Groupes classiques finis et simples

Mémoire

Bastien Desrochers

Sous la direction de:

Hugo Chapdelaine

Résumé

Les groupes finis simples sont les blocs qui permettent de construire tous les autres groupes finis. Il est donc fondamental de les comprendre et de les étudier. Ce mémoire se concentre sur les groupes finis simples de type Lie, en particulier les groupes classiques. On y retrouve des outils mathématiques qui ont été utiles à la classification, ainsi que différents théorèmes de simplicité. De plus, on y présente quelques résultats supplémentaires intéressants, comme certains isomorphismes dans les différentes familles de groupes finis simples, ainsi que des calculs de cardinalité.

Abstract

The finite simple groups are the building blocks of all other finite groups. As such, their study and comprehension is essential. This thesis focuses on the finite groups of Lie type, specifically the classical groups. It contains simplicity theorems and other mathematical tools that were utilized in the classification. Moreover, it presents some more interesting results, such as some isomorphisms in different families of finite simple groups and some order calculations.

Table des matières

Résumé ii

Abstract iii

Table des matières iv

Liste des tableaux v

Remerciements vii

Avant-propos viii

Introduction 1

1 Groupes classiques et autres définitions pertinentes 2
- 1.1 Groupes cycliques et groupes alternés . . . 2
- 1.2 Familles de groupes classiques . . . 5
- 1.3 Autres groupes finis simples . . . 18

2 BN-paires et Frobenius généralisés 20
- 2.1 BN-paires . . . 20
- 2.2 Automorphismes et application de Frobenius . . . 31

3 Théorèmes de simplicité 38
- 3.1 Lemme d'Iwasawa . . . 38
- 3.2 Théorème de simplicité de Tits . . . 49
- 3.3 Lien entre les théorèmes dans le contexte des groupes classiques . . . 52

Conclusion 53

A Énoncé du Théorème de Classification des groupes finis simples 54

B Définitions et résultats utiles sur la théorie des groupes 55

Bibliographie 57

Liste des tableaux

2.1 Liste des graphes de Coxeter associés aux groupes finis simples de type Lie . . . 32
2.2 Torsions possibles dans les graphes de la Table 2.1 35

3.1 Comparaison entre les deux théorèmes de simplicité énoncés 52

Are the finite simple groups, like
the prime numbers, jewels strung
on an as-yet invisible thread ?
And will this thread lead us out of
the current labyrinthine proof to a
radically new proof of the
Classification Theorem ?

Richard Solomon

Remerciements

Merci à Hugo Chapdelaine de m'avoir fait confiance dès le début.

Merci à Juliette et Peha qui m'ont aidé à garder le cap jusqu'à la fin.

Avant-propos

Dans le cadre de ce travail, l'intelligence artificielle (IA) générative a parfois été utilisée pour stimuler les discussions. En particulier, l'astuce de l'Exemple 5 est inspirée d'une telle discussion. L'IA générative n'a pas été utilisée pour rédiger ce document.

Introduction

Bien qu'appelés simples, les groupes finis simples ont été difficiles à classifier. En effet, c'est en 1950 que commencèrent des travaux visant à classifier les groupes finis simples et c'est seulement 55 ans plus tard que le théorème de Classification des groupes finis simples fut complété. Ce théorème fait entre 5000 et 10000 pages et plus de 100 mathématiciens et mathématiciennes ont participé à sa rédaction.

Une particularité du théorème de classification est qu'il permet de prouver certaines conjectures sur les groupes finis simples en procédant par cas. Par exemple, la conjecture de Ore, énoncée en 1951, hypothétise que tous les éléments d'un groupe fini simple non abélien sont des commutateurs. Cette conjecture a été prouvée vraie seulement en 2009, à l'aide du théorème de classification qui permet de séparer la preuve pour les différentes familles de groupes finis simples. Comme il n'y a pas de preuve générale, sans la classification, un groupe fini simple exotique aurait pu démentir la conjecture. De même, la conjecture de Schreier selon laquelle pour tout groupe fini simple non abélien, le groupe des automorphismes extérieurs est résoluble est considérée comme un corolaire du théorème de classification.

Dans ce travail, on s'intéresse à deux méthodes pour prouver la simplicité des familles de groupes classiques, une faisant appel au théorème d'Iwasawa et l'autre passant par l'étude des BN-paires introduites par Jacques Tits.

Chapitre 1

Groupes classiques et autres définitions pertinentes

Dans ce premier chapitre, on présente les groupes concernés et quelques résultats qui seront utiles pour le dernier chapitre. On discute également d'autres familles de groupes pertinentes dans le contexte des groupes finis simples, soit les groupes cycliques, les groupes alternés et les groupes exceptionnels de type Lie.

1.1 Groupes cycliques et groupes alternés

Avant de discuter des groupes classiques, on présente brièvement deux familles de groupes simples plus élémentaires afin de se familiariser avec les définitions. Les groupes cycliques servent souvent de premiers exemples de groupes finis.

Définition 1.1. *Un groupe G est dit* ***cyclique*** *s'il existe un $g \in G$ tel que $G = \langle g \rangle$. Un tel élément g est appelé un* ***générateur*** *de G. Si g est d'ordre n, alors $G \cong \mathbb{Z}/n\mathbb{Z}$.*

On utilise alors des résultats fondamentaux en théorie des groupes pour montrer un résultat sur la simplicité. Plusieurs résultats et définitions se trouvent dans l'Annexe B.

Théorème 1.1. *Un groupe est cyclique et simple si et seulement si son ordre est premier.*

Démonstration. Soit G un groupe cyclique simple d'ordre $n \geq 2$. Soit p un premier qui divise n. Par le théorème de Cauchy, G admet un élément a d'ordre p. Donc, $\langle a \rangle$ est un sous-groupe de G d'ordre p. Comme G est abélien, $\langle a \rangle$ est un sous-groupe normal. Or, comme G est simple, on a $\langle a \rangle = \{1\}$ ou $\langle a \rangle = G$. Le premier cas est impossible puisque $a \in \langle a \rangle$ et $a \neq 1$, donc $\langle a \rangle = G$ et G est d'ordre p. Soit maintenant G un groupe d'ordre premier p. Soit H un sous-groupe normal de G. Par le théorème de Lagrange, l'ordre de H divise l'ordre de G. Donc, $|H| = 1$ ou

$|H| = p$. Cela implique que $H = \{1\}$ ou $H = G$, donc G est simple. De plus, par le théorème de Cauchy, G admet un élément a d'ordre p de sorte que $G = \langle a \rangle$ soit cyclique. □

Remarque 1.1. *Ainsi, les groupes cycliques premiers composent la famille de groupes finis simples la plus élémentaire. Par le théorème fondamental des groupes finis abéliens, chaque groupe fini abélien G peut s'écrire comme la somme directe d'un nombre fini de groupes cycliques. Chacun de ces termes sont isomorphes à un sous-groupe normal de G. Donc, les groupes cycliques premiers sont les seuls groupes finis simples abéliens.*

Définition 1.2. *Soit $E_n = \{1, 2, \cdots, n\}$. Une application $\sigma : E_n \to E_n$ bijective est appelée une **permutation** de E_n. L'ensemble des permutations de E_n forme un groupe S_n appelé le **groupe des permutations**.*

Définition 1.3. *On utilise la notation $(a_1\ a_2\ a_3\ \cdots\ a_r)$ pour la permutation telle que $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, $\cdots$, $a_r \mapsto a_1$. On appelle une telle permutation un **cycle** de longueur r. Un cycle de longueur 2 s'appelle une **transposition**.*

Remarque 1.2. *On dénombre facilement que $|S_n| = n!$. De plus, on peut écrire chaque permutation comme un produit de transpositions. En particulier, il est possible d'utiliser seulement les transpositions de la forme $(i\ i+1)$ pour $i \in \{1, \cdots, n-1\}$.*

Définition 1.4. *Soit $\sigma \in S_n$. $\sigma = t_1 t_2 \cdots t_r$ où les t_i sont des transpositions. On définit le **signe** d'une permutation par* $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ *où r est le nombre de transpositions.*

$$\sigma \mapsto (-1)^r$$

Remarque 1.3. *Bien que r ne soit pas unique (par exemple, on peut multiplier par une transposition t deux fois sans changer la permutation, car $t^2 = 1$), sa parité est invariante, donc l'application* sgn *est bien définie. Ainsi, on dit que σ est une permutation paire si* $\operatorname{sgn}(\sigma) = 1$ *et impaire sinon. De plus,* sgn *est un homomorphisme.*

Définition 1.5. *Les permutations paires de S_n forment le groupe A_n appelé le **groupe alterné**.*

Proposition 1.1. *Le groupe alterné A_n est un sous-groupe normal de S_n.*

Démonstration. Soit $s \in S_n$. Alors, $s = t_1 \cdots t_r$ où les t_i sont des transpositions. On veut montrer que $sA_ns^{-1} \subseteq A_n$. Soit $sas^{-1} \in sA_ns^{-1}$. Alors, $\operatorname{sgn}\left(sas^{-1}\right) = (-1)^r \cdot 1 \cdot (-1)^r = (-1)^{2r} = 1$. Donc, $sas^{-1} \in A_n$. □

Remarque 1.4. *Pour $n \geq 2$, on a $|A_n| = n!/2$. Ainsi, $|A_3| = 3!/2 = 3$ un premier, donc par le Théorème 1.1, $A_3 \cong \mathbb{Z}_3$ est simple.*

Proposition 1.2. *Le groupe A_4 n'est pas simple.*

Démonstration. Soit $B := \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. On vérifie facilement que B est un sous-groupe normal non trivial de A_4. □

Une classe de conjugaison est un ensemble de la forme $\{ghg^{-1} : g \in G\}$ pour un certain $h \in G$. Les classes de conjugaison forment des classes d'équivalence pour l'ensemble G. En particulier, on a toujours que le singleton $\{e_G\}$ est une classe de conjugaison.

Lemme 1.2. *Soit H un sous-groupe normal d'un groupe G. Alors, H est l'union de classes de conjugaison de G.*

Démonstration. Comme H est normal, $H = gHg^{-1}$ pour tout $g \in G$. Donc,

$$H = \bigcup_{h \in H} \{ghg^{-1} : g \in G\} = \bigsqcup_{\overline{h}} \{g\overline{h}g^{-1} : g \in G\}$$

où les $\overline{h}$ sont des représentants de classes de conjugaison distinctes. □

Lemme 1.3. *A_5 est simple.*

Démonstration. Un calcul direct montre que A_5 possède cinq classes de conjugaison distinctes de taille 1, 15, 20, 12 et 12 respectivement. Par le théorème de Lagrange, l'ordre d'un sous-groupe doit diviser l'ordre du groupe. Or, les seules sommes de tailles de classes de conjugaison incluant 1 qui divise $60 = |A_5|$ sont 1 et 60, alors A_5 est simple par le Lemme 1.2. □

Théorème 1.4. *A_n est simple pour $n \geq 5$.*

Démonstration. On procède par induction sur n. Par le Lemme 1.3, le résultat est vérifié pour $n = 5$, on suppose alors que $n > 5$. Supposons qu'il existe un sous-groupe normal non trivial N de A_n. Considérons $N \cap A_{n-1}$ où A_{n-1} est identifié au stabilisateur de l'élément n. Alors, $N \cap A_{n-1}$ est normal dans A_{n-1}. Comme A_{n-1} est simple par hypothèse de récurrence, $N \cap A_{n-1} = 1$ ou A_{n-1}. Supposons que $N \cap A_{n-1} = A_{n-1}$. Alors, $A_{n-1} \leq N$ et N contient tous les cycles de longueur 3 qui fixent n. De plus, pour $a, b, c, d, e < n$, on a que $((a\ n)(d\ e))(a\ b\ c)((a\ n)(d\ e))^{-1} = (n\ b\ c) \in N$, donc N contient tous les cycles de longueur 3 et toutes les paires de transpositions disjointes. Comme ces produits de deux transpositions engendrent A_n, il suit que $N = A_n$. Supposons maintenant que $N \cap A_{n-1} = 1$. Alors, le seul élément de N qui fixe n est 1. Ainsi, si $x, y \in N$ envoient le point n sur le même point, alors $y^{-1}x$ fixe n, donc $x = y$. Alors, $|N| \leq n$. Or, pour $n \geq 6$, toutes les classes de conjugaison non triviales sont de tailles plus grande que n. On doit donc avoir $N = \{1\}$, ce qui montre que A_n est simple. □

1.2 Familles de groupes classiques

Les groupes classiques sont des groupes de matrices qui respectent certaines conditions.

Groupes linéaires

Définition 1.6. *Soit $n \in \mathbb{Z}_{\geq 1}$ et k un corps. Le groupe des matrices inversibles de taille $n \times n$ muni du produit matriciel s'appelle le* ***groupe général linéaire*** *et est noté* $\mathrm{GL}_n(k)$.

Les groupes classiques finis seront essentiellement des sous-groupes du groupe $\mathrm{GL}_n(q)$ où $q = p^a$ pour p un premier et $a \in \mathbb{Z}_{\geq 1}$ représente le corps fini à q éléments $\mathbb{F}_q$.

Définition 1.7. $\mathrm{SL}_n(q) := \{M \in M_n(\mathbb{F}_q) : \det(M) = 1\}$ *s'appelle le* ***groupe spécial linéaire****.*

Le centre $Z(\mathrm{SL}_n(q))$ de $\mathrm{SL}_n(q)$ est composé des matrices scalaires qui sont de la forme λI_n avec $\lambda \in \mathbb{F}_q$ et où $\lambda^n = 1$ pour respecter la condition du déterminant sur $\mathrm{SL}_n(q)$. Dans $\mathbb{F}_q$, le nombre de solutions à $\lambda^n = 1$ est le plus grand commun diviseur $(n, q-1)$.

Définition 1.8. $\mathrm{PSL}_n(q) := \mathrm{SL}_n(q)/Z(\mathrm{SL}_n(q))$ *s'appelle le* ***groupe spécial linéaire projectif****.*

Remarque 1.5. *Sauf pour des petites valeurs de n et q, $\mathrm{PSL}_n(q)$ sera simple. On montre la simplicité au chapitre 3.*

Proposition 1.3.

$$|\mathrm{SL}_n(q)| = q^{n(n-1)/2} \prod_{i=2}^{n} \left(q^i - 1\right).$$

Démonstration. Pour la suite, on identifie les colonnes d'une matrices $\gamma \in \mathrm{SL}_n(q)$ avec le choix d'une base ordonnée de $V = \mathbb{F}_q^n$. Ainsi, $|\mathrm{SL}_n(q)|$ revient à calculer le nombre de façons de choisir une base ordonnée de $\mathbb{F}_q^n$ ayant un déterminant égal à 1. Pour un premier vecteur, on peut prendre n'importe quel vecteur non nul de $\mathbb{F}_q^n$, il y a donc $q^n - 1$ choix. Pour le prochain vecteur, on ne peut pas prendre les q vecteurs colinéaires au premier, il y a alors $q^n - q$ choix. On continue le processus jusqu'au n-ième vecteur de la base pour lequel on aurait $q^n - q^{n-1}$ choix. Or, il faut s'assurer de sélectionner ce dernier vecteur de sorte que le déterminant de la matrice soit 1, il faut donc diviser le nombre de choix à cette dernière étape par $(q-1)$. Ainsi, il y a au total $\dfrac{1}{q-1}\displaystyle\prod_{i=1}^{n}\left(q^n - q^{i-1}\right) = \dfrac{1}{q-1}\displaystyle\prod_{i=1}^{n} q^{i-1}\left(q^{n-i+1} - 1\right) = q^{n(n-1)/2}\displaystyle\prod_{i=2}^{n}\left(q^i - 1\right)$ bases ordonnées dont le déterminant de la matrice associée est 1. □

Remarque 1.6. *Ainsi, on a que* $|\mathrm{PSL}_n(q)| = \dfrac{1}{(n, q-1)} q^{n(n-1)/2} \displaystyle\prod_{i=2}^{n}\left(q^i - 1\right)$.

1.2.1 Formes bilinéaires

Les autres groupes classiques peuvent être définis comme des ensembles d'isométries pour certaines formes bilinéaires.

Définition 1.9. *Une* ***forme bilinéaire*** *sur un k-espace vectoriel V est une application $f : V \times V \to k$ telle que $f(\lambda u + v, w) = \lambda f(u, w) + f(v, w)$ et $f(u, \lambda v + w) = \lambda f(u, v) + f(u, w)$ pour tout $u, v, w \in V$ et $\lambda \in k$. On dit qu'elle est*

$$\textbf{\textit{symétrique}} \text{ si } f(u, v) = f(v, u);$$
$$\textbf{\textit{anti-symétrique}} \text{ si } f(u, v) = -f(v, u);$$
$$\textbf{\textit{alternée}} \text{ si } f(v, v) = 0.$$

Remarque 1.7. *Si f est une forme alternée, alors f est aussi anti-symétrique. En effet, on a que*

$$f(u, v) + f(v, u) = f(u, u) + f(u, v) + f(v, u) + f(v, v) = f(u + v, u + v) = 0.$$

De plus, si la caractéristique de k n'est pas 2, alors une forme anti-symétrique est aussi une forme alternée. En effet, $f(v, v) = -f(v, v)$ implique que $f(v, v) = 0$. Donc, dans ce cas, les formes anti-symétriques et alternées sont confondues.

En caractéristique 2, $a = -a$ pour tout $a \in k$. Il est donc possible pour une forme anti-symétrique de ne pas être alternée. De plus, pour la même raison, les formes anti-symétriques et symétriques sont confondues.

Définition 1.10. *Soit f une forme bilinéaire sur V. On écrit $u \perp v$ si $f(u, v) = 0$. En général, notons que cette relation n'est pas nécessairement symétrique. Dans le cas où pour tout $u, v \in V$, $u \perp v \iff v \perp u$, la forme f est dite* ***réflexive****. Dans ce cas, u et v sont dits* ***perpendiculaires*** *(ou orthogonaux).*

Soit $S \subseteq V$, on écrit $S^\perp = \{v \in V : u \perp v \text{ pour tout } u \in S\}$. On appelle $S^\perp$ le complément orthogonal de S.

Proposition 1.4. *Une forme bilinéaire f sur V est réflexive si et seulement si elle est symétrique ou alternée.*

Démonstration. Une forme symétrique est clairement réflexive. Si f est alternée, alors elle est aussi anti-symétrique selon la Remarque 1.7. Ainsi, si $u \perp v$, il suit que $0 = f(u, v) = -f(v, u)$, de sorte que $f(v, u) = 0$ et donc que $v \perp u$. Ceci montre que f est réflexive.

Réciproquement, supposons que f soit réflexive. On souhaite montrer que f est symétrique ou alternée. Pour des $u, v, w \in V$ donnés on pose $\xi = f(u, v)w - f(u, w)v$. Alors, il suit de la

bilinéarité de f que

$$f(u,\xi) = f(u,v)f(u,w) - f(u,w)f(u,v) = 0, \tag{1.1}$$

et donc $u \perp \xi$. Comme f est réflexive, il en résulte que $\xi \perp u$, i.e.

$$0 = f(\xi,u) = f(u,v)f(w,u) - f(u,w)f(v,u). \tag{1.2}$$

En particulier, cette dernière identité est valide pour tout $u, v, w \in V$. Dans un premier temps, si on pose $u = v$ dans (1.2) on trouve

$$f(v,v)\big(f(w,v) - f(v,w)\big) = 0, \tag{1.3}$$

une identité étant vérifiée pour tout $v, w \in V$. À l'aide de (1.3), on va montrer que la relation plus générale (1.2) entraîne que f est soit symétrique ou alternée.

On raisonne par l'absurde. Supposons qu'il existe des vecteurs $x, y, z \in V$ tels que $f(y,y) \neq 0$ et $f(x,z) \neq f(z,x)$. En faisant la substitution $v \mapsto x$ et $w \mapsto z$ dans (1.3), on trouve que $f(x,x) = 0$. À l'aide de substitutions similaires, on déduit aisément que $f(x,x) = f(z,z) = 0$, $f(x,y) = f(y,x)$ et $f(z,y) = f(y,z)$.

Maintenant, si on pose $u = x$, $v = y$ et $w = z$ dans (1.2), on trouve $f(x,y) = 0$ et donc aussi que $f(y,x) = 0$. De manière similaire on montre aussi que $f(z,y) = f(y,z) = 0$. De cela on déduit que

$$f(y+z, y+z) = f(y,y) + f(y,z) + f(z,y) + f(z,z) = f(y,y) \neq 0 \tag{1.4}$$

et

$$f(x, y+z) = f(x,z) \neq f(z,x) = f(y+z,x). \tag{1.5}$$

Finalement, en posant $u = v = y + z$ et $w = x$ dans l'équation (1.2), on trouve

$$0 = \underbrace{f(y+z,y+z)}_{\neq 0}\underbrace{\big(f(x,y+z) - f(y+z,x)\big)}_{\neq 0} \neq 0,$$

□

ce qui donne une contradiction.

Hypothèse : Pour la suite, sauf mention du contraire, nous supposerons toujours que la forme bilinéaire f est réflexive et donc soit symétrique ou alternée.

Définition 1.11. *Soit V un k-espace vectoriel muni d'une forme bilinéaire f. Pour un vecteur $v \in V$ on définit sa* ***norme*** *par $f(v,v) \in k$. On définit le* ***radical*** *de f par $\mathrm{rad}(f) := V^{\perp}$, c'est-à-dire le sous-ensemble des vecteurs de V qui sont perpendiculaires à tout V. On dit que f est une forme* ***non singulière*** *si $\mathrm{rad}(f) = \{0\}$ et singulière autrement.*

Remarque 1.8. *Toutes les formes f sont déterminées par ses valeurs $f(e_i, e_j)$ sur une k-base $B = \{e_1, e_2, \cdots, e_n\}$ de V. La matrice $A = (a_{ij})$ définie par $a_{ij} = f(e_i, e_j)$ est appelée la matrice associée à f dans la base B.*

Définition 1.12. *Soit $(k^\times)^2 = \left\{a^2 \in k : a \in k^\times\right\}$ l'ensemble des carrés non nuls du corps k. Soit f une forme bilinéaire et soit A sa matrice associée dans une certaine base B. Alors, le* ***discriminant*** *de f est donné par*

$$\operatorname{disc}(f) = \begin{cases} 0 & \text{si } \det A = 0 \\ (\det A) \cdot (k^\times)^2 \in k^\times/(k^\times)^2 & \text{sinon} \end{cases}$$

Remarque 1.9. *Le discriminant d'une forme est indépendant du choix de la base. Une forme est singulière si et seulement si son discriminant est nul.*

Définition 1.13. *Soit f une forme alternée sur V. Une paire de vecteurs $u, v \in V$ telle que $f(u, v) = 1$ est appelée une* ***paire hyperbolique****. L'espace engendré par u et v est appelé un* ***plan hyperbolique****.*

Remarque 1.10. *u et v sont nécessairement linéairement indépendants, car si $v = \lambda u$ pour $\lambda \in k^\times$, on aurait alors $1 = f(u, \lambda u) = \lambda f(u, u) = 0$ ce qui est absurde.*

Définition 1.14. *Une* ***forme quadratique*** *est une application $Q : V \to k$ telle que*

$$Q(\lambda u + v) = \lambda^2 Q(u) + \lambda f(u, v) + Q(v)$$

pour tout $u, v \in V$, $\lambda \in k$ et où f est une forme bilinéaire symétrique.

Donc, une forme quadratique détermine une forme bilinéaire symétrique $f = f_Q$ appelée la forme bilinéaire (symétrique) associée à Q. Notons que si la caractéristique de k n'est pas 2, alors la forme quadratique Q peut être récupérée à partir de f par la règle

$$Q(v) = \frac{1}{2} f(v, v).$$

Si la caractéristique de k est 2, alors la forme bilinéaire associée est aussi alternée, car

$$0 = Q(2v) = Q(v + v) = 2Q(v) + f(v, v) = f(v, v).$$

Définition 1.15. *Le* ***radical*** *de Q, écrit $\operatorname{rad} Q$, est le sous-espace des vecteurs v de $\operatorname{rad}(f)$ tels que $Q(v) = 0$. On dit que Q est une forme* ***non singulière*** *si $\operatorname{rad}(Q) = \{0\}$ et* ***non dégénérée*** *si $\operatorname{rad}(f) = \{0\}$.*

Remarque 1.11. *Sauf en caractéristique 2, une forme quadratique Q sera non singulière si et seulement si sa forme bilinéaire associée f est non singulière.*

Proposition 1.5. *Soit f une forme bilinéaire symétrique non nulle sur un espace vectoriel V et Q sa forme quadratique associée. Alors, il existe $v \in V$ tel que $Q(v) \neq 0$.*

Démonstration. Supposons le contraire. Alors, pour tout $v \in V$, $Q(v) = 0$. Alors,

$$0 = Q(u+v) = Q(u) + f(u,v) + Q(v) = f(u,v).$$

Donc, $f(u,v) = 0$ pour tout $u, v \in V$, ce qui est une contradiction. □

Définition 1.16. *Soit Q une forme quadratique sur V. Un vecteur $v \in V$ non nul est appelé* ***isotrope*** *si $Q(v) = 0$.*

Remarque 1.12. *Si un tel v existe, on dit que V, Q et f la forme bilinéaire associée sont isotropes. Si tous les vecteurs non nuls de V sont isotropes, alors V est appelé totalement isotrope.*

Définition 1.17. *Soit Q une forme quadratique non singulière sur V. Alors, l'****indice de Witt*** *$m(V,Q)$ de V est la dimension d'un sous-espace totalement isotrope maximal de V sous Q.*

Remarque 1.13. *Deux sous-espaces totalement isotropes maximaux de V ont la même dimension, donc $m(V,Q)$ est bien défini. De plus, si la dimension de V est n, alors $m(V,Q) \leq n/2$.*

Définition 1.18. *Soit V admettant une forme bilinéaire symétrique f telle qu'il existe $u, v \in V$ isotropes tels que $f(u,v) = 1$. Alors, l'ensemble $\{u,v\}$ est appelé une* ***paire hyperbolique*** *et l'espace engendré par u et v est appelé un* ***plan hyperbolique****.*

Définition 1.19. *Une forme quadratique Q sur V et sa forme bilinéaire associée sont appelées* ***universelles*** *si $Q(V) = k$, c'est-à-dire que pour tout $\lambda \in k$, il existe $v \in V$ tel que $Q(v) = \lambda$.*

Proposition 1.6. *Si f est une forme bilinéaire symétrique, isotrope et non singulière, alors f est universelle.*

Démonstration. Soit $u \in V$ un vecteur isotrope. Comme f est non singulière, il existe $w' \in V$ tel que $f(u,w') = \mu \neq 0$. Posons $w := \mu^{-1}w'$ et $v = cu + w$ avec $c \in k$ à déterminer. Alors, $f(u,w) = 1$. Donc,

$$Q(v) = Q(cu+w) = c^2Q(u) + cf(u,w) + Q(w) = c + Q(w).$$

Soit $\lambda \in k$. En posant $c = \lambda - Q(w)$, on a

$$Q(v) = \lambda - Q(w) + Q(w) = \lambda.$$

□

Définition 1.20. *Soit $k = \mathbb{F}_{q^2}$ pour un certain $q = p^a$ où p est premier. Pour tout $x \in k$, on écrit $\overline{x} := x^q$, ce qu'on appelle la* ***conjugaison*** *dans k.*

Remarque 1.14. *La conjugaison dans k est un automorphisme d'ordre 2 qui remplace la conjugaison dans $\mathbb{C}$ pour le cas fini.*

Définition 1.21. *Soit $k = \mathbb{F}_{q^2}$ pour un certain $q = p^a$. On appelle une* ***forme sesquilinéaire conjugué-symétrique*** *une application $f : V \times V \to k$ satisfaisant*

$$f(\lambda u + v, w) = \lambda f(u, w) + f(v, w)$$
$$f(w, v) = \overline{f(v, w)}$$

Remarque 1.15. *Cela implique que $f(u, \lambda v + w) = \overline{\lambda} f(u, v) + f(u, w)$. De plus, cette définition est également valide pour tout corps k qui admet un automorphisme d'ordre 2, par exemple $\mathbb{C}$.*

Définition 1.22. *Soit $k^{1+q} = \left\{a\overline{a} = a^{1+q} : a \in k^*\right\}$ inspiré de l'ensemble des carrés du corps k. Soit f une forme sesquilinéaire conjugué-symétrique et soit A sa matrice associée dans une certaine base B. Alors, le* ***discriminant*** *de f est donné par*

$$discr(f) = \begin{cases} 0 & si \det A = 0 \\ (\det A)k^{1+q} \in k^*/k^{1+q} & sinon \end{cases}.$$

Définition 1.23. *L'application $H : V \to k$ définie par $H(v) = f(v, v)$ où f est une forme sesquilinéaire conjugué-symétrique est appelée une* ***forme hermitienne****. Elle respecte la propriété que*

$$H(\lambda u + v) = \lambda\overline{\lambda} H(u) + \lambda f(u, v) + \overline{\lambda} f(v, u) + H(v)$$

Proposition 1.7. *Soit f une forme sesquilinéaire conjugué-symétrique non nulle sur un espace vectoriel V sur un corps k et H sa forme hermitienne associée. Alors, il existe $v \in V$ tel que $H(v) \neq 0$.*

Démonstration. Supposons le contraire. Alors, pour tout $v \in V$, $H(v) = 0$. On prend $u, v \in V$ tels que $f(u, v) = 1$. Soit $\lambda \in k$. Alors,

$$0 = H(\lambda u + v) = \lambda\overline{\lambda} H(u) + \lambda f(u, v) + \overline{\lambda} f(v, u) + H(v) = \lambda + \overline{\lambda}.$$

En spécifiant $\lambda = 1$, on a $1 + 1 = 0$, donc k est de caractéristique 2. Alors, $\overline{\lambda} = -\lambda = \lambda$ pour tout $\lambda \in F$. Donc, l'automorphisme de conjugaison n'est pas d'ordre 2, ce qui est une contradiction. □

Définition 1.24. *Soit f une forme sur un espace vectoriel V. Alors, $g : V \to V$ est une* ***isométrie*** *de f si $f(g(u), g(v)) = f(u, v)$ pour tout $u, v \in V$. De même, on dira que $g : V \to V$ est une isométrique d'une forme quadratique Q si $Q(g(v)) = Q(v)$ pour tout $v \in V$.*

1.2.2 Suite des définitions et résultats sur les groupes classiques

Groupes symplectiques

Soit f une forme bilinéaire alternée sur un espace vectoriel $V \cong \mathbb{F}_q^{2m}$. S'il existe $u, v \in V$ tels que $f(u, v) = \lambda \neq 0$, on pose $e_1 = u$ et $f_1 = \lambda^{-1} v$. On a alors que $f(e_1, e_1) = f(f_1, f_1) = 0$ et

$f(e_1, f_1) = -f(f_1, e_1) = 1$. On continue le procédé sur $\{e_1, f_1\}^\perp$ et ainsi de suite jusqu'à ce que cela devienne impossible. On trouve ainsi un ensemble de vecteurs $e_1, \cdots, e_m$ et $f_1, \cdots, f_m$ tels que pour tout u et v dans cet ensemble, $f(u, v) = 0$, sauf pour $f(e_i, f_i) = -f(f_i, e_i) = 1$. Si cet ensemble forme une base de V, alors f est non singulière et $\dim(V) = 2m$. Sinon, $f(u, v) = 0$ pour tout $u, v \in \{e_1, \cdots, e_m, f_1, \cdots, f_m\}^\perp \neq 0$ et f est singulière. Dans le cas où f est non singulière, la base $\{e_1, \cdots, e_m, f_m, \cdots, f_1\}$ est appelée une base symplectique et la forme f est appelée une forme symplectique.

Définition 1.25. *Le* ***groupe symplectique*** $\mathrm{Sp}_{2m}(q)$ *est le groupe d'isométries d'une forme symplectique* f*.*

Remarque 1.16. *On a que* $\mathrm{Sp}_2(q) = \mathrm{SL}_2(q)$*. En effet, en écrivant les éléments de* $\mathrm{Sp}_2(q)$ *dans une base symplectique* $\{e_1, f_1\}$ *pour une forme symplectique* f*, on a* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_2(q)$ *si et seulement si* $f(ae_1 + bf_1, ce_1 + df_1) = 1$*. Comme*

$$\begin{aligned} f(ae_1 + bf_1, ce_1 + df_1) &= acf(e_1, e_1) + adf(e_1, f_1) + bcf(f_1, e_1) + bdf(f_1, f_1) \\ &= adf(e_1, f_1) - bcf(e_1, f_1) = ad - bc \\ &= \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{aligned}$$

on a $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_2(q) \iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(q)$*.*

Proposition 1.8.

$$|\mathrm{Sp}_{2m}(q)| = q^{m^2} \prod_{i=1}^{m} \left(q^{2i} - 1\right).$$

Démonstration. Calculer l'ordre de $\mathrm{Sp}_{2m}(q)$ se résume à compter le nombre de façons de choisir une base symplectique ordonnée. Pour e_1, on peut prendre n'importe quel vecteur non nul de $\mathbb{F}_q^{2m}$, il y a donc $q^{2m} - 1$ façons. Alors, $e_1^\perp$ est de dimension $2m-1$, donc contient q^{2m-1} vecteurs. Ainsi, il y a $q^{2m} - q^{2m-1} = (q-1)q^{2m-1}$ vecteurs v tels que $f(e_1, v) \neq 0$. En regroupant les vecteurs colinéaires, on trouve des ensembles de taille $q - 1$ avec un seul vecteur v tel que $f(e_1, v) = 1$. Il y a donc q^{2m-1} choix pour f_1. On procède par induction et on trouve qu'il y a $\prod_{i=1}^{m} \left(q^{2i} - 1\right) q^{2i-1}$ choix de base symplectique. Comme $1 + 3 + \cdots + (2m-1) = m^2$, on a le résultat. □

Remarque 1.17. *Soit* A *la matrice associée à une forme symplectique* f *dans la base* $\{e_1, \cdots, e_m,\ f_m, \cdots, f_1\}$*. Alors,* $A = \begin{pmatrix} 0_m & Q_m \\ -Q_m & 0_m \end{pmatrix}$ *où* $Q_m = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$ *et* $\mathrm{Sp}_{2m}(q) = \left\{M \in M_{2m}(\mathbb{F}_q) : M^t A M = A\right\}$*.*

Comme pour $\mathrm{SL}_n(q)$, on considère $Z(\mathrm{Sp}_{2m}(q)) = \{\lambda I_{2m} : \lambda \in \mathbb{F}_q\} \cap \mathrm{Sp}_{2m}(q)$. En particulier, on a $f(\lambda u, \lambda v) = \lambda^2 f(u,v) = f(u,v)$ si et seulement si $\lambda = \pm 1$. Ainsi, $Z(\mathrm{Sp}_{2m}(q)) = \{\pm 1\}$ est généralement d'ordre 2, sauf en caractéristique 2 où il est trivial.

Définition 1.26. *On appelle* $\mathrm{PSp}_{2m}(q) = \mathrm{Sp}_{2m}(q)/Z(\mathrm{Sp}_{2m}(q))$ *le* ***groupe symplectique projectif****.*

Remarque 1.18. *Sauf pour des petites valeurs de* m *et* q, $\mathrm{PSp}_{2m}(q)$ *sera simple. On montre la simplicité au chapitre 3. De plus, à partir de la Proposition 1.8, on a*

$$|\mathrm{PSp}_{2m}(q)| = \frac{q^{m^2}}{(2, q-1)} \prod_{i=1}^{m} \left(q^{2i} - 1\right)$$

où $(2, q-1)$ *représente le plus grand diviseur commun de* 2 *et* $q-1$*.*

Groupes unitaires

Soit f une forme sesquilinéaire conjugué-symétrique sur un espace vectoriel $V \cong \mathbb{F}_{q^2}^n$. S'il existe un vecteur $v \in V$ tel que $f(v,v) \neq 0$, alors $f(v,v) = \lambda^{q+1} = \lambda\overline{\lambda}$ pour un certain $\lambda \in \mathbb{F}_{q^2}$ non nul, car $f(v,v) = \overline{f(v,v)}$. En prenant $e_1 = \lambda^{-1} v$, on a que $f(e_1, e_1) = 1$. On restreint f à $(e_1)^\perp$ et on continue le processus. Si on trouve que $f(v,v) = 0$ pour tous les vecteurs v restants, alors pour deux de ces vecteurs v, w, on a

$$\begin{aligned} 0 &= f(v + \lambda w, v + \lambda w) \\ &= f(v,v) + \overline{\lambda} f(v,w) + \lambda f(w,v) + \lambda\overline{\lambda} f(w,w) \\ &= \overline{\lambda} f(v,w) + \lambda f(w,v) \end{aligned}$$

On peut alors choisir deux valeurs de λ qui forment une base de $\mathbb{F}_{q^2}$ sur $\mathbb{F}_q$, disons $\lambda_1 = 1$ et $\lambda_2 \neq \overline{\lambda_2}$, et résoudre les deux équations simultanément pour trouver $f(v,w) = f(w,v) = 0$, donc la forme est identiquement nulle sur les vecteurs restants. En particulier, si la forme est non singulière, alors la base trouvée est appelée une base orthonormale.

Définition 1.27. *Le* ***groupe*** *(général)* ***unitaire*** $\mathrm{GU}_n(q)$ *est le groupe d'isométries d'une forme hermitienne non singulière* H *sur* $\mathbb{F}_{q^2}$*.*

Remarque 1.19. *De manière équivalente, on peut définir* $\mathrm{GU}_n(q)$ *comme les isométries de la forme sesquilinéaire conjugué-symétrique* f *associée à* H*. De plus, on peut prendre* I_n *comme la matrice associée à* f*. Alors,* $\mathrm{GU}_n(q) = \left\{M \in M_n(\mathbb{F}_{q^2}) : M^t\overline{M} = I_n\right\}$*. Ainsi, pour* $M \in \mathrm{GU}_n(q)$*, on a* $(\det M)(\overline{\det M}) = 1$*, c'est-à-dire* $(\det M)^{q+1} = 1$*.*

Proposition 1.9.

$$|\mathrm{GU}_n(q)| = q^{n(n-1)/2} \prod_{i=1}^{n} \left(q^i - (-1)^i\right)$$

Démonstration. Soit z_n le nombre de vecteurs non nuls de norme 0 et y_n le nombre de vecteurs de norme 1 dans $\mathbb{F}_{q^2}^n$. Le nombre total de vecteurs est $q^{2n} = 1 + z_n + (q-1)y_n$. De plus, $z_{n+1} = z_n + (q^2-1)y_n$, alors $z_{n+1} = \left(q^{2n}-1\right)(q+1) - qz_n$. Comme $y_0 = 0$ et $y_1 = q+1$, on a que $z_0 = z_1 = 0$. On résout ensuite la relation de récurrence pour trouver $z_n = (q^n - (-1)^n)\left(q^{n-1} + (-1)^n\right)$ et ainsi $y_n = q^{n-1}(q^n - (-1)^n)$. Un élément de $\mathrm{GU}_n(q)$ peut être spécifié en choisissant une base orthonormale un vecteur de norme 1 u et continuer le processus dans $u^\perp$. Alors,

$$|\mathrm{GU}_n(q)| = \prod_{i=1}^{n} q^{i-1}\left(q^i - (-1)^i\right) = q^{n(n-1)/2}\prod_{i=1}^{n}\left(q^i - (-1)^i\right).$$

□

Définition 1.28. *Le groupe* $\mathrm{SU}_n(q) = \{M \in \mathrm{GU}_n(q) : \det M = 1\} = \mathrm{GU}_n(q) \cap \mathrm{SL}_n(q^2)$ *s'appelle le* ***groupe spécial unitaire****.*

Remarque 1.20. *Il existe* $q+1$ *valeurs* $\lambda \in \mathbb{F}_{q^2}$ *telles que* $\lambda^{q+1} = 1$*. Donc,*

$$|\mathrm{SU}_n(q)| = \frac{1}{q+1}|\mathrm{GU}_n(q)| = q^{n(n-1)/2}\prod_{i=2}^{n}\left(q^i - (-1)^i\right).$$

Proposition 1.10. $\mathrm{SU}_2(q) \cong \mathrm{SL}_2(q)$.

Ce résultat est montré au Théorème 10.9 de [8].

Remarque 1.21. $Z(\mathrm{SU}_n(q)) = \left\{\lambda I_n : \lambda \in \mathbb{F}_{q^2}\right\} \cap \mathrm{SU}_n(q)$*. On doit alors avoir* $\lambda^{q+1} = \lambda^n = 1$*. Il y a* $(n, q+1)$ *telles valeurs.*

Définition 1.29. *On appelle* $\mathrm{PSU}_n(q) = \mathrm{SU}_n(q)/Z(\mathrm{SU}_n(q))$ *le* ***groupe unitaire projectif****.*

Remarque 1.22. *Ainsi,* $|\mathrm{PSU}_n(q)| = \dfrac{1}{(n, q+1)}q^{n(n-1)/2}\displaystyle\prod_{i=2}^{n}\left(q^i - (-1)^i\right)$. $\mathrm{PSU}_n(q)$ *sera simple en général, sauf pour de petites valeurs de* n *et* q*.*

Groupes orthogonaux (q impair)

Les groupes orthogonaux ont la particularité de dépendre du choix de la forme bilinéaire non singulière. Voici une courte proposition qui sera utilisée afin de bien définir les différents groupes orthogonaux.

Proposition 1.11. *Soit* $\mathbb{F}_q$ *un corps fini et* $a, b \in \mathbb{F}_q^\times$*. Alors, pour tout* $c \in \mathbb{F}_q$*, il existe* $x, y \in \mathbb{F}_q$ *tels que* $ax^2 + by^2 = c$*.*

Démonstration. Si q est pair, alors tous les éléments sont des carrés et on peut prendre $y = 0$ et x tel que $x^2 = a^{-1}c$.

Si q est impair, alors les ensembles $A := \{ax^2 : x \in \mathbb{F}_q\}$ et $B := \{c - by^2 : y \in \mathbb{F}_q\}$ sont de cardinalité $\frac{1}{2}(q+1)$. Donc, $A \cap B \neq \emptyset$. □

Pour commencer, supposons que $q \neq 2^a$. Le cas $q = 2^a$ sera traité par la suite. Soit f une forme symétrique sur $V \cong \mathbb{F}_q^n$. S'il existe $u, v \in V$ tels que $f(u,v) \neq 0$, alors il existe un vecteur $x \in \{u, v, u+v\}$ tel que $f(x,x) \neq 0$. Si $f(x,x) = \lambda^2$ pour un certain $\lambda \in \mathbb{F}_q$, alors $x_1 = \lambda^{-1}x$ est tel que $f(x_1, x_1) = 1$. Sinon, on choisit un $\alpha \in \mathbb{F}_q$ qui n'est pas un carré et on peut trouver le μ approprié tel que pour $x_1 = \mu x$, $f(x_1, x_1) = \alpha$. On restreint ensuite la forme sur $(x_1)^\perp$ jusqu'à avoir une base perpendiculaire $\{x_1, \cdots, x_n\}$ telle que $f(x_i, x_i) = 0, 1$ ou α pour tout i. Supposons que cette base admette deux vecteurs, sans perte de généralité x_1 et x_2, tels que $f(x_1, x_1) = f(x_2, x_2) = \alpha$. Par la Proposition 1.11 avec $a = b = 1$, on peut choisir λ et μ de sorte que $\lambda^2 + \mu^2 = \alpha^{-1}$. Alors, $x_1' = \lambda x_1 + \mu x_2$ et $x_2' = \mu x_1 - \lambda x_2$ forment une base orthonormale de l'espace engendré par x_1 et x_2. Avec cette démarche, on peut s'assurer d'avoir au plus un i tel que $f(x_i, x_i) = \alpha$. Sans perte de généralité, on choisit $i = n$. En particulier, si la forme est non singulière, alors la base n'admet aucun x_i isotrope, car on aurait $x_i \in \mathrm{rad} f = \{0\}$.

Remarque 1.23. *Il y a donc deux formes f symétriques non singulières : celles dont la matrice associée peut s'écrire comme I_n et celles dont la matrice associée peut s'écrire comme $diag(1, \cdots, 1, \alpha)$ pour α qui n'est pas un carré. Ces formes n'ont pas le même discriminant, soit $1 \cdot \mathbb{F}_q^{\times 2}$ et $\alpha \cdot \mathbb{F}_q^{\times 2}$ respectivement.*

Définition 1.30. *Le **groupe orthogonal** $\mathrm{GO}_n(q, f)$ est le groupe d'isométries d'une forme bilinéaire symétrique non singulière f sur $\mathbb{F}_q^n$. On écrit parfois $\mathrm{O}_n(q, f)$.*

Remarque 1.24. *De manière équivalente, on peut définir $\mathrm{GO}_n(q, f)$ comme les isométries de la forme quadratique Q associée à f.*

Proposition 1.12. *Les formes f et λf pour $\lambda \in \mathbb{F}_q^\times$ définissent le même groupe orthogonal.*

Démonstration. Soit $\sigma \in \mathrm{GO}_n(q, f)$, c'est-à-dire que pour tout $u, v \in \mathbb{F}_q^n$, $f(\sigma u, \sigma v) = f(u, v)$. Alors, $\lambda f(\sigma u, \sigma v) = \lambda f(u, v)$, donc $\sigma \in \mathrm{GO}_n(q, \lambda f)$. On obtient le résultat réciproque avec $g = \lambda f$ et $\lambda^{-1} g = f$. □

Proposition 1.13. *Si $n = 2m$, alors f et λf ont le même discriminant. Si $n = 2m+1$, alors f et λf n'ont possiblement pas le même discriminant.*

Démonstration. Supposons que $n = 2m$ et que $\mathrm{discr}(f) = d \cdot \mathbb{F}_q^{\times 2}$. Soit $\lambda \in \mathbb{F}_q^\times$. Alors, $\mathrm{discr}(\lambda f) = \lambda^{2m} d \cdot \mathbb{F}_q^{\times 2} = d \cdot \mathbb{F}_q^{\times 2}$. Supposons maintenant que $n = 2m+1$. Alors, $\mathrm{discr}(df) = d^{2m+1} d \cdot \mathbb{F}_q^{\times 2} = d^{2m+2} \cdot \mathbb{F}_q^{\times 2} = 1 \cdot \mathbb{F}_q^{\times 2}$. En particulier, si d n'est pas un carré, on a que le discriminant de f et de df sont différents. □

Remarque 1.25. *Ainsi, par les deux propositions précédentes, il n'existe qu'un seul groupe orthogonal si $n = 2m+1$. Or, il existe deux groupes orthogonaux non isomorphes si $n = 2m$.*

Définition 1.31. *Soit $n = 2m$. On dit que le groupe orthogonal $\mathrm{GO}_{2m}(q, f)$ est de **type plus** si l'indice de Witt de la définition 1.17 est $m(V, Q) = m$. On dit que $\mathrm{GO}_{2m}(q, f)$ est de **type moins** autrement. On note ces groupes $\mathrm{GO}^+_{2m}(q)$ et $\mathrm{GO}^-_{2m}(q)$ respectivement. Les détails se trouvent dans [5].*

Remarque 1.26. *Pour des résultats généraux qui ne dépendent pas de la parité de la dimension ou du type, on écrira $\mathrm{GO}_n(q)$ pour un groupe orthogonal quelconque.*

Proposition 1.14. *Soit $n = 2$. Posons la forme bilinéaire symétrique non singulière f_1 qui pour une certaine base $\{x, y\}$ est telle que $f_1(x, x) = f_1(y, y) = 1$ et f_2 celle telle que $f_2(x, x) = 1$ et $f_2(y, y) = \alpha$ pour un certain α qui n'est pas un carré. Alors, si $q \equiv 1$ mod 4, alors f_1 détermine un groupe orthogonal de type plus et f_2 de type moins et vice versa si $q \equiv 3$ mod 4.*

Démonstration. Si $q \equiv 1 \bmod 4$, alors -1 est un carré dans $\mathbb{F}_q$, disons avec $i^2 = -1$. Alors, $f_1(x + yi, x + yi) = f_1(x, x) + 2if_1(x, y) + i^2 f(y, y) = 1 + 0 - 1 = 0$. Donc, $\langle x + yi\rangle$ est un sous-espace totalement isotrope maximal de V et $m(V, Q_{f_1}) = 1$ et $\mathrm{GO}_2(q, f_1)$ est de type plus. De plus, pour tout $\lambda \in \mathbb{F}_q$, $f_2(x + \lambda y, x + \lambda y) = 1 + \lambda^2\alpha$, ce qui ne peut pas valoir 0, car sinon $\alpha = -\lambda^2 = (i\lambda)^2$ serait un carré. Donc, $m(V, Q_{f_2}) = 0$ et $\mathrm{GO}_2(q, f_2)$ est de type moins. Si $q \equiv 3 \bmod 4$, alors -1 n'est pas un carré dans $\mathbb{F}_q$. Alors, $-\alpha$ est un carré, disons $-\alpha = \lambda^2$ pour un certain $\lambda \in \mathbb{F}_q$. Ainsi, $f_2(\lambda x + y, \lambda x + y) = \lambda^2 f_2(x, x) + 2\lambda f(x, y) + f(y, y) = -\alpha + 0 + \alpha = 0$. Donc, $\langle \lambda x + y\rangle$ est un sous-espace totalement isotrope maximal de V et $m(V, Q_{f_2}) = 1$ et $\mathrm{GO}_2(q, f_2)$ est de type plus, alors que $f_1(x + \mu y, x + \mu y) \neq 0$ pour tout $\mu \in \mathbb{F}_q$ et donc $m(V, Q_{f_1}) = 0$ et $\mathrm{GO}_2(q, f_1)$ est de type moins. □

Remarque 1.27. *En général, si $n = 2m$, la forme dont la matrice associée est I_{2m} détermine un groupe orthogonal de type moins si et seulement si $q \equiv 3$ mod 4 et m est impair. De plus, on a que pour les groupes orthogonaux de type moins, l'indice de Witt sera $m(V, Q) = m - 1$. Les détails se trouvent dans [9].*

Proposition 1.15.

$$\begin{cases} \left|\mathrm{GO}^+_{2m}(q)\right| = 2q^{m(m-1)}(q^m - 1)\prod_{i=1}^{m-1}\left(q^{2i} - 1\right) \\ \left|\mathrm{GO}_{2m+1}(q)\right| = 2q^{m^2}\prod_{i=1}^{m}\left(q^{2i} - 1\right) \\ \left|\mathrm{GO}^-_{2m+2}(q)\right| = 2q^{m(m+1)}(q^{m+1} + 1)\prod_{i=1}^{m}\left(q^{2i} - 1\right) \end{cases}$$

Démonstration. Soit m l'indice de Witt de $V \cong \mathbb{F}_q^n$ avec $n = 2m$, $2m + 1$ ou $2m + 2$. Posons $\varepsilon = 2m - n + 1$ de sorte que ε est 1, 0 ou -1 selon que le groupe est $\left|\mathrm{GO}^+_{2m}(q)\right|$, $\left|\mathrm{GO}_{2m+1}(q)\right|$ ou $\left|\mathrm{GO}^-_{2m+2}(q)\right|$ respectivement. Soit z^ε_m le nombre de vecteurs isotropes de V. On procède par induction sur m. Soient $u, v \in V$ tels que $\{u, v\}$ soit une paire hyperbolique de la Définition

1.18 et soit $U := \langle u, v\rangle$ le plan hyperbolique engendré par u et v. Alors, $V = U \oplus U^\perp$ avec $U^\perp$ de même type que V. Les vecteurs isotropes de U sont de la forme λu ou λv pour $\lambda \in \mathbb{F}_q^\times$, il y en a donc $2q-2$. Il y a également $q-1$ vecteurs de chaque norme non nulle. Tous les vecteurs isotropes de V peuvent s'écrire comme $w + w'$ avec $w \in U$ et $w' \in U^\perp$ tels que soit w et w' sont tous les deux de norme 0 avec au plus des vecteurs qui est nul, soit w est de norme $\lambda \neq 0$ et w' est de norme $-\lambda$. Ainsi,

$$\begin{aligned} z_m^\varepsilon &= (2q-2+1)\left(z_{m-1}^\varepsilon + 1\right) - 1 + (q-1)\left(q^{n-2} - 1 - z_{m-1}^\varepsilon\right) \\ &= q z_{m-1}^\varepsilon + (q-1)\left(q^{n-2}+1\right) \end{aligned}$$

Pour tout ε, $z_0^\varepsilon = 0$. Ainsi, $z_m^\varepsilon = (q^{m-\varepsilon}+1)(q^m-1)$. Le nombre de paires hyperboliques dans V est $q^{n-2} z_m^\varepsilon$, donc le nombre de choix ordonnées de m plans hyperboliques mutuellement orthogonaux est

$$q^{n-2} z_m^\varepsilon q^{n-4} z_{m-1}^\varepsilon \cdots q^{n-2m} z_1^\varepsilon.$$

En particulier, $n - 2m = 1 - \varepsilon$. Pour $\varepsilon = 1$, l'ordre de $\mathrm{GO}_{2m}^+(q)$ est la valeur ci-haut. Pour $\varepsilon = 0$ ou -1, il reste un espace de dimension 1 ou 2 respectivement qui ne contient aucun vecteur isotrope. On a $\mathrm{GO}_1(q) = \{\pm 1\}$ et $\left|\mathrm{GO}_2^-(q)\right| = 2(q+1)$. Donc,

$$\begin{aligned} \left|\mathrm{GO}_{2m}^+(q)\right| &= \prod_{i=1}^{m} q^{2i-2}\left(q^{i-1}+1\right)\left(q^i-1\right) \\ &= 2q^{m(m-1)}(q^m-1)\prod_{i=1}^{m-1}\left(q^{2i}-1\right) \\ \left|\mathrm{GO}_{2m+1}(q)\right| &= 2\prod_{i=1}^{m} q^{2i-1}\left(q^i+1\right)\left(q^i-1\right) \\ &= 2q^{m^2}\prod_{i=1}^{m}\left(q^{2i}-1\right) \\ \left|\mathrm{GO}_{2m+2}^-(q)\right| &= 2(q+1)\prod_{i=1}^{m} q^{2i}\left(q^{i+1}+1\right)\left(q^i-1\right) \\ &= 2q^{m(m+1)}(q^{m+1}+1)\prod_{i=1}^{m}\left(q^{2i}-1\right) \end{aligned}$$

□

Définition 1.32. *Le groupe* $\mathrm{SO}_n(q) = \{M \in \mathrm{GO}_n(q) : \det M = 1\} = \mathrm{GO}_n(q) \cap \mathrm{SL}_n(q)$ *s'appelle un* ***groupe spécial orthogonal****.*

Remarque 1.28. *Soit A la matrice associée à la forme. Alors, pour $M \in \mathrm{GO}_n(q)$, $MAM^t = A$. Ainsi,* $(\det(M))^2 = 1$ *et* $\det M = \pm 1$*. Donc,*

$$|\mathrm{SO}_n(q)| = \frac{1}{2}\left|\mathrm{GO}_n(q)\right|.$$

On considère encore une fois $\mathbb{Z}(\mathrm{SO}_n(q)) = \{\lambda I_n : \lambda \in \mathbb{F}_q\} \cap \mathrm{SO}_n(q)$. *Comme pour* $\mathrm{Sp}_{2m}(q)$, *on a que* $f(\lambda u, \lambda v) = \lambda^2 f(u,v) = f(u,v)$ *si et seulement si* $\lambda = \pm 1$. *Or,* $\det(-I_n) = (-1)^n$, *donc* $-I_n \in \mathrm{SO}_n(q)$ *si et seulement si* $n = 2m$. *On définit* $\mathrm{PSO}_n(q) := \mathrm{SO}_n(q)/\mathbb{Z}(\mathrm{SO}_n(q))$. *On a* $\mathrm{PSO}_{2m+1}(q) \cong \mathrm{SO}_{2m+1}(q)$ *et* $\left|\mathrm{PSO}^{\pm}_{2m}(q)\right| = \frac{1}{2}\left|\mathrm{SO}^{\pm}_{2m}(q)\right|$.

Remarque 1.29. *Contrairement aux autres groupes classiques,* $\mathrm{PSO}_n(q)$ *possède généralement un sous-groupe normal supplémentaire et ne sera pas simple dans ce cas.*

Définition 1.33. *Soit* $v \in V$ *un vecteur tel que* $f(v,v) \neq 0$. *L'élément* $R_v \in \mathrm{GO}_n(q)$ *défini par*

$$R_v(x) = x - 2\frac{f(x,v)}{f(v,v)}v$$

est appelé une ***réflexion****.*

Remarque 1.30. *Pour* q *impair, les éléments de* $\mathrm{GO}_n(q)$ *peuvent s'écrire comme un produit de réflexions. Le déterminant d'une réflexion est* -1, *donc les éléments de* $\mathrm{SO}_n(q)$ *s'écrivent avec un nombre pair de réflexions. On différencie les réflexions* R_v *selon que* $f(v,v)$ *est un carré ou non.*

Définition 1.34. *Soit* $\sigma \in \mathrm{SO}_n(q)$ *et* $R_{v_1} \cdots R_{v_t}$ *une écriture de* σ *en produit de réflexions. Alors,*

$$\sigma \mapsto f(v_1,v_1) \cdot \cdots \cdot f(v_t,v_t)\mathbb{F}_q^{\times 2}$$

est appelé la ***norme spinorielle*** *de* σ.

Remarque 1.31. *Le noyau de la norme spinorielle se compose des éléments* $\sigma \in \mathrm{SO}_n(q)$ *tels que le nombre de réflexions de chaque type de la Remarque 1.30 est pair.*

Définition 1.35. *Le noyau de la norme spinorielle est noté* $\Omega_n(q)$ *ou* $\Omega^{\pm}_{2m}(q)$ *si le type est spécifié.*

Remarque 1.32. *On a que* $|\Omega_n(q)| = \dfrac{1}{2}|\mathrm{SO}_n(q)|$. *Pour* n *impair, on a que* $\mathrm{P}\Omega_n(q) \cong \Omega_n(q)$ *par la Remarque 1.28. Pour* $n = 2m$, *on a que* $-1 \in \Omega^{\pm}_{2m}$ *si et seulement si la matrice associée à la forme* f *est* I_{2m}. *Donc, par la Remarque 1.27, si* $q \equiv 3 \bmod 4$ *et* m *est impair, alors* $\left|\mathrm{P}\Omega^{-}_{2m}(q)\right| = \dfrac{1}{2}\left|\mathrm{PSO}^{-}_{2m}(q)\right|$ *et* $\mathrm{P}\Omega^{+}_{2m}(q) \cong \mathrm{PSO}^{+}_{2m}(q)$. *Autrement,* $\left|\mathrm{P}\Omega^{+}_{2m}(q)\right| = \dfrac{1}{2}\left|\mathrm{PSO}^{+}_{2m}(q)\right|$ *et* $\mathrm{P}\Omega^{-}_{2m}(q) \cong \mathrm{PSO}^{-}_{2m}(q)$.

Groupes orthogonaux (q pair)

Supposons maintenant que $q = 2^a$. Soit Q une forme quadratique sur $V \cong \mathbb{F}_q^n$. On rappelle que la forme bilinéaire associée f est alternée en caractéristique 2, donc également symétrique et anti-symétrique. On construit alors une base de la même manière que pour le cas symplectique. Ainsi, on s'attarde seulement aux formes telles que $\mathrm{rad}\ f = \{0\}$, c'est-à-dire que Q est non dégénérée et donc $\dim V = 2m$. La particularité ici est qu'on choisit le plus de vecteurs isotropes

possible pour former la base. Soit $\{e_1, \cdots, e_m, f_m, \cdots, f_1\}$ une base symplectique. Si $Q(e_i) = 0$ ou $Q(f_i) = 0$, on remplace e_i par $e_i + Q(e_i)f_i$ et f_i par $f_i + Q(f_i)e_i$ afin d'avoir $Q(e_i) = Q(f_i) = 0$. Sans perte de généralité, classons les e_i et f_i de sorte qu'il existe $1 \leq j \leq m+1$ tels que les e_i et f_i sont isotropes pour $i < j$ et non isotropes pour $i \geq j$. Tant que $j < m$, on fait la procédure suivante. Soit $\lambda = \left(Q(e_{j+1})Q(e_j)^{-1}\right)^{q/2}$. Alors, $\lambda^2 = Q(e_{j+1})Q(e_j)^{-1}$ et $Q(e_{j+1} + \lambda e_j) = 0$. On pose donc $e'_j := e_{j+1} + \lambda e_j$ et $f'_j = \lambda^{-1} f_j + \lambda^{-2} Q(f_j) e'_j$. Ainsi, $Q(e'_j) = Q(f'_j) = 0$ et $f(e'_j, f'_j) = 1$. On incrémente ensuite j. Lorsque $j = m$, quitte à multiplier e_m par un scalaire et f_m par le scalaire inverse, on suppose que $Q(e_m) = 1$. Alors, pour tout $\lambda \in \mathbb{F}_q$, on a que $f(e_m, f_m + \lambda e_m) = 1$ et $Q(f_m + \lambda e_m) = Q(f_m) + \lambda + \lambda^2$. Si $Q(f_m) + \lambda + \lambda^2 = 0$ a une solution $\lambda = \lambda_0$, alors $f'_m = f_m + \lambda_0 e_m$ est tel que $Q(f'_m) = 0$. En particulier, $\lambda_0 \neq 1$, car on aurait que $Q(f_m) = 0$, alors qu'on a supposé que ce n'était pas le cas. Avec $e'_m = e_m + f'_m$, on a que $Q(e'_m) = 0$ et $f(e'_m, f'_m) = 1$. Ainsi, on a une base symplectique et $m(V, Q) = m$. Donc, $\mathrm{GO}_{2m}(q, f)$ est de type plus. Si $Q(f_m) + \lambda + \lambda^2$ est un polynôme irréductible, alors $\mathrm{GO}_{2m}(q, f)$ est de type moins.

Remarque 1.33. *Les équations de la Proposition 1.15 sont encore valides en caractéristique 2, sauf pour* $\mathrm{GO}_{2m+1}(q)$*, mais ce cas a été exclu.*

Définition 1.36. *Soit* $\sigma \in \mathrm{GO}^{\pm}_{2m}(q)$ *et soit* k *la dimension de l'espace fixé par* σ*. Alors,*

$$\sigma \mapsto (-1)^k$$

est appelé le ***quasi-déterminant*** *de* σ*.*

Remarque 1.34. *En caractéristique impaire, le déterminant et le quasi-déterminant coïncident. Or, en caractéristique 2, le seul déterminant possible est 1.*

Définition 1.37. *Le noyau du quasi-déterminant est noté* $\Omega^{\pm}_{2m}(q)$*.*

Remarque 1.35. *Ces groupes sont parfois notés* $\mathrm{SO}^{\pm}_{2m}(q)$*, mais la notation* $\Omega^{\pm}_{2m}(q)$ *permet une définition homogène des groupes finis simples orthogonaux. On a que* $\left|\Omega^{\pm}_{2m}(q)\right| = \frac{1}{2}\left|\mathrm{GO}^{\pm}_{2m}(q)\right|$ *et* $Z\left(\Omega^{\pm}_{2m}(q)\right) = 1$*, donc* $\mathrm{P}\Omega^{\pm}_{2m}(q) \cong \Omega^{\pm}_{2m}(q)$*.*

1.3 Autres groupes finis simples

1.3.1 Groupes exceptionnels de type Lie

Les groupes classiques peuvent être considérés comme des groupes de type Lie. Or, il existe d'autres groupes de type Lie qui ne sont pas des groupes classiques.

Il existe 10 familles de groupes exceptionnels de type Lie. Il y a 5 familles dites de Chevalley, soient $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$ et $G_2(q)$ pour $q \geq 3$. Ensuite, il y a 2 familles de groupes tordus de Steinberg-Tits-Hertzing, soient ${}^3D_4(q)$ et ${}^2E_6(q)$, qui ont des constructions analogues

à celles des groupes unitaires à partir des groupes linéaires. Finalement, il y a 3 familles de groupes de Suzuki et de Ree, soient $\mathrm{Sz}(2^{2n+1}) := {}^2B_2(2^{2n+1})$, $R(2^{2n+1}) := {}^2F_4(2^{2n+1})$ et $R(3^{2n+1}) := {}^2G_2(3^{2n+1})$. Il y a aussi le groupe dérivé de ${}^2F_4(2)$, écrit ${}^2F_4(2)'$ et appelé le groupe de Tits. Ce groupe ne fait pas partie d'une famille infinie de groupes de type Lie, il est donc parfois considéré comme un groupe sporadique. Tous les groupes de type Lie sont associés à un graphe de Coxeter qui se retrouve à la Table 2.1 ou à la Table 2.2.

1.3.2 Groupes sporadiques

Les groupes sporadiques sont des groupes qui ne font pas partie d'une famille infinie dénombrable. 20 des 26 groupes sporadiques peuvent être réalisés comme le quotient d'un sous-groupe du groupe Monstre. Parmi ceux-ci, il y a les 5 groupes de Mathieu M_n pour $n \in \{11, 12, 22, 23, 24\}$ qui sont des groupes de permutations sur n points, les 7 groupes liés au réseau de Leech soient Co_1, Co_2, Co_3, McL, HS, Suz et J_2, les 3 groupes de Fisher Fi_{22}, Fi_{23} et Fi'_{24} ainsi que les cinq groupes monstrueux : $\mathbb{M}$, $\mathbb{B}$, Th, HN et He. Les six groupes restants sont appelés des parias. Ce sont les groupes J_1, J_3, J_4, O'N, Ly et Ru. Le Théorème de Classification des groupes finis simples est énoncé à l'Annexe A.

1.3.3 Exemples de corollaires au Théorème de Classification

En plus de la conjecture de Ore et de la conjecture de Schreier discutées en introduction, d'autres résultats ont pu être démontrés grâce à la Classification des groupes finis simples, c'est-à-dire qu'il n'existe pas de preuve uniforme, le résultat se montre cas par cas selon la Classification. Les exemples suivants sont tirés de [4].

Théorème 1.5. *Tous les groupes simples peuvent être générés par 2 éléments.*

Théorème 1.6. *Un groupe fini qui admet un automorphisme qui fixe uniquement l'identité est résoluble.*

Théorème 1.7. *Les groupes alternés A_n pour $n \geq 5$ et les groupes de Mathieu M_{11}, M_{12}, M_{23} et M_{24} sont les seuls groupes simples qui admettent une action 4-transitive.*

Théorème 1.8. *Soit G un groupe simple dont l'ordre n'est pas divisible par p^2 pour un certain premier p. Alors, l'ordre de $\mathrm{Aut}(G)$ n'est pas divisible par p^2.*

Théorème 1.9. *Soit G un groupe non résoluble admettant une action doublement transitive sur un ensemble de taille n et un cycle de longueur n. Alors, un des cas suivants est vrai*

(i) $G \cong A_n$ *ou* S_n,
(ii) $n = 11$ *et* $G \cong \mathrm{PSL}_2(11)$ *ou* M_{11},
(iii) $n = 23$ *et* $G \cong \mathrm{M}_{23}$,
(iv) $n = \frac{q^k-1}{q-1}$ *pour* $q = p^a$ *avec p premier et G est isomorphe à un sous-groupe de* $\mathrm{Aut}(\mathrm{PSL}_k(q))$ *qui contient* $\mathrm{PSL}_k(q)$.

Chapitre 2

BN-paires et Frobenius généralisés

Dans ce chapitre, on présente un point de vue différent pour étudier les groupes classiques en utilisant le fait qu'ils admettent une BN-paire. Pour ce faire, on introduit des constructions comme les Frobenius généralisés.

2.1 BN-paires

Définition 2.1. *Soit W un groupe tel qu'il existe un sous-ensemble S de W tel que tous les éléments de S sont d'ordre 2 et que tous les éléments de W peuvent s'écrire comme le produit d'une suite finie d'éléments de S. Pour $s, s' \in S$, on pose $m(s, s')$ l'ordre de ss' et I l'ensemble des couples (s, s') tels que $m(s, s')$ soit fini. Si (W, S) respecte la condition*

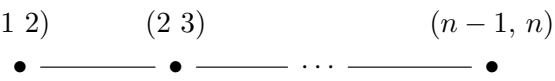
$$\left\{ \begin{array}{c} \textit{pour tout groupe } \overline{W}\textit{, pour tout homomorphisme } f \textit{ de } \overline{W} \textit{ sur } W \textit{ et pour toute application } h \\ \textit{de } S \textit{ dans } \overline{W} \textit{ tels que } f(h(s)) = s\textit{, que } (h(s)h(s)')^{m(s,s')} = 1 \textit{ pour } (s, s') \in I \textit{ et que les } h(s) \\ (s \in S) \textit{ engendrent } \overline{W}\textit{, implique que } f \textit{ est injectif,} \end{array} \right.$$

on dit que (W, S) est un ***système de Coxeter****. Par abus de langage, on dit aussi que W est un groupe de Coxeter.*

Remarque 2.1. *La condition de la définition précédente est équivalente à dire que S et $(ss')^{m(s,s')} = 1$ pour $(s, s') \in I$ forment une présentation du groupe W.*

Remarque 2.2. *Si (W, S) est un système de Coxeter fini, on appelle la matrice $M = (m(s, s'))_{s,s' \in S}$ une matrice de Coxeter de type S. Le graphe de Coxeter Γ associé à M est construit de la manière suivante : les sommets de Γ sont donnés par les éléments de S. Deux sommets s et s' sont reliés si $m(s, s') \geq 3$. En général, on écrit $m(s, s')$ au dessus de l'arête en question, sauf pour $m(s, s') = 3$. Donc, deux sommets s et s' du graphe de Coxeter Γ sont liés si et seulement si s et s' ne commutent pas.*

Par exemple, si $W = S_n$ pour $n \geq 2$, on peut prendre S comme étant les transpositions de la forme $(i, i+1)$ pour $i \in \{1, \cdots, n-1\}$. Alors, le graphe de Coxeter associé à (W, S) est



Ce graphe de Coxeter est dit de type A_{n-1}. D'autres types seront présentés à la Table 2.1.

Définition 2.2. *On dit qu'un système de Coxeter est* ***irréductible*** *si le graphe Γ associé est connexe (et non vide).*

Définition 2.3. *On appelle* ***système de Tits*** *ou* **BN-*paire*** *un quadruplet (G, B, N, S) où G est un groupe, B et N sont deux sous-groupes de G et S est un sous-ensemble de $N/(B \cap N)$, satisfaisant aux axiomes suivants :*
$(BN1)$ L'ensemble $B \cup N$ engendre G.
$(BN2)$ $T := B \cap N$ est un sous-groupe normal de N et l'ensemble S se compose d'éléments d'ordre 2 et engendre le groupe $W = N/T$.
$(BN3)$ Pour tout $s \in S$, on a $n_s B n_s \not\subseteq B$ où n_s est un représentant de s dans N.
$(BN4)$ On a $n_s B n \subseteq BnB \cup Bn_s nB$ pour tout $s \in S$ et $n \in N$.

Le groupe $W = N/T$ est appelé le ***groupe de Weyl*** *du système de Tits.*

Remarque 2.3. *L'axiome $(BN3)$ est parfois remplacé dans la littérature par $(BN3')$ Pour tout $s \in S$, on a $n_s B n_s \neq B$ où n_s est un représentant de s dans N. On inclut également parfois l'axiome de saturation $(BN5)$ $\bigcap_{n \in N} nBn^{-1} = T$.*

Remarque 2.4. *En particulier, (W, S) est un système de Coxeter. Dans le contexte des groupes de type Lie, T est appelé un tore et B est appelé un Borel.*

Définition 2.4. *Soit G un groupe qui admet un système de Tits. On dit que la BN-paire est* ***scindée*** *s'il existe un sous-groupe normal $U \subseteq B$ tel que pour $T = B \cap N$, on a*

- *$B = UT$ et $U \cap T = \{1\}$,*
- *pour tout $n \in N$, on a que $n^{-1} U n \cap B \subseteq U$*

Proposition 2.1. *Soit k un corps et $n \in \mathbb{Z}_{\geq 1}$. Soit $G = GL_n(k)$, Alors, G admet une BN-paire scindée.*

Démonstration. Soit B le sous-groupe de G formé des matrices triangulaires supérieures, soit N le sous-groupe de G formé des matrices n'ayant qu'un seul élément non nul dans chaque ligne et dans chaque colonne et soit U le sous-groupe de B des matrices unipotentes triangulaires supérieures, c'est-à-dire les matrices triangulaires supérieures avec des 1 sur la diagonale. Comme les éléments de N permutent les droites ke_i, où les e_i forment la base standard de k^n, on a un homomorphisme surjectif $N \to S_n$ dont le noyau est le sous-groupe $T = B \cap N$ des

matrices diagonales. Par le premier théorème d'isomorphisme, $W = N/T \cong S_n$ le groupe des permutations. On prend alors S comme étant les transpositions $(i\ i+1)$ pour $i \in \{1, \cdots, n-1\}$. Ainsi, (G, B, N, S) forme une BN-paire. En effet, on vérifie les axiomes

$(BN1)$: Soit $M \in G$ et Q_n défini dans le chapitre précédent. On considère $M = plu$ la décomposition PLU de M. Alors, il existe $b \in B$ tel que $Q_n b Q_n = l$. Ainsi, $M = pQ_n b Q_n u \in \langle B, N\rangle$, car $p, Q_n \in N$ et $b, u \in B$.

$(BN2)$: S a été choisi pour vérifier cet axiome.

$(BN3)$: Soit $s = (i\ i+1) \in S$ une transposition pour $i \in \{1, \cdots, n-1\}$. Sans perte de généralité, prenons pour n_s la matrice identité avec les lignes i et $i+1$ échangées. Ainsi, en prenant un $b \in B$ tel que $b_{i,i+1} \neq 0$, on obtient une matrice $n_s b n_s$ avec $b_{i,i+1}$ en position $i+1, i$, donc $n_s b n_s \notin B$.

Pour $(BN4)$, il sera pratique d'introduire certaines familles de sous-groupes de G. Pour $1 \leq i, j \leq n$, on a la matrice élémentaire E_{ij} avec une entrée 1 en position i, j et 0 autrement. On définit les sous-groupes

$$X_{ij} := \{I_n + \lambda E_{ij} : \lambda \in k\}$$

et

$$V_i := \{V \in U \text{ avec 0 en position } i, i+1\}.$$

Pour la suite, le représentant n_w sera celui avec seulement des 1 et des 0 pour tout $w \in W$. Par calcul matriciel direct, on montre que $U = X_{i,i+1} V_i = V_i X_{i,i+1}$, $V_i \cap X_{i,i+1} = \{1\}$ et $n_w X_{ij} n_w^{-1} = X_{w(i),w(j)}$ pour $w \in W$ et $i \neq j$. Pour $s = (i\ i+1)$, $n_s V_i n_s^{-1} = V_i$. Avec $B = UT = V_i X_{i,i+1} T$, on a donc $n_s B n_s = n_s B n_s^{-1} = V_i n_s X_{i,i+1} n_s^{-1} T = V_i X_{i+1,i} T$. On considère également cette identité dans $\mathrm{GL}_2(k)$ avec $0 \neq t \in k$:

$$\underbrace{\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}}_{=:A} = \underbrace{\begin{pmatrix} 1 & 1/t \\ 0 & 1 \end{pmatrix}}_{=:B} \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{=:C} \underbrace{\begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix}}_{=:D} \underbrace{\begin{pmatrix} t & 0 \\ 0 & -1/t \end{pmatrix}}_{=:E}.$$

Soit $x \in X_{i+1,i}$. Si $x \neq I_n$, alors

$$x = \begin{pmatrix} I_{i-1} & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & I_{n-i-1} \end{pmatrix} = \underbrace{\begin{pmatrix} I_{i-1} & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & I_{n-i-1} \end{pmatrix}}_{\in X_{i,i+1}} \underbrace{\begin{pmatrix} I_{i-1} & 0 & 0 \\ 0 & C & 0 \\ 0 & 0 & I_{n-i-1} \end{pmatrix}}_{=n_s} \underbrace{\begin{pmatrix} I_{i-1} & 0 & 0 \\ 0 & D & 0 \\ 0 & 0 & I_{n-i-1} \end{pmatrix}}_{\in X_{i,i+1}} \underbrace{\begin{pmatrix} I_{i-1} & 0 & 0 \\ 0 & E & 0 \\ 0 & 0 & I_{n-i-1} \end{pmatrix}}_{\in T},$$

donc $X_{i+1,i} \subseteq \{I_n\} \cup X_{i,i+1} n_s X_{i,i+1} T$. Ainsi,

$$n_s B n_s \subseteq V_i \left(\{I_n\} \cup X_{i,i+1} n_s X_{i,i+1} T\right) T \subseteq V_i T \cup U n_s X_{i,i+1} T \subseteq B \cup B n_s B.$$

$(BN4)$ Soit $w \in W$ et $i \in \{1, \cdots, n-1\}$. Supposons pour l'instant que $w^{-1}(i) < w^{-1}(i+1)$. Alors, $n_w^{-1} X_{i,i+1} n_w = X_{w^{-1}(i),w^{-1}(i+1)} \subseteq U$. Ainsi,

$$n_s B n_w = n_s V_i X_{i,i+1} T n_w = V_i n_s n_w n_w^{-1} X_{i,i+1} n_w T \subseteq V_i n_s n_w U T \subseteq B n_s n_w B.$$

Supposons maintenant que $w^{-1}(i) > w^{-1}(i+1)$ et posons $y := sw$. Alors, $y^{-1}(i) = w^{-1}(i+1) < w^{-1}(i) = y^{-1}(i+1)$. Par le cas précédent, on a $n_s B n_y \subseteq B n_s n_y B = B n_w B$. Ainsi,

$$n_s B n_w = n_s B n_s n_y \subseteq (B \cup B n_s B) n_y = B n_y \cup B n_s B n_y \subseteq B n_s n_w B \cup B n_w B.$$

Pour n'_w qui n'aurait pas seulement des entrées 1 ou 0, on a qu'il existe $t, t' \in T$ tels que $t' n'_w = n'_w t = n_w$ où n_w n'admet que des 1 et des 0. Donc, l'identité est vérifiée peut importe le représentant.
De plus, cette BN-paire est bien scindée, car $B = UT$, $U \cap T = \{1\}$ et pour tout $n \in N$ et $u \in U$, $n^{-1}un$ a en particulier l'effet de permuter les éléments sur la diagonale, donc $n^{-1}Un \cap B \subseteq U$. □

Cette proposition introduit la BN-paire qui sera utilisée pour définir des BN-paires sur les autres groupes classiques.

Remarque 2.5. *On peut aussi considérer B comme le stabilisateur du drapeau maximal*

$$0 = V_0 < V_1 < \cdots < V_n \cong \mathbb{F}_q^n$$

où $V_i = \langle e_1, e_2, \cdots, e_i \rangle$.

Définition 2.5. *On définit une fonction de longueur l sur W. On pose $l(1) = 0$. Pour $w \neq 1$, on définit $l(w)$ comme la longueur minimale d'une écriture de w comme un produit d'éléments de S. Une telle écriture de w est appelée une* ***expression réduite*** *de w.*

Remarque 2.6. *Si $w \neq 1$, on peut toujours trouver $s \in S$ tel que $l(sw) = l(w) - 1$, en particulier avec $s = s_1$. De plus, si $l(sw) > l(w)$, alors $ss_1s_2 \cdots s_m$ est une expression réduite de sw, donc $l(sw) = l(w) + 1$. Similairement, si $l(sw) < l(w)$, alors $l(w) = l(s(sw)) > l(sw)$, donc $l(w) = l(sw) + 1$ par le cas précédent et $l(sw) = l(w) - 1$. On ne peut pas avoir que $l(sw) = l(w)$, ce qui sera montré à l'aide de la Proposition 2.4.*

Lemme 2.1. *Soit $J \subseteq S$ et soit $W_J := \langle J \rangle \subseteq W$. Soit $N_J \subseteq N$ la préimage de W_J dans N. Alors, $P_J := BN_JB$ est un sous-groupe de G.*

Démonstration. On a que $P_J^{-1} = P_J$. Il reste à montrer que P_J est fermé sous la multiplication. On a clairement que $BP_J \subseteq P_J$, donc on a qu'à montrer que $N_JP_J \subseteq P_J$. Comme $N_J = \langle T, n_j : j \in J \rangle$ et $T \subseteq B$, on a qu'à montrer que $n_jP_J \subseteq P_J$ pour tout $j \in J$. Par la propriété $(BN4)$, on a que $n_jBn \subset BnB \cup Bn_jnB$ pour $n \in N_J$. En multipliant par B à droite, on a $n_jBnB \subseteq BnB \cup Bn_jnB \subseteq P_J$. Finalement, en prenant l'union sur les $n \in N_J$, on a $n_jP_J \subseteq P_J$. □

Remarque 2.7. *(P_J, B, N_J, J) est un système de Tits pour P_J.*

Définition 2.6. *On appelle* ***cellules de Bruhat*** *les doubles classes de la forme* $C(w) := Bn_wB$ *pour* $n \in N$ *un représentant de* $w \in W$.

Remarque 2.8. $C(w)$ *ne dépend pas du choix de* n_w. *On peut alors réécrire la condition* $(BN4)$ *comme* $n_sBn_w \subseteq C(w) \cup C(sw)$.

Lemme 2.2. *Soient* $w, w_1, w_2 \in W$ *tels que* $C(w) \subseteq C(w_1) \cup C(w_2)$. *Alors,* $C(w) = C(w_1)$ *ou* $C(w) = C(w_2)$.

Démonstration. Soit n_w un représentant de w. Alors, $n_w \in C(w_i)$ pour un certain $i \in \{1, 2\}$. Alors, $n_w = bn_{w_i}b'$ pour certains $b, b' \in B$. Donc, on a que $C(w) \subseteq C(w_i)$. De plus, on a que $n_{w_i} = b^{-1}n_w(b')^{-1}$, donc $C(w) \supseteq C(w_i)$ et on a le résultat. □

Lemme 2.3. *L'application* $w \mapsto C(w)$ *est une bijection.*

Démonstration. Clairement, cette application est surjective. Il reste à montrer que si $C(y) = C(w)$, alors $y = w$. On procède par induction sur $\min\{l(y), l(w)\}$. Sans perte de généralité, on a que $l(y) \leq l(w)$. Si $l(y) = 0$, alors $y = 1$. Donc, $C(y) = B = Bn_wB$. Donc, $n_w \in B \cap N$ et $w = 1 = y$. Supposons maintenant que $l(y) > 0$. Donc, on peut écrire $y = sx$ où $s \in S$, $x \in W$ et $l(y) = l(x) + 1$. Alors,

$$n_sn_xB \subseteq Bn_sn_xB = Bn_yB = Bn_wB.$$

On note que $n_s^{-1} = n'_{s^{-1}} = n'_s$ est aussi un représentant de s, car $s^{-1} = s$. On a alors l'inclusion $n_xB \subseteq n'_sBn_wB$. Donc, en utilisant $(BN4)$, on a

$$C(x) = Bn_xB \subseteq Bn'_sBn_wB \subseteq Bn'_sn_wB \cup Bn_wB = C(sw) \cup C(w).$$

Par le Lemme 2.2, on a que $C(x) = C(sw)$ ou $C(x) = C(w)$. Par l'hypothèse de récurrence, on a que $x = sw$ ou $x = w$. Or, comme $l(x) = l(y) - 1 < l(w)$, on ne peut pas avoir que $x = w$. Ainsi, $x = sw$ et en multipliant par s à gauche, on trouve $y = w$. □

Théorème 2.4. *Décomposition de Bruhat : On a*

$$G = \bigsqcup_{w \in W} C(w).$$

Démonstration. En prenant $J = S$ dans le Lemme 2.1, on a que BNB est un sous-groupe de G qui contient B et N qui génèrent G, donc $G = BNB$. Ainsi, $G = \bigcup_{w \in W} Bn_wB = \bigcup_{w \in W} C(w)$. Par le Lemme 2.3, on a que $C(y) = C(w) \implies y = w$, donc on a le résultat. □

Remarque 2.9. *On peut donc écrire les* P_J *de la même façon, c'est-à-dire* $P_J = \bigsqcup_{w \in \langle J \rangle} C(w)$.

Proposition 2.2. *Soit $s \in S$ et $w \in W$, alors*

$$C(s)C(w) = \begin{cases} C(sw) & si\ l(sw) = l(w) + 1, \\ C(sw) \cup C(w) & si\ l(sw) = l(w) - 1. \end{cases}$$

Démonstration. Supposons que $l(sw) = l(w)+1$. On procède par induction sur $l(w)$. Si $l(w) = 0$, alors $w = 1$ et $C(s)B = C(s)$. Supposons que $l(w) > 0$. Alors, il existe $t \in S$ et $y \in W$ tels que $w = yt$ et $l(w) = l(y) + 1$. De plus, on a $C(s)C(w) = C(sw)$ ou $n_sBn_w \cap C(w) \neq \emptyset$ par $(BN4)$. Dans le deuxième cas, en multipliant à droite par n_t, on a $n_sBn_y \cap C(w)n_t \neq \emptyset$. Comme $l(sy) = l(y) + 1$, par induction, $n_sBn_y \subseteq C(sy)$. Donc, $C(sy) \cap C(w)n_t \neq \emptyset$. En inversant les relations de $(BN4)$, on a $C(sy) \cap C(wt) \neq \emptyset$ ou $C(sy) \cap C(w) \neq \emptyset$. Ainsi, comme pour la démonstration du Théorème 2.4, on a $sy = wt$ ou $sy = w$. Si $sy = wt$, alors $sy = yt^2 = y$, donc $s = 1$, ce qui est une contradiction. Donc, $sy = w$ et $sw = y$. Donc, $l(y) = l(sw) > l(w)$, une contradiction. Alors, le deuxième cas est faux et $C(s)C(w) = C(sw)$. Supposons maintenant que $l(sw) = l(w) - 1$. Par $(BN4)$, $n_sBn_s \subseteq B \cup C(s)$. Avec $(BN3)$, on obtient $n_sBn_s \cap C(s) \neq \emptyset$. Par conséquent, $n_sB \cap C(s)n_s \neq \emptyset$ et $n_sBn_w \cap C(s)n_sn_w \neq \emptyset$. Alors, comme $l(w) = l(s(sw)) = l(sw) + 1$, on peut appliquer la partie précédente pour sw. Donc, $C(s)n_{sw} \subseteq C(w)$. Ainsi, $n_sBn_w \cap C(w) \neq \emptyset$. Or, $n_sn_w \in C(s)C(w)$. Donc, par $(BN4)$, on a $C(s)C(w) = C(sw) \cup C(w)$. □

Proposition 2.3. *On a que $B = \mathrm{N}_G(B) := \{g \in G : gBg^{-1} = B\}$.*

Démonstration. Clairement, $B \subseteq \mathrm{N}_G(B)$. Soit $g \in \mathrm{N}_G(B)$. Alors, par la décomposition de Bruhat, on peut écrire $g = b_1n_wb_2$ pour $b_1, b_2 \in B$ et $w \in W$. Alors, $n_wBn_w^{-1} = b_1^{-1}gb_2^{-1}Bb_2g^{-1}b_1 = b_1^{-1}gBg^{-1}b_1 = b_1^{-1}Bb_1 = B$, donc $n_w \in \mathrm{N}_G(B)$. Supposons que $w \neq 1$. Alors, il existe $s \in S$ tel que $l(sw) = l(w) - 1$. Comme dans la démonstration de la Proposition 2.2, on a $n_sBn_s \subseteq Bn_sB \cup B$ et donc $n_s \in Bn_wBn_w^{-1}B \subseteq \mathrm{N}_G(B)$. Ainsi, $n_sBn_s = n_sBn_s^{-1} = B$, ce qui contredit $(BN3)$. Donc, $w = 1$ et $g \in B$. □

Proposition 2.4. *Soit $w \in W$ et $s \in S$ tel que $l(sw) = m-1$ où $m = l(w)$. Soit $w = s_1s_2 \cdots s_m$ une expression réduite de w. Alors, il existe $i \in \{1, \cdots, m\}$ tel que*

$$sw = s_1 \cdots s_{i-1}s_{i+1} \cdots s_m.$$

Démonstration. Soit i minimal tel que $ss_1 \cdots s_i$ ne soit pas une expression réduite. Alors, $u := ss_1 \cdots s_{i-1}$ et $v := s_1 \cdots s_i$ sont des expressions réduites et $us_i = sv$. Alors, par la Proposition 2.2, on a

$$\begin{aligned} C(us_i) \cup C(u) &= C(s)C(s_1) \cdots C(s_i) \\ &= C(sv) \cup C(v). \end{aligned}$$

Donc, $C(u) = C(v)$ et par le Lemme 2.3, $u = v$. On a ainsi le résultat. □

Remarque 2.10. *Ce résultat est parfois appelé la condition d'échange et c'est une propriété suffisante pour que la paire (W, S) soit un système de Coxeter.*

Remarque 2.11. *La démonstration de la Proposition 2.4 est toujours valide en supposant que $l(sw) \leq l(w)$. On peut conclure que $l(sw) \leq l(w) - 1$. Donc, on ne peut pas avoir que $l(sw) = l(w)$.*

Proposition 2.5. *Soit $w \in W$ et $H_w = \langle C(w)C(w^{-1})\rangle$. Alors, pour toute décomposition réduite $w = s_1 \cdots s_m$, on a $C(s_i) \subseteq H_w$ pour $1 \leq i \leq m$ et le groupe H_w est engendré par $C(w)$.*

Démonstration. Soit $1 \leq i \leq m = l(w)$ et $t_i = s_1 \cdots s_{i-1} s_i s_{i-1} \cdots s_1$. Posons $w' = s_1 \cdots s_{i-1}$ et $w'' = s_{i+1} \cdots s_m$. Alors, $w = w' s_i w''$, $l(w) = l(w') + l(w'') + 1$ et $t_i = w' s_i (w')^{-1}$. Donc, on a

$$C(w)C(w^{-1}) = C(w')C(s_i)C(w'')C\left((w'')^{-1}\right)C(s_i)C\left((w')^{-1}\right).$$

Alors,

$$C(w')C(s_i)C(s_i)C\left((w')^{-1}\right) \subseteq C(w)C(w^{-1}).$$

Comme $C(s_i) \subseteq B \cup C(s_i) = C(s_i)C(s_i)$, on a

$$C(t_i) \subseteq C(w')C(s_i)C\left((w')^{-1}\right) \subseteq C(w)C(w^{-1}) \subseteq H_w.$$

Comme $s_1 = t_1$, on a $C(s_1) \subseteq H_w$. Supposons que $C(s_j) \subseteq H_w$ pour tout $1 \leq j < i$. Alors, comme $C(t_i) \subseteq H_w$, $C(s_i) \subseteq H_w$ et on a la première partie du résultat. Par la suite, comme $C(w) = C(s_1) \cdots C(s_m)$, on a $C(w) \subseteq H_w$ et $C(w^{-1}) \in \langle C(w)\rangle$, donc $H = \langle C(w)\rangle$. □

2.1.1 Sous-groupes paraboliques

Définition 2.7. *On dit qu'un sous-groupe de G est **parabolique** s'il contient un conjugué de B.*

Remarque 2.12. *Clairement, les P_J du Lemme 2.1 sont des groupes paraboliques, car $B \subseteq P_J$.*

Proposition 2.6. *Soit $w \in W$, $w = s_1 \cdots s_m$ une expression réduite de w et $n_w \in N$ une préimage de w. Pour $J = \{s_1, \cdots, s_m\}$, on a*

$$P_J = \langle B, n_w\rangle = \left\langle B, n_w B n_w^{-1}\right\rangle.$$

Démonstration. Clairement, $\left\langle B, n_w B n_w^{-1}\right\rangle \subseteq \langle B, n_w\rangle \subseteq P_J$. Il reste à montrer que $P_J \subseteq \left\langle B, n_w B n_w^{-1}\right\rangle$. Soit $H_w = \langle C(w)C(w^{-1})\rangle$. Alors, par la Proposition 2.5, $C(s_i) \subseteq H_w$ pour tout $s_i \in J$. Soit $y \in \langle J\rangle$ avec comme expression réduite $y = t_1 \cdots t_n$ pour $t_1, \cdots, t_n \in J$. Alors, $C(y) = C(t_1) \cdots C(t_n) \subseteq H_w$. Comme $P_J = \bigsqcup_{y \in \langle J\rangle} C(y)$ par la Remarque 2.9, $P_J \subseteq H_w$. De plus, $C(w)C(w^{-1}) = Bn_wBn_w^{-1}B$, donc $H_w \subseteq \left\langle B, n_w B n_w^{-1}\right\rangle$ et on a le résultat. □

Proposition 2.7. *Pour tout $w \in W \setminus \{1\}$, on a $w \in S$ si et seulement si $B \cup C(w)$ est un groupe.*

Démonstration. $B \cup C(s)$ est un groupe pour tout $s \in S$. Supposons maintenant que $B \cup C(w)$ soit un groupe. Soit $w = s_1 \cdots s_m$ une expression réduite de w et $J = \{s_1, \cdots, s_m\}$. Alors, par la Proposition 2.6, $P_J = \langle B, n_w B n_w^{-1} \rangle = B \cup C(w)$. Alors, $C(s_1) \subseteq B \cup C(w)$ et par le Lemme 2.2 et le Lemme 2.3, $s_1 = 1$ ou $s_1 = w$ et comme s_1 est d'ordre 2, $w = s_1 \in S$. □

Remarque 2.13. *Cette proposition montre que S est déterminé par G, B et N. Cela justifie l'appellation BN-paire, alors que la définition d'un système de Tits demande de spécifier l'ensemble S.*

Proposition 2.8. *Soit P un sous-groupe de G tel que $B \subseteq P$. Alors, $P = P_J$ pour un certain $J \subseteq S$.*

Démonstration. Soit $J := \{s \in S : C(s) \subseteq P\}$. Alors, $P_J \subseteq P$. Soit $p \in P$. Alors, $BpB = C(w)$ pour un certain $w \in W$ et $C(w) \subseteq P$. Si $s_1 \cdots s_m$ est une expression réduite pour w, alors par la Proposition 2.6, on a $C(s_i) \subseteq P$ pour tout $1 \leq i \leq m$. Donc, $s_i \in J$ et donc $p \in P_J$. Alors, $P = P_J$. □

Proposition 2.9. *Soit P un sous-groupe de G. Alors, P est parabolique si et seulement s'il existe $J \subseteq S$ tel que P est un conjugué de P_J.*

Démonstration. C'est un corollaire direct de la proposition précédente. Soit $g \in G$ tel que $gBg^{-1} \subseteq P$. Alors, $B \subseteq g^{-1}Pg$. Par la Proposition 2.8, il existe $J \subseteq S$ tel que $g^{-1}Pg = P_J$. Alors, $P = gP_Jg^{-1}$. □

Proposition 2.10. *Soit $J \subseteq S$ et $g \in G$ tels que $gBg^{-1} \subseteq P_J$. Alors, $g \in P_J$.*

Démonstration. Soit $w \in W$ tel que $g \in C(w)$. Comme B est un sous-groupe de P_J, l'hypothèse gBg^{-1} entraîne $C(w)C(w^{-1}) \subseteq P_J$. Donc, par la Proposition 2.5,

$$g \in C(w) \subseteq H_w = \langle C(w)C(w^{-1}) \rangle \subseteq P_J.$$

□

Proposition 2.11. *Soient $J_1, J_2 \subseteq S$ et $g_1, g_2 \in G$ tels que $P := g_1 P_{J_1} g_1^{-1} = g_2 P_{J_2} g_2^{-1}$. Alors, $J_1 = J_2$ et $g_2 g_1^{-1} \in P$.*

Démonstration. On a que

$$g_1^{-1} g_2 B g_2^{-1} g_1 \subseteq g_1^{-1} g_2 P_{J_2} g_2^{-1} g_1 = P_{J_1}.$$

Par la Proposition 2.10, $g_1^{-1}g_2 \in P_{J_1}$. Alors, $P_{J_1} = P_{J_2}$ et $J_1 = J_2$. De plus,

$$g_2 g_1^{-1} = g_1 \left(g_1^{-1} g_2\right) g_1^{-1} \in P.$$

□

Lemme 2.5. *Soit P_1 et P_2 deux sous-groupes paraboliques de G dont l'intersection $P := P_1 \cap P_2$ est parabolique et soit $g \in G$ tel que $gP_1g^{-1} \subseteq P_2$. Alors, $g \in P_2$ et $P_1 \subseteq P_2$.*

Démonstration. Soit $h \in G$ tel que $hBh^{-1} \subseteq P$. Soient $J_2 \subseteq S$ et $g_2 \in G$ tels que $P_2 = g_2 P_{J_2} g_2^{-1}$. Alors, $g_2^{-1}hBh^{-1}g_2 \subseteq P_{J_2}$. Par la Proposition 2.10, $g_2^{-1}h \in P_{J_2}$ et donc $hg_2^{-1} \in P_2$. De plus, $ghBh^{-1}g^{-1} \subseteq gP_1g^{-1} \subseteq P_2$, donc $g_2^{-1}ghBh^{-1}g^{-1}g_2 \subseteq P_{J_2}$. Ainsi, $g_2^{-1}gh \in P_{J_2}$ et $ghg_2^{-1} \in P_2$. Donc, $g = \underbrace{ghg_2^{-1}}_{\in P_2}\underbrace{\left(hg_2^{-1}\right)}_{\in P_2}^{-1} \in P_2$. Finalement, $P_1 \subseteq g^{-1}P_2g = P_2$. □

Lemme 2.6. *Soit Q_1 et Q_2 deux sous-groupes paraboliques contenus dans un sous-groupe Q de G. Alors, tout $g \in G$ tel que $gQ_1g^{-1} = Q_2$ appartient à Q.*

Démonstration. Soit $g \in G$ tel que $gQ_1g^{-1} = Q_2$. Alors, $gQ_1g^{-1} \subseteq Q$. Alors, avec $P_1 = Q_1$, $P_2 = Q$ et $Q_1 = P_1 \cap P_2$ dans le Lemme 2.5, on a que $g \in Q$ (et trivialement que $Q_1 \subseteq Q$). □

Théorème 2.7. *Soit P un sous-groupe parabolique de G. Alors, $P = \mathrm{N}_G(P)$.*

Démonstration. Avec $Q_1 = Q_2 = Q = P$ dans le Lemme 2.6, on a que $gPg^{-1} = P$ implique $g \in P$, donc $P = \mathrm{N}_G(P)$. □

Remarque 2.14. *Ce résultat peut servir de preuve alternative pour la Proposition 2.3, car B est parabolique.*

Proposition 2.12. *Soit G un groupe qui admet une BN-paire et soit U un sous-groupe normal de B tel que $B = UT$ et $U \cap T = \{1\}$. Soit $G' \subseteq G$ un sous-groupe normal qui contient U. On pose $B' := B \cap G'$ et $N' := N \cap G'$. Alors, B' et N' forment un système de Tits de G'.*

Démonstration. On a que $G = G'T$. En effet, $B = UT \subseteq G'T$ et comme $N \subseteq \mathrm{N}_G(T)$ et $N \subseteq G = \mathrm{N}_G(G')$, alors $N \subseteq \mathrm{N}_G(G') \cap \mathrm{N}_G(T) \subseteq \mathrm{N}_G(G'T) = G'T$, par le Théorème 2.7. Puisque G est engendré par B et N, $G = G'T$. Comme on a à la fois que $G = BNB$, $T \subseteq N$ et $B = UT = TU$, on trouve que $G = UNU$. Donc, $G' = UN'U$. De plus, comme $U \subseteq B'$, $G' = B'N'B'$, donc $G' = \langle B', N' \rangle$, ce qui vérifie $(BN1)$. De plus, on note que $N'T = NT \cap G'T = N \cap G = N$ et $B'T = BT \cap G'T = B \cap G = B$. Comme $N' \subseteq N \subseteq \mathrm{N}_G(T)$ et $T' = B' \cap N'$, par le deuxième théorème d'isomorphisme, on a que

$$W' := N'/T' = N'/(N' \cap T) \cong N'T/T = N/T =: W.$$

Appelons $\alpha : W' \to W$, $n'T' \mapsto n'T$ l'isomorphisme entre W' et W induit par l'inclusion de N' dans N. Soit $S' := \alpha^{-1}(S)$. Donc, S' est un ensemble composé d'éléments d'ordre 2 qui engendre W' et on a également que $T' = B' \cap N'$ est un sous-groupe normal de N'. Ainsi, $(BN2)$ est vérifié. Soit $w' \in W'$ et $n_{w'}$ un représentant dans N'. Alors, $w' = n_{w'}T'$ et $w := \alpha(w') = n_{w'}T$. En particulier, on peut prendre $n_w = n_{w'}$. Pour la condition $(BN3)$, on suppose qu'il existe $s' \in S'$ tel que $n_{s'}B'n_{s'} \subseteq B'$. Alors, pour $s = \alpha(s')$, on a

$$n_{s'}B'n_{s'}T \subseteq B'T \implies n_{s'}B'Tn_{s'} \subseteq B'T \implies n_sBn_s \subseteq B,$$

ce qui contredit l'hypothèse $(BN3)$ pour le système de Tits de G, ce qui la montre pour G'. Similairement, pour $w' \in W'$ et $w = \alpha(w')$, on a

$$Bn_wB = B'Tn_wB = B'n_wTB = B'n_wB = B'n_{w'}B.$$

On en conclut que $Bn_wB \cap G' = B'n_{w'}B'$. Ainsi, les doubles classes $C(w) = Bn_wB$ de G sont en bijection avec les doubles classes $C(w') = B'n_{w'}B'$ de G', ce qui permet de montrer directement $(BN4)$. □

Remarque 2.15. *Cette proposition est très utile pour définir une BN-paire pour les autres groupes classiques. La proposition suivante est aussi pratique pour définir les BN-paires de Tits sur les groupes classiques projectifs.*

Proposition 2.13. *Soit (G, B, N, S) un système de Tits et soit Z un sous-groupe normal de G contenu dans B. Soient $G' = G/Z$, $B' = B/Z$, $N' = N/(Z \cap N)$ et soit S' l'image de S dans $N'/(B' \cap N')$. Alors, B' et N' forment un système de Tits.*

Démonstration. Les propriétés des BN-paires sont directement respectées par le passage au quotient. □

Remarque 2.16. *Par le troisième théorème d'isomorphisme, on a que $N'/(T/Z \cap N) \cong N/T$, donc le groupe de Weyl reste inchangé.*

Remarque 2.17. *Considérons le système de Tits pour $\mathrm{GL}_n(q)$ défini à la Proposition 2.1. Comme U l'ensemble des matrices unipotentes supérieures est tel que $U \in \mathrm{SL}_n(q)$, on peut utiliser la Proposition 2.12 pour définir une BN-paire sur $\mathrm{SL}_n(q)$. La Proposition 2.13 permet ensuite de définir une BN-paire sur $\mathrm{PSL}_n(q)$.*

Proposition 2.14. *Il existe un unique élément $w_0 \in W$ de longueur maximale. De plus, on a que $w_0^2 = 1$ et w_0 est le seul élément avec la propriété que $l(sw_0) = l(w_0) - 1$ pour tout $s \in S$.*

Démonstration. Comme W est fini, il existe $w_0 \in W$ tel que $l(w) \leq l(w_0)$ pour tout $w \in W$. De plus, par la Remarque 2.6, il est clair que $l(sw_0) = l(w_0) - 1$ pour tout $s \in S$. Montrons d'abord que $l(ww_0) = l(w_0) - l(w)$ pour tout $w \in W$. On procède par récurrence sur $l(w)$. Si

$l(w) = 0$, alors $w = 1$ et le résultat est montré automatiquement. Supposons que le résultat est vrai pour $l(w) \leq m$ et supposons que $l(w) = m + 1$. Soit $w = s_1 \cdots s_m s$ pour $s_i, s \in S$ une expression réduite de w. Soit $w' = s_1 \cdots s_m w_0$. Alors, $l(w') = l(w_0) - m =: q$ par l'hypothèse de récurrence. Soit $w' = t_1 \cdots t_q$ une expression réduite de w'. Alors,

$$w_0 = s_m \cdots s_1 t_1 \cdots t_q$$

est une expression réduite de w_0. Par la Proposition 2.4, on a deux possibilités :

$$sw_0 = s_m \cdots s_{i+1} s_{i-1} \cdots s_1 t_1 \cdots t_q \text{ pour un certain } i \in \{1, \cdots, m\} \tag{2.1}$$

$$sw_0 = s_m \cdots s_1 t_1 \cdots t_{j-1} t_{j+1} \cdots t_q \text{ pour un certain } j \in \{1, \cdots, q\} \tag{2.2}$$

Si l'équation 2.1 est vraie, alors $ss_m \cdots s_1 = s_m \cdots s_{i+1} s_{i-1} \cdots s$ et $l\left(w^{-1}\right) = m - 1$, mais $l\left(w^{-1}\right) = l(w) = m$, ce qui est une contradiction. Donc, 2.2 est vraie et $ww_0 = t_1 \cdots t_{j-1} t_{j+1} \cdots t_q$. Ainsi, $l(ww_0) = q - 1 = l(w_0) - (m + 1) = l(w_0) - l(w)$.

En posant $w = w_0$, on a que $l\left(w_0^2\right) = 0$, donc $w_0^2 = 1$. Supposons maintenant que $w \in W$ soit un autre élément tel que $l(w) = l(w_0)$. Alors, $l(ww_0) = 0$, donc $ww_0 = 1$ et $w = w_0^{-1} = w_0$.

Finalement, supposons que $w \in W$ soit tel que $l(sw) = l(w) - 1$ pour tout $s \in S$. Supposons que $l(w) < l(w_0)$. Alors, $l(ww_0) = l(w_0) - l(w) > 0$. Alors, par la Remarque 2.6, il existe $s \in S$ tel que $l(sww_0) = l(ww_0) - 1$. Alors, $l(w_0) - l(sw) = l(w_0) - l(w) - 1$ et $l(sw) = l(w) + 1$, une contradiction. Donc, $l(w) = l(w_0)$ et $w = w_0$ par la partie précédente. □

Remarque 2.18. *Pour la BN-paire de* $\mathrm{GL}_n(q)$ *décrite à la Proposition 2.1 où* $W \cong S_n$ *et* $S = \{(i, i+1) : i \in \{1, \cdots, n-1\}\}$, *on a que* $w_0 = (1, n)(2, n-1)(3, n-2) \cdots (\lfloor n/2 \rfloor, \lceil n/2 \rceil + 1)$. *Un calcul direct montre que* $l(w_0) = n(n-1)/2$.

Théorème 2.8. *Soit* G *un groupe admettant une BN-paire scindée telle que* W *soit fini. Posons*

$$U_w := U \cap n_{w_0 w}^{-1} U n_{w_0 w}$$

pour $w \in W$. *Alors, chaque élément* $g \in Bn_w B$ *s'écrit de manière unique comme* $g = bn_w u$ *avec* $b \in B$, $w \in W$ *et* $u \in U_w$. *Alors, on peut écrire*

$$G = \bigsqcup_{w \in W} Bn_w U_w.$$

De plus, on a $U_w \neq \{1\}$ *pour tout* $1 \neq w \in W$.

La démonstration de ce résultat est omise et se trouve au Théorème 1.6.19 dans [3].

Définition 2.8. *Cette décomposition de* G *est appelée la* ***forme précise*** *de la décomposition de Bruhat.*

Remarque 2.19. *Les* U_w *ne dépendent pas du choix de représentant* n_w.

2.2 Automorphismes et application de Frobenius

En plus des Propositions 2.12 et 2.13, on présente d'autres résultats qui permettent de définir des BN-paires sur les autres groupes classiques étudiés. La plupart des résultats de cette section sont résumés, les détails sont dans [3], en particulier de la section 1.7 et du chapitre 4.

Soit G un groupe admettant une BN-paire scindée telle que son groupe de Weyl W soit fini et $\varphi : G \to G$ un automorphisme de groupes qui satisfait les propriétés suivantes :
$(BN^\varphi 1)$ $\varphi(N) = N$, $\varphi(U) = U$ et $\varphi(T) = T$.
$(BN^\varphi 2)$ Toute classe $nT \in W$ telle que $\varphi(nT) \subseteq nT$ contient un élément fixé par φ.

Une conséquence directe de $(BN^\varphi 1)$ est que $\varphi(B) = \varphi(U)\varphi(T) = UT = B$. Soit $G^\varphi := \{g \in G : \varphi(g) = g\}$ le groupe des points de G fixés par φ. On définit B^φ, N^φ, U^φ et T^φ. Ce sont des sous-groupes de G^φ. Naturellement, on a que $T^\varphi = B^\varphi \cap N^\varphi$. De plus, comme la BN-paire est scindée, on a une décomposition de B^φ similaire à celle de B, c'est-à-dire

$$B^\varphi = U^\varphi T^\varphi \text{ et } U^\varphi \cap T^\varphi = \{1\}\,. \tag{2.3}$$

De plus, pour tout $n \in N^\varphi$, on a que $n^{-1}U^\varphi n \cap B^\varphi \subseteq U^\varphi$. Soit

$$\begin{aligned} \overline{\varphi}\colon W &\to W \\ nT &\mapsto \varphi(n)T \end{aligned}$$

un homomorphisme induit. Comme $\varphi(N) = N$, $\overline{\varphi}$ est surjectif et puisque W est fini, $\overline{\varphi}$ est également bijectif, donc un isomorphisme. Alors, $\overline{\varphi}$ permute les cellules de Bruhat de sorte que $\varphi(C(w)) = C(\overline{\varphi}(w))$ pour tout $w \in W$. Soit $s \in S$. Alors, $\varphi(B \cup C(s)) = B \cup C(\overline{\varphi}(s))$ est un sous-groupe de G, donc par la Proposition 2.7, $\overline{\varphi}(s) \in S$. Ainsi, $\overline{\varphi}(S) = S$. Soit

$$\begin{aligned} \psi\colon N^\varphi/T^\varphi &\to W\,. \\ nT^\varphi &\mapsto nT \end{aligned}$$

ψ est un homomorphisme injectif et son image est égale à $W^{\overline{\varphi}}$ par $(BN^\varphi 2)$. Alors, par le premier théorème d'isomorphisme, $W^{\overline{\varphi}} \cong N^\varphi/T^\varphi$. Soit $\overline{S} := \{\mathrm{Orb}(s) : s \in S\}$ où $\mathrm{Orb}(s) = \{\overline{\varphi}^n(s) : n \in \mathbb{Z}_{\geq 1}\} \subseteq S$ appelé l'ensemble des orbites de $\overline{\varphi}$ sur S. Pour tout $J \in \overline{S}$, on considère $W_J := \langle J \rangle \subseteq W$ comme au Lemme 2.1. Alors, par la Remarque 2.7 et la Proposition 2.14, il existe un unique élément de longueur maximale $w_J \in W_J$ et il est d'ordre 2. De plus, $\overline{\varphi}(w_J) \in W_J$ est un élément de longueur maximale dans W_J, car $\overline{\varphi}$ laisse S invariant. Par l'unicité de w_J, $\overline{\varphi}(w_J) = w_J$, donc $w_J \in W^{\overline{\varphi}}$ pour tout $J \in \overline{S}$. Soit $\mathcal{J} := \left\{w_J : J \in \overline{S}\right\}$. On peut montrer sans difficulté que $W^{\overline{\varphi}} = \langle \mathcal{J} \rangle$.

Ainsi, $(G^\varphi, B^\varphi, N^\varphi, \mathcal{J})$ est un candidat pour être un système de Tits. Or, il reste une dernière condition technique qui est que $U^\varphi_{w_J} \neq \{1\}$ pour tout $J \in \overline{S}$ où U_{w_J} suit la définition donnée au Théorème 2.8. Elle est nécessaire pour montrer l'axiome $(BN3)$ de la Définition 2.3. L'équation 2.3 montre que cette BN-paire est scindée.

Voici trois exemples d'automorphismes $\varphi : G \to G$ pour $G = \mathrm{GL}_n(k)$ avec la BN-paire de la Proposition 2.1. Ces exemples viennent de l'Exemple 1.7.3 et du Théorème 1.7.4 de [3].

Exemple 1. *Supposons que $n = 2m$ et soit*

$$\begin{aligned} \varphi\colon G &\to G \\ M &\mapsto A^{-1}\left(M^t\right)^{-1}A \end{aligned}$$

où $A = \begin{pmatrix} 0_m & Q_m \\ -Q_m & 0_m \end{pmatrix}$ avec $Q_m = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$ est la matrice associée à une forme symplectique f avec la base $\{e_1, \cdots, e_m, f_m, \cdots, f_1\}$. Alors, par la Remarque 1.17, $G^\varphi = \mathrm{Sp}_{2m}(k)$. On a que $A \in N$ et est une préimage de w_0 par la Remarque 2.18. Donc, $\overline{\varphi} : W \to W$ est donné par la conjugaison par $w_0 = (1,n)(2,n-1)\cdots(m,m+1)$. On rappelle que $S = \{(i,i+1) : i \in \{1, \cdots, 2m-1\}\}$, donc

$$\overline{S} = \{\{(1,2),(2m-1,2m)\}, \cdots, \{(m-1,m),(m+1,m+2)\}, \{(m,m+1)\}\}.$$

Posons $J_i = \{(i,i+1),(2m-i,2m-i+1)\}$ pour $i \in \{1, \cdots, m-1\}$ et $J_m = \{(m,m+1)\}$. Posons également $s_i = w_{J_i}$ pour $i \in \{1, \cdots, m-1\}$ et $t = w_{J_m}$. Alors, comme les transpositions impliquées sont disjointes, $s_i = (i,i+1)(2m-i,2m-i+1)$. De plus, $t = (m,m+1)$ et $\mathcal{J} = \{t, s_{m-1}, \cdots, s_1\}$. Afin de construire le graphe de Coxeter associé à $\left(W^{\overline{\varphi}}, \mathcal{J}\right)$, on suit la procédure de la Remarque 2.2. On a que $m(t, s_{m-1}) = 4$, $m(t, s_i) = 2$ pour $i \leq m-2$, $m(s_i, s_{i+1}) = 3$ pour tout i et $m(s_i, s_j) = 2$ si $|i-j| \geq 2$. Donc, le graphe de Coxeter est de type B_m. La Table 2.1 présente les types des graphes de Coxeter qui apparaissent dans l'étude des groupes finis simples de type Lie. Les hypothèses $(BN^\varphi 1)$ et $(BN^\varphi 2)$ sont vérifiées et $U_{s_i}^\varphi \neq \{I_{2m}\}$. De plus,

$$U_t = U \cap n_{w_0 t}^{-1} U n_{w_0 t} = \{I_{2m} + \lambda E_{m,m+1} : \lambda \in \mathbb{F}_q\} \quad \text{où } n_{w_0 t} = \begin{pmatrix} 0 & 0 & 0 & Q_{m-1} \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ -Q_{m-1} & 0 & 0 & 0 \end{pmatrix}$$

et $U_t^\varphi = U_t \neq \{I_{2m}\}$. On aura que B^φ et N^φ forment une BN-paire scindée pour $G^\varphi = \mathrm{Sp}_{2m}(k)$.

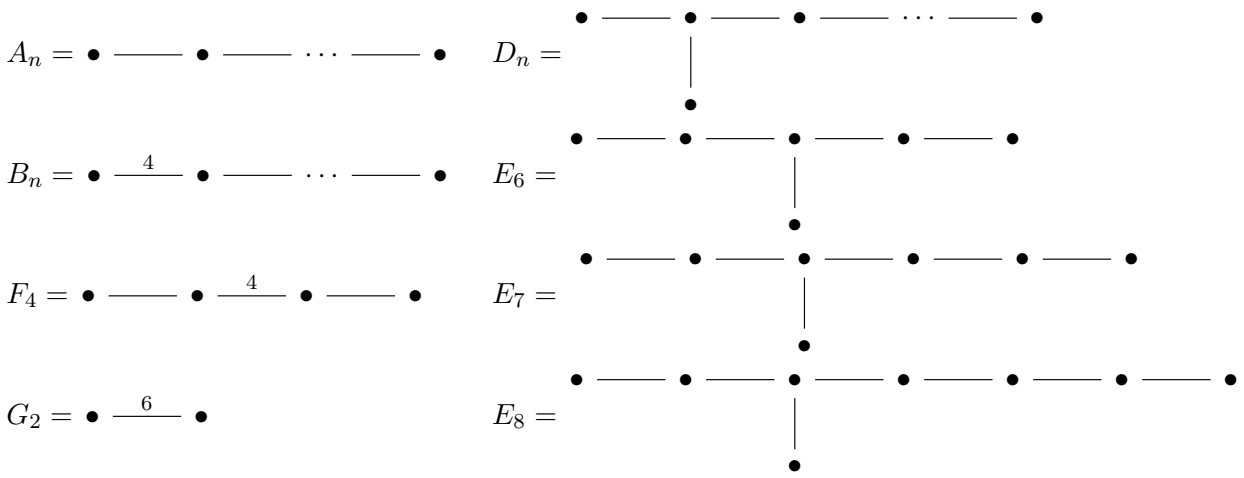


TABLE 2.1 – Liste des graphes de Coxeter associés aux groupes finis simples de type Lie

Remarque 2.20. *Dans la Table 2.1, l'indice représente le nombre de sommets. De plus, pour expliciter le lien entre les graphes de Coxeter et les diagrammes de Dynkin, on pose $C_n := B_n$, car il n'y a pas d'arête dirigée dans les graphes de Coxeter.*

Exemple 2. *Supposons maintenant que q soit impair avec encore $n = 2m$. En caractéristique 2, la construction est différente, mais le résultat est similaire. Soit*

$$\begin{array}{rccc} \varphi\colon & G & \to & G \\ & M & \mapsto & Q_{2m}^{-1}(M^t)^{-1}Q_{2m} \end{array}.$$

On a que Q_{2m} peut être la matrice associée à la forme f de $\mathrm{GO}_{2m}^+(k)$. Alors, par la Remarque 1.28, $G^\varphi = \mathrm{GO}_{2m}^+(k)$. Comme pour l'exemple précédent, $\overline{\varphi} : W \to W$ est donné par la conjugaison par w_0. Or, $\mathcal{J} = \{t, s_{m-1}, \cdots, s_1\}$ ne permet pas d'avoir une BN-paire. En effet, on a encore que les hypothèses $(BN^\varphi 1)$ et $(BN^\varphi 2)$ sont vérifiées, que $U_{s_i}^\varphi \neq \{I_{2m}\}$ et que

$$U_t = U \cap n_{w_0 t}^{-1} U n_{w_0 t} = \{I_{2m} + \lambda E_{m,m+1} : \lambda \in k\} \text{ où } n_{w_0 t} = \begin{pmatrix} 0 & 0\,0 & Q_{m-1} \\ 0 & 1\,0 & 0 \\ 0 & 0\,1 & 0 \\ Q_{m-1} & 0\,0 & 0 \end{pmatrix}.$$

Or, pour tout $u = I_{2m} + \lambda E_{m,m+1} \in U_t$, $\varphi(u) = I_{2m} - \lambda E_{m,m+1}$. Donc, $U_t^\varphi = \{I_{2m}\}$. Il faut alors faire un peu plus de travail afin d'avoir un système de Tits. On considère plutôt le groupe de Weyl W' engendré par $\mathcal{J}' = \{u, s_{m-1}, \cdots, s_1\}$ où $u = ts_{m-1}t$. Ainsi, en plus des relations sur les s_i énoncées à l'Exemple 1, on a que $m(u, s_{m-1}) = 2$, $m(u, s_{m-2}) = 3$ et $m(u, s_i) = 2$ pour $i \in \{1, \cdots, m-2\}$. Donc, le système de Coxeter $(W', \mathcal{J}')$ est de type D_m. On a maintenant que $U_u^\varphi \neq \{I_{2m}\}$. Soit N' la préimage de W' dans N^φ. Alors, $(G^\varphi, B^\varphi, N', \mathcal{J}')$ est un système de Tits pour $G^\varphi = \mathrm{GO}_{2m}^+(k)$.

Exemple 3. *Supposons maintenant que $n = 2m + 1$ avec encore q impair. Soit*

$$\begin{array}{rccc} \varphi\colon & G & \to & G \\ & M & \mapsto & Q_{2m+1}^{-1}(M^t)^{-1}Q_{2m+1} \end{array}.$$

On a que Q_{2m+1} peut être la matrice associée à la forme f de $\mathrm{GO}_{2m+1}(k)$. Alors, par la Remarque 1.28, $G^\varphi = \mathrm{GO}_{2m+1}(k)$. Similairement aux exemples précédents, $\overline{\varphi} : W \to W$ est donné par la conjugaison par $w_0 = (1, 2m+1)(2, 2m)\cdots(m, m+2)$. Donc,

$$\overline{S} = \{\{(1,2), (2m, 2m+1)\}, \cdots, \{(m-1, m), (m+2, m+3)\}, \{(m, m+1), (m+1, m+2)\}\}.$$

Posons $J_i = \{(i, i+1), (2m+1-i, 2m+1-i+1)\}$ pour $i \in \{1, \cdots, m\}$. Posons également $s_i = w_{J_i}$ pour $i \in \{1, \cdots, m-1\}$ et $t = w_{J_m}$. Alors, $s_i = (i, i+1)(2m+1-i, 2m+1-i+1)$ et $t = (m, m+1)(m+1, m+2)(m, m+1)$. On a alors les mêmes relations que l'Exemple 1, alors $W^{\overline{\varphi}}$ est également de type B_m. On a également que toutes les hypothèses nécessaires sont vérifiées, donc B^φ et N^φ forment une BN-paire pour $G^\varphi = \mathrm{GO}_{2m+1}(k)$. On ne considère pas le cas où q est pair, comme à la Remarque 1.33.

Nous pouvons considérer les BN-paires sur $\mathrm{SL}_n(k)$, $\mathrm{SO}^+_{2m}(k)$, $\Omega^+_{2m}(k)$, $\mathrm{SO}_{2m+1}(k)$ et $\Omega_{2m+1}(k)$s obtenus à partir des exemples précédents et de la Proposition 2.12. Pour la suite, on a besoin d'un automorphisme sur la clôture algébrique afin de construire les BN-paires sur tous les groupes classiques finis.

Définition 2.9. *Soit p un premier. On appelle la* ***clôture algébrique*** *de $\mathbb{F}_p$ le corps défini par*

$$k := \bigcup_{a=1}^{\infty} \mathbb{F}_{p^a}$$

Pour le reste du chapitre, k sera la clôture algébrique de $\mathbb{F}_p$ pour un certain p premier.

Définition 2.10. *Soit $a \geq 1$ et $q = p^a$. On appelle l'automorphisme*

$$\begin{array}{rccc} F_q\colon & k^n & \to & k^n \\ & \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} & \mapsto & \begin{pmatrix} x_1^q \\ \cdots \\ x_n^q \end{pmatrix} \end{array}$$

*l'**application de Frobenius standard**.*

Remarque 2.21. *Pour $a \geq 1$ et $q = p^a$, on a que $k^{F_q} = \mathbb{F}_q$ est l'unique sous-corps de k avec q éléments.*

Définition 2.11. *L'application*

$$\begin{array}{rccc} F_q\colon \mathrm{GL}_n(k) & \to & \mathrm{GL}_n(k) \\ (a_{ij}) & \mapsto & \left(a_{ij}^q\right) \end{array}$$

*s'appelle également l'**application de Frobenius standard**.*

Remarque 2.22. *On a que*

$$\begin{array}{ll} \mathrm{GL}_n(k)^{F_q} = \mathrm{GL}_n(q), & \\ \mathrm{SL}_n(k)^{F_q} = \mathrm{SL}_n(q), & GO^+_{2m}(k)^{F_q} = \mathrm{GO}^+_{2m}(q), \\ \mathrm{Sp}_{2m}(k)^{F_q} = \mathrm{Sp}_{2m}(q), & \mathrm{GO}_{2m+1}(k)^{F_q} = \mathrm{GO}_{2m+1}(q), \end{array}$$

Définition 2.12. *Soit $F' : \mathrm{GL}_n(k) \to \mathrm{GL}_n(k)$ un automorphisme. S'il existe un $m \in \mathbb{Z}_{\geq 1}$ tel que $(F')^m = F_{q^m}$, alors F' est appelé un* ***Frobenius généralisé****.*

Voici les deux exemples de groupes classiques finis qui nécessitent l'utilisation d'un Frobenius généralisé afin d'obtenir leur BN-paire à partir de celle de $\mathrm{GL}_n(k)$.

Exemple 4. *Soit*

$$\begin{aligned}\gamma\colon \mathrm{GL}_n(k) &\to \mathrm{GL}_n(k) \\ M &\mapsto Q_n^{-1}(M^t)^{-1}Q_n\end{aligned}.$$

Alors, on a que $\gamma \circ F_q = F_q \circ \gamma$ *et* γ^2 *est l'identité. Soit* $F' := F_q \circ \gamma$*, donc* F' *est un Frobenius généralisé. Alors,* $(F')^2 = F_{q^2}$*. Ainsi,* $\mathrm{GL}_n(k)^{F'} \subseteq \mathrm{GL}_n\left(q^2\right)$*. La restriction de* F_q *à* $\mathrm{GL}_n\left(q^2\right)$ *est un automorphisme d'ordre 2 correspondant à la conjugaison de la Définition 1.20. Alors, comme* $F_q(Q_n) = Q_n$*,*

$$\begin{aligned}F'\colon \mathrm{GL}_n(q^2) &\to \mathrm{GL}_n(q^2) \\ M &\mapsto Q_n^{-1}\left(\overline{M}^t\right)^{-1}Q_n\end{aligned}.$$

Ainsi, $\mathrm{GL}_n(k)^{F'} = \mathrm{GU}_n(q)$*. Par une construction analogue à celle des Exemples 2 et 3, on aura que* $B^{F'}$ *et* $N^{F'}$ *forment une BN-paire pour* $\mathrm{GU}_n(q)$*. Pour le système de Coxeter,* γ *induit encore la conjugaison par* w_0*, envoyant* $(1,2)$ *à* $(n-1,n)$*, et cetera. Puisqu'il y a une torsion dans le Frobenius, on dira que le groupe de Weyl de la BN-paire est de type* ${}^2A_{n-1}$*, où le* 2 *représente la puissance à laquelle on élève* F' *pour obtenir un Frobenius standard.*

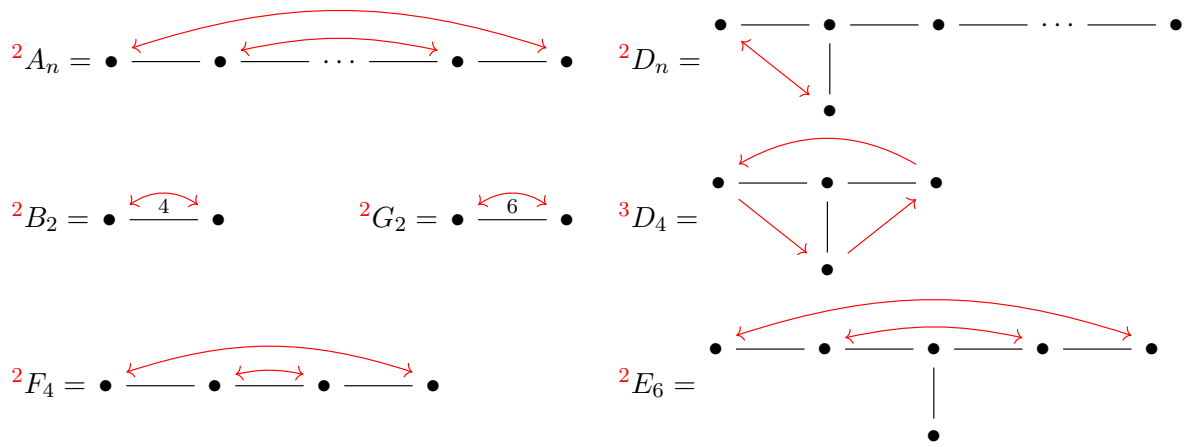


TABLE 2.2 – Torsions possibles dans les graphes de la Table 2.1

Remarque 2.23. *Les torsions sont en général la composition d'un automorphisme sur le graphe de Coxeter et un automorphisme du corps ambiant.*

Exemple 5. *Soit* $n_t = \begin{pmatrix} I_{m-1} & 0\,0 & 0 \\ 0 & 0\,1 & 0 \\ 0 & 1\,0 & 0 \\ 0 & 0\,0 & I_{m-1} \end{pmatrix}$ *qui est une préimage de* t *dans le contexte de l'Exemple 2. Supposons que* q *soit impair. Considérons*

$$\begin{aligned}F'\colon \mathrm{SO}^+_{2m}(k) &\to \mathrm{SO}^+_{2m}(k) \\ M &\mapsto n_t^{-1}F_q(M)n_t\end{aligned}.$$

Alors, comme $n_t^2 = 1$*,* $(F')^2 = F_{q^2}$ *et donc* $\mathrm{SO}^+_{2m}(k)^{F'} \subseteq \mathrm{SO}^+_{2m}(q^2)$*. Afin de réaliser* $\mathrm{SO}^+_{2m}(k)^{F'}$ *sur* $\mathbb{F}_q$*, une conjugaison spéciale est nécessaire. Soit* $\hat{y} = \begin{pmatrix} 1 & 1 \\ \overline{\alpha} & \alpha \end{pmatrix}$ *pour un certain* $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$*.*

Alors,

$$\hat{y}^{-1}F_q(\hat{y}) = \frac{1}{\alpha-\overline{\alpha}}\begin{pmatrix}\alpha & -1\\ -\overline{\alpha} & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ \alpha & \overline{\alpha}\end{pmatrix} = \frac{1}{\alpha-\overline{\alpha}}\begin{pmatrix}0 & \alpha-\overline{\alpha}\\ \alpha-\overline{\alpha} & 0\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$

Posons $y = \begin{pmatrix} I_{m-1} & 0 & 0\\ 0 & \hat{y} & 0\\ 0 & 0 & I_{m-1}\end{pmatrix}$. *Alors,* $y^{-1}F_q(y) = n_t^{-1}(= n_t)$. *Soit* $g \in \mathrm{SO}_{2m}^+(k)$ *et* $h = ygy^{-1}$. *Montrons que* $g \in \mathrm{SO}_{2m}^+(k)^{F'}$ *si et seulement si* $h \in \mathrm{SO}_{2m}^-(q)$. *Supposons que* $g = F'(g)$. *Alors,* $g = n_t^{-1}F_q(g)n_t$ *et donc* $F_q(g) = n_t g n_t^{-1}$. *Ainsi,*

$$\begin{aligned}F_q(h) &= F_q(y^{-1}gy) = F_q(y)F_q(g)F_q(y)^{-1}\\ &= (yn_t^{-1})(n_t g n_t^{-1})(n_t y^{-1})\\ &= ygy^{-1} = h.\end{aligned}$$

Donc, $h \in \mathrm{GL}_{2m}(q)$. *Soit* Q_{2m} *la matrice associée à la forme* f *de* $\mathrm{SO}_{2m}^+(q^2)$. *Alors, comme* $g^tQ_{2m}g = Q_{2m}$, *on trouve*

$$(y^{-1}hy)^tQ_{2m}(y^{-1}hy) = Q_{2m} \text{ et } h^ty^{-t}Q_{2m}y^{-1}h = y^{-t}Q_{2m}y^{-1}$$

Soit $\delta := \alpha - \overline{\alpha}$. *On pose*

$$A' := y^{-t}Q_{2m}y^{-1} = \begin{pmatrix} 0 & 0 & 0 & Q_{m-1}\\ 0 & -2\alpha\overline{\alpha}/\delta^2 & \alpha+\overline{\alpha}/\delta^2 & 0\\ 0 & \alpha+\overline{\alpha}/\delta^2 & -2/\delta^2 & 0\\ Q_{m-1} & 0 & 0 & 0\end{pmatrix}.$$

Ainsi, $h^tA'h = A'$ *et* A' *définit une forme symétrique non singulière. Comme*

$$\overline{(\alpha-\overline{\alpha})^2} = (\alpha-\overline{\alpha})^2, \overline{(\alpha\overline{\alpha})} = \alpha\overline{\alpha} \text{ et } \overline{\alpha+\overline{\alpha}} = \alpha+\overline{\alpha},$$

A' *est défini sur* $\mathbb{F}_q$. *De plus,* $\det A' = (\det y)^{-2}\det Q_{2m}$. *Comme*

$$\det n_t = -1, \det F_q(y) = (\det y)^q \text{ et } y^{-1}F_q(y) = n_t^{-1},$$

on a $(\det y)^{q-1} = -1$. *Ainsi,* $\left((\det y)^{-2}\right)^{(q-1)/2} = (\det y)^{-(q-1)} = -1 \neq 1$, *car* q *est supposé impair. Donc,* $(\det y)^{-2}$ *n'est pas un carré. Alors,* $\operatorname{disc} A' \neq \operatorname{disc} Q_{2m}$. *Comme* Q_{2m} *défini une forme de type plus,* A' *défini une forme de type moins. Donc,* $h \in \mathrm{SO}_{2m}^-(q)$. *Supposons maintenant que* $h \in \mathrm{SO}_{2m}^-(q)$. *Alors,*

$$\begin{aligned}F'(g) &= F'(y^{-1}hy) = n_t^{-1}F_q(y)^{-1}F_q(h)F_q(y)n_t\\ &= y^{-1}hy = g.\end{aligned}$$

Donc, $g \in \mathrm{SO}_{2m}^+(k)^{F'}$. *Ainsi,* $\mathrm{SO}_{2m}^+(k)^{F'} \cong \mathrm{SO}_{2m}^-(q)$ *avec* $B^{F'}$ *et* $N^{F'}$ *qui forment une* BN*-paire où* B *et* N *forment la* BN*-paire de* $\mathrm{SO}_{2m}^+(k)$ *de l'Exemple 2.*

On rappelle que, dans l'Exemple 2, le groupe de Weyl W' de $\mathrm{SO}^+_{2m}(k)$ est engendré par $\mathcal{J}' = \{u, s_{m-1}, \cdots, s_1\}$ où $u = ts_{m-1}t$ et est de type D_m. L'automorphisme du graphe de Coxeter du Frobenius généralisé F' est donné par la conjugaison par t. Appelons cette conjugaison c_t. Alors, $c_t(u) = s_{m-1}$, $c_t(s_{m-1}) = u$ et $c_t(s_i) = s_i$ pour tout $i < m-1$. Donc, c_t permute u et s_{m-1}. Ainsi, le groupe de Weyl de $\mathrm{SO}^-_{2m}(q)$ est de type ${}^2D_m$.

Remarque 2.24. *L'existence d'un y tel que $y^{-1}F_q(y) = n_t$ aurait pu être obtenue à l'aide du puissant Théorème de Lang-Steinberg, mais dans ce cas particulier, il est assez simple d'exhiber un tel y.*

Chapitre 3

Théorèmes de simplicité

3.1 Lemme d'Iwasawa

Proposition 3.1. *Soit G un groupe agissant de manière transitive sur un ensemble X. Soit $G_x = \{g \in G : g.x = x\}$ le stabilisateur d'un élément $x \in X$. Alors, l'action de G sur X est primitive si et seulement si G_x est un sous-groupe maximal de G.*

Démonstration. On procède par contraposée. Si G_x n'est pas maximal, alors il existe un sous-groupe H tel que $G_x < H < G$. Soit $y \in X$. Comme l'action est transitive, il existe $g_y \in G$ tel que $g_y.x = y$. Alors, les points $y \in X$ sont en bijection avec les classes à gauche modulo G_x via l'application $y \mapsto g_y G_x$. Les classes à gauche modulo H sont des unions de classes à gauche modulo G_x et représentent des sous-ensembles de X de cardinalité au moins 2. Comme l'action de G préserve les classes à gauche modulo H, les sous-ensembles de X associés forment un système d'imprimitivité pour G sur X. Réciproquement, si l'action de G sur X est imprimitive, alors il existe un système d'imprimitivité $\{Y_i\}$. Sans perte de généralité, $x \in Y_1$. Soit $G_{Y_1} = \{g \in G : gY_1 = Y_1\}$. Clairement, $G_x \subseteq G_{Y_1}$. Comme l'action de G est transitive et que $|Y_1| \geq 2$, il existe $y \in Y_1$ tel que $y \neq x$ et il existe $g \in G$ tel que $g.y = x$. Ainsi, $G_x \subsetneq G_{Y_1}$. De plus, pour $z \in Y_2$, il existe $g \in G$ tel que $g.y = z$, donc $G_{Y_1} \subsetneq G$. Ainsi, G_x n'est pas maximal. □

Les résultats suivants proviennent de [9].

Théorème 3.1. *(Lemme d'Iwasawa) Soit G un groupe agissant de manière fidèle et primitive sur X un ensemble avec au moins deux éléments. On suppose que G est parfait, c'est-à-dire que $G = \langle aba^{-1}b^{-1} : a, b \in G \rangle = G'$, et on suppose que pour $x \in X$, le stabilisateur G_x admet un sous-groupe normal K résoluble tel que $\{gKg^{-1} : g \in G\}$ engendre G. Alors, G est simple.*

Démonstration. Soit H un sous-groupe normal non trivial de G. H ne fixe pas tous les points de X, on peut donc choisir x tel que $H \not\subseteq G_x$. Par la proposition 3.1, G_x est un sous-groupe maximal de G, donc $G = HG_x$. Ainsi, $g \in G$ peut s'écrire comme $g = hg_x$ où $h \in H$ et $g_x \in G_x$. Donc, $gKg^{-1} = hg_xKg_x^{-1}h^{-1} = hKh^{-1} \subseteq KH$. Donc, $KH = G$. Ainsi, $G/H = KH/H \cong K/(K \cap H)$ par le deuxième théorème d'isomorphisme. Comme K est résoluble, G/H l'est aussi. Or, G est engendré par les commutateurs, donc G/H aussi. Donc, $[G/H, G/H] = G/H$ est trivial, $H = G$ et G est simple. □

Remarque 3.1. *Comme une action doublement transitive implique une action primitive (voir la Proposition B.1 en annexe) et comme un groupe abélien est résoluble, on utilisera parfois le Lemme d'Iwasawa en montrant que l'action de G est doublement transitive et l'existence d'un K abélien.*

Simplicité de $\mathrm{PSL}_n(q)$

Lemme 3.2. $\mathrm{PSL}_2(2) \cong S_3$ *et* $\mathrm{PSL}_2(3) \cong A_4$. *Donc, ces groupes ne sont pas simples.*

Démonstration. Soit $q = 2$ ou 3. On considère l'action naturelle de $\mathrm{GL}_2(q)$ sur l'ensemble X des sous-espaces de $\mathbb{F}_q^2$ de dimension 1 de sorte que le noyau de l'action se réduit à l'ensemble des matrices scalaires, c'est-à-dire $Z(\mathrm{GL}_2(q))$. Cette action induit une action fidèle de $\mathrm{PGL}_2(q) := \mathrm{GL}_2(q)/Z(\mathrm{GL}_2(q))$ sur X. Comme $|X| = q+1$ et que l'action est fidèle, il y a un homomorphisme injectif de $\mathrm{PGL}_2(q)$ à S_{q+1}. Pour $q = 2$, $|\mathrm{PGL}_2(2)| = |\mathrm{PSL}_2(2)| = (2^2-1)(2^2-2) = 6$ et $|S_3| = 3! = 6$, donc $\mathrm{PSL}_2(2) \cong S_3$, qui n'est pas simple, car A_3 est un sous-groupe normal de S_3. Pour $q = 3$, $|\mathrm{PGL}_2(3)| = (3^2-1)(3^2-3)/(3-1) = 24$ et $|S_4| = 24$, donc $\mathrm{PGL}_2(3) \cong S_4$. De plus, $\mathrm{PSL}_2(3)$ est un sous-groupe normal d'indice 2 dans $\mathrm{PGL}_2(3)$ et A_4 est l'unique sous-groupe normal d'indice 2 dans S_4, donc $\mathrm{PSL}_2(3) \cong A_4$, qui n'est pas simple par la Proposition 1.2 □

Définition 3.1. *Une* ***transvection*** *est un élément de* $\mathrm{SL}_n(q) \setminus \{I_n\}$ *laissant fixe un hyperplan.*

Remarque 3.2. *En particulier, dans une base convenable, la matrice d'une transvection peut s'écrire comme $I_n + E_{ij}$ avec $i \neq j$ et E_{ij} une matrice nulle sauf pour un 1 à la position ij. Une transvection peut s'écrire comme*

$$T_v(\lambda) : x \mapsto x + \lambda f(x)v$$

où $v \in \mathbb{F}_q^n$ non nul, f est une forme linéaire non nulle telle que $v \in \ker f$ et $\lambda \neq 0$.

Lemme 3.3. *Les transvections engendrent* $\mathrm{SL}_n(q)$.

Démonstration. On montre d'abord que pour $x, y \in \mathbb{F}_q^n$ non nuls, il existe un produit de transvections t tel que $t(x) = y$. Si x et y ne sont pas colinéaires, on choisit $v = y - x$ et f une forme linéaire nulle sur v, mais non nulle sur x. On pose $\lambda = f(x)$. On a alors

$T_v(\lambda^{-1})(x) = x + \lambda^{-1}f(x)(y-x) = y$, donc on prend $t = T_v(\lambda^{-1})$. Si x et y sont colinéaires, on passe par un troisième vecteur z non colinéaire et deux transvections $t_1(z) = y$ et $t_2(x) = z$, donc on prend $t = t_1t_2$. On remarque aussi que $(T_v(\lambda))^{-1} = T_v(-\lambda)$. Pour $I_n \in \mathrm{SL}_n(q)$ et une transvection t, alors $I_n = tt^{-1}$ est un produit de transvections.

Soit $v \in \mathbb{F}_q^n$ non nul et $S \in \mathrm{SL}_n(q)$. On pose $w := Sv$. Alors, il existe un produit de transvections t tel que $t(w) = v$. On procède par récurrence sur la dimension. En dimension $n = 2$, on a que tS est un élément de $\mathrm{SL}_2(q)$ laissant fixe l'hyperplan $\langle v\rangle$. Donc, tS est une transvection (ou un produit de transvections si $tS = I_2$), disons $tS = t'$. Alors, $S = t^{-1}t'$ est un produit de transvections. Si la dimension est $n \geq 3$, on suppose que les éléments de $\mathrm{SL}_{n-1}(q)$ s'écrivent comme un produit de transvections. Alors, comme tS fixe $\langle v\rangle$, il induit une application $\widetilde{tS}$ sur $\mathbb{F}_q^n/\langle v\rangle \cong \mathbb{F}_q^{n-1}$ qui est de déterminant 1 et peut donc s'écrire comme un produit de transvections, disons $\widetilde{tS} = \widetilde{t'}$. Dans une base de $\mathbb{F}_q^n$ qui comprend v, il est clair que les facteurs de $\widetilde{t'}$ peuvent être relevés en transvections en dimension n qui fixent $\langle v\rangle$. Appelons ce produit de transvections relevées t'. Posons $r := (t')^{-1}tS$. L'application r fixe v et agit trivialement sur $\mathbb{F}_q^n/\langle v\rangle$. Par conséquent, pour tout $x \in \mathbb{F}_q^n$, on a $r(x) - x \in \langle v\rangle$. Il existe donc une forme linéaire $f_0 : \mathbb{F}_q^n \to \mathbb{F}_q$ telle que $r(x) = x + f_0(x)v$. Comme $r(v) = v$, on a $f_0(v) = 0$. Ainsi, r est soit l'identité ou une transvection, donc un produit de transvections. On obtient finalement $tS = t'r$. Donc, $S = t^{-1}t'r$ est un produit de transvection. Ainsi, les transvections engendrent $\mathrm{SL}_n(q)$. □

Lemme 3.4. $\mathrm{SL}_n(q)$ *est parfait, sauf pour* $n = 2$ *et* $q \in \{2, 3\}$.

Démonstration. Si $n \geq 3$, pour $x \in \mathbb{F}_q$ non nul, on a que

$$\left[\begin{pmatrix}1&0&0\\0&1&0\\0&x&1\end{pmatrix}, \begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix}\right] = \begin{pmatrix}1&0&0\\0&1&0\\x&0&1\end{pmatrix}.$$

Donc, dans la base appropriée, on voit que les transvections sont des commutateurs. Si $n = 2$, on a que si $q > 3$, il existe un élément non nul $x \in \mathbb{F}_q$ tel que $x^2 \neq 1$. Alors, le commutateur

$$\left[\begin{pmatrix}x^{-1}&0\\0&x\end{pmatrix}, \begin{pmatrix}1&0\\y&1\end{pmatrix}\right] = \begin{pmatrix}1&0\\y(x^2-1)&1\end{pmatrix}$$

montre qu'encore une fois avec la base appropriée, les transvections peuvent s'écrire comme des commutateurs, puisque $y(x^2 - 1)$ est un élément général de $\mathbb{F}_q$. Ainsi, comme les transvections engendrent $\mathrm{SL}_n(q)$ selon le Lemme 3.3, on a le résultat. □

Remarque : Les résultats des lemmes restent vrais pour $\mathrm{PSL}_n(q)$. En effet, comme les transvections engendrent $\mathrm{SL}_n(q)$, leurs images dans $\mathrm{PSL}_n(q)$ engendrent $\mathrm{PSL}_n(q)$ et $\mathrm{PSL}_n(q)$ est parfait, sauf pour $n = 2$ et $q \in \{2, 3\}$.

Théorème 3.5. *Les groupes* $\mathrm{PSL}_n(q)$ *sont simples sauf pour* $n = 2$ *et* $q \in \{2, 3\}$.

Démonstration. Afin d'utiliser le théorème d'Iwasawa, pour $n \geq 2$, on laisse $\mathrm{SL}_n(q)$ agir sur l'ensemble X des sous-espaces de $\mathbb{F}_q^n$ de dimension 1 de sorte que le noyau de l'action se réduit à l'ensemble des matrices scalaires $Z := Z(\mathrm{SL}_n(q)) = \{\lambda I_n : \lambda^n = 1\}$ et on obtient ainsi une action de $\mathrm{PSL}_n(q) \cong \mathrm{SL}_n(q)/Z$ sur X. Ainsi, l'action de $\mathrm{PSL}_n(q)$ est clairement fidèle. De plus, comme chaque base ordonnée peut être envoyée sur n'importe quelle autre base ordonnée par un élément de $\mathrm{SL}_n(q)$ à une multiplication scalaire près et que deux éléments distincts de X sont nécessairement linéairement indépendants, on a que l'action de $\mathrm{PSL}_n(q)$ est 2-transitive. Soit $x = \langle (1, 0, \cdots, 0)^t \rangle \in X$. Alors, le stabilisateur G_x est composé des éléments de $\mathrm{PSL}_n(q)$ dont la première colonne du représentant est de la forme $(\lambda, 0, \cdots, 0)^t$ où $\lambda \neq 0$. Ainsi,

$$K := \left\{ \begin{pmatrix} 1 & v_{n-1} \\ 0_{n-1} & I_{n-1} \end{pmatrix} Z : v_{n-1}^t \in \mathbb{F}_q^{n-1} \right\} \subseteq G_x$$

est un sous-groupe normal et abélien de G_x. En effet, pour $\begin{pmatrix} 1 & v_{n-1} \\ 0_{n-1} & I_{n-1} \end{pmatrix}$ un représentant d'un élément dans K et $\begin{pmatrix} \lambda & w_{n-1} \\ 0_{n-1} & A_{n-1} \end{pmatrix}$ le représentant d'un élément g_x de G_x, où A_{n-1} est une matrice carrée de taille $n-1$ telle que $\det A_{n-1} = \lambda^{-1}$, on a

$$\begin{pmatrix} 1 & v_{n-1} \\ 0_{n-1} & I_{n-1} \end{pmatrix} \begin{pmatrix} \lambda & w_{n-1} \\ 0_{n-1} & A_{n-1} \end{pmatrix} = \begin{pmatrix} \lambda & v_{n-1}A_{n-1} + w_{n-1} \\ 0_{n-1} & A_{n-1} \end{pmatrix} = \begin{pmatrix} \lambda & w_{n-1} \\ 0_{n-1} & A_{n-1} \end{pmatrix} \underbrace{\begin{pmatrix} 1 & \lambda^{-1}v_{n-1}A_{n-1} \\ 0_{n-1} & I_{n-1} \end{pmatrix}}_{\in K}.$$

Donc, K est bien un sous-groupe normal de G_x, car $Kg_x \subseteq g_xK$. En considérant le cas $\lambda = 1$ et $A_{n-1} = I_{n-1}$, on voit que K est abélien. De plus, les représentants de K sont des transvections. En particulier, avec le bon choix de base (et avec une matrice de changement de base dans $\mathrm{SL}_n(q)$), les transvections dans $\mathrm{PSL}_n(q)$ peuvent toutes s'écrire comme des conjugués d'éléments de K. Ainsi, par le Lemme 3.3, $\mathrm{PSL}_n(q)$ respecte la propriété et par le Lemme 3.4, il est parfait, sauf pour $n = 2$ et $q \in \{2, 3\}$. Donc, par le Lemme d'Iwasawa, $\mathrm{PSL}_n(q)$ est simple sauf pour $n = 2$ et $q \in \{2, 3\}$. □

Simplicité de $\mathrm{PSp}_{2n}(q)$

Lemme 3.6. $\mathrm{PSp}_4(2) = \mathrm{Sp}_4(2) \cong S_6$. *Ainsi,* $\mathrm{PSp}_4(2)$ *n'est pas simple.*

Démonstration. Comme $Z(\mathrm{Sp}_4(2)) = \{I\}$, l'égalité est claire. Pour voir l'isomorphisme, on fait agir S_6 sur $\mathbb{F}_2^6$ par permutation des coordonnées. Le sous-espace $U = \langle (1, 1, 1, 1, 1, 1)^t \rangle$ de dimension 1 est fixé par S_6. Il en va de même pour le sous-espace $W = \left\{ (x_1, \cdots, x_6)^t \in \mathbb{F}_2^6 : \sum_{i=1}^6 x_i = 0 \right\}$ de dimension 5. Soit f la forme bilinéaire alternée sur W donnée par $f(x, y) = \sum_{i=1}^6 x_i y_i$. Alors,

$\mathrm{rad} f = \{x \in W : f(x,y) = 0 \text{ pour tout } y \in W\} = U$. On obtient alors une forme bilinéaire alternée non singulière (symplectique) sur l'espace W/U de dimension 4 et une action induite de S_6 sur W/U qui préserve cette forme. En particulier, chaque vecteur non nul de W/U peut s'écrire comme un vecteur de $\mathbb{F}_2^6$ avec exactement deux entrées non nulles. Ainsi, il y a un homomorphisme de S_6 à $\mathrm{Sp}_4(2)$ où les transpositions $(i\ j)$ de S_6 sont envoyées injectivement sur des transvections symplectiques $T_v(1)$ de $\mathrm{Sp}_4(2)$ où les deux entrées non nulles de v sont en position i et j. Ainsi, comme $|S_6| = |\mathrm{Sp}_4(2)| = 720$, les deux groupes sont isomorphes. □

Remarque 3.3. *On rappelle que* $\mathrm{Sp}_2(q) = \mathrm{SL}_2(q)$*, donc* $\mathrm{PSp}_2(2)$ *et* $\mathrm{PSp}_2(3)$ *ne sont pas simples.*

Définition 3.2. *Une* ***transvection symplectique*** *est une application linéaire donnée par*

$$\begin{aligned} T_v(\lambda)\colon V &\to V \\ x &\mapsto x + \lambda f(x,v)v \end{aligned}$$

pour $x, v \in V$*,* $\lambda \in F$ *et* f *une forme symplectique.*

Les prochains résultats sur les groupes symplectiques sont tirés de [5].

Proposition 3.2. *Soit* $\lambda, \mu \in F$ *et* $\sigma \in \mathrm{Sp}_{2m}(q)$*. Alors,* $T_v(\lambda)T_v(\mu) = T_v(\lambda+\mu)$*,* $T_v(\lambda)^{-1} = T_v(-\lambda)$*,* $T_{\mu v}(\lambda) = T_v(\mu^2\lambda)$ *et* $\sigma T_v(\lambda)\sigma^{-1} = T_{\sigma(v)}(\lambda)$*.*

Démonstration. Soit $x \in \mathbb{F}_q^{2m}$.

$$\begin{aligned} T_v(\lambda)T_v(\mu)(x) &= T_v(\lambda)\left(x + \mu f(x,v)v\right) \\ &= x + \mu f(x,v)v + \lambda f(x + \mu f(x,v)v, v)v \\ &= x + \mu f(x,v)v + \lambda f(x,v)v + \lambda\mu f(x,v)f(v,v)v \\ &= x + (\lambda+\mu)f(x,v)v \\ &= T_v(\lambda+\mu) \end{aligned}$$

$$\begin{aligned} T_v(\lambda)T_v(-\lambda) &= T_v(0) = T_v(-\lambda)T_v(\lambda) \\ &= \mathrm{id}(V) \end{aligned}$$

$$\begin{aligned} T_{\mu v}(\lambda)(x) &= x + \lambda f(x, \mu v)\mu v \\ &= x + \mu^2\lambda f(x,v)v \\ &= T_v(\mu^2\lambda) \end{aligned}$$

$$\begin{aligned} \sigma T_v(\lambda)\sigma^{-1}(x) &= \sigma\left(\sigma^{-1}(x) + \lambda f\left(\sigma^{-1}(x), v\right)v\right) \\ &= x + \lambda f(x, \sigma(v))\sigma(v) \\ &= T_{\sigma(v)}(\lambda). \end{aligned}$$

□

Lemme 3.7. *Les transvections symplectiques engendrent* $\mathrm{Sp}_{2m}(q)$.

Démonstration. Soient $u, v \in V \cong \mathbb{F}_q^{2m}$ non nuls tels que $u \neq v$. Si $f(u,v) \neq 0$, on pose $\lambda = f(u,v)$. Alors, comme la forme f est alternée,

$$T_{u-v}(\lambda^{-1})(u) = u + \lambda^{-1} f(u, u-v)(u-v) = u + \lambda^{-1}(-f(u,v))(u-v) = u - (u-v) = v.$$

Si $f(u,v) = 0$, on prend $w \in V$ tel que $f(u,w) \neq 0$ et $f(v,w) \neq 0$. Alors, on se trouve dans le cas précédent et il existe des transvections symplectique t_1 et t_2 telles que $t_1(u) = w$ et $t_2(w) = v$. Ainsi, $t_2 t_1(u) = v$. Si $u = v$, on peut prendre $t_1^{-1} t_1(u) = u$. Donc, pour tout $u, v \in V$ non nuls, il existe un produit de transvections symplectiques t tel que $t(u) = v$.

Par la suite, prenons (u_1, v_1) et (u_2, v_2) des paires hyperboliques de la Définition 1.13. Soit t un produit de transvections symplectiques tel que $t(u_1) = u_2$ et posons $v_3 := t(v_1)$. Si $\mu := f(v_3, v_2) \neq 0$, alors $T_{v_3 - v_2}(\mu^{-1})(v_3) = v_2$. De plus, $f(u_2, v_3) = f(u_2, v_2) = 1$, donc $f(u_2, v_3 - v_2) = 0$. Ainsi, $T_{v_3-v_2}(\mu^{-1})(u_2) = u_2$. Donc, $T_{v_3-v_2}(\mu^{-1}) t(u_1, v_1) = (u_2, v_2)$. Si $f(v_3, v_2) = 0$, alors $(u_2, u_2 + v_3)$ est une paire hyperbolique telle que $f(v_3, u_2 + v_3) \neq 0$. Par le cas précédent, il existe une transvection symplectique t' telle que $t'(u_2) = u_2$ et $t'(v_3) = u_2 + v_3$. Or, $f(u_2 + v_3, v_2) = f(u_2, v_2) = 1$, donc il existe une transvection symplectique t'' telle que $t''(u_2) = u_2$ et $t''(u_2 + v_3) = v_2$. Ainsi, $t'' t' t(u_1, v_1) = (u_2, v_2)$. Donc, pour toute paire de paires hyperboliques (u_1, v_1), (u_2, v_2), il existe un produit de transvections symplectiques t tel que $t(u_1, v_1) = (u_2, v_2)$.

On procède par récurrence sur m. Si $m = 1$, $\mathrm{Sp}_2(q) = \mathrm{SL}_2(q)$. Soit $v \in \mathbb{F}_q^2$. Soit $L := T_v^{(l)}(\lambda_l)$ une transvection « linéaire » et $S := T_v^{(s)}(\lambda_s)$ une transvection symplectique. Alors, $\ker L = \langle v \rangle$ et $\ker S = v^\perp$. Or, comme $\dim \ker S = 1$ et $v \in v^\perp$, $\ker S = \langle v \rangle$. Donc, à un bon choix de λ_l et λ_s près, $L = S$, c'est-à-dire que les transvections « linéaires » sont aussi des transvections symplectiques. Comme $\mathrm{SL}_2(q)$ est engendré par les transvections par le Lemme 3.3, $\mathrm{Sp}_2(q)$ est bien engendré par les transvections symplectiques. Supposons le résultat vrai pour $m - 1$. Prenons une paire hyperbolique (u, v) dans V et posons $W = \langle u, v \rangle$ le plan hyperbolique. Soit $\sigma \in \mathrm{Sp}_{2m}$. Alors, $(\sigma u, \sigma v)$ est une paire hyperbolique. Par la partie précédente, il existe t un produit de transvections symplectiques tel que $t\sigma u = u$ et $t\sigma v = v$, donc $t\sigma|_W = 1_W$. On a également que $t\sigma|_{W^\perp} \in \mathrm{Sp}_{2m-2}(q)$. Par récurrence, $t\sigma|_{W^\perp}$ est un produit de transvections symplectiques s sur $W^\perp$. Ces transvections s'écrivent comme $T_w(\lambda)$ avec $w \in W^\perp$. Or, on a la même formule en considérant que $w \in V$. On a que ces transvections fixent W et comme $t\sigma|_W = 1_W$, on peut conclure que $t\sigma = s$, donc $\sigma = t^{-1}s$ un produit de transvections symplectiques. □

Lemme 3.8. *Si* $q \geq 4$, *alors* $\mathrm{Sp}_{2m}(q)$ *est parfait.*

Démonstration. Soit $v \in \mathbb{F}_q^{2m}$ non nul et $\lambda \in \mathbb{F}_q \setminus \{0\}$. On choisit $\mu \in \mathbb{F}_q \setminus \{0, \pm 1\}$ et on pose

$$x = \frac{\lambda}{1-\mu^2} \text{ et } y = \frac{-\mu^2\lambda}{1-\mu^2}.$$

Ainsi, $x + y = \lambda$, donc $T_v(x)T_v(y) = T_v(\lambda)$. Soit $\sigma \in \mathrm{Sp}_{2m}(q)$ tel que $\sigma v = \mu v$. Alors,

$$\sigma T_v(x)^{-1}\sigma^{-1} = \sigma T_v(-x)\sigma^{-1} = T_{\sigma(v)}(-x) = T_{\mu v}(-x) = T_v(-\mu^2 x) = T_v(y).$$

Donc, $T_v(x)\sigma T_v(x)^{-1}\sigma^{-1} = T_v(x)T_v(y) = T_v(\lambda) \in \mathrm{Sp}_{2m}(q)'$. Comme les transvections symplectiques engendrent $\mathrm{Sp}_{2m}(q)$, on a le résultat. □

Lemme 3.9. *Si $q = 3$ et $m \geq 2$, alors $\mathrm{Sp}_{2m}(q)$ est parfait.*

Démonstration. Soit une base symplectique $\{e_1, \cdots, e_m, f_m, \cdots, f_1\}$ de $\mathbb{F}_3^{2m}$. On définit

$$\sigma : e_1 \mapsto e_1 + e_2,\ e_2 \mapsto e_1,\ f_1 \mapsto f_2,\ f_2 \mapsto f_1 - f_2$$

avec $e_i \mapsto e_i$ et $f_i \mapsto f_i$ pour $i > 2$. On définit également

$$\tau : e_1 \mapsto e_1 - f_1 + f_2,\ e_2 \mapsto e_2 + f_1$$

avec $e_i \mapsto e_i$ pour $i > 2$ et $f_i \mapsto f_i$ pour tout i. On vérifie avec un calcul direct que $\sigma, \tau \in \mathrm{Sp}_{2m}(3)$. On a également que

$$\sigma\tau\sigma^{-1}\tau^{-1} = T_{f_1}(1),$$

donc $T_{f_1}(1) \in \mathrm{Sp}_{2m}(3)'$. Soit $v \in \mathbb{F}_3^{2m}$ non nul, on prend $\gamma \in \mathrm{Sp}_{2m}(3)$ tel que $\gamma(f_1) = v$. Alors,

$$\gamma T_{f_1}(1)\gamma^{-1} = T_{\gamma(f_1)}(1) = T_v(1).$$

Comme $\mathrm{Sp}_{2m}(3)'$ est un sous-groupe normal de $\mathrm{Sp}_{2m}(3)$, on a que $T_v(1) \in \mathrm{Sp}_{2m}(3)'$. De plus, $T_v(1)^{-1} = T_v(-1) \in \mathrm{Sp}_{2m}(3)'$. Comme toutes les transvections symplectiques sont dans le groupe dérivé, on a le résultat. □

Lemme 3.10. *Si $q = 2$ et $m \geq 3$, alors $\mathrm{Sp}_{2m}(q)$ est parfait.*

Démonstration. On utilise une preuve similaire à celle du Lemme 3.9 en considérant plutôt

$$\sigma : e_1 \mapsto e_1 + e_3,\ e_2 \mapsto e_1,\ e_3 \mapsto e_2,\ f_1 \mapsto f_3,\ f_2 \mapsto f_1 + f_3,\ f_3 \mapsto f_2$$

avec $e_i \mapsto e_i$ et $f_i \mapsto f_i$ pour $i > 3$ ainsi que

$$\tau : e_1 \mapsto e_1 + f_2,\ e_2 \mapsto e_2 + f_1 + f_2 + f_3,\ e_3 \mapsto e_3 + f_2 + f_3$$

avec $e_i \mapsto e_i$ pour $i > 3$ et $f_i \mapsto f_i$ pour tout i. On a $\tau^{-1} = \tau$, puisque l'on travaille en caractéristique 2. De plus,

$$\begin{aligned} &\sigma^{-1}(e_1) = e_2, && \sigma^{-1}(e_2) = e_3, && \sigma^{-1}(e_3) = e_1 + e_2, \\ &\sigma^{-1}(f_1) = f_1 + f_2, && \sigma^{-1}(f_2) = f_3, && \sigma^{-1}(f_3) = f_1. \end{aligned}$$

Un calcul direct donne

$$\begin{aligned}
&\sigma\tau\sigma^{-1}\tau^{-1}(e_1) = e_1 + f_1, \\
&\sigma\tau\sigma^{-1}\tau^{-1}(e_i) = e_i \qquad \text{pour } i \neq 1, \\
&\sigma\tau\sigma^{-1}\tau^{-1}(f_i) = f_i \qquad \text{pour tout } i.
\end{aligned}$$

Rappelons que pour tout $x \in \mathbb{F}_q^n$ on a $T_{f_1}(1)(x) = x + f(x, f_1)f_1$. Par conséquent, on trouve $\sigma\tau\sigma^{-1}\tau^{-1} = T_{f_1}(1)$.

□

Lemme 3.11. *L'action de* $\mathrm{Sp}_{2m}(q)$ *sur* X *l'ensemble des sous-espaces de* $\mathbb{F}_q^{2m}$ *de dimension 1 est primitive.*

Démonstration. Pour $m = 1$, $\mathrm{Sp}_2(q) = \mathrm{SL}_2(q)$ selon la Remarque 1.16 et on a montré dans la démonstration du Théorème 3.5 que l'action est doublement transitive, donc primitive. Pour $m \geq 2$, supposons qu'il existe un sous-ensemble $Y \subseteq X$ avec $|Y| \geq 2$ tel que pour tout $\sigma \in \mathrm{Sp}_{2m}(q)$, soit $\sigma(Y) = Y$, soit $\sigma(Y) \cap Y = \emptyset$. Notons $[u]$ le sous-espace de dimension 1 engendré par $u \in \mathbb{F}_q^{2m}$. Montrons qu'il existe $[u], [v] \in Y$ tels que $f(u, v) \neq 0$. On suppose que $f(u, v) = 0$ pour tout $[u], [v] \in Y$. Prenons $[u] \neq [v]$ dans Y et $x \in \mathbb{F}_2^{2m}$ tel que $f(u, x) = 1$ et $f(v, x) = 0$. Soit $W = \langle u, x \rangle$ un plan hyperbolique et posons le sous-groupe $H = \{\sigma \in \mathrm{Sp}_{2m}(q) : \sigma|_W = 1_W\} \leq \mathrm{Sp}_{2m}(q)$. Soit $w \in W^\perp$ non nul. Comme $v \in W^\perp$, il existe $\sigma \in H$ tel que $\sigma v = w$ par le Lemme 3.7. Comme $\sigma u = u$, on a que $[u] \in \sigma(Y) \cap Y$, donc $\sigma(Y) = Y$. Alors, $[w] = \sigma[v] \in Y$ et w était un vecteur non nul arbitraire de $W^\perp$. Comme $W^\perp \neq 0$, il existe une paire hyperbolique (y, z) dans $W^\perp$, donc $[y], [z] \in Y$, mais $f(y, z) = 1$.

On peut ainsi prendre $[u], [v] \in Y$ avec $f(u, v) \neq 0$. On peut assumer que $f(u, v) = 1$ et que (u, v) est une paire hyperbolique. Soit $[w] \in X$. Si $f(u, w) \neq 0$, on peut assumer que (u, w) est une paire hyperbolique et par le Lemme 3.7, il existe $\sigma \in \mathrm{Sp}_{2m}(q)$ tel que $\sigma u = u$ et $\sigma v = w$. Ainsi, $u \in \sigma(Y) \cap Y$, donc $\sigma(Y) = Y$ et $[w] \in Y$. Si $f(u, w) = 0$, on prend $x \in \mathbb{F}_q^{2m}$ tel que $f(u, x) = f(w, x) = 1$. Alors, comme pour le cas précédent, $[x] \in Y$ et il existe $\tau \in \mathrm{Sp}_{2m}(q)$ tel que $\tau u = w$ et $\tau x = x$. Encore une fois, $\tau(Y) = Y$, car $[x] \in \tau(Y) \cap Y$ et $[w] = \tau[u] \in Y$. Dans les deux cas, $Y = X$. Donc, l'action est primitive. □

Théorème 3.12. *Les groupes* $\mathrm{PSp}_{2m}(q)$ *sont simples sauf pour* $(m, q) \in \{(1, 2), (1, 3), (2, 2)\}$.

Démonstration. Par le Lemme 3.11, l'action de $\mathrm{Sp}_{2m}(q)$ sur X est primitive. Son noyau est $\mathbb{Z}(\mathrm{Sp}_{2m}(q))$, donc l'action induite de $G = \mathrm{PSp}_{2m}(q)$ est fidèle. Soit $[u] \in X$. Alors, pour $K = \{T_u(\lambda) : \lambda \in \mathbb{F}_q\}$ où les $T_u(\lambda)$ sont des transvections symplectiques, on a $K \subseteq G_{[u]}$. De plus, les propriétés de la Proposition 3.2 montrent que K est un sous-groupe normal de $G_{[u]}$ et que l'union des conjugués de K contient toutes les transvections symplectiques, donc $\left\{gKg^{-1} : g \in G\right\}$ engendre G. Par les Lemmes 3.8, 3.9 et 3.10, les groupes $\mathrm{PSp}_{2m}(q)$ sont

parfaits pour $(m,q) \notin \{(1,2),(1,3),(2,2)\}$. Ainsi, par le Lemme d'Iwasawa, ces groupes sont simples. □

Simplicité de $\mathrm{PSU}_n(q)$

Lemme 3.13. $\mathrm{PSU}_3(2)$ *n'est pas simple.*

Démonstration. On a que $|\mathrm{PSU}_3(2)| = 72 = 2^3 \cdot 3^2$. Le théorème de Burnside stipule qu'un groupe d'ordre $p^a q^b$ pour p et q des premiers et $a, b \in \mathbb{Z}_{\geq 0}$ est résoluble. Si $G := \mathrm{PSU}_3(2)$ était simple, on aurait $G' = [G,G] = e_G$ et donc G serait abélien. Or, par la Remarque 1.1, G doit être un groupe cyclique premier, ce qui n'est pas le cas. □

Remarque 3.4. *On rappelle que* $\mathrm{SU}_2(q) \cong \mathrm{SL}_2(q)$*, donc* $\mathrm{PSU}_2(2)$ *et* $\mathrm{PSU}_2(3)$ *ne sont pas simples.*

Théorème 3.14. *Les groupes* $\mathrm{PSU}_n(q)$ *sont simples sauf pour* $(n,q) \in \{(2,2),(2,3),(3,2)\}$.

Voici une ébauche de la preuve de simplicité qui est très similaire à celle pour les groupes symplectiques. On définit les transvections unitaires comme étant $T_v(\lambda) : x \mapsto x + \lambda f(x,v)v$ où f est une forme sesquilinéaire conjugué-symétrique non singulière, $v \in \mathbb{F}_{q^2}^n$ est isotrope et $\lambda \in \mathbb{F}_{q^2}$ est tel que $\lambda^{q-1} = -1$. Ces transvections engendrent $\mathrm{SU}_n(q)$ et sont des commutateurs pour $n > 3$ ou $n = 3$ et $q > 2$. L'action de $\mathrm{SU}_n(q)$ sur les espaces isotropes de dimension 1 est primitive et celle induite sur $\mathrm{PSU}_n(q)$ est également fidèle. Pour un vecteur isotrope donné v, les transvections unitaires $T_v(\lambda)$ forment un sous-groupe normal abélien du stabilisateur de $\langle v \rangle$. Donc, par le lemme d'Iwasawa, $\mathrm{PSU}_n(q)$ est simple pour $n > 3$ ou $n = 3$ et $q > 2$.

Simplicité de $\mathrm{P}\Omega_n(q)$

Dans le cas orthogonal, les transvections orthogonales $T_v(\lambda) : x \mapsto x + \lambda f(x,v)v$ où f est une forme symétrique ne sont pas généralement dans $\mathrm{O}_n(q)$, sauf en caractéristique 2. Or, dans ce cas, elles ne sont pas dans $\mathrm{P}\Omega_n(q)$. On utilise donc une autre famille d'applications, soit les transformations de Siegel.

Définition 3.3. *Une* ***transformation de Siegel****, aussi appelée transformation de Eichler ou élément de racine (long), est donnée par*

$$E_{u,v} : x \mapsto x + f(x,u)v - f(x,v)u - Q(v)f(x,u)u$$

pour f une forme bilinéaire symétrique non singulière, Q sa forme quadratique associée, u un vecteur isotrope et $v \in u^\perp$.

Remarque 3.5. *Ces applications préservent la forme quadratique Q, c'est-à-dire que $Q(E_{u,v}(x)) = Q(x)$. On a également des propriétés utiles comme*

$$E_{u,v}E_{u,w} = E_{u,v+w}, E_{u,v}^{-1} = E_{u,-v} \text{ et } E_{u,v+\lambda u} = E_{u,v},$$

pour un scalaire $\lambda \in \mathbb{F}_q$.

Pour un u fixé, on considère le groupe $K_u = \left\{E_{u,v} : v \in u^\perp\right\}$. Le noyau du paramétrage $a \mapsto E_{u,v}$ est $\mathbb{F}_q u$: si $E_{u,v} = \mathrm{Id}$, sa restriction à $u^\perp$ implique $v \in (u^\perp)^\perp = \mathbb{F}_q u$. Ainsi,

$$K_u \simeq (u^\perp/\mathbb{F}_q u, +),$$

et K_u est abélien.

On a $K_u \subseteq \Omega_n(q)$. Pour q impair, $E_{u,v}$ a un ordre divisant la caractéristique p, ce qui force son déterminant et sa norme spinorielle à être triviaux. Pour q pair, $\mathrm{rang}(E_{u,v} - \mathrm{Id})$ vaut 0 si $v \in \mathbb{F}_q u$ et 2 sinon. Son quasi-déterminant est donc 1. Enfin, pour $g \in \mathrm{O}_n(q)$ et $c \neq 0$,

$$gE_{u,v}g^{-1} = E_{gu,gv}, \qquad E_{cu,v} = E_{u,cv}.$$

Il en résulte que K_u dépend seulement de $\mathbb{F}_q u$ et que

$$K_u \trianglelefteq G_x$$

où $G = \Omega_n(q)$ et $x = \mathbb{F}_q u$.

Théorème 3.15. *Les groupes $\mathrm{P}\Omega_n(q)$ sont simples pour $n \geq 5$.*

Démonstration. Notons X l'ensemble des droites isotropes de V. On a les trois résultats structurels suivants :

$$\Omega = \langle K_v : \mathbb{F}_q v \in X \rangle, \qquad \Omega' = \Omega, \qquad \Omega \text{ agit primitivement sur } X.$$

Pour q impair, ils résultent des Propositions 6.28 à 6.30 de [5], avec le Théorème 9.7 pour identifier le groupe engendré au noyau de la norme spinorielle. Pour q pair, on utilise plutôt les Propositions 14.23, 14.39, 14.41 et 14.42. On a que la norme spinorielle est triviale sur le corps fini puisque tout élément non nul y est un carré. Toutes les restrictions de ces résultats sont satisfaites dans les dimensions considérées.

Le noyau de l'action de Ω sur X est $Z(\Omega)$. Pour le vérifier, soit $g \in \mathrm{O}_n(q)$ fixant toutes les droites isotropes. Choisissons une paire hyperbolique u, v_0, avec $f(u, v_0) = 1$, et posons $W = \langle u, v_0 \rangle^\perp$. Écrivons $gu = \alpha u$ et $gv_0 = \beta v_0$. Comme $gW = W$ et que $v_0 + w - Q(w)u$ est isotrope pour tout $w \in W$, la comparaison des composantes de l'image de ce vecteur montre que

$$gw = \beta w \quad (w \in W), \qquad (\alpha - \beta)Q(w) = 0 \quad (w \in W).$$

Il existe $w \in W$ avec $Q(w) \neq 0$; ainsi $g = \beta \mathrm{Id}$ et $\beta^2 = 1$. Le noyau est donc scalaire. Réciproquement, un élément central de Ω préserve $\mathbb{F}_q v$ pour chaque droite isotrope. Cette égalité résulte directement de la formule de $E_{u,v}$ et de la non-dégénérescence de f. Les éléments centraux appartiennent donc exactement au noyau scalaire.

Posons $G = \Omega_n(q)/Z(\Omega_n(q)) = \mathrm{P}\Omega_n(q)$ et soit A l'image de K_u dans G, pour une droite isotrope fixée $x = \mathbb{F}_q u$. Le groupe G agit fidèlement et primitivement sur X et est parfait. Le groupe A est abélien et normal dans G_x. La transitivité de Ω sur X et l'identité $gK_u g^{-1} = K_{gu}$ impliquent que tous les K_v sont conjugués à K_u dans Ω. Les conjugués de A engendrent donc G. Enfin, $A \simeq K_u \neq 1$, puisque les éléments de K_u sont unipotents et que le seul scalaire unipotent est l'identité. Le lemme d'Iwasawa s'applique et donne la simplicité de G. □

Les autres cas de simplicité (et de non simplicité) s'expliquent via les isomorphismes suivants de la Proposition 3.3. On montre ces isomorphismes à l'aide des propriétés du produit tensoriel d'espaces vectoriels. Les détails se trouvent dans [9].

Proposition 3.3.

$$\begin{aligned}
\mathrm{P}\Omega_3(q) &\cong \mathrm{PSL}_2(q) \\
\mathrm{P}\Omega_4^+(q) &\cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q) \\
\mathrm{P}\Omega_4^-(q) &\cong \mathrm{PSL}_2\left(q^2\right)
\end{aligned}$$

Démonstration. Soit V_1 et V_2 des espaces vectoriels de dimension 2 avec $\{e_1, f_1\}$ et $\{e_2, f_2\}$ les bases de V_1 et V_2 respectivement. Soit b_i la forme bilinéaire alternée sur V_i définie par $b_i(e_i, f_i) = 1$. On définit également une forme bilinéaire symétrique h sur $V_1 \otimes V_2$ par $h\left(x \otimes y, z \otimes t\right) = b_1(x, z) b_2(y, t)$.

Pour le premier cas, posons $V_1 = V_2 = V$ comme étant le module naturel pour $\mathrm{SL}_2(q)$ avec q impair. Soit W le sous-module de $V \otimes V$ engendré par $e_1 \otimes e_1$, $e_1 \otimes f_1 + f_1 \otimes e_1$ et $f_1 \otimes f_1$. La matrice associée à la forme $h|_W$ est donnée par $\begin{pmatrix} 0 & 0 & 1 \\ 0 & -2 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. Cette forme est invariante sous les applications $e_1 \mapsto e_1 + \lambda f_1$ et $e_1 \leftrightarrow f_1$ qui génèrent $\mathrm{SL}_2(q)$ et qui agissent respectivement comme les matrices

$$\begin{pmatrix} 1 & \lambda & \lambda^2 \\ 0 & 1 & 2\lambda \\ 0 & 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Comme -1 dans $\mathrm{SL}_2(q)$ agit trivialement, on a un plongement de $\mathrm{PSL}_2(q)$ dans $\mathrm{GO}_3(q)$ et en comparant les ordres, on a $\mathrm{PSL}_2(q) \cong \Omega_3(q) \cong \mathrm{P}\Omega_3(q)$.

Pour le deuxième cas, on considère V_1 et V_2 comme étant des modules naturels sur deux copies distinctes de $\mathrm{SL}_2(q)$ de sorte que $V_1 \otimes V_2$ soit un module pour $\mathrm{SL}_2(q) \times \mathrm{SL}_2(q)$ avec $(-1, -1)$

qui agit trivialement. Lorsque la caractéristique est paire, on définit la forme quadratique Q ayant h comme forme bilinéaire associée par

$$Q(e_1 \otimes e_1) = Q(e_1 \otimes f_2) = Q(f_1 \otimes e_2) = Q(f_1 \otimes f_2) = 0.$$

Comme $e_1 \otimes e_2$ et $e_1 \otimes f_2$ engendrent un espace totalement isotrope, $m(V_1 \otimes V_2) = 2$ et $V_1 \otimes V_2$ est bien de type plus. De plus, les classes de $(-I, I)$ et de $(I, -I)$ dans ce quotient coïncident et correspondent à la matrice scalaire $-I_{V_1 \otimes V_2}$, qui engendre le centre de $\Omega_4^+(q)$. Après le quotient par ce centre, on obtient

$$\mathrm{P}\Omega_4^+(q) = \frac{\Omega_4^+(q)}{Z(\Omega_4^+(q))} \simeq \frac{\mathrm{SL}_2(q) \times \mathrm{SL}_2(q)}{Z(\mathrm{SL}_2(q)) \times Z(\mathrm{SL}_2(q))} \simeq \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q).$$

Pour le troisième et dernier cas, considérons plutôt V_1 le module naturel pour $\mathrm{SL}_2\left(q^2\right)$ et V_2 son image par l'automorphisme $x \mapsto x^q = \overline{x}$. Alors, l'élément de $\mathrm{SL}_2\left(q^2\right)$ $e_1 \mapsto e_1 + \lambda f_1$ agit comme $e_2 \mapsto e_2 + \overline{\lambda} f_2$. Soit l'espace sur $\mathbb{F}_q$ engendré par $e_1 \otimes e_2$, $f_1 \otimes f_2$ et $\mu e_1 \otimes f_2 + \overline{\mu} f_1 \otimes e_2$ pour $\mu \in \mathbb{F}_{q^2}$. Cet espace est de dimension 4 sur $\mathbb{F}_q$. Encore une fois, en caractéristique 2, on définit la forme quadratique Q comme étant nul sur les tenseurs simples. On a que $e_1 \otimes e_2$ et $f_1 \otimes f_2$ forment une paire hyperbolique. Les vecteurs restants vérifient

$$Q\left(\mu e_1 \otimes f_2 + \overline{\mu} f_1 \otimes e_2\right) = -\mu\overline{\mu} \neq 0$$

pour tout $\mu \neq 0$, ils forment donc un espace de dimension 2 de type moins. Les éléments de $\mathrm{SL}_2\left(q^2\right)$ préservent cet espace. En considérant les ordres, on a que $\mathrm{P}\Omega_4^-(q) \cong \mathrm{PSL}_2\left(q^2\right)$. □

Remarque 3.6. *Ainsi,* $\mathrm{P}\Omega_3(q)$ *est simple sauf si* $q = 2$ *ou* 3*,* $\mathrm{P}\Omega_4^+(q)$ *n'est jamais simple, car* $\{I_2\} \times \mathrm{PSL}_2(q)$ *est toujours un sous-groupe normal de* $\mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q)$ *et* $\mathrm{P}\Omega_4^-(q)$ *est toujours simple. De plus,* $\mathrm{P}\Omega_4^+(q)$ *n'agit pas de manière primitive sur les espaces isotropes de dimension 1 et* $\mathrm{P}\Omega_4^+(2)$ *n'est pas généré par des transformations de Siegel.*

3.2 Théorème de simplicité de Tits

Dans sa quête de démontrer la simplicité des groupes de type Lie, Jacques Tits a voulu généraliser les idées du lemme d'Iwasawa afin de concevoir un théorème de simplicité s'appliquant aux groupes qui admettent une BN-paire. Le Lemme 3.16 et le Théorème 3.17 proviennent de [1] et leurs démonstrations sont superficiellement modifiées.

Lemme 3.16. *Soit* H *un sous-groupe normal d'un groupe* G *admettant un système de Tits* (G, B, N, S)*. Alors, il existe* $J \subseteq S$ *tel que* $BH = P_J$ *et tout élément de* J *commute avec tout élément de* $S \setminus J$*, où* $P_J = BN_JB$ *défini au Lemme 2.1.*

Démonstration. Par la Proposition 2.8, comme BH est un sous-groupe de G contenant B, il existe un unique $J \subseteq S$ tel que $BH = P_J = \bigsqcup_{w \in \langle J \rangle} C(w)$. Soit $s_1 \in J$ et $s_2 \in S \setminus J$.

Soient n_1 et n_2 les représentants de s_1 et s_2 dans N. On a $n_1 \in P_J = BH$, donc il existe $b \in B$ tel que $bn_1 \in H$. Comme H est normal dans G, l'élément $h = n_2 b n_1 n_2^{-1} \in H$. Ainsi, $h \in C(s_2)C(s_1)C(s_2)$. Supposons que $l(s_2s_1s_2) = 3$. Alors, par la Proposition 2.2, $C(s_2)C(s_1)C(s_2) = C(s_2s_1s_2)$ et $h \in H \cap C(s_2s_1s_2)$. Ainsi, $BH \cap C(s_2s_1s_2)$ est non vide et comme les cellules de Bruhat sont disjointes par le Lemme 2.3, alors $\langle C(s_2s_1s_2)\rangle \subseteq BH$. Par la Proposition 2.5, $C(s_2) \subseteq \langle C(s_2s_1s_2)\rangle \subseteq BH$. Donc, $s_2 \in J$, ce qui est une contradiction. Donc, on doit avoir $l(s_2s_1s_2) \leq 2$. Si $l(s_2s_1s_2) = 2$, alors $s_2s_1s_2 = t_1t_2$ où t_1t_2 est une expression réduite. Alors, pour $u := s_1s_2 = s_2t_1t_2$, on a nécessairement que $l(u) = 1$ ou $l(u) = 3$ par la Remarque 2.6. Or, si $l(u) = 3$, s_1s_2 est une écriture de u d'une longueur plus petite que l'écriture de longueur minimale. De plus, clairement $l(s_2) = 1$ et $s_1u = s_2$. Alors, si $l(u) = 1$, $l(u) = l(s_1u)$, ce qui contredit la Remarque 2.11. Si $l(s_2s_1s_2) = 1$, alors par la Proposition 2.4, $s_2(s_1s_2) = s_1$ ou $s_2(s_1s_2) = s_2$. Dans le premier cas, $s_1s_2 = s_2s_1$. Dans le deuxième cas, $s_1 = s_2$, ce qui est une contradiction. □

Théorème 3.17. *(Théorème de simplicité de Tits) Soit G un groupe admettant une BN-paire. Soit $Z := \bigcap_{g\in G} gBg^{-1}$, soit U un sous-groupe de B et soit $G_1 := \langle gUg^{-1} : g \in G\rangle$. On fait les hypothèses supplémentaires suivantes :*
(1) U est normal dans B et $B = UT$.
(2) Pour tout sous-groupe normal V de U, distinct de U, $(U/V)'$ est distinct de U/V.
(3) G_1 est parfait.
(4) Le système de Coxeter (W, S) est irréductible.
Alors, tout sous-groupe H de G normalisé par G_1 est contenu dans Z ou contient G_1.

Démonstration. Comme G_1 est normal dans G, le début de la preuve de la Proposition 2.12 s'applique et $G = G_1T$. Posons $G' = G_1H$, $B' = B \cap G'$, $N' = N \cap G'$, $T' = T \cap G' = B' \cap N'$ et $W' = N'/T'$. On a que $G = G'T$ puisque G' contient G_1. On peut ainsi poursuivre la démonstration de la Proposition 2.12 pour montrer que B' et N' forment un système de Tits pour G'. Comme $G_1 \subseteq \mathrm{N}_G(H)$, H est normal dans G'. D'après le Lemme 3.16, il existe une partie J de S' telle que $B'H = B'N'_JB'$ et tout élément de $S' \setminus J$ commute à tout élément de J. Comme $(W', S') \cong (W, S)$ est irréductible, le graphe de Coxeter associé est connexe et seulement deux cas sont possibles :
a) $J = \emptyset$, i.e. $B'H = B'$ et $H \subseteq B' \subseteq B$. Pour tout $g \in G$, on peut écrire $g = g_1t$ avec $g_1 \in G_1$ et $t \in T$. Alors, $gBg^{-1} = g_1tBt^{-1}g_1^{-1} = g_1Bg_1^{-1} \supseteq H$, car G_1 normalise H. Donc, $H \subseteq Z = \bigcap_{g\in G} gBg^{-1}$.
b) $J = S'$, i.e. $B'H = G'$. Comme $G = G'T$, on a $G = B'HT = HB'T = HB$. Soit $g = hb$ avec $h \in H$ et $b \in B$. Comme U est normal dans B, $gUg^{-1} = hbUb^{-1}h^{-1} = hUh^{-1} \subseteq UH$. Ainsi, $G_1 \subseteq UH$, par définition de G_1. Par le deuxième théorème d'isomorphisme,

$$U/(U \cap H) \cong UH/H = G_1H/H \cong G_1/(G_1 \cap H).$$

D'après l'hypothèse (3), $G_1/(G_1 \cap H)$ est parfait. Or, l'hypothèse (2) stipule que si $U \cap H \neq U$, alors $U/(U \cap H)$ n'est pas parfait. Donc, $U \cap H = U$ et $G_1/(G_1 \cap H) \cong \{1\}$. Alors, $G_1 \cap H = G_1$ et $G_1 \subseteq H$, ce qui termine la démonstration. □

Corollaire 3.17.1. *Sous les hypothèses du Théorème 3.17, le groupe $G_1/(G_1 \cap Z)$ est simple non commutatif ou d'ordre 1.*

Démonstration. Soit $H/(G_1 \cap Z)$ un sous-groupe normal de $G_1/(G_1 \cap Z)$. Alors, H est un sous-groupe de G normalisé par G_1 Par le Théorème 3.17, $H \subseteq Z$ ou $G_1 \subseteq H$. Dans le premier cas, $H \subseteq G_1 \cap Z$, donc $H/(G_1 \cap Z)$ est trivial. Dans le deuxième cas, $H = G_1$ et $H/(G_1 \cap Z) = G_1/(G_1 \cap Z)$. Comme $G_1/(G_1 \cap Z)$ est parfait, s'il était abélien, il serait aussi trivial. □

Proposition 3.4. *Si $Z \cap U = \{1\}$, alors $G_1 \cap Z = Z(G_1)$.*

Démonstration. Soit $z \in Z$ et $u \in U$. Alors, comme Z et U sont des sous-groupes normaux de B, $zuz^{-1}u^{-1} \in Z \cap U = \{1\}$, donc $zu = uz$. Soit $gug^{-1} \in G_1$. Comme Z est normal dans G, il existe $z' \in Z$ tel que $z = gz'g^{-1}$. Alors,

$$\begin{aligned}(gug^{-1})z &= gug^{-1}gz'g^{-1} \\ &= guz'g^{-1} = gz'ug^{-1} \\ &= gz'g^{-1}gug^{-1} \\ &= z(gug^{-1})\end{aligned}$$

Ainsi, Z centralise chacun des sous-groupes gUg^{-1}. Comme $G_1 = \langle gUg^{-1} : g \in G \rangle$, on en déduit que Z centralise G_1.Donc, $G_1 \cap Z \subseteq Z(G_1)$.

Considérons la projection canonique $\pi : G_1 \longrightarrow G_1/(G_1 \cap Z)$. Si $x \in Z(G_1)$, alors $\pi(x)$ appartient au centre de $G_1/(G_1 \cap Z)$. Par le Corollaire 3.17.1, ce quotient est soit simple non commutatif, soit trivial. Dans les deux cas, son centre est trivial. Par conséquent, $\pi(x) = 1$, donc $x \in \ker(\pi) = G_1 \cap Z$. On obtient ainsi l'inclusion réciproque $Z(G_1) \subseteq G_1 \cap Z$ et donc $G_1 \cap Z = Z(G_1)$.

□

Proposition 3.5. *Soit (G, B, N, S) le système de Tits associé à $G = \mathrm{GL}_n(q)$ de la Proposition 2.1. Alors, $G_1 = \mathrm{SL}_n(q)$.*

Démonstration. On rappelle que U est composé des matrices unipotentes triangulaires supérieures. Alors, pour tout $g \in G$ et $u \in U$, $\det(gug^{-1}) = \det(u) = 1$, donc $G_1 \subseteq \mathrm{SL}_n(q)$. Par la Remarque 3.2, il est clair que les transvections $T_v(\lambda) \in G_1$. Par le Lemme 3.3, les transvections engendrent $\mathrm{SL}_n(q)$, donc $G_1 = \mathrm{SL}_n(q)$. □

Théorème 3.18. [*Version 2*] *Les groupes* $\mathrm{PSL}_n(q)$ *sont simples sauf pour* $n = 2$ *et* $q \in \{2, 3\}$.

Démonstration. Avec la BN-paire de $\mathrm{GL}_n(q)$, l'hypothèse (1) est vérifiée, car elle est scindée. Comme U est unipotent, U est respecte l'hypothèse (2). Le système de Coxeter (W, S) est de type A_{n-1} qui est connexe, donc (W, S) est irréductible. Alors, par la Proposition 3.5, le Théorème 3.17, le Corollaire 3.17.1 et la Proposition 3.4, $\mathrm{PSL}_n(q)$ est simple lorsque $\mathrm{SL}_n(q)$ est parfait, donc si $(n, q) \notin \{(2, 2), (2, 3)\}$ par le Lemme 3.4. □

Remarque 3.7. *On peut faire le même genre de raisonnement pour les autres groupes classiques présentés.*

3.3 Lien entre les théorèmes dans le contexte des groupes classiques

Bien que les deux théorèmes de simplicité s'appliquent de manière différente, ils utilisent des principes similaires et possèdent beaucoup de parallèles. Voici un tableau qui résume ces concepts.

Lemme d'Iwasawa	Théorème de simplicité de Tits
L'action de G est primitive	Le système de Coxeter est irréductible
G_x est un stabilisateur	B est le stabilisateur d'un drapeau maximal
K est normal dans G_x	U est normal dans B
K est résoluble	U est unipotent (donc résoluble)
$G = \langle gKg^{-1} : g \in G \rangle$	$G_1 = \langle gUg^{-1} : g \in G \rangle$
G est parfait	G_1 est parfait

TABLE 3.1 – Comparaison entre les deux théorèmes de simplicité énoncés

De plus, dans le contexte des groupes classiques, la fidélité de l'action de G dans le Lemme d'Iwasawa ainsi que le quotient de G_1 par son centre dans le Corollaire 3.17.1 et la Proposition 3.4 sont des idées homologues. Une différence notable entre les deux théorèmes est que G_x est un sous-groupe maximal de G, alors que B n'est pas un sous-groupe maximal, il est contenu en général dans les groupes paraboliques P_J différents de B et G.

Conclusion

Dans un premier temps, on a démontré la simplicité des groupes cycliques premiers et des groupes alternés A_n pour $n \geq 5$ en guise d'amorce au théorème de classification des groupes finis simples. Par la suite, on a défini les différentes familles de groupes classiques sur lesquelles ce mémoire se concentre. On a également nommé les autres groupes finis simples de la Classification, par souci de complétude.

On a ensuite exhibé un outil mathématique puissant introduit par Jacques Tits, soit les BN-paires. La BN-paire de $\mathrm{GL}_n(q)$ sert de point d'ancrage afin de définir les BN-paires sur les autres groupes classiques.

Finalement, on a montré la simplicité des groupes linéaires et symplectiques à l'aide du Lemme d'Iwasawa en se basant sur le travail du Chapitre 1 et on a fait l'esquisse pour les autres groupes classiques, puis on a présenté le Théorème de Tits qui permet une preuve alternative basée sur le Chapitre 2.

Annexe A

Énoncé du Théorème de Classification des groupes finis simples

Tous les groupes finis simples sont isomorphes à un des groupes suivants où p est un premier et q est une puissance p^a d'un premier p :

- un groupe cyclique C_p,
- un groupe alterné A_n pour $n \geq 5$,
- un groupe classique :
  - linéaire, soit $\mathrm{PSL}_n(q)$ pour $n \geq 2$, sauf $\mathrm{PSL}_2(2)$ et $\mathrm{PSL}_2(3)$,
  - unitaire, soit $\mathrm{PSU}_n(q)$ pour $n \geq 3$, sauf $\mathrm{PSU}_3(2)$,
  - symplectique, soit $\mathrm{PSp}_{2m}(q)$ pour $m \geq 2$, sauf $\mathrm{PSp}_4(2)$,
  - orthogonal, soit
    - $\mathrm{P}\Omega_{2m+1}(q)$ pour $m \geq 3$ et q impair,
    - $\mathrm{P}\Omega^+_{2m}(q)$ pour $m \geq 4$,
    - $\mathrm{P}\Omega^-_{2m}(q)$ pour $m \geq 4$,
- un groupe exceptionnel de type Lie :
  - $E_n(q)$ pour $n = 6,7,8$,
  - $F_4(q)$,
  - $G_2(q)$ pour $q \geq 3$,
  - ${}^3D_4(q)$,
  - ${}^2E_6(q)$,
  - ${}^2B_2(2^{2n+1})$ pour $n \geq 1$,
  - ${}^2F_4(2^{2n+1})$ pour $n \geq 1$,
  - ${}^2G_2(3^{2n+1})$ pour $n \geq 1$,
  - le groupe de Tits ${}^2F_4(2)'$,
- un des 26 groupes simples sporadiques soit :
  - les cinq groupes de Mathieu : M_{11}, M_{12}, M_{22}, M_{23}, M_{24},
  - les sept groupes du réseau de Leech : Co_1, Co_2, Co_3, McL, HS, Suz, J_2,
  - les 3 groupes de Fisher : Fi_{22}, Fi_{23}, Fi'_{24},
  - les cinq groupes monstrueux : $\mathbb{M}$, $\mathbb{B}$, Th, HN, He,
  - les six parias : J_1, J_3, J_4, O'N, Ly, Ru.

Annexe B

Définitions et résultats utiles sur la théorie des groupes

Définition B.1. *Un groupe $(G, *)$ est la donnée d'un ensemble G muni d'une opération binaire $*$ telle qu'elle soit associative, qu'elle admette un élément neutre souvent appelé e_G et que tous les éléments admettent un élément inverse. En notation multiplicative, on omet parfois le symbole de l'opération en utilisant la concaténation. Quand l'opération n'est pas ambigüe, on utilise parfois seulement le symbole G pour le groupe.*

Définition B.2. *Soit G un groupe et X un ensemble. Une action de G sur X est une application $_._ : G \times X \to X$ telle que pour $g_1, g_2 \in G$ et $x \in X$, $(g_1 g_2).x = g_1.(g_2.x)$ et pour $(g, x) \mapsto g.x$ e_G, $e_G.x = x$.*

Définition B.3. *Soit G un groupe agissant sur un ensemble X. Soit $x \in X$. Alors, $G_x := \{g \in G : g.x = x\}$ s'appelle le stabilisateur de x.*

Définition B.4. *Soit G un groupe agissant sur un ensemble X de cardinalité au moins 2. On dit que l'action de G sur X est transitive si pour tout $x, y \in X$, il existe $g \in G$ tel que $g.x = y$. On dit que l'action est doublement transitive si pour toutes paires de paires $(x_1, x_2), (y_1, y_2) \in X \times X$ avec $x_1 \neq x_2$ et $y_1 \neq y_2$, il existe $g \in G$ tel que $g.(x_1, x_2) := (g.x_1, g.x_2) = (y_1, y_2)$.*

Définition B.5. *Soit G un groupe agissant sur un ensemble X de cardinalité au moins 2. On dit que l'action de G sur X est primitive s'il n'existe pas de partition propre $\{Y_i\}$ de X tel que $|Y_i| \geq 2$ et pour tout $g \in G$, soit $g.Y_i = Y_i$ ou $g.Y_i \cap Y_i = \emptyset$. Une telle partition s'appelle un système d'imprimitivité.*

Proposition B.1. *Si l'action de G sur X est doublement transitive, alors elle est primitive.*

Démonstration. Supposons le contraire. Alors, il existe un système d'imprimitivité $\{Y_i\}$. Soient $a, b \in Y_1$ et $c \in Y_2$. Alors, il n'existe pas de $g \in G$ tel que $g.(a,b) = (a,c)$ et l'action n'est pas doublement transitive. □

Définition B.6. *Soit G un groupe agissant sur un ensemble X. Alors, on dit que l'action de G sur X est fidèle si le seul élément de G qui fixe tous les éléments de X est le neutre e_G.*

Définition B.7. *Si $H \subseteq G$ est tel que $(H, *|_H)$ forme un groupe, alors H est un sous-groupe de G. De plus, si pour tout $g \in G$, on a que les ensembles $gH := \{gh : h \in H\}$ et $Hg := \{hg : h \in H\}$ sont égaux, alors H est un sous-groupe normal de G. Si un sous-groupe M de G est tel qu'il n'existe pas de sous-groupe de G tel que $M \subsetneq N \subsetneq G$, alors M est un sous-groupe maximal.*

Définition B.8. *Soit G un groupe et S un sous-ensemble de G. Alors, $\langle S \rangle$ est le plus petit sous-groupe de G contenant S. On dit que S engendre $\langle S \rangle$.*

Définition B.9. *Un groupe G non trivial est dit simple si les seuls sous-groupes normaux de G sont $\{e_G\}$ et G.*

Proposition B.2. *Soit G un groupe, N, H deux sous-groupes de G avec N normal. Alors, $NH := \{nh : n \in N, h \in H\}$ est un sous-groupe de G.*

Démonstration. En effet, pour n_1h_1 et $n_2h_2 \in NH$, on a que $(n_1h_1)(n_2h_2)^{-1} = n_1 \underbrace{h_1h_2^{-1}n_2^{-1}}_{\in h_1h_2^{-1}N = Nh_1h_2^{-1}} =$ $n_1n_3h_1h_2^{-1} \in NH$ pour un certain $n_3 \in N$. □

Définition B.10. *Un groupe G est dit parfait si*

$$G = \langle [x,y] : x, y \in G \rangle =: [G,G] =: G'$$

où $[x,y] := xyx^{-1}y^{-1}$ est appelé un commutateur et G' le groupe des commutateurs ou le groupe dérivé.

Définition B.11. *Un groupe est dit résoluble si sa suite dérivée*

$$G' = [G,G], G'' = \left[G', G'\right], G^{(3)} = \left[G'', G''\right], \cdots$$

est stationnaire à $\{e_G\}$, c'est-à-dire s'il existe $n \in \mathbb{Z}_{\geq 1}$ tel que $G^{(n)} = \{e_G\}$.

Définition B.12. *$Z(G) := \{z \in G : xz = zx \ \forall x \in G\}$ est un sous-groupe normal du groupe G appelé le centre de G.*

Bibliographie

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

[2] John H. Conway. *Atlas of Finite Groups : Maximal Subgroups and Ordinary Characters for Simple Groups.* Clarendon Press, 1985.

[3] Meinolf J. Geck. *An Introduction to Algebraic Geometry and Algebraic Groups.* Oxford Graduate Texts in Mathematics. Oxford University Press, 2004.

[4] Daniel Gorenstein. *Finite Simple Groups : An Introduction to Their Classification.* Plenum Press, 1982.

[5] Larry C. Grove. *Classical Groups and Geometric Algebra.* American Mathematical Society, 2002.

[6] Gunter Malle et Donna Testerman. *Linear Algebraic Groups and Finite Groups of Lie Type.* Cambridge University Press, 2011.

[7] Ronald Solomon. A brief history of the classification of the finite simple groups. *Bulletin of the American Mathematical Society*, 2001.

[8] Donald E. Taylor. *The Geometry of the Classical Groups.* Heldermann Verlag, 1992.

[9] Robert A. Wilson. *The Finite Simple Groups.* Graduate Texts in Mathematics. Springer London, 2009.