}}_p \otimes_{\mathbf{F}_q} (\mathbf{F}_q[X_1, \dots, X_m]/I_0) & \longrightarrow & \overline{\mathbf{F}}_p[X_1, \dots, X_m]/I \\ \sum_i \lambda_i \otimes (P_i \bmod I_0) & \longmapsto & \sum_i \lambda_i P_i \bmod I \end{array} \right.$ également. On considère une $\overline{\mathbf{F}}_p$-base $(X^\alpha \bmod I)_{\alpha \in A}$ de $\overline{\mathbf{F}}_p[X_1, \dots, X_m]/I$. Alors $(X^\alpha \bmod I_0)_{\alpha \in A}$ est $\mathbf{F}_q$-libre donc, comme μ est injective, on a les équivalences suivantes :

$$\begin{aligned} \sum_{\alpha \in A} \lambda_\alpha X^\alpha \bmod I = \sigma\left(\sum_{\alpha \in A} \lambda_\alpha X^\alpha \bmod I\right) &\Leftrightarrow \sum_{\alpha \in A} \lambda_\alpha X^\alpha \bmod I = \sum_{\alpha \in A} \lambda_\alpha^q X^\alpha \bmod I \\ &\Leftrightarrow \forall \alpha \in A, \lambda_\alpha = \lambda_\alpha^q \Leftrightarrow \forall \alpha \in A, \lambda_\alpha \in \mathbf{F}_q. \end{aligned}$$

Dans ce cas on a $\sum_{\alpha \in A} \lambda_\alpha \otimes (X^\alpha \bmod I_0) = 1 \otimes \left(\sum_{\alpha \in A} \lambda_\alpha X^\alpha \bmod I_0\right)$. Par conséquent, on a un isomorphisme de $\mathbf{F}_q$-algèbres $A_0 \simeq \mathbf{F}_q[X_1, \dots, X_m]/I_0$.

- Par conséquent, on a les isomorphismes suivants :

$$\begin{aligned} A_0 \otimes_{\mathbf{F}_q} A'_0 &\simeq (\mathbf{F}_q[X_1, \dots, X_m]/I_0) \otimes_{\mathbf{F}_q} (\mathbf{F}_q[Y_1, \dots, Y_n]/I'_0) \\ &\simeq (\mathbf{F}_q[X_1, \dots, X_m] \otimes_{\mathbf{F}_q} \mathbf{F}_q[Y_1, \dots, Y_n])/(I_0 \otimes_{\mathbf{F}_q} \mathbf{F}_q[Y_1, \dots, Y_n] + \mathbf{F}_q[X_1, \dots, X_m] \otimes_{\mathbf{F}_q} I'_0) \\ &\simeq (\mathbf{F}_q[X_1, \dots, X_m] \otimes_{\mathbf{F}_q} \mathbf{F}_q[Y_1, \dots, Y_n])/((I \otimes_{\overline{\mathbf{F}}_p} \overline{\mathbf{F}}_p[Y_1, \dots, Y_n] + \overline{\mathbf{F}}_p[X_1, \dots, X_m] \otimes_{\overline{\mathbf{F}}_p} I') \cap \\ &\qquad (\overline{\mathbf{F}}_q[X_1, \dots, X_m] \otimes_{\mathbf{F}_q} \overline{\mathbf{F}}_q[Y_1, \dots, Y_n])) \\ &\simeq [(\overline{\mathbf{F}}_p[X_1, \dots, X_m] \otimes_{\overline{\mathbf{F}}_p} \overline{\mathbf{F}}_p[Y_1, \dots, Y_n])/(I \otimes_{\overline{\mathbf{F}}_p} \overline{\mathbf{F}}_p[Y_1, \dots, Y_n] + \overline{\mathbf{F}}_p[X_1, \dots, X_m] \otimes_{\overline{\mathbf{F}}_p} I')]_0 \\ &\simeq (A \otimes_{\overline{\mathbf{F}}_p} A')_0. \end{aligned}$$

En regardant les isomorphismes utilisés, on constate que l'on a montré que l'inclusion $A_0 \otimes_{\mathbf{F}_q} A'_0 \hookrightarrow (A \otimes_{\overline{\mathbf{F}}_p} A')_0$ est un isomorphisme. □

3.2 Groupes définis sur $\mathbf{F}_q$

Définition 3.2.1 : *Soit G un groupe algébrique affine sur $\overline{\mathbf{F}}_p$* [5] *possédant une $\mathbf{F}_q$-structure rationnelle. On dit que G est* **défini sur $\mathbf{F}_q$** *si le morphisme de* FROBENIUS *est un morphisme de groupes.*

Exemple 3.2.2 : $F_q : \left| \begin{array}{ccc} \mathrm{GL}_n(\overline{\mathbf{F}}_p) & \longrightarrow & \mathrm{GL}_n(\overline{\mathbf{F}}_p) \\ (m_{ij})_{1 \le i,j \le n} & \longmapsto & (m_{ij}^q)_{1 \le i,j \le n} \end{array} \right.$ munit $\mathrm{GL}_n(\overline{\mathbf{F}}_p)$ d'une structure de groupe algébrique défini sur $\mathbf{F}_q$ et on a $\mathrm{GL}_n(\overline{\mathbf{F}}_p)^{F_q} = \mathrm{GL}_n(\mathbf{F}_q)$. Plus généralement, si G est un sous-groupe fermé de $\mathrm{GL}_n(\overline{\mathbf{F}}_p)$ alors, d'après le corollaire 3.1.9, G est stable par F_q si et seulement si G peut être défini dans $\mathrm{GL}_n(\overline{\mathbf{F}}_p)$ par des équations polynomiales (en les coefficients et en $\det^{-1}$) à coefficients dans $\mathbf{F}_q$. Donc $B_n(\overline{\mathbf{F}}_p)$, $N_n(\overline{\mathbf{F}}_p)$, $H_n(\overline{\mathbf{F}}_p)$, $U_n(\overline{\mathbf{F}}_p)$ ainsi que $\mathrm{SL}_n(\overline{\mathbf{F}}_p)$ et $\mathrm{Sp}_{2m}(\overline{\mathbf{F}}_p)$ sont définis sur $\mathbf{F}_q$ et les sous-groupes des points fixes associés sont les groupes correspondants à coefficients dans $\mathbf{F}_q$.

5. Pour les définitions, on pourra se reporter à l'annexe A.1.

On dispose d'un analogue pour les groupes du théorème 3.1.7.

Théorème 3.2.3 : *Soit G un groupe algébrique défini sur $\mathbf{F}_q$, de morphisme de* Frobenius *F. Alors il existe $n \in \mathbf{N}^*$ et une immersion fermée $\iota : G \hookrightarrow \mathrm{GL}_n(\overline{\mathbf{F}}_p)$ qui est un morphisme de groupes et telle que $F_q \circ \iota = \iota \circ F$.*

Démonstration :

• On note $\mu : G \times G \longrightarrow G$ la multiplication et A l'algèbre des fonctions régulières sur G. F est un morphisme de groupes donc, pour $f \in A_0$, on a $(F \times F)^*(\mu^*(f)) = \mu^*(F^*(f)) = \mu^*(f^q) = \mu^*(f)^q$. Donc on a $\mu^*(A_0) \subseteq (A \otimes_{\overline{\mathbf{F}}_p} A)_0 = A_0 \otimes_{\mathbf{F}_q} A_0$ d'après la proposition 3.1.10.

• D'après le lemme 3.1.5, il existe des éléments $f_1, \dots, f_m$ de A_0 tels que l'on ait $A = \overline{\mathbf{F}}_p[f_1, \dots, f_m]$. Soit $i \in \{1, \dots, m\}$. Soit $r \geq 1$ minimal tel qu'il existe des éléments $g_{i1}, \dots, g_{ir}, h_{i1}, \dots, h_{ir}$ dans A_0 tels que l'on ait $\mu^*(f_i) = \sum_{j=1}^{r} g_{ij} \otimes h_{ij}$. Si les h_{ij} n'étaient pas $\overline{\mathbf{F}}_p$-linéairement indépendants alors, d'après la remarque 3.1.6, ils ne seraient pas $\mathbf{F}_q$-linéairement indépendants donc on obtiendrait une expression de $\mu^*(f_i)$ comme somme d'au plus $r-1$ tenseurs élémentaires de $A_0 \otimes_{\mathbf{F}_q} A_0$, ce qui contredirait la minimalité de r. Par conséquent, il existe des éléments $y_{i1}, \dots, y_{ir}$ dans G tels que la matrice $(h_{ij}(y_{il}))_{1 \leq j,l \leq r}$ soit inversible.

• Pour $y \in G$ et $f \in A$, on pose $\delta(y)(f) : \left| \begin{array}{ccc} G & \longrightarrow & \overline{\mathbf{F}}_p \\ x & \longmapsto & f(xy) \end{array} \right.$. Alors on a $\forall y \in G, \delta(y)(f_i) = \sum_{j=1}^{r} h_{ij}(y) g_{ij}$ et, par le même calcul et en inversant le système obtenu, les g_{ij} sont combinaisons $\overline{\mathbf{F}}_p$-linéaires des élémets de la forme $\delta(y_l)(f_i)$. Donc, des g_{ij}, on peut extraire une $\overline{\mathbf{F}}_p$-base $(e_1, \dots, e_s)$ de $\{\delta(y)(f_i) | 1 \leq i \leq m, y \in G\}$.

• Alors, pour $x \in G$ et $z \in G$, on a $\mu^*(\delta(y_l)(f_i))(x,z) = f_i(xzy_l) = \mu^*(f_i)(x, zy_l)$. Donc $\mu^*(\delta(y_l)(f_i)) = \sum_{j=1}^{r} g_{ij} \otimes \delta(y_l)(h_{ij})$. Comme μ^* est $\overline{\mathbf{F}}_p$-linéaire, on peut écrire, pour $1 \leq j \leq m$, $\mu^*(e_j) = \sum_{i=1}^{s} e_i \otimes a_{ij}$ avec $a_{ij} \in A$. De plus, les e_i sont $\overline{\mathbf{F}}_p$-linéairement indépendants donc les e_i^q aussi, or on a $\sum_{i=1}^{s} e_i^q \otimes F^*(a_{ij}) = (F^* \otimes F^*)\left(\sum_{i=1}^{s} e_i \otimes a_{ij}\right) = (F^* \otimes F^*)(\mu^*(e_j)) = \mu^*(F^*(e_j)) = \mu^*(e_j^q) = \mu^*(e_j)^q = \sum_{i=1}^{s} e_i^q \otimes a_{ij}^q$, donc $\mathbf{F}^*(a_{ij}) = a_{ij}^q$ donc $a_{ij} \in A_0$.

• On pose $\iota : \left| \begin{array}{ccc} G & \longrightarrow & M_s(\overline{\mathbf{F}}_p) \\ x & \longmapsto & (a_{ij}(x))_{1 \leq i,j \leq s} \end{array} \right.$. On a $e_j = \delta(1)(e_j) = \sum_{i=1}^{s} a_{ij}(1) e_i$ donc $a_{ij}(1) = \delta_{ij}$, c'est-à-dire $\iota(1) = I_s$. De plus, pour $x \in G$ et $y \in G$, on a $\sum_{i=1}^{s} a_{ij}(xy) e_i = \delta(xy)(e_j) = \delta(x)(\delta(y)(e_j)) = \delta(x)\left(\sum_{l=1}^{s} a_{lj}(y) e_l\right) = \sum_{l=1}^{s} a_{lj}(y) \delta(x)(e_l) = \sum_{1 \leq i,l \leq s} a_{lj}(y) a_{il}(x) e_i$ donc $a_{ij}(xy) = \sum_{l=1}^{s} a_{il}(x) a_{lj}(y)$, c'est-à-dire $\iota(xy) = \iota(x)\iota(y)$. Donc ι est à valeurs dans $\mathrm{GL}_n(\overline{\mathbf{F}}_p)$ et $\iota : G \longrightarrow \mathrm{GL}_n(\overline{\mathbf{F}}_p)$ est un morphisme de groupes abstraits. Comme on a $a_{ij} \in A_0$, c'est même un morphisme de groupes algébriques, qui commute avec les morphismes de Frobenius.

• Les f_i sont combinaisons $\overline{\mathbf{F}}_p$-linéaires des e_j donc on a $A = \overline{\mathbf{F}}_p[e_1, \dots, e_s]$. Comme on a $e_j = \sum_{i=1}^{s} e_i(1) a_{ij} = \iota^*\left(\sum_{i=1}^{s} e_i(1) X_{ij}\right)$, on en déduit que ι^* est surjectif donc que ι est une immersion fermée. □

On énonce enfin un théorème qui sera utile dans la suite.

Théorème 3.2.4 (Théorème de Lang-Steinberg) : *Soit G un groupe algébrique affine connexe défini sur $\mathbf{F}_q$, $F : G \longrightarrow G$ un morphisme de* Frobenius *généralisé et $L : \left| \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & g^{-1}F(g) \end{array} \right.$, appelée* **application de Lang**. *Alors L est un morphisme de variétés surjectif.*

Démonstration :

• L est clairement un morphisme. Montrons que L est dominant. Pour $x \in G$ et $y \in G$, si $L(x) = L(y)$ alors $xy^{-1} = F(x)F(y)^{-1} = F(xy^{-1})$ donc $xy^{-1} \in G^F$. Donc les fibres de L sont des translatés de G^F donc sont finies (car, d'après la remarque 3.1.8, G^F est fini). Donc, d'après la proposition A.1.6 en annexe, on a $\dim \overline{L(G)} = \dim G$. Or G est un groupe algébrique connexe donc irréductible. Donc, par contraposée du résultat

de la proposition A.1.3 en annexe, $\overline{L(G)} = G$.

• Montrons que L est fini, ce qui suffit, d'après la proposition A.1.7 en annexe. Soit $d \in \mathbf{N}^*$ tel que F^d soit un morphisme de Frobenius. Pour $g \in G$, on pose $\psi(g) := gF(g)\cdots F^{d-1}(g)$ et $L_d(g) := g^{-1}F^d(g)$. On a $\psi \circ L(g) = (g^{-1}F(g))F(g^{-1}F(g))\cdots F^{d-1}(g^{-1}F(g)) = g^{-1}F^d(g) = L_d(g)$ donc $\psi \circ L = L_d$ donc $L_d^*(A) \subseteq L^*(A)$ donc il suffit de montrer que L_d est fini, donc il suffit de traiter le cas $d = 1$. Soit $(e_1, \ldots, e_s)$ construite dans la démonstration du théorème 3.2.3. Alors, pour $g \in G$, on a $e_j^q(g) = F^*(e_j)(g) = e_j(F(g)) = e_j(gg^{-1}F(g)) = \mu^*(e_j)(g, L(g)) = \sum_{i=1}^{s} e_i(g)a_{ij}(L(g))$, donc $e_j^q = \sum_{i=1}^{s} e_i L^*(a_{ij})$. Comme on a déjà $A = \overline{\mathbf{F}}_p[e_1, \ldots, e_s]$, on en déduit par division euclidienne des puissances des e_j que A peut être engendrée comme $L^*(A)$-module par l'ensemble fini $\{e_1^{r_1}\cdots e_s^{r_s} | r_i < q\}$, donc L est fini. □

Remarques 3.2.5 :

• Serge Lang a démontré ce théorème en 1956 (voir [6]). En 1968, Robert Steinberg a montré que le résultat reste vrai si on suppose seulement que G est un groupe algébrique affine connexe et que F est un morphisme de groupes surjectif tel que G^F soit fini (voir [8]).

• Ce théorème a de nombreuses conséquences. Par exemple, il implique que si de plus G est réductif alors il existe une (B,N)-paire réductive stable par F et les (B,N)-paires réductives stables par F sont conjuguées par G^F (voir par exemple [3, pp. 245-247]).

3.3 Cardinal des groupes finis de type Lie

Définition 3.3.1 : *On appelle* **groupe fini de type Lie** *tout groupe de la forme G^F où G est un groupe algébrique affine défini sur $\mathbf{F}_q$ muni d'une (B,N)-paire réductive et F est un morphisme de* Frobenius *généralisé laissant stable la (B,N)-paire.*

L'objectif de cette sous-section est d'expliquer comment on peut calculer le cardinal des groupes finis de type Lie. On a d'abord besoin du résultat général suivant, dû à Maxwell Rosenlicht, que l'on admet car la démonstration est un peu longue et technique (voir par exemple [3, pp. 237-241], où l'on raisonne par récurrence sur $\dim U$ en utilisant notamment le théorème de Lang-Steinberg 3.2.4).

Théorème 3.3.2 : *Soit U un groupe algébrique affine unipotent défini sur $\mathbf{F}_q$, de morphisme de* Frobenius *F. Alors on a $|U^F| = q^{\dim U}$.*

Remarque 3.3.3 : Ce résultat est quand même évident pour le groupe U_n de la section 2 (et même pour $U_{2m} \cap \mathrm{Sp}_{2m}$, puisqu'un calcul élémentaire permet de décrire ce groupe explicitement).

Les résultats présentés précédemment permettent alors d'établir le théorème suivant.

Théorème 3.3.4 : *Soit G un groupe algébrique affine défini sur $\mathbf{F}_q$ muni d'une (B,N)-paire réductive et F un morphisme de* Frobenius *généralisé. Si F laisse stables B et N alors F est un automorphisme de groupe qui induit un automorphisme $\overline{F} : W \longrightarrow W$ et on a $G^F = \bigsqcup_{w \in W^{\overline{F}}} U^F H^F n_w U_w^F$ avec unicité de l'écriture. Si de plus F est un morphisme de* Frobenius *alors B^F et N^F constituent une (B,N)-paire scindée par U^F pour G^F, de groupe de* Weyl *$W^{\overline{F}}$, et on a $|G^F| = q^{l(w_0)}|H^F| \sum_{w \in W^{\overline{F}}} q^{l(w)}$ (avec l la longueur dans W).*

Démonstration :

• B et N sont stables par F donc $H = B \cap N$ et $U = [B, B]$ aussi, donc F vérifie (BN$^\varphi$1).

• Montrons que F vérifie (BN$^\varphi$2). Soit $n \in N$ tel que l'on ait $F(nH) = nH = Hn$. Alors $F(n) \in Hn$ donc il existe $t \in H$ tel que $F(n) = t^{-1}n$ or H est connexe, d'après le corollaire 3.1.9, $F : H \longrightarrow H$ est un morphisme de Frobenius généralisé donc, d'après le théorème de Lang-Steinberg 3.2.4, il existe $h \in H$ tel que $t = h^{-1}F(h)$ et alors $F(hn) = F(h)F(n) = htt^{-1}n = hn$ donc $nH = Hn$ contient un point fixe par F.

• Les U_w sont connexes, unipotents et stables par F donc, d'après le théorème de Rosenlicht 3.3.2, si F est un morphisme de Frobenius alors $|U_w^F| = q^{l(w)} > 1$ donc, a fortiori, les $U_{w_J}^F$ ne sont pas triviaux. Il suffit donc d'appliquer le théorème 1.3.4, le théorème de Rosenlicht 3.3.2 et d'utiliser $U = U_{w_0}$. □

Exemple 3.3.5 : Utilisons ce résultat pour calculer le cardinal de $\mathrm{GL}_n(\mathbf{F}_q)$. D'après la proposition 2.1.3, on a $l(w_0) = \dfrac{n(n-1)}{2}$, H^F est l'ensemble des matrices diagonales inversibles à coefficients dans $\mathbf{F}_q$ donc $|H^F| = (q-1)^n$, on a $W \simeq \mathfrak{S}_n$, $\overline{F} = \mathrm{id}_{\mathfrak{S}_n}$ et, pour $w \in W$, $l(w)$ est le nombre d'inversions de w. Il reste donc à calculer $\displaystyle\sum_{w\in\mathfrak{S}_n} q^{l(w)}$. On peut procéder de façon purement combinatoire et par récurrence sur n (voir par exemple [7, pp. 441-477]). On peut également utiliser le théorème 1.4.8. Pour cela, on munit $\mathbf{R}^n$ de sa base canonique $(e_1,\dots,e_n)$ et de son produit scalaire canonique, et on pose $\Phi^+ := \{e_i - e_j | 1 \leq i < j \leq n\}$, $\Phi^- := -\Phi^+$ et $\Phi := \Phi^+ \cup \Phi^-$. On vérifie facilement que Φ est un système de racines et que Φ^+ est un ensemble de racines positives dont l'ensemble des racines simples est $\Delta := \{e_i - e_{i+1} | 1 \leq i \leq n-1\}$. Le groupe de réflexion associé est donc engendré par les $s_{e_i - e_{i+1}}$. La symétrie $s_{e_i-e_{i+1}}$ échange e_i et e_{i+1} donc, comme l'action est linéaire, le groupe de réflexion agit fidèlement et transitivement sur $\{e_1,\dots,e_n\}$. Par conséquent, en tant que groupe de Coxeter, il est isomorphe au groupe $\mathfrak{S}_n$ engendré par les transpositions élémentaires, c'est-à-dire à W. $e_i - e_j$ étant de hauteur $j-i$, on a donc, avec les notations de la remarque 1.4.9, $(k_1,\dots,k_{n-1}) = (n-1,\dots,1)$ donc $(m_1,\dots,m_{n-1}) = (n-1,\dots,1)$, donc $W(q) = \displaystyle\prod_{i=1}^{n-1} \frac{q^{m_i+1}-1}{q-1} = \frac{1}{(q-1)^{n-1}} \prod_{i=2}^{n} (q^i - 1)$. On en déduit $|\mathrm{GL}_n(\mathbf{F}_q)| = q^{\frac{n(n-1)}{2}} \displaystyle\prod_{i=1}^{n} (q^i - 1)$.

Exemple 3.3.6 : On peut également calculer le cardinal de $\mathrm{Sp}_{2m}(\mathbf{F}_q)$. D'après la proposition 2.2.1, la remarque 2.2.2 et la proposition 2.2.3, on a $l(w_0) = m^2$, $|H^F| = (q-1)^m$, $W \simeq W'_{2m}$ et $F = \mathrm{id}_{W'_{2m}}$. On pose $\Phi^+ := \{e_i - e_j | 1 \leq i < j \leq m\} \cup \{e_i + e_j | 1 \leq i < j \leq m\} \cup \{2e_i | 1 \leq i \leq m\}$, $\Phi^- := -\Phi^+$ et $\Phi := \Phi^+ \cup \Phi^-$. On vérifie facilement que Φ est un système de racines et que Φ^+ est un ensemble de racines positives dont l'ensemble des racines simples est $\Delta := \{e_i - e_{i+1} | 1 \leq i \leq m-1\} \cup \{2e_m\}$. Comme précédemment, en notant $e_{m+i} := -e_{m+1-i}$ pour $1 \leq i \leq m$, le groupe de réflexion associé agit fidèlement sur $\{e_1,\dots,e_{2m}\}$ et, en tant que groupe de Coxeter, il est isomorphe au groupe W'_{2m} engendré par les $s_i := (m-i, m-i+1)(m+i, m+i+1)$ et $t := (m, m+1)$, c'est-à-dire à W. La racine $e_i - e_j$ est de hauteur $j-i$; $2e_i = 2(e_i - e_{i+1}) + \cdots + 2(e_{m-1} - e_m) + 2e_m$ donc $2e_i$ est de hauteur $2m - 2i + 1$; $e_i + e_j = (e_i - e_{i+1}) + \cdots + (e_{j-1} - e_j) + 2e_j$ donc $e_i + e_j$ est de hauteur $2m - j - i + 1$. Donc $(k_1,k_2,k_3,k_4,k_5,\dots,k_{2m-2},k_{2m-1}) = (m, m-1, m-1, m-2, m-2, \dots, 1, 1)$ donc $(m_1, m_2, \dots, m_m) = (2m-1, 2m-3, \dots, 1)$, donc $W(q) = \dfrac{1}{(q-1)^m} \displaystyle\prod_{i=1}^{m} (q^{2i} - 1)$. On en déduit $|\mathrm{Sp}_{2m}(\mathbf{F}_q)| = q^{m^2} \displaystyle\prod_{i=1}^{m} (q^{2i} - 1)$.

Annexes

A.1 Rudiments sur les groupes algébriques

On rappelle sans démonstration quelques définitions et résultats de géométrie algébrique et de théorie des groupes algébriques (voir [5]). Dans la suite, $\mathbf{K}$ est un corps algébriquement clos.

Définition A.1.1 : *On appelle* **variété algébrique affine sur $\mathbf{K}$** *tout couple (X, A) où X est un ensemble et A est une sous-$\mathbf{K}$-algèbre de type fini de* $\mathrm{Appl}(X, \mathbf{K})$*, appelée* **algèbre des fonctions régulières sur X**, *telle que l'application* $\left|\begin{array}{ccc} X & \longrightarrow & \mathrm{Hom}_{\mathbf{K}-alg}(A, \mathbf{K}) \\ x & \longmapsto & \mathrm{ev}_x \end{array}\right.$ *soit bijective. Dans ce cas, on appelle* **dimension** *de X l'entier* $\dim X := \max\{m \in \mathbf{N} |$ *il existe m éléments de A algébriquement indépendants*$\}$.

Remarques A.1.2 :

- A est une $\mathbf{K}$-algèbre de type fini donc est isomorphe à un quotient $\mathbf{K}[X_1,\dots,X_n]/I$.
- Les fermés algébriques de $\mathbf{K}^n$ sont bien des variétés algébriques affines sur $\mathbf{K}$. De plus, toute variété algébrique affine sur $\mathbf{K}$ est isomorphe à un fermé algébrique d'un $\mathbf{K}^n$.
- Toute variété algébrique affine (X, A) est naturellement munie de la **topologie de Zariski**, dont les fermés sont les $\mathcal{Z}(I) := \{x \in X | \forall f \in I, f(x) = 0\}$ pour I idéal de A.
- Si (X, A) et (Y, B) sont deux variétés algébriques affines sur $\mathbf{K}$ alors $(X \times Y, A \otimes_{\mathbf{K}} B)$ aussi et on a $\dim X \times Y = \dim X + \dim Y$.

Proposition A.1.3 : *Soit (X, A) une variété algébrique affine irréductible et Y un fermé de X. Si Y est un fermé strict alors* $\dim Y < \dim X$.

Définition A.1.4 : *Soit (X, A) et (Y, B) deux variétés algébriques affines sur $\mathbf{K}$ et $f : X \longrightarrow Y$. On dit que f est un* **morphisme** *(de variétés algébriques affines) si $f^* : \left| \begin{array}{ccc} B & \longrightarrow & \mathrm{Appl}(X, \mathbf{K}) \\ h & \longmapsto & h \circ f \end{array} \right.$ est à valeurs dans A. Dans ce cas, $f^* : B \longrightarrow A$ est un morphisme de $\mathbf{K}$-algèbres appelé le* **comorphisme**. *On dit que f est* **dominant** *si de plus $f(X)$ est dense dans Y. On dit que f est une* **immersion fermée** *si f est une application fermée et $f : X \longrightarrow f(X)$ est un isomorphisme. On dit que f est* **fini** *si A est un $f^*(B)$-module de type fini.*

Proposition A.1.5 : *f est dominant si et seulement si f^* est injectif. f est une immersion fermée si et seulement si f^* est surjectif. f est un isomorphisme si et seulement si f^* est un isomorphisme.*

Proposition A.1.6 : *Soit $f : X \longrightarrow Y$ un morphisme dominant avec X et Y irréductibles. Si les fibres de f (c'est-à-dire les $f^{-1}(\{f(x)\})$ pour $x \in X$) sont finies alors on a $\dim X = \dim Y$.*

Proposition A.1.7 : *Soit $f : X \longrightarrow Y$ un morphisme fini. Alors les fibres de f sont finies et f est fermé. En particulier, si de plus X et Y sont irréductibles et f est dominant alors f est surjectif.*

Définition A.1.8 : *Soit (X, A) une variété algébrique affine. On dit que X est un* **groupe algébrique affine** *si X est munie d'une structure de groupe telle que la multiplication et l'inversion soient des morphismes. Pour (X, A) et (Y, B) des groupes algébriques affines et $f : X \longrightarrow Y$, on dit que f est un* **morphisme de groupes algébriques affines** *si f est un morphisme de variétés algébriques affines et un morphisme de groupes.*

Proposition A.1.9 : *Un groupe algébrique affine est irréductible si et seulement s'il est connexe.*

Proposition A.1.10 : *Tout morphisme de groupes algébriques affines est fermé.*

On reprend les notations de la section 2.

Définition A.1.11 : *Soit G un groupe algébrique affine. On appelle* **tore** *de G tout sous-groupe T fermé, diagonalisable connexe, c'est-à-dire isomorphe à un D_n ; on dit que T est un* **tore maximal** *si de plus T est maximal pour l'inclusion parmi les tores. On appelle* **sous-groupe de Borel** *tout sous-groupe B fermé, connexe, résoluble*[6] *et maximal.*

Proposition A.1.12 : *Soit G un groupe algébrique affine. Alors tout tore maximal de G est contenu dans un sous-groupe de* Borel. *De plus, si T_1 et T_2 sont des tores maximaux et si B_1 et B_2 sont des sous-groupes de* Borel *contenant respectivement T_1 et T_2 alors il existe un élément $g \in G$ tel que l'on ait $T_2 = gT_1g^{-1}$ et $B_2 = gB_1g^{-1}$.*

Définition A.1.13 : *Soit G un groupe algébrique affine et U un sous-groupe fermé de G. On dit que U est* **unipotent** *s'il est isomorphe à un certain sous-groupe fermé d'un U_n.*

Remarque A.1.14 : La « vraie » définition est nettement plus compliquée, mais un théorème de Lie assure que U est unipotent si et seulement s'il est isomorphe à un certain sous-groupe fermé d'un U_n.

Proposition et définition A.1.15 : *Soit G un groupe algébrique affine. Alors G possède un unique sous-groupe fermé, connexe, résoluble, distingué et maximal, appelé le* **radical** *de G, et G possède un unique sous-groupe fermé, connexe, unipotent et maximal, appelé le* **radical unipotent** *de G. On dit que G est* **réductif** *si son radical unipotent est trivial. On dit que G est* **semi-simple** *si son radical est trivial.*

A.2 Calculs de l'exemple 1.1.4

Déterminons W et vérifions (BN2). Soit $x \in \mathbf{K}^\times$; soit $p \in A \setminus \{0\}$ et $q \in A \setminus \{0\}$ tels que $x = \frac{p}{q}$. Alors $\begin{pmatrix} x & 0 \\ 0 & \frac{1}{x} \end{pmatrix} H = \begin{pmatrix} t^{v(x)} & 0 \\ 0 & \frac{1}{t^{v(x)}} \end{pmatrix} \begin{pmatrix} \frac{p}{t^{v(p)}} & 0 \\ 0 & \frac{t^{v(p)}}{p} \end{pmatrix} \begin{pmatrix} \frac{t^{v(q)}}{q} & 0 \\ 0 & \frac{q}{t^{v(q)}} \end{pmatrix} H = \begin{pmatrix} t^{v(x)} & 0 \\ 0 & \frac{1}{t^{v(x)}} \end{pmatrix} H$ et $\begin{pmatrix} 0 & x \\ -\frac{1}{x} & 0 \end{pmatrix} H = \begin{pmatrix} 0 & t^{v(x)} \\ -\frac{1}{t^{v(x)}} & 0 \end{pmatrix} H$. Or on a $n_1^2 = n_2^2 = -I_2$ et $\forall n \in \mathbf{Z}, (n_1n_2)^n = \begin{pmatrix} t^n & 0 \\ 0 & \frac{1}{t^n} \end{pmatrix}$, $n_1(n_1n_2)^n = \begin{pmatrix} 0 & -\frac{1}{t^n} \\ t^n & 0 \end{pmatrix}$, $n_2(n_1n_2)^n = \begin{pmatrix} 0 & -\frac{1}{t^{n+1}} \\ t^{n+1} & 0 \end{pmatrix}$, $(n_1n_2)^n n_1 = \begin{pmatrix} 0 & -t^n \\ \frac{1}{t^n} & 0 \end{pmatrix}$ et $(n_1n_2)^n n_2 = \begin{pmatrix} 0 & -t^{n-1} \\ \frac{1}{t^{n-1}} & 0 \end{pmatrix}$. Par conséquent, on a $W = \langle n_1H, n_2H \rangle$, n_1H et n_2H sont d'ordre 2 et $W \simeq \langle n_1H \rangle * \langle n_2H \rangle$.

6. C'est-à-dire que la suite dérivée, définie par récurrence par $D^0(B) := B$ et $D^{i+1}(B) := [D^i(B), D^i(B)]$, stationne à $\{1\}$.

D'après le premier point de la remarque 1.1.2, pour vérifier (BN4), il suffit de considérer les quatre produits $M_1 := n_1 \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} t^n & 0 \\ 0 & \frac{1}{t^n} \end{pmatrix}$, $M_2 := n_1 \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{t^n} \\ -t^n & 0 \end{pmatrix}$, $M_3 := n_2 \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} t^n & 0 \\ 0 & \frac{1}{t^n} \end{pmatrix}$ et $M_4 := n_2 \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{t^n} \\ -t^n & 0 \end{pmatrix}$ pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in B$ et $n \in \mathbf{Z}$. Notons que, comme $ad - bc = 1$ et $v(c) \geq 1$, on a nécessairement $v(a) = v(d) = 0$ donc $a \in A^\times$ et $d \in A^\times$.

On a $M_1 = \begin{pmatrix} \frac{1}{b} & -\frac{bc}{a} \\ 0 & b \end{pmatrix} n_1 \begin{pmatrix} t^n & 0 \\ 0 & \frac{1}{t^n} \end{pmatrix} \begin{pmatrix} \frac{a}{b} & \frac{1}{t^{2n}} \\ 0 & \frac{b}{a} \end{pmatrix}$ si $n \leq 0$ et $v(b) = 0$, $M_1 = \begin{pmatrix} d & -c \\ -b & b \end{pmatrix} n_1 \begin{pmatrix} t^n & 0 \\ 0 & \frac{1}{t^n} \end{pmatrix}$ si $v(b) \geq 1$ et $M_1 = \begin{pmatrix} 1 & -\frac{d}{b} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t^n & 0 \\ 0 & \frac{1}{t^n} \end{pmatrix} \begin{pmatrix} \frac{1}{b} & 0 \\ at^{2n} & b \end{pmatrix}$ si $n \geq 1$ et $v(b) = 0$, donc $M_1 \in Bn_1 \begin{pmatrix} t^n & 0 \\ 0 & \frac{1}{t^n} \end{pmatrix} B \cup B \begin{pmatrix} t^n & 0 \\ 0 & \frac{1}{t^n} \end{pmatrix} B$.

On a $M_2 = \begin{pmatrix} \frac{1}{b} & -\frac{bc}{a} \\ 0 & b \end{pmatrix} n_1 \begin{pmatrix} 0 & \frac{1}{t^n} \\ -t^n & 0 \end{pmatrix} \begin{pmatrix} \frac{b}{a} & 0 \\ -t^{2n} & \frac{a}{b} \end{pmatrix}$ si $n \geq 1$ et $v(b) = 0$, $M_2 = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} n_1 \begin{pmatrix} 0 & \frac{1}{t^n} \\ -t^n & 0 \end{pmatrix}$ si $v(b) \geq 1$ et $M_2 = \begin{pmatrix} 1 & -\frac{d}{b} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{t^n} \\ -t^n & 0 \end{pmatrix} \begin{pmatrix} b & -\frac{a}{t^{2n}} \\ 0 & \frac{1}{b} \end{pmatrix}$ si $n \leq 0$ et $v(b) = 0$, donc $M_2 \in Bn_1 \begin{pmatrix} 0 & \frac{1}{t^n} \\ -t^n & 0 \end{pmatrix} B \cup B \begin{pmatrix} 0 & \frac{1}{t^n} \\ -t^n & 0 \end{pmatrix} B$.

On a $M_3 = \begin{pmatrix} ad & 0 \\ -abt^2 & \frac{1}{ad} \end{pmatrix} n_2 \begin{pmatrix} t^n & 0 \\ 0 & \frac{1}{t^n} \end{pmatrix} \begin{pmatrix} a & 0 \\ \frac{ct^{2n}}{ad} & \frac{1}{a} \end{pmatrix}$ si $n \geq 0$, $M_3 = \begin{pmatrix} d & -\frac{c}{t^2} \\ -bt^2 & a \end{pmatrix} n_2 \begin{pmatrix} t^n & 0 \\ 0 & \frac{1}{t^n} \end{pmatrix}$ si $v(c) \geq 2$ et $M_3 = \begin{pmatrix} 1 & 0 \\ -\frac{at^2}{c} & 1 \end{pmatrix} \begin{pmatrix} t^n & 0 \\ 0 & \frac{1}{t^n} \end{pmatrix} \begin{pmatrix} \frac{c}{t} & \frac{d}{t^{2n+1}} \\ 0 & \frac{t}{c} \end{pmatrix}$ si $n \leq -1$ et $v(c) = 1$ (donc $\frac{c}{t} \in A^\times$), donc $M_3 \in Bn_2 \begin{pmatrix} t^n & 0 \\ 0 & \frac{1}{t^n} \end{pmatrix} B \cup B \begin{pmatrix} t^n & 0 \\ 0 & \frac{1}{t^n} \end{pmatrix} B$.

On a $M_4 = \begin{pmatrix} ad & 0 \\ -abt^2 & \frac{1}{ad} \end{pmatrix} n_2 \begin{pmatrix} 0 & \frac{1}{t^n} \\ -t^n & 0 \end{pmatrix} \begin{pmatrix} -\frac{c}{adt^{2n}} & -\frac{1}{a} \\ a & 0 \end{pmatrix}$ si $n \leq 0$, $M_4 = \begin{pmatrix} d & -\frac{c}{t^2} \\ -bt^2 & a \end{pmatrix} n_2 \begin{pmatrix} 0 & \frac{1}{t^n} \\ -t^n & 0 \end{pmatrix}$ si $v(c) \geq 2$ et $M_4 = \begin{pmatrix} 1 & 0 \\ -\frac{at^2}{c} & 1 \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{t^n} \\ -t^n & 0 \end{pmatrix} \begin{pmatrix} 0 & -\frac{t}{c} \\ \frac{c}{t} & dt^{2n-1} \end{pmatrix}$ si $n \geq 1$ et $v(c) = 1$, donc $M_4 \in Bn_2 \begin{pmatrix} 0 & \frac{1}{t^n} \\ -t^n & 0 \end{pmatrix} B \cup B \begin{pmatrix} 0 & \frac{1}{t^n} \\ -t^n & 0 \end{pmatrix} B$.

Références

[1] Nicolas Bourbaki : *Groupes et algèbres de Lie*, Chapitres 4, 5 et 6. Masson, Paris, 1981.

[2] Roger Carter : *Simple groups of Lie type*. Wiley Classics Library. John Wiley and Sons, New York, 1989.

[3] Meinolf Geck : *An Introduction to Algebraic Geometry and Algebraic Groups*, volume 10 de *Oxford Graduate Texts in Mathematics*. Oxford Science Publications, New York, 2003.

[4] James Humphreys : *Reflexion groups and Coxeter groups*, volume 29 de *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1990.

[5] James Humphreys : *Linear Algebraic Groups*, volume 21 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[6] Serge Lang : Algebraic groups over finite fields. *American Journal of Mathematics*, 78(3): pp. 555–563, 1956.

[7] Thomas Muir : On a simple term of a determinant. *Proceedings of the Royal Society of Edinburgh*, 21: pp. 441–477, 1898–1899.

[8] Robert Steinberg : Endomorphisms of linear algebraic groups. *Memoirs of the American Mathematical Society*, 80, 1968.

[9] Jacques Tits : Théorème de Bruhat et sous-groupes paraboliques. *Comptes Rendus des Séances de l'Académie des Sciences*, 254(2): pp. 2910–2912, 1962.