Filières MP/MPI - ENS de Paris-Saclay, Lyon, Rennes et Paris - Session 2024

Page de garde du rapport de TIPE

NOM : REENAN	Prénoms : Oscar Remy Fabien Rafaël
Classe : 932 (MP*)	
Lycée : Lycée du Parc	Numéro de candidat : 54579
Ville : Lyon	

Concours auxquels vous êtes admissible, dans la banque MP inter-ENS (les indiquer par une croix) :

ENS Cachan	MP - Option MP X Informatique	MP - Option MPI
ENS Lyon	MP - Option MP X Informatique - Option M	MP - Option MPI Informatique - Option P
ENS Rennes	MP - Option MP X Informatique	MP - Option MPI
ENS Paris	MP - Option MP Informatique	MP - Option MPI

Matière dominante du TIPE (la sélectionner d'une croix inscrite dans la case correspondante) :

Informatique		Mathématiques	X	Physique	

Titre du TIPE : Le "non-isomorphisme" entre les groupes simples $PSL_3(\mathbb{F}_4)$ et $PSL_4(\mathbb{F}_2)$.

Nombre de pages (à indiquer dans les cases ci-dessous) :

Texte	9	Illustration	1	Bibliographie	1

Attention, les illustrations doivent figurer dans le corps du texte et non en fin du document !

Résumé ou descriptif succinct du TIPE (6 lignes, maximum) :

On va realiser une étude succinte des groupes $PSL_3(\mathbb{F}_4)$ et $PSL_4(\mathbb{F}_2)$, le but etant de classifier les classes de conjugaisons d'elements d'ordre deux pour montrer qu'ils sont non isomorphe tout en etant de même cardinal et simple.
Pour ce faire on établira un théorème de Jordan en s'aidant du formalisme de Young.

À Lyon

Le 04/06/2024

Signature du (de la) candidat(e)

Signature du professeur responsable de la classe préparatoire dans la discipline

Cachet de l'établissement

LYCEE DU PARC
1, Boulevard Anatole France
69006 LYON
tél. 04 37 51 15 51 - INE 0690026d

Rapport TIPE ENS

Oscar REEMAN

2023-2024

Table des matières

Chapitre 1

Premiers pas

1.1 Introduction

Peut-il arriver que deux groupes finis G et H de même cardinal ne soient pas isomorphes ? La réponse est évidemment oui. On connait nombre d'exemples dans les petits groupes, par exemple $\mathfrak{S}_3$ et $\mathbb{Z}/6\mathbb{Z}$ pour le cardinal 6 ou encore $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. En revanche, si l'on rajoute comme hypothèse sur G et H qu'ils vérifient une propriété de plus, la *simplicité*, c'est immédiatement plus rare, on ne trouve plus aucun exemple à petits cardinaux (inférieur à 20 par exemple). En réalité, un premier exemple se trouve à l'ordre 20160 avec les groupes projectifs spéciaux linéaires (voir [1], [4] et [7]) $PSL_3(\mathbb{F}_4)$ et $PSL_4(\mathbb{F}_2)$. C'est la démonstration d'une partie de ce résultat que nous allons étudier. Nous laisserons de côté la preuve de la simplicité de ces deux groupes en raison de sa longueur, une idée de démonstration sera présentée en annexe.

1.2 Préléminaires

1.2.1 Définitions et notations

Sauf précision contraire on notera les lois des groupes multiplicativement

Définition 1 (Sous-groupe distingué) *Un groupe H de G est dit distingué dans G ou simplement normal (noté $H \trianglelefteq G$) s'il est stable par automorphisme intérieur (dit de conjuguaison), c'est à dire si*

$$\forall g \in G \quad gHg^{-1} := \{ghg^{-1}; h \in H\} = H$$

Définition 2 (Groupe simple) *Un groupe G est dit simple s'il n'admet pour sous-groupes distingués que le groupe trivial et lui-même.*

Définition 3 (Quotient d'un groupe par un sous groupe) *On définit le quotient d'un groupe G par un de ses sous groupes H (noté G/H) comme l'ensemble des classes à gauche de G suivant H, i.e. les gH. Quotienter G par H revient à créer la relation d'équivalence sur G suivante et définir G/H comme l'ensemble des classes d'équivalence par cette relation (on notera $\bar{g}$ la classe d'un élément $g \in G$ par la relation)*

$$\forall g_1, g_2 \in G \quad g_1 \sim g_2 \Leftrightarrow g_1^{-1} g_2 \in H$$

Définition 4 (Groupe spécial linéaire) *On définit le groupe spécial linéaire de degré n sur un corps commutatif $\mathbb{K}$ noté $SL_n(\mathbb{K})$, par les matrices carrées d'ordre n de déterminant 1.*

Définition 5 (Centre d'un groupe) *Le centre d'un groupe G est son commutant donc l'ensemble des éléments de G qui commutent avec tous autres.*

Définition 6 (Groupe projectif spécial linéaire) *On définit le Groupe projectif spécial linéaire noté $PSL_n(\mathbb{K})$ comme le quotient du groupe spécial linéaire par son centre (noté $SZ_n(\mathbb{K})$).*

1.2.2 Étude du groupe projectif spécial linéaire

Proposition 1 ($PSL_n(\mathbb{K})$ est un groupe)

Lemme 1 (groupe quotient) *Soient G un groupe et H un sous-groupe distingué de G, alors l'opération $\cdot$ sur les classes suivantes munit G/H d'une structure de groupe*

$$\forall g_1, g_2 \in G \quad (g_1H)\cdot(g_2H) = (g_1g_2H)$$

(i) H est évidemment neutre pour $\cdot$, l'operation est bien définie et ne dépend pas du représentant

(ii) $\cdot$ est une loi de composition interne car G est un groupe

(iii) Tout élément de G/H possède un inverse, en effet : $\forall g_1H \in G/H \quad (g_1H)\cdot(g_1^{-1}H) = H$

(iv) $\cdot$ est associative

$$\begin{aligned}\forall g_{1,2,3} \in G \quad ((g_1H)\cdot(g_2H))\cdot(g_3H) &= (g_1g_2H)\cdot(g_3H)\\ &= ((g_1g_2)g_3H)\\ &= (g_1(g_2g_3)H) \qquad \text{G un groupe donc loi associative}\\ &= (g_1H)\cdot(g_2g_3H)\\ &= (g_1H)\cdot((g_2H)\cdot(g_3H)) \qquad (1.1)\end{aligned}$$

Démonstration proposition 1 *On quotiente $SL_n(\mathbb{K})$ par un de ses sous-groupes $SZ_n(\mathbb{K})$*

(i) Le centre d'un groupe est toujours distingué dans ce dernier par construction

(ii) Par le lemme 1 on a alors immédiatement que $PSL_n(\mathbb{K})$ est un groupe pour la loi $\cdot$

On conclut bien que $(PSL_n(\mathbb{K}), \cdot)$ est un groupe.

Proposition 2 ($\mathbb{F}_q$ est un corps) *Si q est une puissance d'un nombre premier p alors $\mathbb{F}_q$ est un corps de caractéristique p.*

Démonstration proposition 2 *On admet cette preuve, une idée de démonstration ainsi que la construction des $\mathbb{F}_q$ pourra se trouver en annexe.*

Théorème 1 (Cardinal de $PSL_n(\mathbb{F}_q)$) *Soient n,q éléments de $\mathbb{N}$ supérieurs ou égals à deux alors le cardinal de $PSL_n(\mathbb{F}_q)$ noté $|PSL_n(\mathbb{F}_q)|$ vaut*

$$|PSL_n(\mathbb{F}_q)| = \prod_{k=0}^{n-1} \frac{(q^n - q^k)}{(q-1)pgcd(q-1,n)}$$

Démontrons quelques lemmes pour arriver à ce résultat :

Lemme 2 (Premier théorème d'isomorphisme) *Soient G et H des groupes, ϕ un morphisme de groupe de G vers H, alors ϕ se factorise et induit une injection de $G/ker(\phi)$ dans H (on note l'injection à l'aide du symbole $\hookrightarrow$).*

(i) Montrons que le noyau de ϕ est distingué dans G. Fixons $k \in Ker(\phi)$

$$\begin{aligned}\forall g \in G \quad \phi(gkg^{-1}) &= \phi(g)\phi(k)\phi(g^{-1})\\ &= \phi(g) * 1_H * \phi(g^{-1})\\ &= \phi(gg^{-1})\\ &= \phi(1_G)\\ &= 1_H\end{aligned}$$

On a donc bien pour tout g dans G, $\quad gKer(\phi)g^{-1} = Ker(\phi)$ et ainsi $Ker(\phi) \trianglelefteq G$

(ii) Montrons que ϕ est constante sur chaque classe d'équivalence modulo $Ker(\phi)$. Fixons $x, y \in G$ tels que $x \equiv y[Ker(\phi)] \Leftrightarrow xy^{-1} \in Ker(\phi)$, alors

$$\phi(xy^{-1}) = 1_H \quad \Leftrightarrow \quad \phi(x)\phi(y)^{-1} = 1_H \quad \Leftrightarrow \quad \phi(x) = \phi(y)$$

Donc ϕ est bien constante sur chaque classe modulo $Ker(\phi)$ et l'application passe bien au quotient

(iii) Montrons que l'application induite est injective. Fixons $\bar{g_1}, \bar{g_2} \in G/Ker(\phi)$ telles que $\bar{\phi}(\bar{g_1}) = \bar{\phi}(\bar{g_2})$, on a alors notamment

$$\phi(g_1) = \phi(g_2) \Leftrightarrow g_1 g_2^{-1} \in Ker(\phi) \Leftrightarrow g_1 \equiv g_2[Ker(\phi)] \Leftrightarrow \bar{g_1} = \bar{g_2}$$

Ainsi $\bar{\phi}$ est injective ce qui conclut la preuve de ce lemme

Lemme 3 (Lagrange) *Soit G un groupe fini et H un sous-groupe alors le cardinal de H divise celui de G et*

$$|G/H| \cdot |H| = |G|$$

(i) Grâce à la définition du groupe quotient, on sait que les éléments de G/H sont les classes d'équivalences par la relation introduite.

(ii) Or l'ensemble des classes d'équivalence forme une partition de G, on en déduit ainsi que

$$\begin{aligned} |\mathrm{G}| &= \sum_{\bar{g} \in G/H} |\bar{g}| \\ &= \sum_{\bar{g} \in G/H} |H| \qquad \big) \forall g \in G \quad |gH| = |H| \\ &= |G/H| \cdot |H| \qquad \big) \textit{on somme } |H| \textit{ } |G/H| \textit{ fois} \end{aligned} \tag{1.2}$$

On a alors bien le résultat voulu.

Lemme 4 (Cardinal de $Gl_n(\mathbb{F}_q)$) *Soient n,q éléments de $\mathbb{N}^*$ alors*

$$|Gl_n(\mathbb{F}_q)| = \prod_{k=0}^{n-1} (q^n - q^k)$$

On va procéder par étapes en dénombrant le nombre de bases de $\mathcal{M}_n(\mathbb{F}_q)$ ce qui, sur un corps fini, nous donnera alors le nombre d'éléments inversibles de $\mathcal{M}_n(\mathbb{F}_q)$ et donc le cardinal de $Gl_n(\mathbb{F}_q)$ ($\star$).

(i) N'importe quel n-uplet x_1 non nul de $\mathbb{F}_q$ est une famille libre à n éléments. On a donc $q^n - 1$ possibilités

(ii) Pour choisir le second n-uplet x_2 dans $\mathbb{F}_q$ tel que (x_1, x_2) soit libre, on a désormais accès à tout les n-uplets de $\mathbb{F}_q$ qui ne sont ni nuls ni liés à x_1, on a donc $q^n - 1 - (q-1) = q^n - q$ possibilités. Ceci nous donne $(q^n - 1)(q^n - q)$ familles libres à deux n-uplets de $\mathbb{F}_q$

(iii) on continu à construire notre base vecteur par vecteur et on aboutit bien à un total de $\prod_{k=0}^{n-1} (q^n - q^k)$ bases.

Ainsi par (iii) et ($\star$) on obtient bien le résultat voulu.

Proposition 3 *Le cardinal de $SL_n(\mathbb{F}_q)$ est* $\prod_{k=0}^{n-1} \frac{(q^n - q^k)}{(q-1)}$

Démonstration proposition 3 *On a*

$$det \quad : \quad (GL_n(\mathbb{F}_q), \times) \to (\mathbb{F}_q^*, \times)$$

Un morphisme surjectif (on construit facilement des antécédents en prenant une matrice diagonale avec des 1 sur la diagonale sauf en haut à gauche par exemple)

(i) Le noyau de ce morphisme est exactement $Sl_n(\mathbb{F}_q)$

(ii) Par le lemme 2, on en déduit que ce morphisme se factorise et induit une bijection de $(GL_n(\mathbb{F}_q)/SL_n(\mathbb{F}_q), \cdot)$ dans $(\mathbb{F}_q^*)$

(iii) Grâce au lemme 3, on a alors l'égalité de cardinaux entre ces deux groupes et on en déduit alors à l'aide du lemme 4 que

$$|GL_n(\mathbb{F}_q)|/|SL_n(\mathbb{F}_q)| = |\mathbb{F}_q^*| \Leftrightarrow |SL_n(\mathbb{F}_q)| = \prod_{k=0}^{n-1} \frac{(q^n - q^k)}{(q-1)}$$

Proposition 4 *Le Cardinal de $SZ_n(\mathbb{F}_q)$ est $pgcd(n, q-1)$.*

Démonstration proposition 4 *On va d'abord montrer que $SZ_n(\mathbb{F}_q)$ est isomorphe à une autre structure que nous dénombrerons ce qui nous donnera le cardinal de $SZ_n(\mathbb{F}_q)$*

(i) Premièrement $SZ_n(\mathbb{F}_q)$ est isomorphe à $A := \{\alpha \in \mathbb{F}_q^* \quad | \quad \alpha^n = 1\}$

(ii) Notons $d := pgcd(n, q-1)$ et montrons par double inclusion que A est égal à $B := \{\alpha \in \mathbb{F}_q^* \quad | \quad \alpha^d = 1\}$
$\boxed{\subset}$ Fixons $x \in A$, alors

$$\begin{cases} x^n & = 1 \quad car\ x\ appartient\ à\ A \\ x^{q-1} & = 1 \quad par\ Lagrange\ car\ le\ groupe\ des\ inversibles\ est\ d'ordre\ q\text{-}1 \\ d & = (q-1) * r + s * n \quad s, r \in \mathbb{Z}^* \quad par\ Bézout \end{cases}$$

D'où

$$x^d = x^{sn} x^{(q-1)r} = 1 \Leftrightarrow x \in B$$

$\boxed{\supset}$ Fixons $x \in B$, en gardant les mêmes notations que pour l'inclusion précédente on a immédiatement, comme d divise n,

$$x^n = 1 \Leftrightarrow x \in A$$

Ainsi $A = B$

(iii) Le Polynôme $X^{q-1} - 1$ a $q-1$ racines dans $\mathbb{F}_q^*$ (Lagrange) et $X^d - 1$ divise $X^{q-1} - 1$ par (ii) et a donc d racines dans $\mathbb{F}_q^*$ ce qui conclut la preuve de cette proposition.

Démonstration Théorème 1 *Le résultat est immédiat grâce aux lemmes et propositions précédentes.*

Chapitre 2

De même cardinal mais non isomorphes

2.1 Étude de nos groupes spéciaux linéaires

2.1.1 Réduction du problème

Dans les préléminaires on a annoncé que ces deux groupes sont de même cardinal (à savoir 20160), observons la structure de ces deux groupes

(i)

$$\begin{aligned} SZ_4(\mathbb{F}_2) &= \{\alpha I_4 \mid \alpha \in \mathbb{F}_2, det(\alpha I_4) = 1\} \\ &= \{\alpha I_4 \mid \alpha^4 = 1, \quad \alpha \in \mathbb{F}_2\} \\ &= \{\alpha I_4 \mid \alpha^2 = 1, \quad \alpha \in \mathbb{F}_2\} \\ &= \{\alpha I_4 \mid \alpha = \pm 1, \quad \alpha \in \mathbb{F}_2\} \\ &= \{I_4\} \end{aligned}$$

D'où $PSL_4(\mathbb{F}_2) = SL_4(\mathbb{F}_2) = GL_4(\mathbb{F}_2)$

(ii) De même, on montre que $SZ_3(\mathbb{F}_4) = \mathbb{U}_3$ et ainsi

$$PSL_3(\mathbb{F}_4) = SL_3(\mathbb{F}_4)/\mathbb{U}_3$$

2.1.2 Structure de la démonstration

(i) On va établir un certain nombre de résultats importants de réduction notamment sur la correspondance entre orbites nilpotentes et partitions de n

(ii) Ensuite, on montrera qu'étudier l'orbite par conjuguaison d'éléments d'ordres deux de notre groupe revient à étudier les orbites nilpotentes (orbites par conjuguaison d'éléments nilpotents) de leur décomposition de Jordan

(iii) Enfin, on montrera grâce à ces résultats que nos deux groupes n'ont pas le même nombre de classes de conjuguaisons d'élements d'ordre 2, ce qui rend impossible l'existence d'un isomorphisme entre les deux groupes et permettra de conclure

2.2 Un Théorème de Jordan

2.2.1 Nilpotents et Diagramme de Young

On notera $\mathcal{N}_n(\mathbb{C})$ l'ensemble des matrices nilpotentes sur $\mathbb{C}$ d'ordre $n \in \mathbb{N}^*$

Proposition 5 (Noyaux Itérés) *Fixons $A \in \mathcal{N}_n(\mathbb{C})$ et notons $K_i = Ker(A^i)$, alors la suite $(Dim(K_i))_{i\in\mathbb{N}}$ est concave, c'est à dire*

$$\forall i \in \mathbb{N}^* \quad 0 \leq Dim(K_{i+1}) - Dim(K_i) \leq Dim(K_i) - Dim(K_{i-1})$$

Démonstration proposition 5 *Notons $m \in \mathbb{N}^*$ le nihlindice de A qu'on supposera supérieur à 1 (le résultat est trivialement vrai pour $A = 0_{\mathcal{M}_n(\mathbb{C})}$)*

(i) On a alors la suite suivante qui prouve la positivité de la suite $\lambda_i := Dim(K_i) - Dim(K_{i-1})$

$$0 = K_0 \subset K_1 \subset \cdots \subset K_m = \mathbb{C}^n$$

(ii) Fixons-nous $i > 1$, on considère la suite de fonctions suivante

$$\begin{array}{ccccc} K_{i+1} & \xrightarrow{\psi} & K_i & \xrightarrow{\pi_i} & K_i/K_{i-1} \\ X & \mapsto & AX & \mapsto & \overline{AX} \end{array}$$

π_i est donc la projection canonique, montrons que le noyau de $\pi_i \circ \psi$ est K_i

On a de plus

$$M \in \pi^{-1}(\bar{0}) \quad \Leftrightarrow \quad \overline{M} = \bar{0} \quad \Leftrightarrow \quad M - 0 \in K_{i-1} (\star\star)$$
$$\text{Par construction de } \psi, \quad \psi^{-1}(K_{i-1}) = K_i (\star\star\star)$$

Ce qui nous permet d'expliciter le noyau de $\pi \circ \psi$

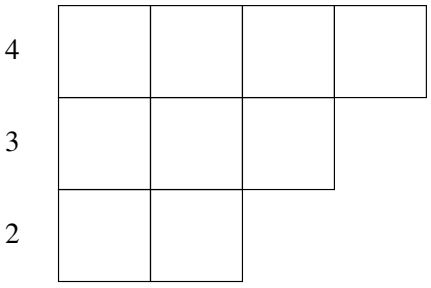
$$\begin{aligned} Ker(\pi_i \circ \psi) &= \{M \in K_{i+1} \quad | \quad \pi_i(\psi(M)) = \{\bar{0}\}\} \\ &= (\pi_i \circ \psi)^{-1}(\{\bar{0}\}) \\ &= \psi^{-1} \circ \pi_i^{-1}(\{\bar{0}\}) \\ &= \psi^{-1}(K_{i-1}) \qquad \curvearrowright \star\star \\ &= K_i \qquad \curvearrowright \star\star\star \end{aligned} \tag{2.1}$$

Donc par les Théorème d'isomorphisme et de Lagrange on conclut que

$$K_{i+1}/K_i \hookrightarrow K_i/K_{i-1} \Rightarrow \boxed{Dim(K_{i+1}) - Dim(K_i) \leq Dim(K_i) - Dim(K_{i-1})}$$

Définition 7 *Un diagramme de Young est un tableau qui permet de représenter une partition de l'entier n* $(\sum_{i=1}^{r} \alpha_i = n$ *tels que* $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_r > 0$, $r \in \mathbb{N}^*)$.

***Exemple* 1** *Voici le tableau de Young associé à la partition de 9 : (4,3,2)*



Définition 8 *Un diagramme de Young associé à une orbite nilpotente est le diagramme de Young associé à la partition de n les $(\lambda_i)_{i \in \mathbb{N}}$.*

Proposition 6 *Il existe une base dans laquelle une matrice nilpotente s'écrit comme une matrice diagonale par bloc où les blocs sont de Jordan de taille décroissante et associé à la partition duale des noyaux itérés (obtenue par symétrie par rapport à la diagonale partant du coin haut gauche du tableau de Young de λ).*

Lemme 5 *En conservant les notations de la proposition précédente avec $A \in \mathcal{N}_n(\mathbb{C})$ de nilindice m, on peut noter G_i le supplémentaire de K_{i-1} dans K_i de telle sorte que $\forall i \in [\![1\ ;\ m]\!]$, $K_i = K_{i-1} \bigoplus G_i$ et ainsi, si ces conditions sont vérifiées pour i fixé*

$$\begin{cases} v \in G_i \\ A^{i-1}v = 0 \end{cases}$$

alors v est nul

L'application $A^{i-1}_{|G_i}$ ($M \mapsto A^{i-1}M$ restreinte à G_i) est injective par construction.

Démonstration proposition 6 *On va construire une base adaptée par récurrence descendante. On conserve les notations utilisées pour les supplémentaires des K_m*

(i) On a $K_m = K_{m-1} \bigoplus G_m$ avec notamment $dim(G_m) = dim(K_m) - dim(K_{m-1}) = \lambda_m$. On se construit alors une base de G_m avec le théorème de la base incomplète $(v_m^1, \cdots, v_m^{\lambda_m})$.

(ii) On a également $K_{m-1} = K_{m-2} \bigoplus G_{m-1}$. Par décroissance de la suite $(\lambda_i)_i$ on a $\lambda_m = dim(G_m) \leq dim(G_{m-1}) = \lambda_{m-1}$ or grâce au lemme 5 on sait que la famille $(Av_m^1, \cdots, Av_m^{\lambda_m})$ est libre dans G_{m-1}, on peut alors la compléter en une base : $(Av_m^1, \cdots, Av_m^{\lambda_m}, v_{m-1}^{\lambda_m+1}, \cdots, v_{m-1}^{\lambda m-1})$

(iii) Par récurrence descendante, on peut remplir le diagramme de Young en partant du bas en ayant dans la ligne i la base de G_{m-i} et ainsi obtenir une base de $\mathbb{C}^n$ par la décomposition en somme directe du lemme 5.

$A^{m-1}v_m^1$	$\cdots$	$\cdots$	$A^{m-1}v_m^{\lambda m}$	$\cdots$	$\cdots$	$A^{m-2}v_{m-1}^{\lambda_{m-1}}$	$\cdots$	$\cdots$	$v_1^{\lambda_1}$
$\vdots$	$\vdots$	$\vdots$				$\vdots$			
Av_m^1	Av_m^2	$\cdots$	$Av_m^{\lambda_m}$	$v_{m-1}^{\lambda_m+1}$	$\cdots$	$v_{m-1}^{\lambda_{m-1}}$			
v_m^1	v_m^2	$\cdots$	$v_m^{\lambda_m}$						

Ainsi en lisant de haut en bas de gauche à droite on obtient la base suivante :
$\mathcal{B} = (A^{m-1}v_m^1, Av_m^1, \cdots, v_m^1, \cdots, A^{m-1}v_m^{\lambda_m}, \cdots, v_m^{\lambda_m}, \cdots, v_1^{\lambda_1})$ dans laquelle l'endomorphisme associé à A est la diagonale par blocs de Jordan suivante

$$A = \begin{pmatrix} J_{\lambda_1^*} & & 0 \\ & \ddots & \\ 0 & & J_{\lambda_k^*} \end{pmatrix}$$

Où λ_i^* est un élément de la partition duale de λ définie par $\lambda_i^* := |\{j \geq 1, \quad \lambda_j \geq i\}|$

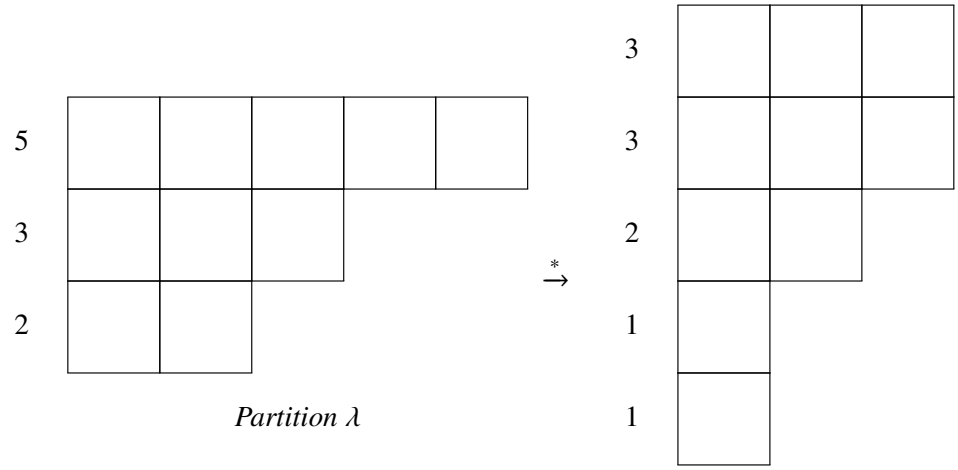
Exemple 2 *Prenons $A \in \mathcal{N}_{10}(\mathbb{C})$ de nilhindice 3 tel que $dim(K_1) = 5$, $dim(K_2) = 8$, $dim(K_3) = 10$, par exemple*

$$A = \begin{pmatrix} 0 & 1 & & & 0 & & & & & 0 \\ & 0 & 1 & & & \ddots & & & & \\ & & 0 & & & & \ddots & & & \\ & & & 0 & 1 & & & \ddots & & \\ 0 & & & & 0 & 1 & & & \ddots & \\ & \ddots & & & & 0 & & & & 0 \\ & & \ddots & & & & 0 & 1 & & \\ & & & \ddots & & & & 0 & & \\ & & & & \ddots & & & & 0 & \\ 0 & & & & & 0 & & & & 0 \end{pmatrix}$$

On a alors

(i) $\lambda_1 = 5$, $\lambda_2 = 3$ *et enfin* $\lambda_3 = 2$ *qui forment bien une partition de 10*

(ii) Ainsi, par la définition de partition duale, on a $\lambda^* = (3, 3, 2, 1, 1)$ *(également une partition de 10)*



Partition λ *Partition duale* λ^*

(iii) Enfin, dans la base adaptée qu'on construit comme dans la proposition 6 , A s'écrit

$$A = \begin{pmatrix} J_3 & & & & 0 \\ & J_3 & & & \\ & & J_2 & & \\ & & & J_1 & \\ 0 & & & & J_1 \end{pmatrix}$$

Ce qui pouvait ici se voir immédiatement sur A

2.2.2 Revenons aux orbites nilpotentes

Les résultats de la partie précédente nous permettent enfin d'établir la correspondance entre les orbites nilpotente et les partitions de l'entier n

Théorème 2 (Jordan) *En notant* $\mathcal{O}_A$ *l'orbite de la matrice A par l'action de conjuguaison et* $\mathcal{Y}(A)$ *le diagramme de Young de la matrice A alors on a l'équivalence suivante pour* $n \in \mathbb{N}^*$

$$\forall A, B \in \mathcal{N}_n(\mathbb{C}), \quad \mathcal{O}_A = \mathcal{O}_B \Leftrightarrow \mathcal{Y}(A) = \mathcal{Y}(B)$$

Ce qui, en notant J_ν *la réduite de Jordan associée à une partition* $\nu = (\nu_1, \cdots, \nu_m)$ *de n (notée* $\nu \vdash n$*) se reformule de facon équivalente par*

$$\begin{array}{rcl} \psi : \{\text{Partitions de } n\} & \longrightarrow & \{\text{Classes de similitudes de} \mathcal{N}_n(\mathbb{C})\} \\ \nu \vdash n & \longmapsto & \mathcal{O}_{J_\nu} \end{array}$$

est une bijection.

Démonstration Théorème 2 *L'équivalence est évidente grâce aux résultats de la partie précédente*

2.3 Un non-isomorphisme exceptionnel

Théorème 3 (Le "non-isomorphisme") *$PSL_4(\mathbb{F}_2)$ et $PSL_3(\mathbb{F}_4)$ ne sont pas isomorphes.*

On entame la démonstration.

Proposition 7 (Classes dans $PSL_4(\mathbb{F}_2)$) *$PSL_4(\mathbb{F}_2)$ a deux classes de conjuguaisons d'éléments d'ordre deux.*

Démonstration proposition 7 *Étudions les éléments d'ordre 2 de $PSL_4(\mathbb{F}_2)$.*

(i) Soit $M \in PSL_4(\mathbb{F}_2) = GL_4(\mathbb{F}_2)$ alors $M^2 = I_4$. Ainsi le polynôme $(X-1)(X+1) = (X-1)^2$ (caractéristique 2) annule M. La décomposition de Dunford d'une telle M est donc $M = I_4 + N$ ou N est nilpotente d'indice 2

(ii) Cette décomposition nous permet notamment de conclure que le nombre de classes de conjuguaisons d'élements d'ordre 2 de $GL_4(\mathbb{F}_2)$ est donné par le nombre d'orbites nilpotentes d'éléments de nilhindice 2 dans $GL_4(\mathbb{F}_2)$ ($M \mapsto M - I_4$ établit une bijection entre les deux), et donc par le nombre de partitions de 4 commencant par 2 (Sinon on aurait par exemple les classes de J_4, J_3 qui ne sont pas de nilhindice 2)

(iii) Ainsi $GL_4(\mathbb{F}_2)$ possède 2 classes de conjuguaisons d'ordre 2 (associés à $2 \geq 2, 2 \geq 1 \geq 1$) ce qui conclut cette démonstration

On montre de la même manière que $GL_3(\mathbb{F}_4)$ possède une classe de conjugaison d'ordre 2, de plus, comme sa caractéristique est également 2 (grâce à la proposition 2). Il nous faut désormais nous ramener à $SL_3(\mathbb{F}_4)$ puis a $PSL_3(\mathbb{F}_4)$.

Proposition 8 (Classes dans $PSL_3(\mathbb{F}_4)$) *$PSL_3(\mathbb{F}_4)$ possède une seule classe de conjuguaison d'élements d'ordre 2.*

Démontrons d'abord un lemme.

Lemme 6 *$SL_3(\mathbb{F}_4)$ possède également une seule classe de conjugaison d'éléments d'ordre 2*

Pour démontrer ce résultat il suffit de montrer que si deux éléments d'ordre 2 sont conjugués dans $GL_3(\mathbb{F}_4)$, alors ils le sont dans $SL_3(\mathbb{F}_4)$.

(i) Quitte à prendre un élément d'ordre 2 de $GL_3(\mathbb{F}_4)$ autant prendre la réduite de Jordan associée à la partition $\nu = 2 \geq 1$

(ii) Soit M conjuguée à $I_3 + J_\nu$ alors on a $M = P(I_3 + J_\nu)P^{-1}$, $\quad P \in GL_3(\mathbb{F}_4)$. Il nous suffit de prendre

$$Q = P \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & det(P^{-1}) \end{pmatrix}$$

et on a $M = Q(I_3 + J_\nu)Q^{-1}$, $\quad Q \in SL_3(\mathbb{F}_4)$

(iii) Conclusion M est bien $SL_3(\mathbb{F}_4)$-conjuguée à $(I_3 + J_\nu)$ et $SL_3(\mathbb{F}_4)$ possède bien 1 seule classe de conjuguaison d'éléments d'ordre 2

On veut désormais montrer que le résultat passe au quotient et que $PSL_3(\mathbb{F}_4)$ possède une seule classe de conjuguaison d'éléments d'ordre 2.

Démonstration proposition 8 *Montrons que si $\bar{B}$ est d'ordre 2 dans $PSL_3(\mathbb{F}_4)$ alors $\bar{B}$ est conjugué à $\overline{(I_3 + J_v)}$.*

(i) Si $\overline{B}^2 = \overline{I_3}$ alors par définition de $PSL_3(\mathbb{F}_4)$ on a $B^2 = \lambda I_3, \quad \lambda \in \mathbb{U}_3$

(ii) Comme $x \mapsto x^2$ est un automorphisme sur $\mathbb{F}_4^*$ il existe $\mu \in \mathbb{U}_3$ tel que $\mu^2 = \lambda$.

(iii) En posant $A := \mu^{-1}B$ on remarque deux choses. Premièrement que $A^2 = I_3$ et donc que A est dans la classe de $(I_3 + J_v)$ par le lemme 6 et le théorème 2. Deuxièmement que $AB^{-1} = \mu I_3$ et donc que $\bar{B} = \bar{A} = \overline{(I_3 + J_v)}$. Ainsi $\bar{B}$ est bien conjugué à $\overline{(I_3 + J_v)}$.

Ainsi tout élément d'ordre 2 de $PSL_3(\mathbb{F}_4)$ est conjugué a $\overline{(I_3 + J_v)}$ ce qui permet de conclure que le résultat du lemme 6 passe bien au quotient et que $PSL_3(\mathbb{F}_4)$ ne possède qu'une classe d'éléments d'ordre 2.

Démonstration Théorème 3 *À l'aide des propositions 7 et 8 on a démontré que $PSL_4(\mathbb{F}_2)$ et $PSL_3(\mathbb{F}_4)$ n'ont pas le même nombre de classes de conjuguaisons d'éléments d'ordre deux. Or la présence d'un isomorphisme entre ces deux groupes assurerait non seulement l'envoi des éléments d'ordre deux de l'un sur l'autre mais aussi la préservation des classes de conjugaisons. Ce qui permet de conclure que $PSL_4(\mathbb{F}_2)$ et $PSL_3(\mathbb{F}_4)$ bien que simples et de même cardinal ne sont pas isomomorphes* [1].

1. On pourra noter que la présence d'une telle situation semble extrêmement rare puisque si l'on en croit [7] il faut pousser jusqu'à l'ordre 4 585 351 680 pour trouver à nouveau deux groupes simples non isomorphes de même cardinal.

Chapitre 3

Annexes

3.1 La simplicité des groupes étudiés

L'idée générale est de ramener l'étude du groupe à l'étude de certaines classes de conjuguaisons. On procèderait alors ainsi

(i) On se donne $\overline{H}$ un sous groupe distingué de $PSL_n(\mathbb{K})$ (ou si n vaut 2, $\mathbb{K}$ est différent de $\mathbb{F}_2$ ou de $\mathbb{F}_3$) non réduit au neutre. Ce qui nous donne un sous groupe distingué H non réduit au neutre de $SL_n(\mathbb{K})$ qui contient $SZ_n(\mathbb{K})$

(ii) Puisque les transvections engendrent $SL_n(\mathbb{K})$ et qu'elles sont conjuguées entre elles, il suffit de montrer que H en contient une et on a gagné. On part de $\sigma \in H$ et on utilise les commutateurs pour fabriquer de nouveaux éléments de H à partir d'éléments de $SL_n(\mathbb{K})$

(iii) On va chercher un élément de H qui laisse invariant un hyperplan pour la raison suivante. Si τ est une transvection d'hyperplan N (c'est a dire que $N = ker(\tau - Id)$) alors $\sigma\tau\sigma^{-1}$ est une transvection d'hyperplan $\sigma(N)$ et le commutateur de σ et τ ($c = (\sigma\tau\sigma^{-1})\tau^{-1} = \sigma(\tau\sigma^{-1}\tau^{-1})$) est un produit de deux transvections et surtout un élément de H comme produit de deux éléments de H. On peut alors remarquer que si $\sigma(N) = N$ et $c \neq Id$ alors c est une transvection également ! On aura alors construit une transvection dans H et montré la simplicité de $PSL_n(\mathbb{K})$ [1]

3.2 La structure des corps ayant pour cardinal une puissance d'un nombre premier

On connaît bien les corps de cardinaux premiers à savoir les $\mathbb{Z}/p\mathbb{Z}$ qui sont les uniques corps de cardinaux p, mais moins ceux de cardinaux une puissance d'un nombre premiers qui donnent donc d'autres corps de même caractéristique que les $\mathbb{Z}/p\mathbb{Z}$. Un certains nombre de résultats assez classiques existent sur les corps qui nous permettent de définir les $\mathbb{F}_q$ évoqués plus haut.

(i) Un corps est soit de caractéristique nulle (comme $\mathbb{Q}$) soit de caractéristique un nombre premier

(ii) Le cardinal d'un corps fini est p^n pour un certain $n \in \mathbb{N}^*$ avec p sa caractéristique et il est unique (à isomorphisme près)

(iii) Sa construction se réalise à partir de l'algèbre $\mathbb{F}_p[X]$ qu'on quotiente par un polynôme irréductible de degré n sur $\mathbb{F}_p[X]$ (sous réserve d'existence) en utilisant notamment le théorème de Bézout pour les polynômes [2]

1. Le lecteur curieux pourra se reporter à [1] pour une preuve complète et détaillée de ce résultat

2. Pour une construction rigoureuse de ces corps comportant notamment la preuve de l'existence d'un polynôme irréductible de degré voulu on pourra se raporter a [8]

Bibliographie

[1] Daniel Perrin : *Cours d'Algèbre* Ellipses, première édition, 1996.

[2] Xavier Gourdon : *Les maths en tête* Ellipses, deuxième édition, 2009.

[3] Jérôme Germoni et Philippe Caldero : *Nouvelles histoires hédonistes de groupes et de géométries : Tome premier* Calvage & Mounet, première édition, 2013.

[4] Jérôme Germoni et Philippe Caldero : *Nouvelles histoires hédonistes de groupes et de géométries : Tome second* Calvage & Mounet, première édition, 2015.

[5] Gérard Rauch, dirigé par Charles Michel Marle et Philippe Pilobossian : *Les groupes finis et leurs représentations* Ellipses, première édition, 2000.

[6] Nicolas Bourbaki : *Éléments de Mathématiques, Livre II, Algèbre V : corps commutatifs* Hermann, deuxième édition, 1952.

[7] John Horton Conway, R.T. Curtis, S.P. Norton, R.A. Parker et R.A. Wilson : *Atlas of Finite Groups : Maximal Subgroups and Ordinaray Characters for Simple Groups* With computational assistance from J.G Thackray, 1985.

[8] Lindsay N. Childs : *A Concrete Introduction to Higher Algebra* Springer, troisième édition, 2009.

[9] Leslie Lamport : *LaTeX : a document preparation system*. Addison-Wesley, second édition, 1994.