Université de Montréal

Les groupes simples de Conway

par

Christian Côté

Département de mathématiques et de statistique

Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures

en vue de l'obtention du grade de

Maître ès sciences (M.Sc.)
en mathématiques

16 décembre 2002

Université de Montréal

Faculté des études supérieures

Ce mémoire intitulé

Les groupes simples de Conway

présenté par

Christian Côté

a été évalué par un jury composé des personnes suivantes :

Dana Schlomiuk

(président-rapporteur)

Abraham Broer

(directeur de recherche)

Gert Sabidussi

(membre du jury)

Mémoire accepté le:

12 février 2003

RÉSUMÉ ET MOTS CLÉS

RÉSUMÉ

Ce mémoire présente la construction, faite par John Horton Conway en 1968, de trois groupes simples sporadiques. Tout le matériel est basé sur l'article original de Conway (voir [**Conway**]).

Tout commence avec le réseau de Leech. Ce réseau, qu'on dénote par Λ, se situe dans $\mathbb{R}^{24}$. On s'intéresse au groupe de symétrie de Λ qui fixe l'origine. Ce groupe sera dénoté par $\cdot 0$. On donne d'abord une définition de Λ différente de celle donnée par Leech (Chapitre 3). Cette définition nécessite l'existence d'un système de Steiner de type $S(5,8,24)$ (Chapitre 1). Le groupe d'automorphismes de ce système est le groupe de Mathieu M_{24} (Chapitre 2). Les propriétés de $S(5,8,24)$ et de son groupe d'automorphismes nous aiderons à calculer l'ordre de $\cdot 0$ (Chapitre 4).

Avec cet ordre, ainsi qu'avec la connaissance de deux éléments explicites de M_{24}, on peut démontrer la simplicité de trois groupes reliés à $\cdot 0$: le quotient de $\cdot 0$ par son centre, que nous dénoterons par $\cdot 1$, le stabilisateur dans $\cdot 1$ d'un vecteur de Λ à distance $4\sqrt{2}$ de l'origine et le stabilisateur dans $\cdot 1$ d'un vecteur de Λ à distance $4\sqrt{3}$ de l'origine (Chapitre 5).

MOTS CLÉS

Systèmes de Steiner de type $S(5,8,24)$, Groupes de Mathieu, Réseau de Leech, Groupes de Conway, Groupes simples sporadiques.

ABSTRACT AND KEY WORDS

ABSTRACT

This memoir present the discovery, by John Horton Conway in 1968, of three sporadic simple groups. All the material is based on the article of Conway (see [**Conway**]).

This story begins with the Leech lattice. This lattice, that we denote by Λ, lives in $\mathbb{R}^{24}$. We will be interested by the symmetry group of Λ that fixes the origin. This group will be denoted by $\cdot 0$. We first give a definition of Λ , different from the one given by Leech (Chapter 3). This definition requires the existence of a Steiner system of type $S(5,8,24)$ (Chapter 1). The automorphism group of this system is the Mathieu group M_{24} (Chapter 2). The properties of $S(5,8,24)$ and of its automorphism group will help us to compute the order of $\cdot 0$ (Chapter 4).

With this order, and with the knowledge of two special elements of M_{24}, we can show the simplicity of three groups related to $\cdot 0$: the quotient of $\cdot 0$ by its center, we will denote it by $\cdot 1$, the stabilizer in $\cdot 1$ of a vector in Λ which has distance $4\sqrt{2}$ to the origin and the stabilizer in $\cdot 1$ of a vector in Λ which has distance $4\sqrt{3}$ to the origin (Chapter 5).

KEY WORDS

Steiner System of type $S(5,8,24)$, Mathieu groups, Leech lattice, Conway groups, sporadic simple groups.

Table des matières

REMERCIEMENTS

Avant toute chose, je voudrais remercier Émilie Raymond sans qui je ne me serais jamais rendu si loin. Merci d'avoir cru en moi et merci pour ta patience.

Je remercie également mes parents et ma soeur pour m'avoir toujours écouté et remonté le moral.

Mon directeur de maîtrise, Abraham Broer, a su trouver un sujet qui m'a passionné du début jusqu'à la fin. Il a également fait germer des questions intéressantes dans mon esprit. Merci pour tout.

Grâce au CRSNG, j'ai pu me consacrer entièrement à mes études sans me soucier des problèmes monétaires. Je remercie donc l'organisme de m'avoir accordé une bourse.

En terminant, je tiens à dire un gros merci à tous les étudiants du département de mathématiques et statistique de l'Université de Montréal, en particulier : Dimitri Zuchowski, Gabriel Chênevert, Jérôme Fournier, Pehoh et surtout Nicolas Beauchemin.

INTRODUCTION

Un des plus gros accomplissements des mathématiques, lors du XX^e siècle, est sans nul doute la classification des groupes simples finis. Ce théorème s'énonce comme suit :

> Soit G un groupe simple fini (un groupe ne possédant aucun sous-groupe normal propre). Alors G est isomorphe à un des groupes suivants :
>
> i) un groupe cyclique d'ordre premier ou un groupe alterné avec $n \geq 5$;
>
> ii) un groupe de type de Lie ;
>
> iii) un des 26 groupes sporadiques (qui ne font pas parti des groupes en i) et ii)).

Pour arriver à énoncer ce théorème, il a d'abord fallu découvrir tous les groupes simples finis. Ce périple débuta en 1861 lorsqu'Émile Mathieu découvrit cinq groupes simples sporadiques. À cette époque, on connaissait déja, grâce à Galois, la simplicité de A_n pour $n \geqslant 5$. Dans la première moitié du XX^e, on découvrit toutes les familles infinies de groupes simples (A_n pour $n \geqslant 5$ est un exemple de famille infinie de groupe simples). Entre les années 1965 et 1981, on découvrit un total de 21 groupes simples sporadiques.

On conjectura par la suite qu'il n'existait pas d'autre groupes simples que ceux qui avaient été trouvés. Cette conjecture est devenu le théorème de la classification des groupes simples finis. En 1985, on annonça que le Théorème avait été démontré. Cependant, on s'aperçu par après que la preuve n'était pas complète. L'ouvrage récent de M. Aschbacher et S.D. Smith devrait la compléter.

En comptant tous les écrits relatifs à cet édifice des mathématiques, on obtient environ 10 000 pages d'articles, de livres, etc !

Ce mémoire présente une incursion dans cette gigantesque oeuvre en expliquant la construction des groupes simples de John H. Conway en 1968. Tout commenca avec John Leech qui s'intéressa au problème d'empilement de sphères en plusieurs dimensions. Ce problème consiste à placer des boules de même dimension dans $\mathbb{R}^n$, avec au plus un point d'intersection entre deux boules données, qui occupent le plus d'espace possible. Il découvra, en 1965, un réseau dans $\mathbb{R}^{24}$. Lorsqu'on placait une boule, de rayon approprié, centrée en chaque point de ce réseau, cela donnait un empilement qui occupait une grande proportion de $\mathbb{R}^{24}$. Conway s'intéressa au groupe de symétrie de ce réseau. Il calcula son ordre et démontra grâce à ceci la simplicité de trois nouveaux groupes sporadiques.

On trouve une vaste littérature concernant les groupes de Conway. Plusieurs de ces écrits utilisent des outils avancés en théorie des groupes. Cet ouvrage, par contre, ne fait appel qu'à des méthodes élémentaires. Ce mémoire donne la totalité des arguments trouvés dans l'article original de Conway (voir [**Conway**]).

Le premier chapitre présente une généralisation des plans projectifs, les systèmes de Steiner. Une attention particulière est accordée au système $S(5,8,24)$. Celui-ci permettra, d'abord, de donner une définition plus pratique du réseau de Leech et ensuite aidera à calculer l'ordre de son groupe de symétrie.

Le chapitre deux porte sur les groupes de Mathieu, plus précisément sur le groupe M_{24}. Deux propriétés importantes de celui-ci sont démontrées : sa 5-transitivité ainsi que le fait qu'il est isomorphe au groupe d'automorphismes du système de Steiner $S(5,8,24)$. Cette dernière information est nécessaire pour le calcul de l'ordre du groupe de symétrie du réseau de Leech.

Le chapitre trois expose la définition du réseau de Leech en utilisant les résultats sur le système de Steiner $S(5,8,24)$. Le but principal, ici, est de trouver un ensemble de générateurs facilitant le travail avec le réseau de Leech.

Le quatrième chapitre utilise tous ce qui précède pour calculer l'ordre de $\cdot 0$, le groupe de symétrie du réseau de Leech.

Notons que ces quatre premiers chapitres servent presque qu'exclusivement au calcul de l'ordre de $\cdot 0$.

Enfin, le dernier chapitre utilise l'ordre de $\cdot 0$, ainsi que la présence de deux éléments particulier dans M_{24}, pour démontrer la simplicité des groupes $\cdot 1$, $\cdot 2$ et $\cdot 3$ reliés à $\cdot 0$.

Chapitre 1

SYSTÈMES DE STEINER

§1. INTRODUCTION

Les systèmes de Steiner sont des généralisations des plans projectifs (on peut voir [**Doyen**]). Dans la première section, on expose les définitions de base. Les sections suivantes seront allouées au système de Steiner $S(5,8,24)$. Les propriétés de ce système seront essentielles pour le reste de cet ouvrage.

§2. DÉFINITIONS

Pour ce chapitre, ainsi que pour le reste de l'ouvrage, l'ensemble $\Omega := \{\infty, 0, 1, \ldots, 22\}$ sera vue comme la droite projective du corps $\mathbb{F}_{23}$. On verra, au Chapitre 2, la raison de ce choix. Soit X un ensemble. Un q-ensemble de X désignera un sous-ensemble de X de cardinalité q . De plus, X_q représentera l'ensemble des q-ensembles de X.

Définition 1.1. *Soient $p < q < r$ des entiers positifs. Un système de Steiner de type $S(p,q,r)$ est une paire ordonnée $(X, \mathscr{F})$, où X est un ensemble de cardinalité r et $\mathscr{F} \subset X_q$ est tel que chaque p-ensemble de X est inclus dans un unique élément de $\mathscr{F}$.*

Exemple 1.2. *Les plans projectifs sont des exemples de système de Steiner. En effet, chaque paire de points doit être incluse dans une unique ligne. Tous les plans projectifs sont des systèmes de Steiner de type $S(2, t+1, t^2+t+1)$ pour $t \geqslant 2$.*

Exemple 1.3. *Les systèmes de Steiner de type $S(1,q,r)$ sont, en fait, des partitions de l'ensemble X en ensembles de cardinalité q. Les systèmes de ce type existent si et seulement si q divise r. Si on prend $X = \{1,2,\ldots,6\}$, alors $\{\{1,2\}\{3,4\}\{5,6\}\}$ et $\{\{1,2,3\},\{4,5,6\}\}$ sont respectivement des systèmes de type $S(1,2,6)$ et $S(1,3,6)$.*

Remarque 1.4. *Le dernier exemple soulève la problématique de l'existence d'un système de type $S(1,q,r)$. En général, on ne connaît pas tous les paramètres (p,q,r) pour lesquels des systèmes de Steiner de type $S(p,q,r)$ existent.*

On termine cette section avec une définition qui sera nécessaire pour le prochain chapitre.

Définition 1.5. *Soit $(X,\mathscr{A})$ et $(Y,\mathscr{B})$ deux systèmes de Steiner. Un isomorphisme de système de Steiner est une bijection $f : X \to Y$ telle que $A \in \mathscr{A} \iff f(A) \in \mathscr{B}$. Si $(X,\mathscr{A}) = (Y,\mathscr{B})$ alors f est appelé un automorphisme.*

§3. Le système S(5,8,24)

Dans cette section, on fait ressortir plusieurs propriétés propres à un système $(\Omega,\mathscr{F})$ de type $S(5,8,24)$. Ces propriétés vont nous permettre de trouver un ensemble de générateurs du réseau de Leech et d'établir des résultats fondamentaux de son groupe de symétrie (chapitre 3 et 4).

§3.1. Le triangle des octades

On sait par définition que chaque 5-ensemble de Ω est inclus dans un unique élément de $\mathscr{F}$. Qu'en est-il pour un k-ensemble où $k \neq 5$? La réponse à cette question suit ainsi qu'une généralisation.

Pour simplifier la notation, les constituants de $\mathscr{F}$ seront appelés des octades.

Proposition 1.6. *Soit N_A le nombre d'octades contenant $A \subseteq \Omega$. Alors*

$$N_A = \begin{cases} \dfrac{\binom{24-k}{5-k}}{\binom{8-k}{5-k}} & \text{si } |A| = k \leqslant 5 \\ 0 \text{ ou } 1 & \text{si } |A| > 5 \end{cases}$$

PREUVE. (Si $|A| = k \leqslant 5$) Le nombre de 5-ensembles de Ω contenant A est donné par $\binom{24-k}{5-k}$. Chaque octade contient $\binom{8-k}{5-k}$ de ces 5-ensembles. Le nombre recherché est donc

$$N_A = \frac{\binom{24-k}{5-k}}{\binom{8-k}{5-k}}.$$

(Si $|A| = k \geq 5$) L'ensemble A ne peut pas être inclus dans deux octades différentes par définition de système de Steiner. Donc $N_A = 0$ ou 1.

□

Remarque 1.7. *Si on impose que A doit être inclus dans au moins une octade, alors N_A ne dépend que de la cardinalité de A. Par exemple, un 6-ensemble A de Ω n'est pas nécessairement inclus dans une octade.*

Définition 1.8. *Soit $A \subseteq B$, alors on définit $N_{B,A} := |\{O \in \mathscr{F} | O \cap B = A\}|$.*

On aimerait construire une table formée des entrées $N_{B,A}$ pour $0 \leq |B| \leq 8$, $0 \leq |A| \leq |B|$, où les $N_{B,A}$ ne dépendent que de la cardinalité de B et de A.

Proposition 1.9. *Soit $A \subseteq B \subseteq \Omega$, on définit*

$$B' = B \cup \{y\}, \text{ où } y \in \Omega \setminus B \quad \text{et} \quad A' = A \cup \{x\}, \text{ où } x \in B' \setminus A.$$

Alors

i) $x = y \Rightarrow N_{B,A} = N_{B',A} + N_{B',A'}$

ii) $N_{B,A} = \sum_{A \subseteq S \subseteq B} (-1)^{|S \setminus A|} N_S$

et si B est inclus dans une octade alors $N_{B,A}$ ne dépend que de la cardinalité de B et de A et donc le cas 1 s'applique même si $x \neq y$.

PREUVE. i) En prenant la cardinalité des deux côtés de l'équation suivante :

$$\begin{aligned} \{O \in \mathscr{F} | O \cap B = A\} &= \{O \in \mathscr{F} | O \cap B = A,\ x \in O\} \dot{\cup} \{O \in \mathscr{F} | O \cap B = A,\ x \notin O\} \\ &= \{O \in \mathscr{F} | O \cap B' = A'\} \dot{\cup} \{O \in \mathscr{F} | O \cap B' = A\} \end{aligned}$$

on obtient la conclusion.

ii) Posons $x = y$. On va procéder par induction sur $|B \setminus A|$. Si $|B \setminus A| = 0$ alors $B = A$ et $N_{B,A} = N_{B,B} = N_B = (-1)^{|B \setminus B|} N_B$. Supposons que c'est vrai pour $|B \setminus A|$ et montrons pour $|B' \setminus A|$. D'après la construction de B' et A', on a $|B \setminus A| = |B' \setminus A'|$ et donc

$$\begin{aligned} \sum_{A \subseteq S \subseteq B'} (-1)^{|S \setminus A|} N_S &= \sum_{A \subseteq S \subseteq B} (-1)^{|S \setminus A|} N_S + \sum_{A' \subseteq S \subseteq B'} (-1)^{|S \setminus A|} N_S \\ &= \sum_{A \subseteq S \subseteq B} (-1)^{|S \setminus A|} N_S + \sum_{A' \subseteq S \subseteq B'} (-1)^{|S \setminus A'|-1} N_S \\ &= N_{B,A} - N_{B',A'} \text{ par l'hypothèse d'induction} \\ &= N_{B',A} \text{ par le cas 1} \end{aligned}$$

Si B est inclus dans une octade, alors chaque S est aussi dans une octade et donc, par la remarque 1.7, chaque N_S ne dépend que de la cardinalité de S. Avec la formule trouvée en 2, on trouve directement que $N_{B,A}$ ne dépend que de la cardinalité de B et A et ainsi 1 s'applique même si $x \neq y$. □

À la position (i, j) de la table suivante, on retrouve la valeur de $N_{B,A}$ où $|B| = i$, $|A| = j$ et où on suppose que B est inclus dans une octade. Les nombres $N_{A,A} = N_A$ sont à la position (j, j). Ils ont été calculés à la Proposition 1.6 et, grâce à la Proposition 1.9, sont suffisants pour construire la table.

Triangle des octades

	0	1	2	3	4	5	6	7	8
0	759								
1	506	253							
2	330	176	77						
3	210	120	56	21					
4	130	80	40	16	5				
5	78	52	28	12	4	1			
6	46	32	20	8	4	0	1		
7	30	16	16	4	4	0	0	1	
8	30	0	16	0	4	0	0	0	1

Pour la suite, nous utiliserons la notation $N_{i,j}$ pour faire référence à l'entrée en position (i, j) et N_i pour l'entrée en position (i, i).

§3.2. Le sous-espace $\mathscr{C}$

On peut munir $\mathcal{P}(\Omega)$ (tous les sous-ensembles de Ω) d'une somme :

$$A + B := (A \backslash B) \cup (B \backslash A)$$

qu'on appelle la différence symétrique. L'intersection est distributive sur cette somme. Avec cette opération $\mathcal{P}(\Omega)$ devient un groupe abélien et ainsi on peut le voir comme un espace vectoriel sur le corps à deux éléments $\mathbb{F}_2$. Dans cet espace, on s'intéresse au sous-espace $\mathscr{C} =< \mathscr{F} >$. Ce dernier servira à définir le réseau de Leech.

On aura besoin, au Chapitre 4, de connaître la cardinalité de $\mathscr{C}$. Pour ce faire, on démontre que sa dimension sur le corps $\mathbb{F}_2$ est 12, auquel cas $|\mathscr{C}| = 2^{12}$.

Proposition 1.10. *$\mathscr{C}$ est de dimension au plus 12.*

PREUVE. Considérons la forme bilinéaire suivante sur $\mathcal{P}(\Omega)$:

$$\begin{array}{ccc} \mathcal{P}(\Omega)\times\mathcal{P}(\Omega) & \longrightarrow & \mathbb{F}_2 \\ (A,B) & \longmapsto & |A\cap B| \mod (2) \end{array}$$

Cette forme est symétrique et non dégénérée.

On sait du triangle des octades que $\forall_{O_1,O_2\in\mathscr{F}}\ |O_1\cap O_2|\equiv 0 \bmod(2)$ (la 8e ligne nous dit que deux octades s'intersectent en 0, 2, 4 ou 8 points). Donc, comme $\mathscr{F}$ engendre $\mathscr{C}$, on obtient $\forall_{X,Y\in\mathscr{C}}\ |X\cap Y|\equiv 0 \bmod(2)$, c'est-à-dire

$$\mathscr{C}\subseteq\mathscr{C}^{\perp}=\{X\in\mathcal{P}(\Omega)|\forall_{Y\in\mathscr{C}}\ |X\cap Y|\equiv 0 \bmod(2)\}.$$

Or, d'après l'annexe C :

$$\dim(\mathcal{P}(\Omega))=\dim(\mathscr{C})+\dim(\mathscr{C}^{\perp})$$

et on a $\dim(\mathcal{P}(\Omega))=24$. Posons $\dim(\mathscr{C})=k$. Comme $\mathscr{C}\subseteq\mathscr{C}^{\perp}$, il découle

$$\dim(\mathscr{C})\leqslant\dim(\mathscr{C}^{\perp})\Longrightarrow k\leqslant 24-k\Longrightarrow k\leqslant 12.$$

□

Définition 1.11. *Une dodécade est un 12-ensemble de Ω dans $\mathscr{C}$. On dénote par $\mathscr{D}$ l'ensemble de toutes les dodécades.*

Proposition 1.12. *Il y a au moins 2576 dodécades.*

PREUVE. Soit

$$\mathscr{A}=\{D\in\mathscr{D}|\exists_{O,O'\in\mathscr{F}}\ D=O+O'\}\text{ et }\mathscr{B}=\{(O,O')\in\mathscr{F}\times\mathscr{F}||O\cap O'|=2\}.$$

Tout d'abord, on obtient du triangle des octades que $\mathscr{A}$ et $\mathscr{B}$ sont non vides puisque $N_{8,2}=16$ et, qu'ainsi, il existe au moins deux octades O,O' qui s'intersectent en deux points auquel cas $O+O'$ est une dodécade.

L'application

$$\begin{array}{ccc} f:\mathscr{B} & \longrightarrow & \mathscr{A} \\ (O_1,O_2) & \longmapsto & O_1+O_2 \end{array}$$

est surjective, mais pas injective. On veut trouver une borne inférieure sur le nombre d'éléments de $\mathscr{A}$ et donc de $\mathscr{D}$. Pour ce faire, trouvons d'abord le nombre d'éléments de $\mathscr{B}$. Soit $\mathscr{B}_O := \{(O_1, O_2) \in \mathscr{B} | O_1 = O\}$. Alors d'après le triangle des octades, on a

$$|\mathscr{B}| = |\mathscr{F}| \cdot |\mathscr{B}_O| = 759 \cdot \binom{8}{2} \cdot N_{8,2} = 759 \cdot \binom{8}{2} \cdot 16.$$

À chaque fois que l'on a une décomposition $D = O_1 + O_2$, alors $D \cap O_1$ est un 6-ensemble de D inclus dans O_1. Ce 6-ensemble contient six 5-ensembles de D. On a donc la borne suivante sur $f^{-1}(D)$:

$$|f^{-1}(D)| \leqslant \frac{\binom{12}{5}}{6}$$

et ainsi

$$|\mathscr{B}| \leqslant |\mathscr{A}| \cdot \frac{\binom{12}{5}}{6}$$

d'où

$$|\mathscr{A}| \geqslant \frac{759 \cdot \binom{8}{2} \cdot 16}{\frac{\binom{12}{5}}{6}} = 2576.$$

□

Définition 1.13. *Un* 16*-ensemble de* Ω *dans* $\mathscr{C}$ *est appelé une hexadécade.*

Théorème 1.14. $\dim(\mathscr{C}) = 12$ *et* $\mathscr{C}$ *est constitué de l'ensemble vide, de 759 octades, de 2576 dodécades, de 759 hexadécades et de l'ensemble* Ω*. De plus, si un ensemble est dans* $\mathscr{C}$*, alors son complément l'est aussi.*

PREUVE. Soit $k = \dim(\mathscr{C})$, alors $|\mathscr{C}| = 2^k$. Or $\mathscr{C}$ contient au moins 2576 dodécades, d'où $2^k \geqslant 2576 > 2048 = 2^{11}$. Donc, d'après la Proposition 1.10, $k = 12$.

Comme $\dim(\mathscr{C}) = 12$, $\dim(\mathscr{C}^\perp) = \dim(\mathscr{P}(\Omega)) - \dim(\mathscr{C}) = 24 - 12 = 12$. Mais dans la preuve de la Proposition 1.10, on a montré que $\mathscr{C} \subseteq \mathscr{C}^\perp$, donc $\mathscr{C} = \mathscr{C}^\perp$. L'élément Ω de $\mathscr{P}(\Omega)$ est orthogonal à tous les ensembles de cardinalité paire, donc en particulier $\Omega \in \mathscr{C}^\perp = \mathscr{C}$. Le fait que Ω soit dans $\mathscr{C}$ implique que $\forall_{X \in \mathscr{C}}\, X^c = X + \Omega \in \mathscr{C}$.

$\mathscr{C}$ contient donc $\emptyset$, Ω, au moins 759 octades, au moins 2576 dodécades et au moins 759 hexadécades (les complémentaires des octades). La somme de ces bornes donne $4096 = 2^{12}$ et donc ces bornes sont les valeurs exactes. □

Remarque 1.15. *Une conséquence de ce théorème est que tous les 8-ensembles de* Ω *dans* $\mathscr{C}$ *sont des octades. On écrira maintenant* $\mathscr{C}_8$, $\mathscr{C}_{12}$ *et* $\mathscr{C}_{16}$ *pour dénoter, respectivement, l'ensemble des octades, des dodécades et des hexadécades.*

Remarque 1.16. *Dans la preuve de la Proposition 1.12, on a montré que*

$$|\mathscr{A}| \geqslant \frac{|\mathscr{B}|}{\frac{\binom{12}{5}}{6}} = 2576$$

Or on sait maintenant, grâce au Théorème 1.14, que $|\mathscr{C}_{12}| = 2576$ *et puisque* $\mathscr{A} \subseteq \mathscr{C}_{12}$, $|\mathscr{A}| \leqslant |\mathscr{C}_{12}| = 2576$. *On a donc* $|\mathscr{A}| = 2576$, *d'où* $|f^{-1}(D)| = 132$ *pour chaque* $D \in \mathscr{C}_{12}$. *Autrement dit chaque dodécade s'écrit de 132 façons différentes comme somme ordonnée de deux octades.*

§3.3. Le triangle des dodécades

On s'intéresse ici à la même question que dans la section du triangle des octades, mais avec des dodécades. C'est-à-dire on veut déterminer le nombre de dodécades qui intersectent un ensemble B en A.

Définition 1.17. *Soit* $A \subseteq B$, *alors on définit* $M_{B,A} := |\{D \in \mathscr{C}_{12} | D \cap B = A\}|$ *et* M_A *le nombre de dodécades qui contiennent l'ensemble A.*

Proposition 1.18. *Soit A un k-ensemble de* Ω *inclus dans une octade. Alors* M_A *ne dépend que de k et on dénote ce nombre par* M_k. *Les nombres* M_k *pour* $0 \leqslant k \leqslant 8$ *sont*

$$\begin{array}{cccccccc} M_0 & = & 2576 & M_3 & = & 280 & M_6 & = & 16 \\ M_1 & = & 1288 & M_4 & = & 120 & M_7 & = & 0 \\ M_2 & = & 616 & M_5 & = & 48 & M_8 & = & 0. \end{array}$$

PREUVE. Pour démontrer cette proposition, nous allons calculer M_A pour $|A| = 0, 1, 2$ et 3 en utilisant uniquement la cardinalité de A ainsi que l'hypothèse que A est inclus dans une octade. Les autres cas sont semblables. Tout d'abord, le nombre M_0 représente en fait le nombre de dodécades dans $\mathscr{C}_{12}$, c'est-à-dire 2576. Pour $|A| = 1, 2$ et 3, on compte le nombre de couples ordonné d'octades qui s'intersectent en deux points n'appartenant pas à A. Pour avoir le nombre de dodécades, il suffira de diviser par 132 (voir la Remarque 1.16).

(Si $|A| = 1$) Posons $A = \{x\}$. Pour trouver M_A, on compte le nombre de paires d'octades (O, O') telle que $O + O' \in \mathscr{C}_{12}$ et O contient x. D'après le triangle des octades il

y a $N_1 = 253$ octades qui contiennent x. Toujours d'après le triangle des octades il y a $N_{8,2} = 16$ octades qui intersectent O en 2 points. Il y a enfin $\binom{7}{2}$ façons de choisir les deux points d'intersection entre O et O' de telle sorte que x n'y fasse pas partie. On obtient le calcul suivant :

$$M_A = \frac{1}{132} \cdot [2 \cdot N_1 \cdot \binom{7}{2} \cdot N_{8,2}] = 1288.$$

(Si $|A|$ =2) Posons $A = \{x,y\}$. Soit (O,O') une paire d'octades telle que $O+O'$ contient A. Il y a deux cas à considérer : soit $A \subset O$ ou soit $x \in O$, $y \in O'$. Dans le premier cas, le raisonnement est similaire au cas $|A| = 1$ et le nombre de dodécade contenant A est donc :

$$\frac{1}{132} \cdot [2 \cdot N_2 \cdot \binom{6}{2} \cdot N_{8,2}].$$

Dans le deuxième cas, on a $N_{2,1} = 176$ octades contenant x, mais pas y. Comme dans le cas $|A| = 1$, on a $\binom{7}{2}$ façons de choisir les deux points d'intersection. Supposons que les deux points d'intersection soient z et w.

Il reste à calculer le nombre d'octades **contenant** x qui intersectent O en $\{z,w\}$. Pour ce faire, on calcule le nombre d'octades qui intersectent l'ensemble $\{x,y,z,w\}$ en $\{y,z,w\}$. Ce nombre est $N_{4,3} = 16$. Il faut retrancher de cette quantité le nombre d'octades qui intersectent O en plus de deux points. Soit O'' une telle octade. O'' doit intersecter O en exactement 4 points, c'est-à-dire en $\{z,w\}$ et deux points de $O \setminus \{x,z,w\}$, disons u et v. Mais O'' contient également le point y et alors O'' est l'unique octade contenant l'ensemble $\{y,z,w,u,v\}$. Le nombre d'octades qui intersectent O en plus de deux points est donc égal au nombre de paires de points de $O \setminus \{x,z,w\}$, c'est-à-dire $\binom{5}{2}$. Le nombre d'octades **contenant** x qui intersectent O en $\{z,w\}$ est donc $N_{4,3} - \binom{5}{2}$. Dans ce cas, le nombre de dodécades contenant A est

$$\frac{1}{132}[2 \cdot N_{2,1} \cdot \binom{7}{2} \cdot (N_{4,3} - \binom{5}{2})]$$

et alors

$$M_A = \frac{1}{132} \cdot [2 \cdot N_2 \cdot \binom{6}{2} \cdot N_{8,2} + 2 \cdot N_{2,1} \cdot \binom{7}{2} \cdot (N_{4,3} - \binom{5}{2})] = 616.$$

(Si $|A|$ =3) Le calcul est similaire au deux cas précédents :

$$M_A = \frac{1}{132} \cdot [2 \cdot N_3 \cdot \binom{5}{2} \cdot N_{8,2} + 2 \cdot \binom{3}{2} \cdot N_{3,2} \cdot \binom{6}{2} \cdot (N_{5,3} - \binom{4}{2})] = 280.$$

On obtient tous les autres M_A de la même façon. Dans tous les cas la cardinalité de A est suffisante pour trouver M_A. □

La Proposition 1.9 demeure vraie si on remplace $N_{B,A}$ par $M_{B,A}$. Dans la dernière proposition, on a calculé les nombres $M_{A,A} = M_A$ avec l'hypothèse que A était inclus dans une octade. Ces nombres sont suffisants pour construire la table suivante où on retrouve la valeur de $M_{B,A}$ avec $|B| = i$, $|A| = j$ à la position (i, j) et où B est inclus dans une octade.

Triangle des dodécades

	0	1	2	3	4	5	6	7	8
0	2576								
1	1288	1288							
2	616	672	616						
3	280	336	336	280					
4	120	160	176	160	120				
5	48	72	88	88	72	48			
6	16	32	40	48	40	32	16		
7	0	16	16	24	24	16	16	0	
8	0	0	16	0	24	0	16	0	0

§3.4. Les hexades

La notion d'hexades reviendra à quelques reprises dans les prochains chapitres. On la développe une première fois ici et on référera à cette section lorsqu'on l'utilisera.

Définition 1.19. *Soit T un 4-ensemble de Ω. D'après le triangle des octades, T est contenu dans exactement cinq octades différentes. Deux octades différentes ne peuvent s'intersecter qu'en $0, 2$ ou 4 éléments. Donc si $O_1, \ldots, O_5$ sont les cinq octades contenant T, alors les ensembles*

$$T_1 := O_1 \backslash T, \ldots, T_5 := O_5 \backslash T$$

sont deux à deux disjoints (sinon $|O_i \cap O_j| > 4$ pour une paire i, j). L'ensemble

$$P(T) = \{T, T_1, \ldots, T_5\}$$

est appelé une hexade. On constate que $P(T)$ forme une partition de Ω en 4-ensembles.

Proposition 1.20. *Soit $P(T_0) = \{T_0, T_1, \ldots, T_5\}$ une hexade, alors*

$$\forall_{i,j}\ T_i + T_j \in \mathscr{C}_8.$$

PREUVE. Par définition on a

$$\forall_i\ T_0 + T_i = T_0 + O_i \backslash T_0 = O_i \in \mathscr{C}_8$$

et donc

$$\forall_{i,j}\ T_i + T_j = \underbrace{(T_i + T_0)}_{\in \mathscr{C}_8} + \underbrace{(T_0 + T_j)}_{\in \mathscr{C}_8} \in \mathscr{C}.$$

Comme $|T_i + T_j| = 8$ et que les seuls 8-ensemble de $\mathscr{C}$ sont les octades, on obtient $T_i + T_j \in \mathscr{C}_8$. □

§3.5. Réalisation d'un système de type S(5,8,24)

Jusqu'à présent, on a établi les propriétés d'un système de Steiner $(\Omega, \mathscr{C}_8)$ de type $S(5,8,24)$ ainsi que les propriétés du sous-espace engendré par ce système. Mais, on ne sait toujours pas si un tel système existe.

Pour démontrer ceci, on construit un sous-espace de dimension 12 de $\mathscr{P}(\Omega)$ sur le corps $\mathbb{F}_2$.

Dans [**Thompson**], on suggère de considérer l'espace ligne de la matrice suivante.

$$C = \begin{pmatrix}
0&1&1&1&1&1&0&1&0&1&1&0&0&1&1&0&0&1&0&1&0&0&0&0\\
0&0&1&1&1&1&1&0&1&0&1&1&0&0&1&1&0&0&1&0&1&0&0&0\\
0&0&0&1&1&1&1&1&0&1&0&1&1&0&0&1&1&0&0&1&0&1&0&0\\
0&0&0&0&1&1&1&1&1&0&1&0&1&1&0&0&1&1&0&0&1&0&1&0\\
0&0&0&0&0&1&1&1&1&1&0&1&0&1&1&0&0&1&1&0&0&1&0&1\\
0&1&0&0&0&0&1&1&1&1&1&0&1&0&1&1&0&0&1&1&0&0&1&0\\
0&0&1&0&0&0&0&1&1&1&1&1&0&1&0&1&1&0&0&1&1&0&0&1\\
0&1&0&1&0&0&0&0&1&1&1&1&1&0&1&0&1&1&0&0&1&1&0&0\\
0&0&1&0&1&0&0&0&0&1&1&1&1&1&0&1&0&1&1&0&0&1&1&0\\
0&0&0&1&0&1&0&0&0&0&1&1&1&1&1&0&1&0&1&1&0&0&1&1\\
0&1&0&0&1&0&1&0&0&0&0&1&1&1&1&1&0&1&0&1&1&0&0&1\\
0&1&1&0&0&1&0&1&0&0&0&0&1&1&1&1&1&0&1&0&1&1&0&0\\
0&0&1&1&0&0&1&0&1&0&0&0&0&1&1&1&1&1&0&1&0&1&1&0\\
0&0&0&1&1&0&0&1&0&1&0&0&0&0&1&1&1&1&1&0&1&0&1&1\\
0&1&0&0&1&1&0&0&1&0&1&0&0&0&0&1&1&1&1&1&0&1&0&1\\
0&1&1&0&0&1&1&0&0&1&0&1&0&0&0&0&1&1&1&1&1&0&1&0\\
0&0&1&1&0&0&1&1&0&0&1&0&1&0&0&0&0&1&1&1&1&1&0&1\\
0&1&0&1&1&0&0&1&1&0&0&1&0&1&0&0&0&0&1&1&1&1&1&0\\
0&0&1&0&1&1&0&0&1&1&0&0&1&0&1&0&0&0&0&1&1&1&1&1\\
0&1&0&1&0&1&1&0&0&1&1&0&0&1&0&1&0&0&0&0&1&1&1&1\\
0&1&1&0&1&0&1&1&0&0&1&1&0&0&1&0&1&0&0&0&0&1&1&1\\
0&1&1&1&0&1&0&1&1&0&0&1&1&0&0&1&0&1&0&0&0&0&1&1\\
0&1&1&1&1&0&1&0&1&1&0&0&1&1&0&0&1&0&1&0&0&0&0&1\\
1&0&0&0&0&0&1&0&1&0&0&1&1&0&0&1&1&0&1&0&1&1&1&1
\end{pmatrix}$$

On verra dans le prochain chapitre, que l'ensemble des vecteurs formés de huit "1"dans l'espace ligne de C est un système de Steiner de type $S(5,8,24)$. On montre d'abord que la dimension de l'espace ligne de C est 12.

En indexant les colonnes de C avec Ω (la première colonne est associée à ∞, la deuxième à 0, la troisième à 1, etc), on peut voir chaque ligne comme un sous-ensemble de Ω. En effet, le 0 représente l'absence de l'élément du sous-ensemble et le 1 la présence de l'élément. La première ligne de C correspond à l'ensemble

$$\begin{aligned} Q_0 &:= \{0,1,2,3,4,6,8,9,12,13,16,18\} \\ &= \{0, 2^0 \bmod(23), 2^1 \bmod(23), \ldots, 2^{11} \bmod(23)\} \end{aligned}$$

Pour simplifier l'écriture, on utilisera la notation

$$Q_i := \{(q+i) \bmod(23) | q \in Q_0\}$$

et ce pour chaque $i \in \Omega \setminus \{\infty\}$. Avec cette notation, la i^e ligne de C, où $i = 0, 1, \ldots, 22$, correspond à l'ensemble Q_i tandis que la 24e ligne de C, elle, correspond à

$$Q_\infty := \Omega + Q_0.$$

On dénotera par $\mathcal{L}(C)$ le sous-espace de $\mathcal{P}(\Omega)$ engendré par ces ensembles.

Montrons que la dimension de $\mathcal{L}(C)$ est 12. Les 11 ensembles suivants :

$$\begin{aligned}
Q_0 + Q_2 + Q_{20} + Q_{21} &= \{0,1,2,3,4,7,10,12\} \\
Q_1 + Q_3 + Q_{21} + Q_{22} &= \{1,2,3,4,5,8,11,13\} \\
Q_2 + Q_4 + Q_{22} + Q_0 &= \{2,3,4,5,6,9,12,14\} \\
Q_3 + Q_5 + Q_0 + Q_1 &= \{3,4,5,6,7,10,13,15\} \\
\vdots \qquad\quad \vdots &\qquad\quad \vdots \\
Q_{10} + Q_{12} + Q_7 + Q_8 &= \{10,11,12,13,14,17,20,22\}
\end{aligned}$$

ainsi que Q_∞ sont linéairement indépendants (il suffit de former la matrice associée à ces 12 ensembles pour s'en rendre compte). $\mathcal{L}(C)$ est donc de dimension au moins 12.

Supposons qu'il existe 13 Q_i qui sont linéairement indépendants. En appliquant l'algorithme de Gauss à la matrice ayant les Q_i comme ligne, on obtient

$$\begin{bmatrix}
1 & 0 & 0 & \ldots & 0 & a_{1,14} & a_{1,15} & \ldots & a_{1,24} \\
0 & 1 & 0 & \ldots & 0 & a_{2,14} & a_{2,15} & \ldots & a_{2,24} \\
0 & 0 & 1 & \ldots & 0 & a_{3,14} & a_{3,15} & \ldots & a_{3,24} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\
0 & 0 & 0 & \ldots & 1 & a_{13,14} & a_{13,15} & \ldots & a_{13,24}
\end{bmatrix}$$

en effectuant les permutations de colonnes appropriées. Considérons les vecteurs
$r_i = (a_{i,14}, \ldots, a_{i,24})$ pour $i = 1, 2, \ldots, 13$.

Tous les Q_i ont un nombre pair de "1". De plus, pour $i \neq j$, $Q_i + Q_j$ a un nombre pair de "1". Puisque l'on travaille sur $\mathbb{F}_2$, l'algorithme de Gauss ne fait intervenir que des sommes et des permutations de lignes. Donc la parité du nombre de "1" est conservée pour chaque ligne de la matrice échelonnée. En termes des r_i, ceci revient à dire que pour i, j

$$\forall_{i,j}\, r_i \cdot r_j = \delta_{ij} \text{ ($\cdot$ représente le produit scalaire usuel)}$$

d'où les r_i sont linéairement indépendants et forment donc un sous-espace de dimension 13. Ceci est une contradiction car les r_i sont dans $\mathbb{F}_2^{11}$. $\mathcal{L}(C)$ est donc de dimension 12.

Chapitre 2

GROUPES DE MATHIEU

§1. INTRODUCTION

Les groupes de Mathieu ont été découvert par Émile Mathieu dans les années 1861 et 1873 (voir [**Mathieu1**] et [**Mathieu2**]). Ces groupes, au nombre de cinq, sont les premiers exemples connus de groupes simples sporadiques, c'est-à-dire ne faisant parti d'aucune des familles infinies de groupes simples (voir Annexe B pour les familles infinies).

Cependant, ce n'est pas cette propriété qui attira l'attention de Mathieu, mais bien leur haute transitivité. Mathieu travaillait sur les fonctions transitives et reçu, en 1859, un doctorat honorifique pour ses travaux. Deux années plus tard, il trouva quatre groupes de permutations hautement transitifs, qu'on dénote aujourd'hui par M_{11}, M_{12}, M_{22} et M_{23}, et compléta sa découverte en 1873 avec le groupe M_{24}.

C'est ce dernier groupe qui nous intéressera. On démontrera deux propriétés importantes de celui-ci : sa 5-transitivité ainsi que le fait qu'il est isomorphe au groupe d'automorphismes du système de Steiner $(\Omega, \mathscr{C}_8)$.

§2. DÉFINITIONS

La définition suivante mettra en évidence le fait que le groupe $PSL_2(23)$ se retrouve, de façon isomorphe, dans le groupe de Mathieu M_{24}. En plus d'expliquer le choix de Ω comme ensemble dans le Chapitre 1, cette information sera essentielle pour le Chapitre 5.

Définition 2.1. *L'ensemble des matrices inversibles sur le corps à 23 éléments, $\mathbb{F}_{23}$, est dénoté par $GL_2(23)$. Le sous-groupe des matrices de déterminant 1 est noté $SL_2(23)$. Le*

centre de ce sous-groupe est engendré par la matrice d'ordre deux

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

On définit enfin $PSL_2(23) := SL_2(23)/\left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$.

Proposition 2.2. *$SL_2(23)$ est engendré par les matrices.*

$$\alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad , \quad \gamma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad et \quad \beta = \begin{pmatrix} 18 & 0 \\ 0 & 9 \end{pmatrix}.$$

PREUVE. Regardons le sous-groupe G engendré par les matrices α et γ.

La présence de $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ dans G donne la présence des matrices de la forme $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ dans G. De plus, en utilisant le calcul suivant

$$\gamma \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \gamma^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

on montre que G contient toutes les matrices de la forme $\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$.

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(23)$.

i) Si $c = 0$, alors en utilisant le fait que $det(A) = a \cdot d = 1$, on trouve

$$A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1-a^{-1} \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a^{-1}(d+b)-d \\ 0 & 1 \end{pmatrix},$$

c'est-à-dire que $A \in G$.

ii) Si $c \neq 0$, on considère les cas $a = 0$ et $a \neq 0$ séparément :

– si $a = 0$, on applique le cas i) à la matrice

$$\begin{pmatrix} c & d \\ 0 & -b \end{pmatrix} = \gamma \cdot \begin{pmatrix} 0 & b \\ c & d \end{pmatrix};$$

– si $a \neq 0$ on applique la cas i) à la matrice

$$\begin{pmatrix} c & d \\ 0 & adc^{-1} - b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ ac^{-1} & 1 \end{pmatrix} \cdot \gamma \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

et dans ces deux cas $A \in G$.

□

Remarque 2.3. *Dans la dernière proposition, on a introduit l'élément* β*, même s'il n'était pas nécessaire pour cette preuve, car on en aura besoin pour ce chapitre ainsi qu'au Chapitre 5, où l'on verra que le normalisateur de* α *est engendré par* α *et* β*.*

On veut maintenant définir le groupe de Mathieu M_{24} en représentant les matrices α, β et γ comme permutations d'un ensemble à 24 éléments (l'ensemble Ω rencontré lors du Chapitre 1). Pour ce faire, on fait agir le groupe $SL_2(23)$ sur la droite projective du corps $\mathbb{F}_{23}$. La droite projective de $\mathbb{F}_{23}$ est définie comme suit.

Définition 2.4. *Soit la relation d'équivalence suivante sur l'ensemble* $\mathbb{F}_{23} \times \mathbb{F}_{23} \setminus \{(0,0)\}$ *:*

$$(x,y) \sim (x',y') \quad si \quad \exists_{0 \neq \lambda \in \mathbb{F}_{23}} (\lambda \cdot x = x' \text{ et } \lambda \cdot y = y').$$

Les classes d'équivalences sont dénotées par :

$$\begin{aligned}
\infty &:= \{(1,0),(2,0),\ldots,(22,0)\} \\
0 &:= \{(0,1),(0,2),\ldots,(0,22)\} \\
1 &:= \{(1,1),(2,2),\ldots,(22,22)\} \\
2 &:= \{(2,1),(4,2),\ldots,(21,22)\} \\
&\vdots \\
22 &:= \{(22,1),(21,2),\ldots,(1,22)\}.
\end{aligned}$$

On peut voir chacune de ces classes d'équivalences comme le quotient de la première coordonnée sur la deuxième. L'ensemble

$$\Omega := \{\infty, 0, 1, 2, \ldots, 22\}$$

est appelé la droite projective de $\mathbb{F}_{23}$*.*

Pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(23)$ et pour $(x,y) \in \mathbb{F}_{23} \times \mathbb{F}_{23} \setminus \{(0,0)\}$, on définit l'action :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}.$$

Remarquons que cette action est bien définie sur Ω. C'est-à-dire que si $(x,y) \sim (x',y')$ alors

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Les matrices α, β et γ induisent une permutation des éléments de Ω. Sous forme de cycle ces permutations sont :

$$\begin{aligned}
\alpha &= (0,1,2,\ldots,22)\\
\beta &= (1,2,4,8,16,9,18,13,3,6,12)(5,10,20,17,11,22,21,19,15,7,14)\\
\gamma &= (0,\infty)(1,22)(2,11)(3,15)(4,17)(5,9)(6,19)(7,13)(8,20)(10,16)(12,21)(14,18).
\end{aligned}$$

Remarquons que la permutation β est en fait la fonction qui envoie i sur $2i \mod (23)$ et fixe ∞. La permutation α, elle, est tout simplement la fonction qui envoie i sur $(i+1)$ mod (23) et fixe ∞.

Le groupe de Mathieu M_{24} est le sous-groupe de S_Ω (le groupe des permutations de Ω) engendré par α, β et une troisième permutation δ.

Définition 2.5 (Groupe de Mathieu)**.** *Le sous-groupe de S_Ω engendré par α,β, γ et δ où*

$$\begin{aligned}
\alpha &= (0,1,2,\ldots,22)\\
\beta &= (1,2,4,8,16,9,18,13,3,6,12)(5,10,20,17,11,22,21,19,15,7,14)\\
\gamma &= (0,\infty)(1,22)(2,11)(3,15)(4,17)(5,9)(6,19)(7,13)(8,20)(10,16)(12,21)(14,18)\\
\delta &= (1,18,4,2,6)(5,21,20,10,7)(8,16,13,9,12)(11,19,22,14,17)
\end{aligned}$$

est dénoté par M_{24} et est appelé le premier groupe de Mathieu.

Définition 2.6. *Le groupe M_{24} contient deux autres groupes simples qui font partie des groupes découverts par Mathieu :*

$$\begin{aligned}
M_{23} &:= Stab_{M_{24}}(x) \quad x \in \Omega\\
M_{22} &:= Stab_{M_{23}}(y) \quad y \in \Omega\backslash\{x\}
\end{aligned}$$

Remarquons que comme ces deux groupes sont transitifs sur Ω, la définition ne dépend pas de x et de y.

Remarque 2.7. *On peut voir* [**Rotman**] *pour la définition des deux derniers groupes de Mathieu, M_{11} et M_{12}. On ne démontrera pas la simplicité des groupes de Mathieu, mais on peut voir* [**Suzuki**] *ou* [**Rotman**] *pour ceci.*

§3. Transitivité des groupes de Mathieu

Comme il a été mentionné plus haut, c'est la haute transitivité de ces groupes qui attira l'attention d'Émile Mathieu. En effet, M_{11}, M_{12}, M_{22}, M_{23} et M_{24} sont respectivement 4, 5, 3, 4 et 5-transitifs. Les groupes M_{12} et M_{24} sont les seuls groupes 5-transitifs à part S_n

et A_n. En supposant démontré la classification des groupes simples finis, [**Camero**] montre qu'aucun groupe autre que S_n et A_n n'est 6-transitif.

On démontre ici la 5-transitivité du groupe M_{24}. Cette propriété de M_{24} joue un rôle primordial dans le calcul de l'ordre du groupe de symétrie du réseau de Leech (voir Chapitre 4) ainsi que pour la dernière section de ce chapitre.

Théorème 2.8. *M_{24} est 5-transitif.*

PREUVE. Pour faire cette preuve, on va montrer successivement que M_{24} est 1-transitif, 2-transitif, 3-transitif, 4-transitif et 5-transitif.

1-transitif - La présence de α dans M_{24} nous donne la transitivité sur $\Omega\backslash\{\infty\}$. L'élément γ contient le 2-cycle $(\infty,0)$ ce qui nous donne la transivité sur Ω.

2-transitif - On remarque que $Stab_{M_{24}}(\infty)$ contient l'élément α et donc $Stab_{M_{24}}(\infty)$ est transitif sur $\Omega\backslash\{\infty\}$. La transitivité de M_{24} sur Ω nous donne

$$\forall_{x\in\Omega}\exists_{\lambda\in M_{24}}\ Stab_{M_{24}}(x) = \lambda\cdot Stab_{M_{24}}(\infty)\cdot\lambda^{-1}.$$

Donc $Stab_{M_{24}}(x)$ est transitif sur $\Omega\backslash\{x\}$, pour chaque $x\in\Omega$. Montrons que M_{24} est 2-transitif sur Ω. Soit (a,b), $(c,d)\in\Omega\times\Omega$, par la transitivité de M_{24} on peut trouver un élément τ de M_{24} tel que $\tau(a)=c$. La transitivité de $Stab_{M_{24}}(c)$ nous donne l'existence de $\psi\in M_{24}$ tel que $\psi(\tau(b))=d$ et donc

$$\psi(\tau(a,b)) = (\psi(c),\psi(\tau(b))) = (c,d).$$

3-transitif - En procédant de la même façon que dans le cas précédent, il suffit de montrer que pour un certain $(x,y)\in\Omega\times\Omega, x\neq y$, $Stab_{M_{24}}(x,y)$ est transitif sur $\Omega\backslash\{x,y\}$. Le stabilisateur de 0 et ∞ contient l'élément β et l'élément

$$\alpha^{-3}\cdot\delta\cdot\alpha^3 = (21,15,1,22,3)(2,18,17,7,4)(5,13,10,6,9)(8,16,19,11,14).$$

Ce dernier élément permet de passer d'un des 11-cycles de β à l'autre d'où la transitivité de $Stab_{M_{24}}(0,\infty)$ et donc la 3-transitivité de M_{24} sur Ω.

4-transitif - Regardons le stabilisateur des points ∞, 0 et 3. Il contient δ et l'élément

$$\sigma = \alpha^{-2}\cdot\delta\cdot\alpha^4 = (7,17,18,12,11,13,9)(20,16,8,6,5,10,15)(19,21,4,14,2,22,1).$$

Le cycle $(5,21,20,10,7)$ de δ permet de passer du premier 7-cycle de σ au deuxième et du deuxième au troisième ce qui nous donne la transitivité du $Stab_{M_{24}}(\infty,0,3)$ sur $\Omega\backslash\{\infty,0,3\}$.

5-transitif - Enfin $Stab_{M_{24}}(0,\infty,3,15)$ contient δ et l'élément

$$\beta^8\cdot(\delta\cdot\alpha)\cdot\beta^{-8}=(6,9)(12,22)(21,1)(4,10)(7,11)(13,2)(16,17)(19,5).$$

Ce dernier élément permet de passer d'un 5-cycle de δ à n'importe quel autre 5-cycle de δ. C'est-à-dire que $Stab_{M_{24}}(0,\infty,3,15)$ est transitif sur $\Omega\backslash\{\infty,0,3,15\}$ et donc M_{24} est 5-transitif.

□

§4. M_{24} STABILISE $(\Omega,\mathscr{C}_8)$

On montre maintenant que M_{24} est isomorphe au groupe d'automorphismes du système de Steiner $(\Omega,\mathscr{C}_8)$ de type $S(5,8,24)$.

Pour faire cette preuve, on aura besoin de la réalisation du sous-espace $\mathscr{C}$ de la section §3.5 du Chapitre 1. On montrera, par la suite, que $\mathcal{L}(C)$ contient un système de Steiner de type $S(5,8,24)$ (voir Proposition 2.10).

Lemme 2.9. *$M_{24}\lesssim Aut(\mathcal{L}(C))$ où $\mathcal{L}(C)$ est le sous-espace construit à la section §3.5 du Chapitre 1.*

PREUVE. L'action de $\pi\in M_{24}$ sur $D\in\mathcal{L}(C)$ est définie de façon naturelle par $\pi(D):=\{\pi(d)|d\in D\}$ et on obtient donc que $\pi(A+B)=\pi(A)+\pi(B)$ pour $A,B\in\mathcal{L}(C)$.

On a

$$\gamma=(\delta^2\cdot\gamma)^5\quad,\quad\delta=(\delta^2\cdot\gamma)^8\quad\text{et}\quad\beta=\alpha^{18}\cdot\gamma\cdot\alpha^{14}\cdot\gamma\cdot\alpha^5\cdot\gamma\cdot\alpha^5$$

d'où $M_{24}=<\alpha,\delta^2\gamma>$.

Pour montrer que M_{24} préserve $\mathcal{L}(C)$, il est alors suffisant de montrer que

$$\forall_{i\in\Omega}\,\alpha(Q_i)\in\mathcal{L}(C)\quad\text{et}\quad\delta^2\gamma(Q_i)\in\mathcal{L}(C).$$

Les ensembles Q_i ont été définis à la section §3.5 du Chapitre 1.

i) On a d'abord pour chaque $i \in \Omega\backslash\{\infty, 22\}$

$$\alpha(Q_i) = Q_{i+1} \in \mathcal{L}(C),\ \alpha(Q_{22}) = Q_0 \in \mathcal{L}(C) \quad \text{et} \quad \begin{aligned} \alpha(Q_\infty) &= \alpha(\Omega + Q_0) \\ &= \alpha(\Omega) + \alpha(Q_0) \\ &= \Omega + Q_1 \\ &= Q_\infty + Q_0 + Q_1 \in \mathcal{L}(C) \end{aligned}$$

ii) Il reste à montrer que $\delta^2\gamma(Q_i) \in \mathcal{L}(C)$. On trouve directement que

$$\delta^2\gamma(Q_0) = Q_\infty \quad \text{et} \quad \delta^2\gamma(Q_\infty) = Q_0$$

et également que

$$\delta^2\gamma(Q_1) = Q_2 + Q_{11} + Q_{20} \in \mathcal{L}(C) \quad \text{et} \quad \delta^2\gamma(Q_{22}) = Q_\infty + Q_1 + Q_{20} + Q_{22} \in \mathcal{L}(C)$$

Les deux calculs seront utiles pour faire les autres cas :

– $\delta^2 \cdot \gamma \cdot \beta = \beta^2 \cdot \delta^2 \cdot \gamma$

– $$\begin{aligned} \beta(Q_i) &= \{\beta(q+i) | q \in Q_0\} \\ &= \{\beta(q) + \beta(i) | q \in Q_0\} \\ &= \{q + 2i \bmod(23) | q \in Q_0\},\ \text{car } \beta(Q_0) = Q_0 \\ &= Q_{2i \bmod(23)} \in \mathcal{L}(C) \end{aligned}$$

On utilise ces deux calculs pour trouver les valeurs de $\delta^2\gamma(Q_i)$ lorsque $i \in \Omega\backslash\{0, \infty, 1, 22\}$.

– Si $i \in Q_0\backslash\{0\}$ alors $\exists_{l\in\mathbb{N}}\ i \equiv 2^l \bmod(23)$ et donc

$$\begin{aligned} \delta^2\gamma(Q_i) &= \delta^2\gamma(Q_{2^l \bmod(23)}) \\ &= \delta^2\gamma\beta^l(Q_1) \\ &= \beta^{2l}(\delta^2\gamma(Q_1)) \\ &= \beta^{2l}(Q_2 + Q_{11} + Q_{20}) \\ &= Q_{4l\cdot 2 \bmod(23)} + Q_{4l\cdot 11 \bmod(23)} + Q_{4l\cdot 20 \bmod(23)} \in \mathcal{L}(C) \end{aligned}$$

– Si $i \in \Omega\backslash(Q_0 \cup \infty)$ alors $\exists_{k\in\mathbb{N}}\ i \equiv 22 \cdot 2^k \bmod(23)$ et similairement

$$\begin{aligned} \delta^2\gamma(Q_i) &= \delta^2\gamma(Q_{22\cdot 2^k \bmod(23)}) \\ &= \delta^2\gamma\beta^k(Q_{22}) \\ &= \beta^{2k}\delta^2\gamma(Q_{22}) \\ &= \beta^{2k}(Q_\infty + Q_1 + Q_{20} + Q_{22}) \\ &= Q_\infty + Q_{4k\cdot 1 \bmod(23)} + Q_{4k\cdot 20 \bmod(23)} + Q_{4k\cdot 22 \bmod(23)} \in \mathcal{L}(C) \end{aligned}$$

On a donc montré que M_{24} préserve $\mathcal{L}(C)$. De plus, comme chaque élément de M_{24} laisse la cardinalité de chaque ensemble fixe, il découle qu'il préserve $S(5,8,24)$ (puisqu'il envoie les octades sur des 8-ensembles de $\mathcal{L}(C)$ c'est-à-dire des octades).

□

La prochaine proposition complète la section §3.5 du Chapitre 1.

Proposition 2.10. *L'ensemble des éléments de $\mathcal{L}(C)$ de cardinalité 8 forme un système de Steiner de type $S(5,8,24)$.*

PREUVE. $\mathcal{L}(C)$ contient l'ensemble $Q_0+Q_2+Q_{20}+Q_{21}=\{0,1,2,3,4,7,10,12\}$ (voir §3.5 au Chapitre 1). Donc par la 5-transitivité de M_{24} chaque 5-ensemble de Ω est inclus dans au moins un 8-ensemble de Ω dans $\mathcal{L}(C)$.

Montrons que si $D \in \mathcal{L}(C)$, alors $|D| \geqslant 8$. Posons $|D| = k \neq 0$.

i) Si $k \leqslant 5$, alors par la 5-transitivité de M_{24} sur Ω, tous les k-ensembles de Ω sont dans $\mathcal{L}(C)$. Soit D' un k-ensemble de Ω qui ne diffère de D que par un seul élément. Alors

$$D+D' \in \mathcal{L}(C) \quad \text{et} \quad |D+D'|=2$$

et la 5-transitivité de M_{24} implique que tous les 2-ensembles de Ω sont dans $\mathcal{L}(C)$, d'où $\dim(\mathcal{L}(C)) \geqslant 23$. Ceci est une contradiction car $\dim(\mathcal{L}(C))=12$.

ii) Si $k=6$ ou 7, alors on peut trouver un 8-ensemble O de Ω dans $\mathcal{L}(C)$ qui contient au moins 5 éléments de D. L'ensemble $D+O$ est dans $\mathcal{L}(C)$ et $2 \leqslant |D+O| \leqslant 5$. En appliquant le cas i) sur $D+O$, on obtient une contradiction.

Pour montrer que les 8-ensembles de Ω dans $\mathcal{L}(C)$ forment un système de Steiner de type $S(5,8,24)$, il reste à montrer que chaque 5-ensemble de Ω est inclus dans un unique 8-ensemble de Ω dans $\mathcal{L}(C)$. Soit O et O' deux tels 8-ensembles contenant un 5-ensemble. Si $O \neq O'$ alors $2 \leqslant |O+O'| \leqslant 6$, ce qui est une contradiction. □

Pour la suite, on dénotera par $\mathscr{C}_8$ l'ensemble des éléments de cardinalité 8 dans $\mathcal{L}(C)$.

Pour démontrer que $M_{24} \simeq Aut((\Omega,\mathscr{C}_8)) =: M$, on détermine la cardinalité de M_{24} et on montre ensuite que $|M_{24}| = |M|$.

Lemme 2.11. *M_{24} agit transitivement sur les octades.*

PREUVE. Soit O, O' deux octades et $X \subset O$, $X' \subset O'$ deux 5-ensembles. Alors par 5-transitivité de M_{24}, il existe $\pi \in M_{24}$ tel que $\pi(X) = X'$. Mais par le Lemme 2.9, $\pi(O)$ est une octade. Cette octade contient l'ensemble X' et donc, par définition de système de Steiner, égale à O'. □

Lemme 2.12. *Soit $K \in \mathscr{C}_8$, on définit*

$$P_K := \{\pi \in M_{24} | \forall_{k \in K}\, \pi(k) = k\}$$

Alors P_K est transitif sur $\Omega \backslash K$.

PREUVE. On trouve dans M_{24} la permutation

$$\mu := (\delta\alpha^5)^4 = (0,20)(2,9)(3,19)(5,17)(6,21)(7,14)(8,22)(16,18)$$

qui fixe les éléments d'un ensemble $K = \{a_1, a_2, \ldots, a_8\} := \{1,4,10,11,12,13,15,\infty\}$.

Supposons que K n'est pas une octade. Soit A l'unique octade qui contient l'ensemble $\{a_1, \ldots, a_5\}$. Étant donné que μ est dans M_{24} et comme M_{24} stabilise $(\Omega, \mathscr{C}_8)$, $\mu(A) \in \mathscr{C}_8$ (voir Lemme 2.9). Mais $\mu\{a_1, \ldots, a_5\} = \{a_1, \ldots, a_5\}$ et deux octades différentes ne peuvent s'intersecter en 5 points d'où $\mu(A) = A$. Il faut alors que A contienne un 6^e point de K (disons a_6), car sinon il faudrait que μ stabilise un sous-ensemble de $\Omega \backslash K$ de taille 3 ce qui est impossible. Les deux points restant de A doivent se retrouvés dans un même 2-cycle de μ, disons (a_9, a_{10}). On a donc $A = \{a_1, \ldots, a_6, a_9, a_{10}\}$.

Soit maintenant B l'octade qui contient le 5-ensemble $\{a_3, \ldots, a_7\}$, alors, comme précédemment, B doit contenir un point supplémentaire de K. Ce ne peut être ni a_1, ni a_2 car sinon B intersecterait A en 5 points. Donc le 6^e point que l'on cherche est a_8. Pour que B soit stabilisé par μ, il doit contenir les deux points d'un 2-cycle de μ, disons a_{11} et a_{12}. On a ainsi $B = \{a_3, \ldots, a_8, a_{11}, a_{12}\}$. À ce moment on est dans la situation suivante :

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}
K	■	■	■	■	■	■	■	■				
A	■	■	■	■	■	■			■	■		
B			■	■	■	■	■	■			■	■
C		■	■	■	■			■				

où C représente l'octade qui contient l'ensemble $\{a_2,\ldots,a_5,a_8\}$. Or, C doit contenir un autre point de K. Ce point ne peut être a_6 ou a_7, car sinon C intersecterait B en 5 points. Il ne peut être a_1 non plus, car sinon C intersecterait A en 5 points. D'où une contradiction et K est une octade.

Il découle de ce qui précède que

$$\forall_{\pi\in M_{24}}\ \pi\cdot\mu\cdot\pi^{-1}\ \text{ fixe l'octade } \pi(K) \text{ point par point.}$$

Par la 5-transitivité de M_{24}, on peut envoyer (à l'aide de π) 5 points fixés par μ sur n'importe quel autre 5 points (fixés cette fois-ci par $\pi\cdot\mu\cdot\pi^{-1}$). Puisque chaque 5-ensemble est inclus dans une unique octade, ceci revient à dire que

$$\forall_{L\in\mathscr{C}_8}\exists_{\pi\in M_{24}}\ \pi\cdot\mu\cdot\pi^{-1}\ \text{ fixe L, point par point.}$$

Il est donc suffisant de montrer que P_K est transitif sur $\Omega\backslash K$ (où $K=\{a_1,a_2,\ldots,a_8\}=\{1,4,10,11,12,13,15,\infty\}$). Le groupe M_{24} contient la permutation

$$\alpha^{11}\cdot\delta=(0,11,7,16,1,6,12,19,10,18,15,3,14,5,9)(2,17,22)(4,13,20,21,8).$$

On peut trouver $\varphi\in M_{24}$ tel que les éléments du 5-cycle de $\theta=\varphi\cdot(\alpha^{11}\cdot\delta)\cdot\varphi^{-1}$ sont dans K. L'ensemble $\theta(K)$ est une octade (car M_{24} préserve $(\Omega,\mathscr{C}_8)$), qui contient 5 points de K, c'est-à-dire que $\theta(K)=K$ et donc que les éléments du 3-cycle de θ sont dans K.

Considérons les permutations

$$\mu_0=\mu,\ \mu_1=\theta\cdot\mu\cdot\theta^{-1},\ \mu_2=\theta^2\cdot\mu\cdot\theta^{-2},\ldots,\ \mu_{14}=\theta^{14}\cdot\mu\cdot\theta^{-14},$$

elles sont toutes dans P_K et sont formées de huit 2-cycles, donc d'ordre deux. Soit a_9 le seul élément fixé par θ et soit (a_9,a_{10}) le 2-cycle de μ contenant a_9. Comme les éléments du 3-cycle et du 5-cycle de θ sont dans K et comme θ fixe a_9, a_{10} est dans le 15-cycle de θ. Chaque μ_i contient donc un seul des 2-cycles suivants :

$$(a_9,a_{10}),\ (a_9,a_{11}),\ldots,\ (a_9,a_{24}),$$

et deux μ_i différents ne contiennent pas le même 2-cycle. Ces quinze 2-cycles, avec l'identité nous donne la transitivité de P_K sur $\Omega\backslash K$. □

Théorème 2.13. $|M_{24}|=244\,823\,040=2^{10}\cdot3^3\cdot5\cdot7\cdot11\cdot23.$

PREUVE. L'idée globale de cette preuve est de construire deux sous-groupes :

$$H < F < M_{24}$$

et de calculer $[M_{24} : F]$, $[F : H]$ et $|H|$ d'où

$$|M_{24}| = [M_{24} : F] \cdot [F : H] \cdot |H|.$$

Soit F le sous-groupe des éléments de M_{24} qui stabilise

$$K = \{a_1, a_2, \ldots, a_8\} := \{1, 4, 10, 11, 12, 13, 15, \infty\} \text{ (voir preuve précédente)}$$

et H le sous-groupe qui, en plus, fixe l'élément a_9.

- D'après la Proposition 2.11, $[M_{24} : F] = |\mathscr{C}_8| = 759$.
- D'après le Lemme 2.12, on a $[P_K : H] = 16$ or $P_K < F$ et alors F est transitif sur $\Omega \setminus K$ et ainsi $[F : H] = 16$
- $|H| = 20\,160$. En premier lieu, on montre que $|H| \leqslant |\mathrm{GL}_4(2)|$ et ensuite que $|A_8| \leqslant |H|$. La conclusion suivra du fait que

$$|A_8| = \frac{8!}{2} = 20\,160 = (2^4 - 1)(2^4 - 2^1)(2^4 - 2^2)(2^4 - 2^3) = |\mathrm{GL}_4(2)|.$$

i) $|H| \leqslant |\mathrm{GL}_4(2)|$ D'après le triangle des octades, 30 octades sont disjointes de $K = \{a_1, \ldots, a_8\}$. Soit O_1 une de ces octades, alors il existe O_1' une autre octade telle que $O_1 \dot{\cup} O_1' = \Omega \backslash K$. En effet, comme $K \in \mathscr{C}_8 \Rightarrow \Omega \backslash K \in \mathscr{C}$ et puisque

$$|O_1 + (\Omega \backslash K)| = 8 \Longrightarrow O_1 + (\Omega \backslash K) \in \mathscr{C}_8,$$

il suffit de poser $O_1' = O_1 + (\Omega \backslash K)$. Ces 30 octades viennent donc par paires : $O_1, O_1', O_2, O_2', \ldots, O_{15}, O_{15}'$, où $O_i \dot{\cup} O_i' = \Omega \backslash K$. La moitié de ces octades contiennent le point a_9 et l'autre moitié ne le contiennent pas. Soit $O_1, O_2, \ldots, O_{15}$ les octades ne contenant pas a_9. Montrons que

$$\forall_{i \neq j} \; |O_i \cap O_j| = 4. \tag{2.1}$$

On sait que $|O_i \cap O_j| = 0,\ 2$ ou 4. Si $|O_i \cap O_j| = 0$ alors $\Omega \backslash K = O_i \dot{\cup} O_j$ ce qui est impossible puisque ni O_i, ni O_j ne contiennent le point a_9 de $\Omega \backslash K$. Si $|O_i \cap O_j| = 2$, alors O_j doit contenir 6 points de O_i' ce qui est impossible car O_j et O_i' sont deux

octades différentes. Donc 2.1 est vraie et alors pour $i \neq j$, $O_i + O_j \in \Omega_8 \cap \mathscr{C}$, c'est-à-dire que $O_i + O_j$ est une octade. L'ensemble

$$\mathscr{V} = \{\emptyset, O_1, \ldots, O_{15}\}$$

est donc un sous-espace vectoriel de $\mathscr{C}$ de dimension 4.

Puisque H stabilise K, fixe a_9 et préserve $\mathscr{C}_8$, chacun de ses éléments permute les constituants de $\mathscr{V}$ et donc H agit sur $\mathscr{V}$. De plus, comme tous les éléments de M_{24} agissent de façon linéaire sur $\mathscr{C}$, il existe un homomorphisme de groupe :

$$\chi : H \longrightarrow Aut(\mathscr{V}) \simeq \mathrm{GL}_4(2).$$

Pour montrer que $|H| \leqslant |\mathrm{GL}_4(2)|$, il suffit de montrer que χ est injective. Pour ce faire, on démontre que le seul élément $h \in H$ qui agit trivialement sur $\mathscr{V}$ est l'identité de H (ou l'identité de M_{24} puisque $H < M_{24}$).

Construisons des éléments de $\mathscr{V}$ de telle sorte que si $h \in H$ fixe ces derniers alors h fixe chacun des éléments de Ω (et donc est l'identité de M_{24}). Soit $P(T) = \{T, T_1, \ldots, T_5\}$ une hexade (voir §3.4 Chapitre 1) tel que $T \cup T_5 = K$. Alors T_1, T_2, T_3 et T_4 sont des sous-ensembles de $\Omega \backslash K$. L'un de ces quatre ensembles, disons T_1, contient le point a_9. Alors les ensembles $V_1 = T_3 + T_4$, $V_2 = T_2 + T_4$ et $V_3 = T_2 + T_3$ sont des octades ne contenant pas le point a_9, c'est-à dire qu'ils sont dans $\mathscr{V}$. Il découle de 2.1 que tout élément de $\mathscr{V} \backslash \{V_1, V_2, V_3\}$ intersecte chacun des ensembles T_2, T_3 et T_4 en exactement deux points. En renommant les éléments de $\Omega \backslash (K \cup \{a_9\})$, on peut illustrer un tel élément, que nous appelerons V_4. Dans la figure suivante, les octades V_5, V_6 et V_7 sont respectivement $V_3 + V_4$, $V_2 + V_4$ et $V_1 + V_4$:

	T_1				T_2				T_3				T_4			
	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	a_{19}	a_{20}	a_{21}	a_{22}	a_{23}	a_{24}
V_1									■	■	■	■	■	■	■	■
V_2					■	■	■	■					■	■	■	■
V_3					■	■	■	■	■	■	■	■				
V_4			■	■			■	■			■	■			■	■
V_5			■	■	■	■			■	■					■	■
V_6			■	■	■	■					■	■	■	■		
V_7			■	■			■	■	■	■			■	■		
V_8		■		■		■		■		■		■		■		■

et V_8 représente une octade de $\mathscr{V}$ différente de $V_1,\ldots,V_7$. Il est à noter qu'en renommant les éléments de $\Omega\backslash K$, on est assuré d'avoir une telle octade.

Étant donné que $h(V_i)=V_i$, il faut que $h(T_i)=(T_i)$. Mais alors comme $V_4\in\mathscr{V}$, il faut que h préserve les ensembles $\{a_9,a_{10}\}$, $\{a_{11},a_{12}\}$,..., $\{a_{23},a_{24}\}$. La présence de V_8 dans $\mathscr{V}$ force h à fixer les éléments $a_{11},a_{12},\ldots,a_{24}$. De plus, on sait que les éléments de H fixent a_9 d'où h fixe a_{10} aussi. On a donc montré que h fixe $\Omega\backslash K$ point par point.

Supposons maintenant que h ne fixe pas K. Soit $h(a_1)=a_5$ et soit

$$L=\{a_1,a_2,a_3,a_4,a_9,a_{10},a_{11},a_{12}\},$$

l'octade contenant le 5-ensemble $\{a_1,a_2,a_3,a_4,a_9\}$, alors

$$h(L)=\{a_5,a_6,a_7,a_8,a_9,a_{10},a_{11},a_{12}\},$$

car $h(L)\in\mathscr{C}_8$ et que $h(a_1)=a_5$ implique que $L\neq h(L)$. L'élément h ne fixe donc aucun des membres de K. D'après le triangle des octades, il existe 16 octades qui intersectent K en exactement $\{a_1,a_2\}$. Prenons J une de ces octades. Puisque J contient six points de $\Omega\backslash K$ et que h fixe $\Omega\backslash K$ point par point, $h(J)=J$. Mais ceci est impossible car $h(\{a_1,a_2\})\cap\{a_1,a_2\}=\emptyset$, d'où h fixe chaque point de K.

ii) $|A_8|\leqslant|H|$ Considérons l'élément θ construit dans la preuve du Lemme 2.12. Cet élément stabilise K et par la 5-transitivité de M_{24}, on a $\forall_{(x_1,\ldots,x_5)\in K^5,\,x_i\neq x_j}\exists_{\psi\in M_{24}}\,\psi\cdot\theta\cdot\psi^{-1}$ possède (x_1,x_2,x_3) comme 3-cycle et x_4, x_5 se retrouvent dans le 5-cycle.

L'ensemble $\psi\cdot\theta\cdot\psi^{-1}(K)$ intersecte alors K en 5 points et est donc égal à celui-ci.

Remarquons que le ψ n'est peut-être pas unique. C'est donc dire qu'il y a peut-être plusieurs transformations $\psi\cdot\theta\cdot\psi^{-1}$ ayant (x_1,x_2,x_3) comme 3-cycle. Dénotons par $\theta_{(x_1,x_2,x_3)}$ l'une de ces transformations.

D'après le Lemme 2.12, $\exists_{\mu_j\in P_K}\,\mu_j\cdot\theta_{(x_1,x_2,x_3)}\cdot\mu_j^{-1}$ fixe l'élément a_9 auquel cas l'élément

$$\Phi_{(x_1,x_2,x_3)}:=\mu_j\cdot\theta_{(x_1,x_2,x_3)}\cdot\mu_j^{-1}\in H$$

Par construction $\Phi_{(x_1,x_2,x_3)}$ est formé du 3-cycle (x_1,x_2,x_3), d'un 5-cycle et d'un 15-cycle et donc $\Phi^{10}_{(x_1,x_2,x_3)}$, lui, est formé du même 3-cycle, d'un 15-cycle, mais d'aucun 5-cycle.

Étant donné que H agit sur K, qui possède 8 éléments, on peut trouver un homomorphisme tel que

$$\begin{array}{rccc} \rho : & H & \longrightarrow & S_8 \\ & \Phi^{10}_{(x_1,x_2,x_3)} & \longmapsto & (x_1,x_2,x_3) \end{array}$$

et donc $|A_8| \leqslant |Im(\rho)| \leqslant |H|$.

On peut maintenant déterminer l'ordre de M_{24}

$$|M_{24}| = [M_{24} : F] \cdot [F : H] \cdot |H| = 759 \cdot 16 \cdot 20\,160 = 244\,823\,040.$$

□

Corollaire 2.14. $M_{24} \simeq Aut(\Omega, \mathscr{C}_8)$

PREUVE. Par le Lemme 2.9, $M_{24} < Aut(\Omega, \mathscr{C}_8)$ et en réappliquant la preuve précédente sur $Aut(\Omega, \mathscr{C}_8)$, on obtient $|Aut(\Omega, \mathscr{C}_8)| = 244\,823\,040$. □

Une conséquence de ce corollaire est que le groupe M_{24} se retrouve, de façon isomorphe, dans le groupe de symétrie du réseau de Leech. Au Chapitre 4, on déterminera la cardinalité de ce dernier groupe, grâce, entre autre, à l'ordre de M_{24}.

Chapitre 3

RÉSEAU DE LEECH

§1. INTRODUCTION

La saga des groupes de Conway commenca avec la découverte du réseau de Leech. Dans les années 60, John Leech s'intéressa au problème d'empilements de sphères dans $\mathbb{R}^n$ pour $n \geqslant 3$. Ce problème consiste à placer des boules de même dimension, avec au plus un point d'intersection entre deux boules quelconques, de telle sorte que le volume occupé par les boules est le plus grand possible.

Leech découvra, en 1964, un réseau qui donnait un empilement très efficace dans $\mathbb{R}^{24}$ (voir [**Leech2**]). Trois années plus tard, soit en 1967, Leech présenta un deuxième réseau encore plus efficace que le premier (voir [**Leech1**]). C'est ce réseau qu'on appelle maintenant le réseau de Leech.

Leech suspectait la présence d'un nouveau groupe simple dans le groupe de symétrie de son réseau. Il exposa le problème à la communauté mathématique et environ une année plus tard, John Conway découvra trois nouveaux groupes simples relié à ce groupe de symétrie (voir [**Conway**]).

On expose ici la définition du réseau de Leech présentée par John Conway, plutôt que celle de Leech. Cette définition utilise le sous-espace $\mathscr{C}$ (voir §3.2).

§2. DÉFINITION

Soit, $S \subset \Omega$ et $m \in \mathbb{Z}$, on définit

$$[S,m] := \{x \in \mathbb{Z}^{\Omega} | \sum_{i\in\Omega} x_i = 4m,\ x_i \equiv m \bmod(4) \text{ si } i \notin S,\ x_i \equiv (m+2) \bmod(4) \text{ si } i \in S\}$$

Ici $\mathbb{Z}^{\Omega}$ représente les applications de Ω dans $\mathbb{Z}$ et $x_i := x(i)$. La première composante d'un vecteur est associée à ∞, la deuxième à 0, la troisième à 1 et ainsi de suite.

Soit maintenant $P \subset \mathcal{P}(\Omega)$ et $M \subset \mathbb{Z}$ alors on définit

$$[P,M] := \bigcup_{Q\in P, m\in M} [Q,m]$$

Le réseau de Leech est défini comme étant

$$\Lambda := [\mathscr{C},\mathbb{Z}]$$

où $\mathscr{C} =< \mathscr{C}_8 >_{\mathbb{F}_2}$ (voir Chapitre 1).

Pour un ensemble $T \subseteq \Omega$, on utilisera la notation e_T pour représenter le vecteur $\sum_{i\in T} e_i$.

Exemple 3.1. *Le vecteur* $w = e_\Omega - 4e_\infty = (-3,1,1,\ldots,1) \in \Lambda$. *En effet,*

$$\sum_{i\in\Omega} w_i = -3+23 = 20 = 4\cdot 5 \in 4\mathbb{Z} \quad et \quad \forall_{i\in\Omega}\, w_i \equiv 1 \equiv 5 \ mod(4)$$

donc $w \in [\emptyset, 5] \subset \Lambda$.

Remarque 3.2. *Dans le dernier exemple, on remarque que toutes les coordonnées de* $e_\Omega - 4e_\infty$ *sont impaires. En général les coordonnées d'un vecteur de* Λ *sont soit toutes paires, soit toutes impaires. Pour voir ceci prenons* $x \in [C,m] \subset \Lambda$, *alors*

$$x_i \equiv \begin{cases} m \ mod(4) & si \notin C \\ m+2 \ mod(4) & si \in C \end{cases}$$

et puisque $m \equiv (m+2) \ mod(2) \Rightarrow x_i \equiv m \ mod(2)$.

Définition 3.3 (Réseau)**.** *Soit* $E \subset \mathbb{R}^n$. E *est appelé un réseau s'il existe* $f_1, f_2, \ldots, f_m \in \mathbb{R}^n$, *linéairement indépendants, tels que*

$$E = \sum_{i=1}^{m} \mathbb{Z}\cdot f_i.$$

On verra dans la prochaine section que Λ est bel et bien un réseau. La proposition qui suit sera utile pour démontrer ceci.

Proposition 3.4. *Soient* $[C,m],[D,n] \in \Lambda$. *Alors*

$$\forall_{k,l\in\mathbb{Z}}\, k\cdot[C,m] + l\cdot[D,n] = [A, k\cdot m + l\cdot n]$$

où A est l'ensemble à la position $(k \mod (4), l \mod (4))$ *dans le tableau suivant :*

	0	1	2	3
0	$\emptyset$	D	D	D
1	C	$C+D$	C	$C+D$
2	C	D	$\emptyset$	D
3	C	$C+D$	C	$C+D$

PREUVE. Nous allons faire le cas $k \equiv 2 \mod (4)$, $l \equiv 1 \mod (4)$. Les autres cas seront semblables. On veut donc montrer que

$$k \cdot [C,m] + l \cdot [D,n] = [D, k \cdot m + l \cdot n].$$

i) ($\subseteq$) Soient $v \in [C,m]$ et $w \in [D,n]$. Posons $z = k \cdot m + l \cdot n$. On a tout d'abord

$$\sum_{i \in \Omega} z_i = \sum_{i \in \Omega} (k \cdot v_i + l \cdot w_i) = k \cdot 4m + l \cdot 4n = 4 \cdot (k \cdot m + l \cdot n).$$

De plus,

$$\begin{aligned} k \cdot v_i &\equiv \begin{cases} (k \cdot m) \bmod (4) & \text{si } i \notin C \\ k \cdot (m+2) \bmod (4) & \text{si } i \in C \end{cases} \\ &\equiv \begin{cases} (2 \cdot m) \bmod (4) & \text{si } i \notin C \\ 2 \cdot (m+4) \bmod (4) & \text{si } i \in C \end{cases} \\ &\equiv 2m \mod (4) \end{aligned}$$

et

$$\begin{aligned} l \cdot w_i &\equiv \begin{cases} (l \cdot n) \bmod (4) & \text{si } i \notin D \\ l \cdot (n+2) \bmod (4) & \text{si } i \in D \end{cases} \\ &\equiv \begin{cases} n \bmod (4) & \text{si } i \notin D \\ (n+2) \bmod (4) & \text{si } i \in D \end{cases} \end{aligned}$$

d'où

$$k \cdot v_i + l \cdot w_i \equiv \begin{cases} (2m+n) \bmod (4) & \text{si } i \notin D \\ (2m+n+2) \bmod (4) & \text{si } i \in D \end{cases}$$

et ainsi $z \in [D, k \cdot m + l \cdot n]$.

ii) ($\supseteq$) Pour faire cette direction, il suffit de démontrer que

$$[D, k \cdot m + l \cdot n] - k \cdot [C,m] \subset l \cdot [D,n].$$

On retombe alors dans le cas i).

□

§3. Ensemble de générateurs pour le réseau de Leech

Comme on vient de voir, la définition du réseau de Leech est intimement relié au sous-espace $\mathscr{C}$ et donc, par la même occasion, au système $(\Omega, \mathscr{C}_8)$ de type $S(5,8,24)$. Pour simplifier la manipulation du réseau de Leech, on aimerait pouvoir utiliser les propriétés de $(\Omega, \mathscr{C}_8)$ développées lors du Chapitre 1. La prochaine proposition permettra de faire ceci et démontrera en même temps que Λ est un réseau de $\mathbb{R}^{24}$.

Proposition 3.5. $\Lambda =< \{2e_K | K \in \mathscr{C}_8\} \cup \{w\} >_{\mathbb{Z}}$ *où w est un vecteur de* Λ *à coordonnées impaires (un tel vecteur existe d'après l'exemple 3.1).*

Pour démontrer cette proposition, on construit d'abord trois sous-réseaux de Λ :

- $X =< \{2e_K | K \in \mathscr{C}_8\} >_{\mathbb{Z}}$
- $Y =< \{4e_T | T \in \Omega_4\} >_{\mathbb{Z}}$
- $Z =< \{4e_i - 4e_j | i, j \in \Omega\} >_{\mathbb{Z}}$.

Les sous-réseaux Y et Z serviront à démontrer que X engendre tous les vecteurs de Λ dont les coordonnées sont des multiples de 4. En ajoutant un vecteur à coordonnées impaires de Λ, on obtiendra Λ au complet.

Lemme 3.6. $Z \subset Y \subset X \subset \Lambda$

Preuve. – $(Z \subset Y)$ Il suffit de remarquer que

$$4e_i - 4e_j = 4e_{\{i,a,b,c\}} - 4e_{\{j,a,b,c\}} \text{ où } \{i,j\} \cap \{a,b,c\} = \emptyset$$

D'où $\{4e_i - 4e_j | i, j \in \Omega\} \subset < \{4e_T | T \in \Omega_4\} >_{\mathbb{Z}}$.

– $(Y \subset X)$ Soit $P(T)$ une hexade (voir §3.4) et soit $T \neq U, V \in P(T)$. Alors

$$\begin{aligned} Y \ni 4e_T &= 2e_T + 2e_U + 2e_T + 2e_V - 2e_U - 2e_V \\ &= 2e_{T+U} + 2e_{T+V} - 2e_{U+V} \in X, \end{aligned}$$

car $T+U$, $T+V$ et $U+V$ sont des octades par définition d'hexade.

– $(X \subset \Lambda)$ Il suffit de constater que pour chaque $K \in \mathscr{C}_8$, $2e_K \in [K,4] \subset [\mathscr{C}, \mathbb{Z}] = \Lambda$

□

Lemme 3.7. *i)* $Z = [\emptyset, 0]$

ii) $Y = [\emptyset, 4\mathbb{Z}]$

iii) $X = [\mathscr{C}, 4\mathbb{Z}]$

PREUVE. On vérifie aisément les inclusions $Z \subset [\emptyset, 0]$, $Y \subset [\emptyset, 4\mathbb{Z}]$ et $X \subset [\mathscr{C}, 4\mathbb{Z}]$.

i) ($Z \supset [\emptyset, 0]$) Soit $v \in [\emptyset, 0]$ alors $\sum_{i \in \Omega} v_i = 0$ et $\forall_{i \in \Omega}\, v_i \equiv 0 \bmod(4)$. Chaque composante est donc un multiple de 4 :

$$\exists_{k_\infty, k_0, \ldots, k_{22} \in \mathbb{Z}}\, v = (4k_\infty, 4k_0, \ldots, 4k_{22}) \text{ et } \sum_{i \in \Omega} k_i = 0.$$

Cette dernière égalité nous donne $k_{22} = -\sum_{i \in \Omega \setminus \{22\}} k_i$ et alors :

$$\begin{aligned} v &= \textstyle\sum_{i \in \Omega \setminus \{22\}} (4k_i) e_i + 4k_{22} e_{22} \\ &= \textstyle\sum_{i \in \Omega \setminus \{22\}} (4k_i) e_i - \sum_{i \in \Omega \setminus \{22\}} 4k_i e_{22} \\ &= \textstyle\sum_{i \in \Omega \setminus \{22\}} k_i (4e_i - 4e_{22}). \end{aligned}$$

Étant donné que $\forall_{i \in \Omega}\, 4e_i - 4e_{22} \in Z$, on obtient l'inclusion désirée.

ii) ($Y \supset [\emptyset, 4\mathbb{Z}]$) Soit $v \in [\emptyset, 4\mathbb{Z}]$,

$$\exists_{m \in \mathbb{Z}} \sum_{i \in \Omega} v_i = 4(4m) \text{ et } \forall_{i \in \Omega}\, v_i \equiv 0 \bmod(4)$$

Soit $T \in \Omega_4$, alors $4e_T \in Y \cap [\emptyset, 4]$ et par conséquent $m \cdot 4e_T \in Y \cap [\emptyset, 4m]$. On construit maintenant le vecteur $y = v - m \cdot 4e_T$. Ce vecteur est dans $[\emptyset, 0]$ car

$$\begin{aligned} \sum_{i \in \Omega} y_i &= \sum_{i \in \Omega} v_i - m \sum_{i \in \Omega} (4e_T)_i \\ &= 4(4m) - m(4 \cdot 4) \\ &= 0 \end{aligned}$$

et $\forall_{i \in \Omega}\, y_i \equiv v_i - m \cdot (4e_T)_i \equiv 0 - 0 \equiv 0 \bmod(4)$

Donc $y \in [\emptyset, 0] = Z \subset Y$ et le fait que $4e_T \in Y$ implique $v = y + m \cdot e_T \in Y$.

iii) ($X \supset [\mathscr{C}, 4\mathbb{Z}]$) Montrons tout d'abord que

$$\forall_{K \in \mathscr{C}_8}\, [K, 4] \subset X$$

Soit $v \in [K, 4]$. Alors, par définition,

$$\sum_{i \in \Omega} v_i = 4 \cdot 4 \text{ et } v_i \equiv \begin{cases} 0 \bmod(4) & \text{si } i \notin K \\ 2 \bmod(4) & \text{si } i \in K \end{cases}$$

Donc $v - 2e_K \in [\emptyset, 0]$ car

$$\sum_{i\in\Omega}[v_i - (2e_K)_i] = \sum_{i\in\Omega} v_i - \sum_{i\in\Omega}(2e_K)_i = 4\cdot 4 - 2\cdot 8 = 0$$

et

$$(2e_K)_i \equiv \begin{cases} 0 \bmod(4) & \text{si } i \notin K \\ 2 \bmod(4) & \text{si } i \in K \end{cases} \Rightarrow \forall_{i\in\Omega}\, v_i - (2e_K)_i \equiv 0 \bmod(4)$$

Mais comme $[\emptyset, 0] = Z \subset Y \subset X$ et $2e_K \in X$, $v \in X$. On a donc montré que

$$\forall_{K\in\mathscr{C}_8}\, [K, 4] \subset X$$

et puisque $Y = [\emptyset, 4\mathbb{Z}] \subset X$, on a d'après le Proposition 3.4 :

$$[K, 4\mathbb{Z}] = [\emptyset, 4\mathbb{Z}] + [K, 4] \subset X \tag{3.1}$$

Enfin, prenons $[D, 4\mathbb{Z}] \subset [\mathscr{C}, 4\mathbb{Z}]$. Comme $\mathscr{C}_8$ engendre $\mathscr{C}$ (voir Chapitre 1),

$$\exists_{K_1,\ldots,K_r\in\mathscr{C}_8}\, D = \sum_{i=1}^{r} K_i \Rightarrow [D, 4\mathbb{Z}] = [\sum_{i=1}^{r} K_i, 4\mathbb{Z}] = \sum_{i=1}^{r} [K_i, 4\mathbb{Z}]$$

Enfin par 3.1, on trouve pour chaque i que $[K_i, 4\mathbb{Z}] \subset X$, d'où $[\mathscr{C}, 4\mathbb{Z}] \subset X$.

□

On vient maintenant de démontrer que X engendre bel et bien les vecteurs de Λ dont les coordonnées sont des multiples de 4. On peut donc démontrer la proposition :

Proposition 3.5. $\Lambda = < \{2e_K | K \in \mathscr{C}_8\} \cup \{w\} >_{\mathbb{Z}} = < X \cup \{w\} >_{\mathbb{Z}}$ *où w est un vecteur de Λ à coordonnées impaires.*

PREUVE. ($\Lambda \supseteq < X \cup \{w\} >_{\mathbb{Z}}$) Ceci est clair d'après la construction de X et le choix de w.

($\Lambda \subseteq < X \cup \{w\} >_{\mathbb{Z}}$) Soit $v \in \Lambda$, alors il existe $C \in \mathscr{C}$ et $m \in \mathbb{Z}$ tels que $v \in [C, m]$. Si $m \equiv 0 \bmod(4)$, alors $v \in X \subset < X \cup \{w\} >_{\mathbb{Z}}$.

Supposons donc que $m \not\equiv 0 \bmod(4)$. Comme $w \in \Lambda$ on a $w \in [D, n] \subset \Lambda$ pour un certain $D \in \mathscr{C}$ et où $n \equiv 1$ ou $3 \bmod(4)$. Regardons maintenant le vecteur

$$z = v - nm \cdot w.$$

D'après la Proposition 3.4, on a

i) Si $m \not\equiv 2 \bmod(4)$ alors $z \in [C + D, m - m \cdot n^2] \subset [C + D, 4\mathbb{Z}] \subset X$;

ii) si $m \equiv 2 \bmod(4)$ alors $z \in [C, m - m \cdot n^2] \subset [C, 4\mathbb{Z}] \subset X$.

Et, donc, dans les deux cas $v = z + nm \cdot w \in < X \cup \{w\} >_{\mathbb{Z}}$

□

Pour fixer les idées, nous allons choisir $w = e_\Omega - 4e_\infty$. On a vu dans l'exemple 3.1 que ce vecteur est dans Λ et que toutes ses coordonnées sont impaires. On prend donc $W = \{2e_K | K \in \mathscr{C}_8\} \cup \{e_\Omega - 4e_\infty\}$ comme ensemble de générateurs de Λ.

§4. POLYTOPE DE LEECH

Ce qui nous intéresse dans le réseau de Leech est l'ensemble des transformations qui le stabilisent et qui fixent l'origine. On va voir que l'ensemble des générateurs de Λ, trouvés à la section précédente, fait parti des vecteurs les plus près de l'origine. Les symétries de Λ qui fixent l'origine seront donc en bijection avec les symétries qui stabilisent les vecteurs les plus près de l'origine.

On veut identifier et caractériser les vecteurs les plus près de l'origine. Pour ce faire, il est naturel d'étudier la valeur de $x \cdot x$ quand $x \in \Lambda$ ($\cdot$ représente le produit scalaire usuel). Le réseau de Leech est engendré par W et pour chaque $w \in W$, $w \cdot w \in 32\mathbb{Z}$. De plus, on a

$$\forall_{v,w \in W}\ v \cdot w \in 8\mathbb{Z}.$$

En effet, si $v = 2e_K$ et $w = 2e_{K'}$, où $K, K' \in \mathscr{C}_8$, alors

$$\begin{aligned} v \cdot w &= (2e_K) \cdot (2e_{K'}) \\ &= 4 \cdot |K \cap K'| \\ &\equiv 0 \bmod(8) \text{ car } \forall_{K,K' \in \mathscr{C}_8}\ |K \cap K'| \equiv 0 \bmod(2) \end{aligned}$$

et si $v = 2e_K$, où $K \in \mathscr{C}_8$, et $w = e_\Omega - 4e_\infty$ alors

$$\begin{aligned} v \cdot w &= (2e_K) \cdot (e_\Omega - 4e_\infty) \\ &= \begin{cases} 16 & \text{si} \quad \infty \notin K \\ 8 & \text{si} \quad \infty \in K \end{cases} \\ &\equiv 0 \bmod(8) \end{aligned}$$

Sachant ceci, on peut maintenant généraliser à tous les vecteurs de Λ :

$$\forall_{x \in \Lambda}\ x \cdot x \in 16\mathbb{Z}.$$

Comme W engendre Λ, $\exists_{w_1,\ldots,w_r\in W}\exists_{\alpha_1,\ldots,\alpha_r\in\mathbb{Z}}\, x=\alpha_1 w_1+\cdots+\alpha_r w_r$ et en calculant le carré de la norme on trouve :

$$\begin{aligned} x\cdot x &= \sum_{i=1}^{r}\alpha_i^2(w_i\cdot w_i)+\sum_{i\neq j}\alpha_i\alpha_j(w_i\cdot w_j) \\ &= \sum_{i=1}^{r}\alpha_i^2\underbrace{(w_i\cdot w_i)}_{\equiv 0 \bmod(32)}+2\sum_{i<j}\alpha_i\alpha_j\underbrace{(w_i\cdot w_j)}_{\equiv 0\bmod(8)} \\ &\equiv 0 \bmod(16) \end{aligned}$$

À l'aide de cette propriété des vecteurs, on partitionne Λ en classes de distance :

$$\Lambda_n := \{x\in\Lambda | x\cdot x = 16\cdot n\} = \left\{ x\in\mathbb{Z}^{\Omega} \,\middle|\, \exists_m \begin{array}{l} 1) x\cdot x = 16\cdot n \\ 2) \sum x_i = 4m \\ 3) \forall_{i\in\Omega}\, x_i \equiv m \bmod(2) \\ 4) \forall_{p\in\{0,1,2,3\}}\, \{i\in\Omega | x_i \equiv p \bmod(4)\}\in\mathscr{C} \end{array} \right\}$$

À l'aide de cette partition des vecteurs on va montrer que Λ_1 est vide et que Λ_2 n'est pas vide d'où les vecteurs les plus près de l'origine sont ceux de Λ_2. Nous aurons besoin de la notation suivante pour caractériser les vecteurs de Λ_2. Le vecteur $((\pm 4)^2, 0^{22})$ représentera un vecteur de $\mathbb{Z}^{\Omega}$ constitué de deux ± 2 et de vingt-deux 0 (à n'importe quelle position).

- $\Lambda_0 = \{0\}$
- $\Lambda_1 = \emptyset$. Soit $x\in[C,n]\subset\Lambda$, tel que $x\cdot x = 16$ Si les coordonnées de x sont impaires alors $x\cdot x \geqslant 24$, ce qui est une contradiction. Si les coordonnées de x sont paires et $C\neq\emptyset$, alors

  $$x\cdot x \geqslant 4\cdot|C| \geqslant 32, \text{ car } C\in\mathscr{C} \text{ et donc } |C|\geqslant 8 \text{ (voir Théorème 1.14).}$$

  Si $C=\emptyset$, alors x doit être constitué d'un seul ± 4 comme coordonnée non nulle. Ceci contredit la propriété 3 car $\sum x_i = \pm 4\cdot 1$ et $x_i \equiv 0 \not\equiv 1 \bmod(2)$.
- Λ_2 n'est pas vide puisqu'il contient les vecteurs $2e_K$, où $K\in\mathscr{C}_8$. Ces vecteurs de Λ sont les plus près de l'origine (car $\Lambda_0=\{0\}$ et $\Lambda_1=\emptyset$). Décrivons tous les éléments de Λ_2. Tout d'abord, $x\in\Lambda_2 \Rightarrow x\cdot x = 32 \Rightarrow \forall_i\, |x_i| \leq 4\sqrt{2} < 6$. Soit $|x_j|$ la plus grande coordonnée de x en valeur absolue.
  - Si $|x_j| = 5$, on doit avoir $\sum_{i\neq j} x_i^2 = 32-25 = 7$ ce qui oblige x à avoir une composante nulle. Mais alors $x\notin\Lambda_2$ puisque qu'il possède une coordonnée paire et une coordonnée impaire (voir remarque 3.2).

– Si $|x_j| = 4$, alors $x = ((\pm 4)^2, 0^{22})$ ou $x = (\pm 4, (\pm 2)^4, 0^{19})$ sont les seuls vecteurs possibles avec toutes les coordonnées paires. Dans le premier cas, $x \in \Lambda_2$ parce que pour tout $i \neq j$, $4e_i - 4e_j \in [\emptyset, 0]$ et $4e_i + 4e_j \in [\emptyset, 2]$.Dans le deuxième cas, la position des ± 2 forme un 4-ensemble dans Ω. Or, $\mathscr{C}$ ne contient pas de 4-ensemble d'où la propriété 4) n'est pas satisfaite, c'est-à-dire que $x \notin \Lambda$.
– Si $|x_j| = 3$ alors $x = (\pm 3, (\pm 1)^{23})$. Ce x satisfait toutes les conditions excepté la 4e. Pour que x soit dans Λ_2, il faut que la position des coordonnées de x congrues à 1 modulo 4 forme un $\mathscr{C}$-ensemble.
– Si $|x_j| = 2$ alors $x = ((\pm 2)^8, 0^{16})$. Tout d'abord, d'après la condition 4, les ± 2 doivent être à la position d'un $\mathscr{C}$-ensemble (une octade). Mais x doit également satisfaire les conditions 2 et 3 :

$$\exists_m \sum x_i = 4 \cdot m \text{ et } x_i \equiv m \bmod(2)$$

Comme $x_i \equiv 0 \bmod(2)$, $m \equiv 0 \bmod(2)$. Soit k le nombre de "-2" dans x. En recalculant la somme des composantes, on trouve :

$$\begin{aligned} \sum x_i &= 2 \cdot (8-k) - 2k \\ &= 16 - 2k - 2k \\ &= 4 \cdot (4-k) \end{aligned}$$

et alors $m = 4 - k \equiv -k \equiv k \bmod(2)$. Bref, $x = ((\pm 2)^8, 0^{16}) \in \Lambda_2$ implique qu'il y a un nombre pair de -2 (k est pair) et les ± 2 sont en position d'un $\mathscr{C}$-ensemble.
– Si $|x_j| = 1$, $x \cdot x = \sum x_i \leq 24 < 32$, d'où $x \notin \Lambda_2$.

En résumé, les points de Λ_2 sont :

– $\Lambda_2^4 := \{((\pm 4)^2, 0^{22})\}$
– $\Lambda_2^3 := \{(\pm 3, (\pm 1)^{23}) |$ la position des coordonnées congrues à 1 modulo 4 forme un $\mathscr{C}$-ensemble $\}$
– $\Lambda_2^2 := \{((\pm 2)^8, 0^{16}) |$ les ± 2 sont en position d'une octade et il y a un nombre pair de $-2\}$

On peut maintenant vérifier que les générateurs de Λ sont dans L_2. Les vecteurs de la forme $2e_K$ où $K \in \mathscr{C}_8$ sont dans Λ_2^2, tandis que le vecteur $w = e_\Omega - 4e_\infty \in \Lambda_2^3$. Le groupe de symétrie du réseau de Leech pourra donc être vu comme le groupe de symétrie de Λ_2 (les symétries qui fixent l'origine).

La cardinalité de Λ_2 sera une information essentielle pour les prochains chapitres. Pour la trouver, on calcule la cardinalité de chacun des Λ_2^i. On a donc

- $|\Lambda_2^4|$ = (position des deux ± 4)· (les signes des 4) $= \binom{24}{2} \cdot 2^2 = 1104$
- $|\Lambda_2^3|$ = (position du ± 3)·(les coordonnées congrues à 1 modulo 4 sont en position d'un $\mathscr{C}$-ensemble)$= 24 \cdot 2^{12} = 98\,304$
- $|\Lambda_2^2|$ = (les ± 2 sont en position d'une octade)· (les signes des ± 2) $= 759 \cdot 2^7 = 97\,152$

D'où $|\Lambda_2| = |\Lambda_2^4| + |\Lambda_2^3| + |\Lambda_2^2| = 1104 + 98\,304 + 97\,152 = 196\,560 = 2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13.$

- De façon similaire, on trouve que Λ_3 est formé des orbites Λ_3^2 ,Λ_3^3, Λ_3^4, Λ_3^5 où
  - $\Lambda_3^2 := \{((\pm 2)^{12}, 0^{12}) |$les ± 2 sont en position d'une dodécade et il y a un nombre pair de $-2\}$
  - $\Lambda_3^3 := \{((\pm 3)^3, (\pm 1)^{21}) |$les coordonnées congrues à 1 modulo 4 sont en position d'un $\mathscr{C}$-ensemble$\}$
  - $\Lambda_3^4 := \{((\pm 4), (\pm 2)^8, 0^{15}) |$les ± 2 sont en position d'une octade et il y a un nombre impair de $-2\}$
  - $\Lambda_3^5 := \{(\pm 5, (\pm 1)^{23}) |$les coordonnées congrues à 1 modulo 4 sont en position d'un $\mathscr{C}$-ensemble $\}$

  et leur cardinalité est
  - $|\Lambda_3^2| = 2576 \cdot 2^{11}$
  - $|\Lambda_3^3| = \binom{24}{3} \cdot 2^{12}$
  - $|\Lambda_3^4| = 759 \cdot 16 \cdot 2^8$
  - $|\Lambda_3^5| = 24 \cdot 2^{12}$

  D'où $|\Lambda_3| = |\Lambda_3^2| + |\Lambda_3^2| + |\Lambda_3^2| + |\Lambda_3^2| = 16\,773\,120 = 2^{12} \cdot 3^2 \cdot 5 \cdot 7 \cdot 13.$

La cardinalité de Λ_2 et de Λ_3 est nécessaire car dans le Chapitre 5 on fera agir $\cdot 1$, le groupe de symétrie du réseau de Leech quotienté par son centre, sur ces ensembles et on aura besoin de la cardinalité du stabilisateur d'un point.

L'ensemble de générateurs W sera utile dans le prochain chapitre où on tentera de déterminer la cardinalité du groupe de symétrie du réseau de Leech.

Chapitre 4

GROUPE DE SYMÉTRIE DU RÉSEAU DE LEECH

§1. INTRODUCTION

Ce chapitre utilise toutes les notions principales des trois premiers chapitres dans le but de calculer la cardinalité du groupe de symétrie du réseau de Leech. Cette information est nécessaire dans le prochain chapitre pour démontrer la simplicité des trois groupes simples reliés au groupe de symétrie du réseau de Leech.

§2. DÉFINITION

Définition 4.1. *On dénote par* $\cdot 0$ *le sous-groupe de toutes les transformations orthogonales* ($\in O_{24}(\mathbb{Q})$) *qui stabilisent* Λ. *Autrement dit*

$$\cdot 0 := \{\lambda \in O_{24}(\mathbb{Q}) | \lambda(\Lambda) \subseteq \Lambda\}$$

§3. LE SOUS-GROUPE N

Le but ultime de ce chapitre est de calculer la cardinalité de $\cdot 0$. Il n'est pas nécessaire de connaître toute la structure de $\cdot 0$ pour y arriver. Par contre, on aimerait connaître un sous-groupe explicite de $\cdot 0$. Dans cette section, on construira un sous-groupe de $\cdot 0$, qu'on dénotera par N, qui sera relié au sous-espace $\mathscr{C}$ (voir Section §3.2 au Chapitre 1) ainsi qu'au groupe de Mathieu M_{24} (voir Chapitre 2). On pourra ainsi utiliser les propriétés de ces derniers pour travailler avec les éléments de N.

On verra à la Section §5 que N est maximal et grâce à ceci, on pourra trouver la cardinalité de $\cdot 0$.

Définition 4.2. – *Soit $\pi \in S_\Omega$. On définit l'application suivante de $O_{24}(\mathbb{Q})$:*

$$\begin{array}{rccc} m_\pi : & \mathbb{Q}^\Omega & \longrightarrow & \mathbb{Q}^\Omega \\ & e_i & \longmapsto & e_{\pi(i)} \end{array}$$

– *Soit maintenant $T \subseteq \Omega$, on définit une nouvelle application de $O_{24}(\mathbb{Q})$:*

$$\begin{array}{rccc} \varepsilon_T : & \mathbb{Q}^{24} & \longrightarrow & \mathbb{Q}^{24} \\ & e_i & \longmapsto & \begin{cases} e_i & si\ i \notin T \\ -e_i & si\ i \in T \end{cases} \end{array}$$

Exemple 4.3. *Soit $w = e_\Omega - 4e_\infty = (-3,1,1,\ldots,1)$. Alors*

$$\varepsilon_{\{\infty,1,2\}}(w) = (3,1,-1,-1,1,1,\ldots,1) \quad et \quad m_{(\infty,2)}(w) = (1,1,1,-3,1,1,\ldots,1).$$

On se rappelle que la première coordonnée est associée à ∞, la deuxième à 0, etc.

Proposition 4.4. *i) $m_\pi \in \cdot 0 \Leftrightarrow \pi(\mathscr{C}) = \mathscr{C}$, c'est-à-dire π préserve $(\Omega, \mathscr{C}_8)$. On dénote l'ensemble de toutes ces transformations par :*

$$M := \{m_\pi | \pi(\mathscr{C}) = \mathscr{C}\} = \{m_\pi | \pi \in M_{24}\} \simeq M_{24}.$$

Donc $|M| = |M_{24}|$.

ii) $\varepsilon_T \in \cdot 0 \Leftrightarrow T \in \mathscr{C}$ et

$$E := \{\varepsilon_T | T \in \mathscr{C}\} \simeq (\mathscr{C}, +).$$

L'isomorphisme découle du fait que $\varepsilon_T \cdot \varepsilon_S = \varepsilon_{T+S}$ et donc $|E| = |\mathscr{C}| = 2^{12}$.

PREUVE. i)

$$\begin{array}{rcl} m_\pi \in \cdot 0 & \Longleftrightarrow & \forall_{v \in \Lambda}\ m_\pi(v) \in \Lambda \\ & \Longleftrightarrow & \forall_{K \in \mathscr{C}_8}\ (m_\pi(2e_K) = 2e_{\pi(K)} \in \Lambda) \text{ et } (m_\pi(e_\Omega - 4e_\infty) = e_\Omega - 4e_{\pi(\infty)} \in \Lambda) \\ & \Longleftrightarrow & \forall_{K \in \mathscr{C}_8}\ m_\pi(2e_K) \in \Lambda, \text{ car } e_\Omega - 4e_{\pi(\infty)} \in \Lambda_2^3 \text{ pour tout } \pi \in S_\Omega \\ & \Longleftrightarrow & \forall_{K \in \mathscr{C}_8}\ \text{les positions des 2 dans } 2e_{\pi(K)} \text{ forment un } \mathscr{C}\text{-ensemble} \\ & \Longleftrightarrow & \forall_{K \in \mathscr{C}_8}\ \pi(K) \in \mathscr{C}_8 \\ & \Longleftrightarrow & \pi(\mathscr{C}) = \mathscr{C} \\ & \Longleftrightarrow & \pi \in M_{24}, \text{ d'après le chapitre 2.} \end{array}$$

ii) On utilise la même astuce qu'en i) :

$$\begin{aligned}
\varepsilon_T \in \cdot 0 &\iff \forall_{v\in\Lambda}\, \varepsilon_T(v) \in \Lambda \\
&\iff \forall_{K\in\mathscr{C}_8}\, (\varepsilon_T(2e_K) \in \Lambda) \text{ et } (\varepsilon_T(e_\Omega - 4e_\infty) \in \Lambda) \\
&\iff \forall_{K\in\mathscr{C}_8}\, (\text{le nombre de "-2" dans } \varepsilon_T(2e_K) \text{ est pair}) \text{ et } (T \in \mathscr{C}, \text{ car} \\
&\qquad \text{les coordonnées congrues à } 3 \bmod(4) \text{ sont en position de } T \text{ et} \\
&\qquad \text{la propriété 4 (voir la définition de } \Lambda_n \text{ à la page 37) donne} \\
&\qquad \text{donc } T \in \mathscr{C}) \\
&\iff \forall_{K\in\mathscr{C}_8}(|T\cap K| \equiv 0 \bmod(2)) \text{ et } (T \in \mathscr{C}) \\
&\iff T \in \mathscr{C}^\perp = \mathscr{C} \text{ (voir preuve du Théorème 1.19) et } T \in \mathscr{C} \\
&\iff T \in \mathscr{C}
\end{aligned}$$

□

Définition 4.5. *À partir de ces deux sous-groupes, on construit l'ensemble* $N := E \cdot M$

La prochaine proposition nous assure que N est un sous-groupe de $\cdot 0$.

Proposition 4.6. $\forall_{m_\pi\in M}\, m_\pi \cdot E \cdot m_\pi^{-1} \subseteq E$.

PREUVE. Soit $\varepsilon_T \in E$. Pour chaque $i \in \Omega$ on a

$$\begin{aligned}
m_\pi \cdot \varepsilon_T \cdot m_\pi^{-1}(e_i) &= m_\pi \cdot \varepsilon_T \cdot m_{\pi^{-1}}(e_i) \\
&= m_\pi \cdot \varepsilon_T(e_{\pi^{-1}(i)}) \\
&= \begin{cases} m_\pi(-e_{\pi^{-1}(i)}) \text{ si } \pi^{-1}(i) \in T \\ m_\pi(e_{\pi^{-1}(i)}) \text{ si } \pi^{-1}(i) \notin T \end{cases} \\
&= \begin{cases} -e_i \text{ si } \pi^{-1}(i) \in T \\ e_i \text{ si } \pi^{-1}(i) \notin T \end{cases} \\
&= \begin{cases} -e_i \text{ si } i \in \pi(T) \\ e_i \text{ si } i \notin \pi(T) \end{cases} \\
&= \varepsilon_{\pi(T)}(e_i) \in E
\end{aligned}$$

□

§4. PROPRIÉTÉS DE N

On énumère ici toutes les propriétés de N qui seront nécessaires pour la prochaine section.

Théorème 4.7. *Soit* $\lambda \in \cdot 0$. *Si* $\exists_{i,j\in\Omega}\, \lambda(e_i) = \pm e_j$ *alors* $\lambda \in N$.

PREUVE. On remarque d'abord que $\forall_{k\neq i}\, \lambda(e_k) \perp e_j$ (toujours par rapport au produit scalaire usuel). En effet, si $i \neq k$

$$\begin{aligned} 0 &= e_i \cdot e_k &&= \lambda(e_i)\cdot\lambda(e_k) \text{ car } \lambda \in \cdot 0 < O_{24}(\mathbb{R}) \\ &&&= \pm e_j \cdot \lambda(e_k) \end{aligned}$$

Ensuite, on sait que si $i \neq k$, $4e_i + 4e_k \in \Lambda_2$ et, donc, comme $\lambda \in \cdot 0$,

$$\Lambda_2 \ni z := \lambda(4e_i + 4e_k) = 4\lambda(e_i) + 4\lambda(e_k) = \pm 4e_j + 4\lambda(e_k)$$

Or, e_j étant perpendiculaire à $\lambda(e_k)$, on obtient l'existence d'au moins une coordonnée égale à ± 4 dans z. La classification de Λ_2 (voir Section §4, Chapitre 3) oblige z à être dans Λ_2^4 et ainsi $\lambda(e_k) = \pm e_l$ pour $l \in \Omega$, chaque k donnant des valeurs de l différentes.

La transformation λ est en fait une permutation et un changement de signe des éléments de la base. Symboliquement, on obtient

$$\lambda = \varepsilon_T \cdot m_\pi, \text{ pour } T \subseteq \Omega, \pi \in S_\Omega.$$

Pour montrer que $\lambda \in N$, il reste à montrer que $T \in \mathscr{C}$ et $\pi \in M_{24}$.

– ($\pi \in M_{24}$) Puisque $\lambda \in \cdot 0$, $\forall_{K\in\mathscr{C}_8}\, \lambda(2e_K) \in \Lambda$. Mais les coordonnées non nulles des vecteurs $\lambda(2e_K)$ sont en position $\pi(K)$. Pour que $\lambda(2e_K) \in \Lambda$, il faut donc que $\pi(K) \in \mathscr{C}_8$, et ce pour tout $K \in \mathscr{C}_8$. D'où $\pi \in M_{24}$.

– ($T \in \mathscr{C}$) Enfin on regarde le vecteur $e_\Omega - 4e_\infty$ dans Λ. Toutes les coordonnées de ce vecteur sont congrues à 1 modulo 4. Si on applique λ à $e_\Omega - 4e_\infty$, les coordonnées aux positions de T changent de signe et deviennent alors congrues à 3 modulo 4. Donc pour que $\lambda(e_\Omega - 4e_\infty)$ soit dans Λ, il faut que T soit dans $\mathscr{C}$.

□

N étant un sous-groupe de $\cdot 0$, il agit sur Λ_2. La proposition qui suit donne les orbites de cette action.

Proposition 4.8. *N agit sur Λ_2 avec les trois orbites : Λ_2^2, Λ_2^3 et Λ_2^4 (voir §4 dans le Chapitre 3).*

PREUVE. Réécrivons d'abord ces ensembles sous la forme :

$$\Lambda_2^2 = \{\varepsilon_T(2e_K) | T, K \in \mathscr{C}_8\}$$
$$\Lambda_2^3 = \{\varepsilon_T(e_\Omega - 4e_l) | T \in \mathscr{C}, l \in \Omega\}$$
$$\Lambda_2^4 = \{\varepsilon_T(4e_i + 4e_j) | i, j \in \Omega, i \neq j, T \in \mathscr{C}\}$$

Soit

i) $x = \varepsilon_T(2e_K)$ et $y = \varepsilon_{T'}(2e_{K'})$ dans Λ_2^2 ou

ii) $x = \varepsilon_T(e_\Omega - 4e_l)$ et $y = \varepsilon_{T'}(e_\Omega - 4e_{l'})$ dans Λ_2^3 ou

iii) $x = \varepsilon_T(4e_i + 4e_j)$ et $y = \varepsilon_{T'}(4e_{i'} + 4e_{j'})$ dans Λ_2^4.

Par la 5-transitivité de M_{24} sur Ω, il existe π tel que soit

i) $\pi(K) = K'$, voir le lemme 2.11 dans le Chapitre 2 ou

ii) $\pi(l) = l'$ ou

iii) $\pi(i, j) = (i', j')$.

La transformation $\varepsilon_{T'+\pi(T)} \cdot m_\pi$ est dans N, car $\pi(T) \in \mathscr{C}$ étant donné que $M_{24} \simeq Aut(\mathscr{C})$ et $T' + \pi(T)$ est donc également dans $\mathscr{C}$. Cette transformation envoie x sur y dans chaque cas. Par exemple, pour le cas 1) :

$$\begin{aligned} \varepsilon_{T'+\pi(T)} \cdot m_\pi(\varepsilon(2e_K)) &= \varepsilon_{T'+\pi(T)}(\varepsilon(2e_{K'})) \\ &= \varepsilon_{T'+\pi(T)+\pi(T)}(2e_{K'}) \\ &= \varepsilon_{T'}(2e_{K'}) \end{aligned}$$

Les autres cas sont semblables. Les orbites Λ_2^i sont disjointes car les éléments de N préservent le nombre de coordonnées non nulles. □

Théorème 4.9. *Soit $\lambda \in \cdot 0$, si $ord(\lambda)$ est premier alors $ord(\lambda) \leqslant 23$.*

PREUVE. Soit A la matrice qui représente λ, un élément d'ordre $p \in \mathbb{P}$ dans $\cdot 0$, dans la base standard. Les entrées de la matrice A sont rationnelles car λ préserve Λ. Soit maintenant $T(x)$ le polynôme minimal de A sur $\mathbb{Q}$. Puisque λ est d'ordre p, la matrice A est une racine du polynôme

$$x^p - 1 = (x-1) \cdot (x^{p-1} + x^{p-2} + \ldots + x + 1)$$

et donc $T(x)$ divise $x^{p-1}+x^{p-2}+\ldots+x+1$. Ce dernier polynôme est irréductible sur $\mathbb{Q}$ et alors $T(x)=x^{p-1}+x^{p-2}+\ldots+x+1$. Enfin le Théorème de Cayley-Hamilton stipule que $T(x)$ divise le polynôme caractéristique de A qui est de degré au plus 24. Il faut donc que $p-1\leqslant 24$, ce qui laisse $p\leqslant 23$ car p est premier. □

Théorème 4.10. *Soit* $\lambda\in\cdot 0$. *Si* $\lambda(\Lambda_2^4)\subset\Lambda_2^4$ *alors* $\lambda\in N$.

PREUVE. Soit H, le sous-groupe constitué des transformations de $\cdot 0$ qui stabilisent Λ_2^4, et soit $x=4e_i+4e_j$.

La 5-transitivité de M_{24} sur Ω, donne la 5-transitivité de N sur $\{e_i|i\in\Omega\}$.

Regardons l'action de N_x (ici $N_x:=Stab_N(x)$) sur $\Lambda_2^4(x)$ ($\Lambda_2^4(x)$ représente l'ensemble des vecteurs de Λ_2^4 perpendiculaires à x). Cette action possède les deux orbites suivantes :

Orbite 1 $\{\pm(4e_i-4e_j)\}$ contenant 2 éléments

Orbite 2 $\{\pm 4e_h\pm 4e_k|h,k,i,j\,distincts\}$ car la 5-transitivité de N sur les coordonnées nous assure, pour tout (l,m), l'existence d'une transformation qui fixe i et j (donc dans N_x) et envoie (h,k) sur (l,m) . Cette orbite contient $\binom{22}{2}\cdot 2^2=924$ éléments.

Par la Proposition 4.8, N stabilise Λ_2^4 et ainsi $N\subseteq H$, d'où $N_x\subseteq H_x$. Les orbites de H_x sur $\Lambda_2^4(x)$ doivent alors être une union de ceux de N_x sur $\Lambda_2^4(x)$.

Si $\Lambda_2^4(x)$ possédait une seule orbite sur H_x, elle contiendrait $924+2=926$ éléments et alors :

$$|H_x|=|Orb_{H_x}(y)|\cdot|H_{x,y}|=926\cdot|H_{x,y}|=2\cdot 463\cdot|H_{x,y}|.$$

$H_{x,y}$ représente les éléments de H qui stabilise x et y. Or comme 463 est premier, le Théorème de Cauchy (qui stipule que pour chaque premier p qui divise l'ordre d'un groupe G, il existe un élément de G d'ordre p) nous donne l'existence d'un élément d'ordre 463 dans H_x et ceci contredit le Théorème 4.9. H_x possède ainsi deux orbites sur $\Lambda_2^4(x)$ et si $\lambda\in H_x$ alors $\lambda(4e_i+4e_j)=4e_i+4e_j$ et

$$(\lambda(4e_i-4e_j)=4e_i-4e_j\Rightarrow\lambda(e_i)=e_i)\ \text{ ou }\ (\lambda(4e_i-4e_j)=4e_j-4e_i\Rightarrow\lambda(e_i)=e_j).$$

D'après le Théorème 4.7, $\lambda\in N_x$ et donc $N_x=H_x$. On sait, d'après la Proposition 4.8, que N agit transitivement sur Λ_2^4 et donc H aussi agit transitivement sur Λ_2^4. On a alors

$$|N|=|\Lambda_2^4|\cdot|N_x|=|\Lambda_2^4|\cdot|H_x|=|H|$$

d'où $H=N$. □

§5. MAXIMALITÉ DE N ET CARDINALITÉ DE $\cdot 0$

Pour démontrer la maximalité de N, on prend un sous-groupe H de $\cdot 0$ qui le contient strictement. On démontre qu'alors H est transitif sur Λ_2 et que, pour chaque $x \in \Lambda_2$, H_x est transitif sur $\Lambda_2(x)$ (l'ensemble des vecteurs de Λ_2 perpendiculaires à x). À l'aide de ces deux faits, on obtient l'égalité :

$$|H| = |\Lambda_2| \cdot |\Lambda_2(x)| \cdot |H_{x,y}| \text{ où } y \in \Lambda_2(x).$$

En choisissant x et y convenablement, il est possible de calculer la cardinalité de $H_{x,y}$, d'où nécessairement N est maximal.

Pour pouvoir choisir un H contenant N strictement, on doit d'abord s'assurer que $N \neq \cdot 0$.

Théorème 4.11. *N est un sous-groupe propre de $\cdot 0$.*

PREUVE. Pour prouver ceci, nous allons construire une transformation dans $\cdot 0 \backslash N$. Soit $P(T)$ une hexade (voir §3.4 dans le Chapitre 1). On définit l'application

$$\begin{array}{rccc} \eta: & \mathbb{Q}^\Omega & \longrightarrow & \mathbb{Q}^\Omega \\ & e_i & \longmapsto & e_i - \frac{1}{2} e_U \text{ si } i \in U \in P(T) \end{array}$$

La transformation voulue est $\zeta_T := \varepsilon_T \cdot \eta$. Cette transformation n'est pas dans N puisqu'elle envoie e_i, qui ne possède qu'une seule coordonnée non nulle, sur un vecteur qui en possède quatre. Or, toutes les transformations de N sont une permutation suivie d'un changement de signes des éléments de la base d'où le nombre de coordonnées non nulles demeure invariant.

Il reste à vérifier que $\zeta_T \in \cdot 0$. Pour ce faire, il est suffisant, d'après le Chapitre 3, de montrer que

$$\forall_{K \in \mathscr{C}_8} \ \zeta_T(2e_K) \in \Lambda \text{ et } \zeta_T(w) \in \Lambda \text{ où w est un vecteur à coordonnées impaires.}$$

Posons, tout d'abord, $P(T) = \{U, V, W, X, Y, Z\}$. Alors, pour tout $K \in \mathscr{C}_8$, on a un des trois cas suivants (en renommant les éléments de $P(T)$, on se réduit à un de ces trois cas pour chaque K) :

i) $|K \cap U| = |K \cap V| = 4$

ii) $|K \cap U| = |K \cap V| = |K \cap W| = |K \cap X| = 2$

iii) $|K \cap Z| = 3$ et $|K \cap U| = |K \cap V| = |K \cap W| = |K \cap X| = |K \cap Y| = 1$

Remarquons que, d'après le triangle des octades (voir Chapitre 1), chaque cas est réalisable. Regardons l'effet de $\varepsilon_Z \cdot \eta$ sur $2e_K$ dans chacune de ces situations :

$$\begin{aligned}
\text{i)}\quad \varepsilon_Z \cdot \eta(2e_K) &= \varepsilon_Z \cdot \eta(2e_U + 2e_V) \\
&= \varepsilon_Z(2e_U - 4e_U + 2e_V - 4e_V) \\
&= \varepsilon_Z(-2e_U - 2e_V) \\
&= \varepsilon_Z(-2e_K) \\
&= -2e_K \in \Lambda,
\end{aligned}$$

$$\begin{aligned}
\text{ii)}\quad \varepsilon_Z \cdot \eta(2e_K) &= \varepsilon_Z \cdot \eta(2e_{K\cap U} + 2e_{K\cap V} + 2e_{K\cap W} + 2e_{K\cap X}) \\
&= \varepsilon_Z(2e_{K\cap U} - 2e_U + 2e_{K\cap V} - 2e_V + 2e_{K\cap W} - 2e_W + 2e_{K\cap X} - 2e_X) \\
&= \varepsilon_Z(-2e_{U\setminus K} - 2e_{V\setminus K} - 2e_{W\setminus K} - 2e_{X\setminus K}) \\
&= \varepsilon_Z(-2e_{U\setminus K+V\setminus K+W\setminus K+X\setminus K}) \\
&= \varepsilon_Z(-2e_{K+U+V+W+X}) \\
&= -2e_{K+U+V+W+X} \in \Lambda,
\end{aligned}$$

$$\begin{aligned}
\text{iii)}\quad \varepsilon_Z \cdot \eta(2e_K) &= \varepsilon_Z(2e_K - 3e_Z - e_{U+V+W+X+Y}) \\
&= \varepsilon_Z(2e_{K\setminus Z} + 2e_{K\cap Z} - 3e_Z - e_{\Omega\setminus Z}) \\
&= 2e_{K\setminus Z} - 2e_{K\cap Z} + 3e_Z - e_{\Omega\setminus Z} \\
&= 2e_{K\setminus Z} - 2e_{K\cap Z} + 4e_Z - (e_Z + e_{\Omega\setminus Z}) \\
&= \varepsilon_K(-2e_{K\setminus Z} + 2e_{K\cap Z} + 4e_{Z\setminus K} - 4e_{Z\cap K} + 2e_K - e_\Omega) \\
&= \varepsilon_K(4e_{Z\setminus K} - e_\Omega) \in \Lambda, \text{ car } \varepsilon_K \in \cdot 0 \text{ et } (4e_{Z\setminus K} - e_\Omega) \in \Lambda.
\end{aligned}$$

Dans chaque cas, on obtient $\varepsilon_Z \cdot \eta(2e_K) \in \Lambda$. On a de plus $T + Z \in \mathscr{C}$, d'où $\varepsilon_{T+Z} \in \cdot 0$ et ainsi :

$$\zeta_T(2e_K) = \varepsilon_T \cdot \eta(2e_K) = \varepsilon_{T+Z} \cdot (\varepsilon_Z \cdot \eta(2e_K)) \in \Lambda.$$

Pour montrer que $\zeta_T \in \cdot 0$, il reste à démontrer que $\zeta_T(w) \in \Lambda$, où w est un vecteur à coordonnées impaires. En utilisant le fait que $\zeta_T^2 = id$, il découle du cas iii) que

$$\Lambda \ni 2e_K = \zeta_T(\zeta_T(2e_K)) = \zeta_T(\varepsilon_{T+Z} \cdot \varepsilon_K(4e_{Z\setminus K} - e_\Omega)).$$

Ceci termine la preuve puisque les coordonnées de $(\varepsilon_{T+Z} \cdot \varepsilon_K(4e_{Z\setminus K} - e_\Omega))$ sont ± 1 et ± 3, donc impaires. □

La proposition nous permet de choisir $N \lneqq H < \cdot 0$. Ce H sera fixé pour le reste de la section.

Théorème 4.12. *H est transitif sur* Λ_2.

PREUVE. D'après le Théorème 4.8, N possède trois orbites sur Λ_2 : Λ_2^2, Λ_2^3 et Λ_2^4 (voir §4, chapitre 3). N étant inclus dans H, les orbites de H sur Λ_2 sont des unions des orbites de N sur Λ_2. Considérons l'orbite de H contenant Λ_2^4. Par le Théorème 4.10, cette orbite ne peut être Λ_2^4. De plus,

$$|\Lambda_2^4 \cup \Lambda_2^2| = 2^4 \cdot 3 \cdot 23 \cdot 89 \text{ et } |\Lambda_2^4 \cup \Lambda_2^3| = 2^4 \cdot 3 \cdot 19 \cdot 109$$

et puisque 89 et 109 sont premiers, le Théorème 4.9 et le Théorème de Cauchy excluent $\Lambda_2^4 \cup \Lambda_2^2$ et $\Lambda_2^4 \cup \Lambda_2^2$ comme possibilités. L'orbite qui contient Λ_2^4 est donc $\Lambda_2^2 \cup \Lambda_2^3 \cup \Lambda_2^4 = \Lambda_2$. □

Théorème 4.13. $\forall_{x \in \Lambda_2}$ H_x *est transitif sur* $\Lambda_2(x)$. *On rappelle que* $\Lambda_2(x)$ *représente tous les vecteurs de* Λ_2 *perpendiculaires à x.*

PREUVE. Regardons d'abord ce qui se passe pour $x = e_\Omega - 4e_\infty \in \Lambda$. On sait du Chapitre 2 que M_{24} contient l'élément $\alpha = (0,1,2,\ldots,21,22)$ et donc N contient l'élément m_α. Cet élément fixe le vecteur e_∞ et ainsi appartient à $N_x \subseteq H_x$. L'élément m_α est d'ordre 23 dans N et ne fixe aucun élément de $\Lambda_2(x)$ (il suffit d'utiliser la classification de Λ_2 à la page 38). En utilisant le même principe, on trouve que

$$n \in \{1,\ldots,22\} \Rightarrow (m_\alpha)^n = m_{\alpha^n} \text{ ne fixe aucun élément de } \Lambda_2(x). \tag{4.1}$$

Il découle de ceci que toutes les orbites de $< m_\alpha >$ sur $\Lambda_2(x)$ ont exactement 23 éléments. Or comme $< m_\alpha > < H_x$ et comme les orbites de H_x sur $\Lambda_2(x)$ sont des unions des orbites de $< m_\alpha >$ sur $\Lambda_2(x)$, la cardinalité de chaque orbite de H_x sur $\Lambda_2(x)$ est divisible par 23.

Soit y un point quelconque de Λ. Puisque H est transitif sur Λ, on trouve l'existence de $\lambda \in \Lambda$ tel que $\lambda^{-1} \cdot H_y \cdot \lambda = H_x$. Étant donné que la conjugaison conserve l'ordre des éléments et la propriété 4.1, tout ce qui a été décrit précédemment pour le point x est vrai pour y aussi.

Prenons donc $y = 4e_i + 4e_j$ (pour faciliter les calculs) et trouvons les orbites de N_y sur $\Lambda_2(y)$:

$$\begin{aligned}
\overline{\Lambda}_2^4 &:= \{\pm(4e_i - 4e_j)\} \\
\overline{\overline{\Lambda}}_2^4 &:= \{\pm 4e_k \pm 4e_l || \{k,l,i,j\}| = 4\} \\
\overline{\Lambda}_2^2 &:= \{\varepsilon_T(2e_K) | \{i,j\} \cap K = \emptyset, T \in \mathscr{C}\} \\
\overline{\overline{\Lambda}}_2^2 &:= \{\varepsilon_T(2e_K) | \{i,j\} \subset K, T \in \mathscr{C}, |\{i,j\} \cap T| = 1\} \\
\overline{\Lambda}_2^3 &:= \{\varepsilon_T(e_\Omega - 4e_z) | z \in \Omega \backslash \{i,j\}, |\{i,j\} \cap T| = 1, T \in \mathscr{C}\}
\end{aligned}$$

Soit X une orbite de H_y sur $\Lambda_2(y)$. Étant donné que $N_y < H_y$, X est une union de ces dernières orbites. La cardinalité de X est donc une somme de la cardinalité des orbites qui le constituent.

Calculons, à l'aide des triangles des octades et des dodécades, la cardinalité des orbites de N_y sur $\Lambda_2(y)$:

- $|\overline{\Lambda}_2^4| = 2$
- $|\overline{\overline{\Lambda}}_2^4| = \binom{22}{2} \cdot 2 = 2^2 \cdot 3 \cdot 7 \cdot 11$
- $|\overline{\Lambda}_2^2|$ = (nombre d'octades qui n'intersectent pas $\{i,j\}$) $\cdot$ (toutes les façons d'avoir un nombre pair de $'-2'$) $= 330 \cdot 2^7 = 2^8 \cdot 3 \cdot 5 \cdot 11$
- $|\overline{\overline{\Lambda}}_2^2|$ = (nombre d'octades contenant $\{i,j\}$) $\cdot$ (toutes les façons d'avoir un nombre pair de $'-2'$ et un seul $'-2'$ en position i ou j) $= 77 \cdot 2 \cdot 2^5 = 2^6 \cdot 7 \cdot 11$
- $|\overline{\Lambda}_2^3|$ =(nombre de $\mathscr{C}$-ensemble qui intersectent $\{i,j\}$ en un seul point)$\cdot$(les positions possibles du ± 3, c'est-à-dire n'importe quelle position sauf i et j) = 2(nombre d'octades qui intersectent $\{i,j\}$ en i + nombre de dodécades qui intersectent $\{i,j\}$ en i + nombre d'hexadécades qui intersectent $\{i,j\}$ en i)$\cdot(|\Omega \backslash \{i,j\}|) = 2(176+672+176) \cdot 22 = 2^{12} \cdot 11$

Comme $|X|$ doit être divisible par 23, regardons chacun des nombres qui viennent d'être calculé modulo 23.

$$\begin{aligned}
|\overline{\Lambda}_2^4| &= 2 \equiv 2 \bmod(23) \\
|\overline{\overline{\Lambda}}_2^4| &= 2^2 \cdot 3 \cdot 7 \cdot 11 \equiv 4 \bmod(23) \\
|\overline{\Lambda}_2^2| &= 2^8 \cdot 3 \cdot 5 \cdot 11 \equiv 12 \bmod(23) \\
|\overline{\overline{\Lambda}}_2^2| &= 2^6 \cdot 7 \cdot 11 \equiv 6 \bmod(23) \\
|\overline{\Lambda}_2^3| &= 2^{12} \cdot 11 \equiv 22 \bmod(23)
\end{aligned}$$

Le seul moyen d'additionner ces nombres pour obtenir 0 modulo 23 est de tous les additionner, c'est-à-dire que $X = \Lambda_2(y)$, d'où la conclusion. □

Lemme 4.14. *Soient les vecteurs $x = 4e_i + 4e_j$ et $y = 4e_i - 4e_j$, alors*

$$N_{x,y} = E_{x,y} \cdot Stab_{M_{24}}(x,y)$$

et $N_{x,y}$ est de cardinalité

$$2^{10} \cdot |Stab_{M_{24}}(x,y)| = 2^{10} \cdot |M_{24}|/(24 \cdot 23).$$

PREUVE. Soit $\lambda = \varepsilon_T \cdot m_\pi \in N_{x,y}$. Pour que λ fixe x et y, il faut d'abord que $i, j \notin T$. De plus, pour que m_π fixe x, π doit soit contenir le deux-cycle (i, j) ou soit fixer i et j. Mais, dans le premier cas, m_π ne fixe pas y, d'où π doit fixer i et j. Alors

$$N_{x,y} = E_{x,y} \cdot Stab_{M_{24}}(x,y).$$

Trouvons la cardinalité de $E_{x,y}$ et de $Stab_{M_{24}}(x,y)$.

La cardinalité de $E_{x,y}$ correspond au nombre de $\mathscr{C}$-ensembles ne contenant pas les points i et j. À l'aide du triangle des octades et des dodécades, on trouve

$$|E_{x,y}| = 1 + 330 + 616 + 77 = 1024 = 2^{10}.$$

La 5-transitivité de M_{24}, nous donne l'équation suivante

$$|M_{24}| = |\Omega| \cdot |Stab_{M_{24}}(x)| = |\Omega| \cdot |\Omega \setminus \{x\}| \cdot |Stab_{M_{24}}(x,y)| = 24 \cdot 23 \cdot |Stab_{M_{24}}(x,y)|$$

et donc $|Stab_{M_{24}}(x,y)| = |M_{24}|/(24 \cdot 23)$. □

Théorème 4.15. *N est un sous-groupe maximal de $\cdot 0$ et*

$$ord(\cdot 0) = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23.$$

PREUVE. On a vu à la Section §4 du Chapitre 3 que $|\Lambda_2| = 196\,560$ et en additionnant les orbites dans la preuve du Théorème 4.13, on trouve $\forall_{x \in \Lambda_2} \ |\Lambda_2(x)| = 93\,150$. Prenons $x = 4e_i + 4e_j$. L'orbite de H sur ce point est, d'après le Théorème 4.12, Λ_2 et ainsi

$$|H| = |Orb_H(x)| \cdot |H_x| = |\Lambda_2| \cdot |H_x| = 196\,560 \cdot |H_x|.$$

On fait maintenant agir H_x sur $\Lambda_2(x)$. On prend $y = 4e_i - 4e_j \in \Lambda_2(x)$ et grâce au Théorème 4.13, on trouve :

$$|H_x| = |Orb_{H_x}(y)| \cdot |H_{x,y}| = |\Lambda_2(x)| \cdot |H_{x,y}| = 93\,150 \cdot |H_{x,y}|.$$

Enfin, on remarque que $H_{x,y} = N_{x,y}$, car si λ fixe x et y, alors il fixe e_i et, par le Théorème 4.7, $\lambda \in N_{x,y}$. Or d'après le Lemme 4.14, $|N_{x,y}| = 2^{10} \cdot |M_{24}|/(24 \cdot 23)$. On obtient donc

$$|H| = 196\,560 \cdot 93\,150 \cdot 2^{10} \cdot |M_{24}|/(24 \cdot 23) = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$$

pour chaque H qui satisfait $N \lneqq H < \cdot 0$. Le sous-groupe H doit donc être égal à $\cdot 0$. □

La seule information de ce chapitre qui sera nécessaire pour le prochain chapitre est la cardinalité de $\cdot 0$ que l'on vient de calculer.

Chapitre 5

GROUPES DE CONWAY

§1. INTRODUCTION

Ce chapitre est l'aboutissement de cet ouvrage. On y définit les groupes de Conway et on démontre leur simplicité.

§2. DÉFINITIONS ET CARDINALITÉS DES GROUPES DE CONWAY

On définit les groupes de Conway comme étant :

$$\cdot 1 := \cdot 0 / < -1 >,$$
$$\cdot 2 := \cdot 1_v \text{ où } v \in \Lambda_2 \text{ et}$$
$$\cdot 3 := \cdot 1_w \text{ où } w \in \Lambda_3.$$

C'est ici que la cardinalité de $\cdot 0$ prend toute son importance. On l'utilise pour calculer la cardinalité de $\cdot 2$ et $\cdot 3$. En effet, on montre préalablement que ces groupes agissent, respectivement, de façon transitive sur Λ_2 et Λ_3 et ainsi

$$|\cdot 0| = |\Lambda_2| \cdot |\cdot 2| \quad \text{et} \quad |\cdot 0| = |\Lambda_3| \cdot |\cdot 3|.$$

Lemme 5.1. $\cdot 0$ *agit transitivement sur* Λ_2 *et* Λ_3.

PREUVE. ($\cdot 0$ agit transitivement sur Λ_2) Le théorème 4.12 donne la conclusion.

($\cdot 0$ agit transitivement sur Λ_3) On remarque, d'abord, que Λ_3^5 et Λ_3^3 sont deux orbites disjointes lorsque N agit sur Λ_3.

Or, lorsque $\cdot 0$ agit sur Λ_3, l'orbite qui contient Λ_3^5 contient également Λ_3^3 (voir Section §4 du Chapitre 3). En effet, il suffit de prendre l'élément $\zeta_T \in \cdot 0$ (voir preuve du Théorème

4.11) avec T qui correspond au quatre premières coordonnées de $w = (5,1,\ldots,1)$, c'est-à-dire $T = \{\infty,0,1,2\}$, pour se rendre compte que

$$\zeta_T(w) = (1,-3,-3,-3,-1,\ldots,-1) \in \Lambda_3^3.$$

Donc, tous les vecteurs à coordonnées impaires de Λ_3 ($\Lambda_3^3 \cup \Lambda_3^5$) se retrouvent dans la même orbite sur $\cdot 0$.

Soit, maintenant, $y \in \Lambda_3^2 \cup \Lambda_3^4$ et soit $T \in \Omega_4$, formé de la position des coordonnées ± 2, ± 2, ± 2 et 0. Alors $\zeta_T(y)$ est à coordonnées impaires et donc $\cdot 0$ agit sur Λ_3 avec une seule orbite. □

Remarque 5.2. *Grâce à ce lemme, les groupes $\cdot 2$ et $\cdot 3$ sont bien définis.*

Corollaire 5.3.

$$|\cdot 1| = |\cdot 0|/2 = 2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$$
$$|\cdot 2| = 2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$$
$$|\cdot 3| = 2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$$

PREUVE. De la façon dont $\cdot 1$ a été défini, il est clair que $|\cdot 1| = |\cdot 0|/2$. En utilisant le dernier lemme, on trouve que :

$$|\cdot 2| = |\cdot 0|/|\Lambda_2|$$
$$|\cdot 3| = |\cdot 0|/|\Lambda_3|$$

Or, dans le chapitre sur le réseau de Leech, on avait trouvé que

$$|\Lambda_2| = 196\,560 = 2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$$
$$|\Lambda_3| = 16\,773\,120 = 2^{12} \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$$

Pour terminer la preuve, il suffit de déterminer la cardinalité de $\cdot 0$, ce qui a été fait au Théorème 4.15. □

§3. $\cdot 1$ EST SIMPLE

Pour démontrer la simplicité de $\cdot 1$, on aura besoin de la cardinalité de $\cdot 0$ ainsi que les résultats qui suivent.

Lemme 5.4. *Soient α, β les éléments définis dans le Chapitre 2. Alors*

$$C_{\cdot 0}(m_\alpha) = < -1 > \cdot < m_\alpha > \text{ et } N_{\cdot 0}(< m_\alpha >) = < -1 > \cdot < m_\alpha, m_\beta >,$$

où $C_{\cdot 0}(m_\alpha)$ est le centralisateur de m_α dans $\cdot 0$ et $N_{\cdot 0}(< m_\alpha >)$ le normalisateur de $< m_\alpha >$ dans $\cdot 0$.

PREUVE. – ($C_{\cdot 0}(m_\alpha) \subseteq < -1 > \cdot < m_\alpha >$) Montrons que si $\lambda \in C_{\cdot 0}(m_\alpha)$ alors $\lambda \in N$.

Grâce au Théorème 4.7, il est suffisant de montrer qu'il existe i et j tels que $\lambda(e_i) = \pm e_j$. Pour ce faire nous allons montrer que $\lambda(e_\infty) = \pm e_\infty$.

Supposons que $\lambda(e_\infty) = v = (v_\infty, v_0, \ldots, v_{22})$. On doit avoir $\lambda \cdot m_\alpha = m_\alpha \cdot \lambda$ et en particulier :

$$(v_\infty, v_1, \ldots, v_{22}, v_0) = m_\alpha(v) = m_\alpha(\lambda(e_\infty)) = \lambda(m_\alpha(e_\infty)) = \lambda(e_\infty) = v.$$

Donc, $v = (a, b, b, \ldots, b)$ où $a = v_\infty$ et $b = v_0 = v_1 = \cdots = v_{22}$. On sait, par définition, que $\cdot 0 < \mathrm{O}_{24}(\mathbb{Q})$, d'où

$$1 = ||e_\infty||^2 = ||\lambda(e_\infty)||^2 = ||v||^2 = a^2 + 23b^2.$$

Cette dernière équation n'a que $(a, b) = (\pm 1, 0)$ comme solution rationnelle. Or, $\lambda \in \mathrm{O}_{24}(\mathbb{Q})$, d'où $\lambda(e_\infty) = v \in \mathbb{Q}^\Omega$ et ainsi $v = \pm e_\infty$.

Donc, $\lambda = \varepsilon_T \cdot m_\pi$ pour $T \in \mathscr{C}$ et $\pi \in M_{24}$. Montrons qu'alors $T = \emptyset$ ou $T = \Omega$ et que $\pi = \alpha^i$ pour un certain i dans $\{0, 1, 2, \ldots, 22\}$. Il y a deux possibilités à considérer : $\lambda(e_0) = +e_i$ ou $\lambda(e_0) = -e_i$.

– Si $\lambda(e_0) = e_i$, alors

$$\lambda(e_1) = \lambda(m_\alpha(e_0)) = m_\alpha(\lambda(e_0)) = m_\alpha(e_i) = e_{i+1}$$

et, similairement, on peut montrer que pour tout $j \neq \infty$, $\lambda(e_j) = e_{i+j \bmod (23)}$. De plus, on doit avoir

$$\lambda(e_{\Omega\setminus\{\infty\}} - 3e_\infty) = \lambda(e_{\Omega\setminus\{\infty\}}) - 3\lambda(e_\infty) = e_{\Omega\setminus\{\infty\}} - 3 \cdot \pm e_\infty \in \Lambda_2$$

car $\lambda \in \cdot 0$ et $e_{\Omega\setminus\{\infty\}} - 3e_\infty = e_\Omega - 4e_\infty \in \Lambda_2^3$. Or, la seule possibilité est que $\lambda(e_\infty) = e_\infty$ et alors $T = \emptyset$ ce qui revient à dire que $\varepsilon_T = id$.

– Si $\lambda(e_0) = -e_i$ alors on obtient $T = \Omega$ et $\varepsilon_T = -id$.

On sait maintenant que $\lambda = m_\pi$ ou $\lambda = -m_\pi$. Enfin, les seuls éléments de S_Ω qui commutent avec α sont les puissances de α, d'où la conclusion.

– $(N_{.0}(< m_\alpha >) =< -1 > \cdot < m_\alpha, m_\beta >)$ Comme au cas précédent, on obtient que, si $\lambda \in N_{.0}(< m_\alpha >)$, alors $\lambda \in N$. On peut également montrer qu'il existe $\pi \in M_{24}$ tel que $\lambda = m_\pi$ ou $\lambda = -m_\pi$.

Pour terminer la preuve, il reste à montrer que $m_\pi \in < m_\alpha, m_\beta >$. Ceci revient à démontrer que

$$N_{M_{24}}(< \alpha >) =< \alpha, \beta > .$$

– $(\supseteq)$ Il suffit de se rendre compte que

$$\beta \cdot \alpha \cdot \beta^{-1} = \alpha^2$$

pour avoir l'inclusion.

– $(\subseteq)$ Soit $\lambda \in N_{M_{24}}(< \alpha >)$. On doit avoir $\lambda \cdot \alpha \cdot \lambda^{-1} \in < \alpha >$, c'est-à-dire

$$\lambda \cdot \alpha = \alpha^k \cdot \lambda$$

pour $k \in \{1, \ldots, 22\}$.

Si $\lambda(\infty) = i \neq \infty$ alors

$$i = \lambda(\infty) = \lambda \cdot \alpha(\infty) = \alpha^k \cdot \lambda(\infty) = \alpha^k(i) = (i+k) \bmod(23)$$

qui n'est vraie que si $k = 0$, d'où une contradiction. Donc $\lambda(\infty) = \infty$. Si $\lambda(0) = j$, alors la transformation $\eta := \alpha^{-j} \cdot \lambda$ est dans $N_{M_{24}}(< \alpha >)$. Elle fixe ∞ et envoie 0 sur 0.

Si $\eta \cdot \alpha = \alpha^l \cdot \eta$ pour $l \in \{1, \ldots, 22\}$ alors

$$\begin{aligned}
&\eta(1) = \eta \cdot \alpha(0) = \alpha^{1 \cdot l} \cdot \eta(0) = \alpha^{1 \cdot l}(0) = l \bmod(23) \\
&\eta(2) = \eta \cdot \alpha^2(0) = \alpha^{2 \cdot l} \cdot \eta(0) = \alpha^{2 \cdot l}(0) = 2 \cdot l \bmod(23) \\
&\vdots \\
&\eta(h) = \eta \cdot \alpha^h(0) = \alpha^{h \cdot l} \cdot \eta(0) = \alpha^{h \cdot l}(0) = h \cdot l \bmod(23)
\end{aligned}$$

– Si $l = 2^n \bmod(23)$, alors $\eta = \beta^n$ et

$$\lambda = \alpha^j \cdot \beta^n \in < \alpha, \beta > .$$

– Si l n'est pas une puissance de 2 modulo 23, alors on peut trouver m tel que $l = 5 \cdot 2^m$. L'élément $\beta^{-m} \cdot \eta \in N_{M_{24}}(< \alpha >)$ et $\beta^{-m} \cdot \eta(1) = 5$, d'où

$$\beta^{-m} \cdot \eta = (0,5,10,15,20,2,7,12,17,22,4,9,14,19,1,6,11,16,21,3,8,13,18) = \alpha^{14}$$

et ainsi $\lambda = \alpha^j \cdot \beta^m \cdot \alpha^{14} \in < \alpha, \beta >$.

□

Lemme 5.5 (Argument de Frattini)**.** *Soit G, un groupe fini, et soit H, un sous-groupe normal de celui-ci. Pour tout Sylow sous-groupe P de H on a*

$$G = H \cdot N_G(P).$$

De plus, si p est un diviseur premier de $|G|$, alors p divise $|H|$ ou $|N_G(P)|$.

PREUVE. Soit $g \in G$, comme $H \lhd G$, on a $gPg^{-1} \subset H$ et puisque gPg^{-1} a la même cardinalité que P, $gPg^{-1} \in Syl(H)$. Donc, par le Théorème de Sylow, il existe $h \in H$ tel que $gPg^{-1} = hPh^{-1}$, d'où $(h^{-1}g)P(h^{-1}g)^{-1} = P$. Autrement dit $h^{-1}g \in N_G(P)$ et, ainsi, il suffit de prendre $g = h(h^{-1}g)$ comme décomposition.

Supposons que $p \not| O(H)$, alors $p|[G : H]$. Par le Deuxième Théorème d'Isomorphie

$$G/H = (H \cdot N_G(P))/H \simeq N_G(P)/(H \cap N_G(P)),$$

d'où $p \mid O(N_G(P)/H \cap N_G(P)) \mid O(N_G(P))$. □

Lemme 5.6. $|SL_2(23)| = \dfrac{(23^2-1)\cdot(23^2-23)}{22} = 2^4 \cdot 3 \cdot 11 \cdot 23.$

PREUVE. On sait que la cardinalité de $GL_2(23)$ est $(23^2-1)\cdot(23^2-23)$. Pour avoir la conclusion, il suffit de remarquer que les ensembles

$$\{A \in GL_2(23) | \det(A) = k\}$$

sont tous en bijections. □

Proposition 5.7. *Le groupe $PSL_2(23)$ est simple.*

PREUVE. Soit $\left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle < H \lhd SL_2(23)$. Montrons qu'alors $H = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$ ou $H = SL_2(23)$.

– Si 23 divise $|H|$, alors il existe un 23-Sylow sous-groupe P de H. D'après la cardinalité de $SL_2(23)$ (voir lemme précédent), P est également un 23-Sylow sous-groupe de $SL_2(23)$. L'élément $\alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ de $SL_2(23)$ est d'ordre 23 et donc $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$ est un 23-Sylow sous-groupe de $SL_2(23)$. Par le Théorème de Sylow, il existe $g \in SL_2(23)$

tel que $g \cdot P \cdot g^{-1} = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$. La normalité de H implique que $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle < H$ et que l'élément

$$\gamma \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \gamma^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

est dans H. Mais alors H doit contenir toutes les matrices de la forme

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$$

d'où $H = SL_2(23)$ (voir Proposition 2.2).

– Si 23 ne divise pas $|H|$, soit p un diviseur premier de H et P un p-Sylow sous-groupe de H. Alors, d'après l'argument de Frattini, $23||N_{SL_2(23)}(P)|$. Soit B un élément d'ordre 23 dans $N_{SL_2(23)}(P)$. Il découle du Lemme 5.4 que

$$C_{SL_2(23)}(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}) = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \cdot \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Par le Théorème de Sylow, il existe $g \in SL_2(23)$ tel que

$$< B >= g \cdot \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \cdot g^{-1}$$

d'où

$$B = g \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^i \cdot g^{-1} \text{ pour un certain } i \in \{1, 2, \ldots, 22\}$$

Avec ceci, on obtient

$$\begin{aligned} C_{SL_2(23)}(B) &= g \cdot C_{SL_2(23)}(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}) \cdot g^{-1} \\ &= \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \cdot \left\langle g \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot g^{-1} \right\rangle \\ &= \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \cdot < B > \end{aligned}$$

i) Si $p \neq 2$, alors le seul élément de P qui est dans $C_{SL_2(23)}(B)$ est l'identité. En effet, d'après ce qui précède $|C_{SL_2(23)}(B)| = 2 \cdot 23$. Or $|P|$ n'est ni divisible par 2, ni divisible par 23. Le sous-groupe $< B >$ agit donc par conjugaison sur P avec des orbites de longueur 23, sauf l'orbite de l'identité qui, elle, contient 1 élément. Grâce à ceci, on obtient la condition suivante sur $|P|$:

$$|P| \equiv 1 \; mod(23).$$

En regardant la cardinalité de $SL_2(23)$, on s'aperçoit que cette équation n'est jamais satisfaite.

ii) Si $p = 2$, alors on peut supposer que $P = H$. En effet, dès qu'un nombre premier différent de 2 divise l'ordre de H, on retombe dans le cas i). Comme $P = H$, $C_{SL_2(23)}(B)$ contient maintenant deux éléments de P : l'identité et l'inverse additif de l'identité. On obtient alors la condition suivante sur $|P|$ $(= |H|)$:

$$|H| = |P| \equiv 2 \; mod(23),$$

qui n'a que $|H| = 2$ comme seule solution. C'est-à-dire

$$H = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle.$$

□

Proposition 5.8. *Le groupe* $\cdot 1$ *est simple.*

PREUVE. Soit $H \triangleleft \cdot 0$ tel que $< -1 > \subset H$. Nous allons montrer qu'alors $H =< -1 >$ ou $H = \cdot 0$. Pour ce faire, on va séparer la preuve en deux parties.

a) (Si 23 divise $|H|$.) Alors H contient un 23-Sylow sous-groupe P. Comme $|\cdot 0|$ n'est pas divisible par 23^2, $P \in Syl_{23}(\cdot 0)$ et, donc, il existe $g \in G$ tel que $gPg^{-1} =< m_\alpha >$. Par la normalité de H, on obtient $< m_\alpha >< H$ et alors $< m_\alpha > \in Syl_{23}(H)$. En utilisant le Lemme 5.5, on trouve

$$\cdot 0 = H \cdot N_{\cdot 0}(< m_\alpha >).$$

D'après le Lemme 5.4 et le fait que $\alpha, \beta \in PSL_2(23)$, on a

$$N_{\cdot 0}(< m_\alpha >) =< -1 > \cdot < m_\alpha, m_\beta >< < -1, PSL_2(23) >$$

Considérons le sous-groupe suivant de $PSL_2(23)$:

$$L =< g m_\alpha g^{-1} | g \in PSL_2(23) >$$

Ce sous-groupe, non trivial, est normal dans $PSL_2(23)$ et est donc égal à celui-ci, d'après le Lemme 5.7. Or, puisque $m_\alpha \in H$ et $H \triangleleft \cdot 0$, H contient tout les conjugués de m_α et donc

$$PSL_2(23) = L \subset H.$$

Enfin, comme $-1 \in H$, on trouve

$$N_{\cdot 0}(< m_\alpha >) \subset < -1, PSL_2(23) > \subset H$$

d'où $\cdot 0 = H \cdot N_{\cdot 0}(< \alpha >) = H$.

b) (Si 23 ne divise pas $|H|$.) Soit p un nombre premier qui divise l'ordre de H et soit $P \in Syl_p(H)$. Alors, par le Lemme 5.5, 23 divise l'ordre de $N_{\cdot 0}(P)$ et donc $N.0(P)$ contient un élément m' d'ordre 23. En utilisant le Lemme 5.4 et le fait que $< m' >$ est conjugué à $< m_\alpha >$ (car ce sont deux 23 Sylow sous-groupes), on trouve :

$$< m' >= h < m_\alpha > h^{-1} \Rightarrow m' = h \cdot m_\alpha^i \cdot h^{-1},\ i \neq 0$$

et alors

$$\begin{aligned} C_{\cdot 0}(m') &= h \cdot C_{\cdot 0}(m_{\alpha^i}) \cdot h^{-1} \\ &= h \cdot C_{\cdot 0}(m_\alpha) \cdot h^{-1},\ \text{car } C_{\cdot 0}(m_\alpha) = C_{\cdot 0}(m_\alpha^i) \text{ pour } i \neq 0 \\ &= h(< -1 > \cdot < m_\alpha >) h^{-1} \\ &= < -1 > \cdot < m' > . \end{aligned}$$

i) (Si $p \neq 2$) On remarque, d'abord, que l'ordre de $C_{\cdot 0}(m')$ est $2 \cdot 23$ et par conséquent tous les éléments de P, autre que l'identité, ne peuvent être dans $C_{\cdot 0}(m')$. Il découle de ceci, et du fait que $m' \in N_{\cdot 0}(P)$ que le groupe $< m' >$ agit par conjugaison sur P avec des orbites possédant 23 éléments excepté l'orbite contenant l'identité P. Pour que cette dernière propriété soit vraie, P doit satisfaire

$$|P| \equiv 1 \mod(23).$$

ce qui est impossible, étant donné la cardinalité de $\cdot 0$.

ii) (Si $p = 2$) Dès qu'un nombre premier différent de 2 divise l'ordre de H on se retrouve dans le cas précédent. Alors ici on suppose que le seul nombre premier qui divise l'ordre de H est 2, auquel cas $P = H$. En répétant le raisonnement du cas i), on se rend compte que $< m' >$ agit cette fois-ci sur P $(= H)$ avec deux points fixes : 1 et -1 ($-1 \in H$ par définition). D'où

$$|P| \equiv 2 \mod(23)$$

qui laissent $|H| = 2$ ou $|H| = 2^{12}$ comme seules possibilités.

Supposons que $|H| = 2^{12}$. Regardons le sous-groupe

$$C_{\cdot 0}(H) := \{g \in \cdot 0 | \forall_{h \in H}\, gh = hg\}.$$

Si $C_{\cdot 0}(H) = \cdot 0$ alors $H < C_{\cdot 0}(m')$ ce qui est impossible puisque 2^{12} ne divise pas $2 \cdot 23$. On remarque de plus que $C_{\cdot 0}(H)$ est un sous-groupe normal de $\cdot 0$ qui contient -1. En appliquant i) et ii) sur ce celui-ci, on conclut qu'il est de cardinalité 2^n.

Montrons maintenant que ceci est impossible. Soit ρ un élément d'ordre 13 dans $\cdot 0$. Posons $|C_H(\rho)| = 2^a$ comme $-1 \in H$, $1 \leqslant a \leqslant 12$. La normalité de H dans $\cdot 0$ implique que le sous-groupe $< \rho >$ agit sur H par conjugaison avec des orbites de longueur 13, en laissant exactement 2^a points fixes. En équation ceci nous donne :

$$2^{12} = |H| \equiv 2^a \bmod(13)$$

qui n'a comme solution que $a = 12$ ou 0. Cette dernière solution est à rejeter car $-1 \in H$. Donc $a = 12$ et $C_H(\rho) = H$ d'où $\rho \in C_{\cdot 0}(H)$ ce qui contredit le fait que $C_{\cdot 0}(H)$ est un groupe de cardinalité 2^n.

$|H| = 2$ et alors $H =< -1 >$.

□

§4. $\cdot 2$ ET $\cdot 3$ SONT SIMPLES

Étant donné que l'ordre des groupes $\cdot 2$ et $\cdot 3$ est plus petit que l'ordre de $\cdot 1$, la preuve de leur simplicité s'avère plus simple. L'idée demeure la même que celle employée pour la simplicité de $\cdot 1$ et de $PSL_2(23)$.

Lemme 5.9. *Soit p un nombre premier et G un groupe abélien de cardinalité p^n. Si l'exposant du groupe est p, alors*

$$G \simeq \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p = \mathbb{Z}_p^n$$

et G peut être vu comme un espace vectoriel sur $\mathbb{Z}_p$ de dimension n. De plus, les homomorphismes de G sont isomorphes avec les applications linéaires de G. En particulier, $Aut(G) \simeq Aut_{\mathbb{F}_p}(G) \simeq GL_n(p)$.

PREUVE. Soient $x_1, x_2, \ldots, x_n$ des éléments d'ordres p dans G tels que $x_i \notin < x_1, x_2, \ldots, x_{i-1} >$. La commutativité de G implique que pour chaque i, $< x_i > \triangleleft G$. Il est immédiat que pour

$i \neq j$, $< x_i > \cap < x_j >= \{1\}$. Enfin le sous-groupe $< x_1, x_2, \ldots, x_n >$ est d'ordre p^n et est donc égale à G. Mais $< x_1, x_2, \ldots, x_n >=< x_1 > \cdot < x_2 > \cdot \ldots \cdot < x_n >$ et ainsi

$$G \simeq \mathbb{Z}_p^n.$$

Le reste du théorème découle directement des définitions. □

Proposition 5.10. *Les groupes $\cdot 2$ et $\cdot 3$ sont simples.*

PREUVE. Posons $G = \cdot 2$ ou $\cdot 3$. On sait du Chapitre 2 que

$$< \alpha, \beta >< PSL_2(23) < G.$$

L'élément -1 de $\cdot 0$ ne fixe aucun élément de Λ_2 et de Λ_3 d'où -1 $\notin G$ et

$$N_G< m_\alpha >=< m_\alpha, m_\beta > .$$

Soit H un sous-groupe normal de G. Encore une fois, nous allons séparer la preuve en deux parties.

- (Si 23 divise $|H|$) Il suffit de refaire le cas a) de la preuve du Théorème 5.8 pour trouver $H = G$.
- (Si 23 ne divise pas $|H|$) Soit p un diviseur premier de $|H|$ et soit $P \in Syl_p(H)$. On applique le cas b) de la preuve du Théorème 5.8 mais cette fois comme $-1 \notin H$, on a

  $$|P| \equiv 1 \bmod(23)$$

  pour les deux cas $p \neq 2$ et $p = 2$.
  - (Si $G = \cdot 2$) La seule possibilité qui satisfait cette égalité est $|H| = 2^{11}$.

    Regardons le sous-groupe $C_{\cdot 2}(H)$. Tout d'abord, on a $C_{\cdot 2}(H) \neq \cdot 2$ et $C_{\cdot 2}(H) \triangleleft \cdot 2$ comme dans la preuve du Théorème 5.8. Les seules possibilités qui restent pour $|C_{\cdot 2}(H)|$ et pour $|C_{\cdot 2}(H) \cap H|$ sont 1 et 2^{11}. Or, le centre d'un p-groupe est non trivial (il suffit de faire agir H sur lui-même par conjugaison et d'utiliser l'équation des classes), d'où $|C_{\cdot 2}(H)| = 2^{11}$ et $|C_{\cdot 2}(H) \cap H| = 2^{11}$. C'est donc dire que $C_{\cdot 2}(H) = H$ et que H est abélien.

    Montrons que tous les éléments de H sont d'ordre deux. Par le Théorème de Cauchy, H contient un élément $\hat{h}$ d'ordre deux. Considérons le sous-groupe

    $$K =< g \cdot \hat{h} \cdot g^{-1} | g \in \cdot 2 > .$$

K est non trivial, est un sous-groupe de H et est un sous-groupe normal de $\cdot 2$. La cardinalité de K est alors 2^{11} et ceci implique $K = H$. Or tous les générateurs de K sont d'ordres deux et commutent entre eux d'où chaque élément de $K = H$ est d'ordre deux. D'après le Lemme 5.9, on a donc $\mathrm{Aut}(H) \simeq \mathrm{GL}_2(11)$. On peut faire agir $\cdot 2$ sur H par conjugaison (car $H \triangleleft \cdot 2$) et on obtient, par le Premier Théorème d'isomorphie :

$$\begin{array}{ccc} \cdot 2 & \xrightarrow{\quad\varphi\quad} & \mathrm{Aut}(H) \simeq \mathrm{GL}_2(11) \\ & \searrow \quad \nearrow & \\ & \cdot 2/ker(\varphi) \simeq \cdot 2/H & \end{array}$$

Ce qui donne comme conclusion que $\cdot 2/H$ peut être vu comme un sous-groupe de $\mathrm{GL}_2(11)$. Or

$$|\cdot 2/H| = 2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$$
$$|\mathrm{GL}_2(11)| = 2^{55} \cdot 3^6 \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 17 \cdot 23 \cdot 31^2 \cdot 73 \cdot 89 \cdot 127$$

et ceci est impossible car 5^3 divise l'ordre de $\cdot 2/H$ et ne divise pas l'ordre de $\mathrm{GL}_2(11)$.

– (Si $G = \cdot 3$) La cardinalité de $\cdot 3$ suffit pour montrer qu'il n'existe pas de tel P.

□

On sait donc maintenant que les groupes $\cdot 1$, $\cdot 2$ et $\cdot 3$ sont simples. Pour démontrer leur sporadicité, il resterait à démontrer que ces groupes ne peuvent faire parti d'aucune famille infinie de groupes simples (voir Annexe B). Pour réussir à démontrer ceci, il est suffisant de regarder l'ordre des groupes de Conway et de démontrer qu'il ne correspond à l'ordre d'aucun des groupes faisant parti des familles infinies.

Par exemple, les groupes de Conway ne peuvent être des groupes de type $G_2(q)$. Un groupe de ce type est de cardinalité

$$q^6 \cdot (q^6 - 1) \cdot (q^2 - 1)$$

où $q = p^n$, p est premier. Supposons que la cardinalité d'un des groupes de Conway, appelons le G, est égale à $p^{6n} \cdot (p^{6n} - 1) \cdot (p^{2n} - 1)$. Le nombre premier p doit alors se retrouver au moins 6 fois dans la décomposition en nombre premier de l'ordre de G. Ceci ne laisse que

$q = 2, 2^2, 2^3$ ou 3 comme possibilités. Si $q = 2, 2^2$ ou 3, alors

$$|G| > q^6 \cdot (q^6 - 1) \cdot (q^2 - 1)$$

d'où on peut rejeter ces possibilités. Si $q = 2^3$ alors G ne peut être égal à $\cdot 3$, car $\cdot 3$ n'est pas divisible par 2^{18}. On a alors

$$|G| > q^6 \cdot (q^6 - 1) \cdot (q^2 - 1)$$

si $G \neq \cdot 3$. Donc les groupes de Conway ne font pas partis de la famille $G_2(q)$.

La procédure est semblable pour les autres familles.

CONCLUSION

Il est intéressant de constater que les Chapitres 1 à 4 ont comme but principal le calcul de l'ordre de $\cdot 0$. Avec cette donnée, on trouve la cardinalité des trois groupes de Conway. La simplicité de ceux-ci découle de leur cardinalité et du Lemme 5.4, une propriété propre au groupe $\cdot 0$.

Lorsque John Conway, en 1967, travailla sur le groupe de symétrie du réseau de Leech, il recourra à l'aide de John Thompson. L'anecdote suivante traduit bien le fait que la cardinalité est une information essentielle.

> Conway appella Thompson et lui donna la cardinalité de $\cdot 0$. Quelques minutes plus tard, Thompson rappela Conway en affirmant que $\cdot 0$ contenait trois groupes simples. On blaguait à ce sujet en disant que si vous aviez un entier, il suffisait d'appeler Thompson pour savoir s'il y avait un groupe simple de cet ordre.[1]

Ce mémoire est donc un bel exemple qu'une des richesses de la théorie des groupes est le lien qui existe entre celle-ci et l'arithmétique.

[1] Voir [**Thompson**] pour plus de détails.

Annexe A

INDEX DES NOTATIONS

On retrouve dans cet index les pages où chaque symbole a été défini.

Annexe B

LISTE DES GROUPES SIMPLES FINIS

GROUPES ALTERNÉS ET CYCLIQUES

Groupe	Ordre
$\mathbb{Z}_p, p \in \mathbb{P}$	p
$A_n, n \geqslant 5$	$n!/2$

GROUPES DE TYPE DE LIE

Soit q une puissance d'un nombre premier.

Groupe	Ordre
$A_n(q), n \geqslant 1$	$q^{n(n+1)/2} \prod_{i=1}^{n} (q^{i+1} - 1)$
$B_n(q), n \geqslant 2$	$q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1)$
$C_n(q), n \geqslant 3$	$q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1)$
$D_n(q), n \geqslant 4$	$q^{n(n-1)} (q^n - 1) \prod_{i=1}^{n-1} (q^{2i} - 1)$
$G_2(q)$	$q^6(q^6 - 1)(q^2 - 1)$
$F_4(q)$	$q^{24}(q^{12} - 1)(q^8 - 1)(q^6 - 1)(q^2 - 1)$
$E_6(q)$	$q^{36}(q^{12} - 1)(q^9 - 1)(q^8 - 1)(q^6 - 1)(q^5 - 1)(q^2 - 1)$
$E_7(q)$	$q^{63}(q^{18} - 1)(q^{14} - 1)(q^{12} - 1)(q^{10} - 1)(q^8 - 1)(q^6 - 1)(q^2 - 1)$
$E_8(q)$	$q^{120}(q^{30} - 1)(q^{24} - 1)(q^{20} - 1)(q^{18} - 1)(q^{14} - 1)(q^{12} - 1)(q^8 - 1)(q^2 - 1)$

Groupe	Ordre
${}^2A_n(q), n \geqslant 2$	$q^{n(n+1)/2}\prod_{i=1}^{n}(q^{i+1}-(-1)^{i+1})$
${}^2B_2(q), q = 2^{2m+1}$	$q^2(q^2+1)(q-1)$
${}^2D_n(q), n \geqslant 4$	$q^{n(n-1)}(q^n+1)\prod_{i=1}^{n-1}(q^{2i}-1)$
${}^3D_4(q)$	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$
${}^2G_2(q), q = 3^{2m+1}$	$q^3(q^3+1)(q-1)$
${}^2F_4(q), q = 2^{2m+1}$	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$
${}^2E_6(q)$	$q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1)$

GROUPES SPORADIQUES

Groupe	Ordre
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
J_3	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$
J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$
McL	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$
Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 23$
Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$
He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$
Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$
ON	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$

Groupe	Ordre
$\cdot 1$	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
$\cdot 2$	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
$\cdot 3$	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Fi_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 23$
Fi_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
Fi_{24}	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
F_5	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$
F_3	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$
F_2	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$
F_1	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$

Ces tables sont tirées de [**Atlas**].

Annexe C

THÉORÈME SUR LES DIMENSIONS

On donne ici la preuve que pour chaque espace vectoriel E de dimension finie et pour chaque sous-espace F de E

$$\dim E = \dim F + \dim F^{\perp}.$$

où $F^{\perp}$ représente les vecteurs orthogonaux à F par rapport à n'importe quelle forme bilinéaire non dégénérée et symétrique sur E.

Lemme C.1. *Soit E un espace vectoriel de dimension fini sur K et F un sous-espace de E. On définit l'espace dual de E comme étant l'espace*

$$E^* := \{l : E \to K | l \text{ est linéaire}\}$$

et l'annulateur du sous-espace F comme étant l'espace

$$F^{\circ} := \{f \in E^* | \forall_{v \in F}\ f(v) = 0\}.$$

Alors

$$\dim E = \dim F + \dim F^{\circ}$$

PREUVE. Soit $\{b_1, \ldots, b_r, \ldots, b_n\}$ une base de E telle que $\{b_1, \ldots, b_r\}$ soit une base de F. Considérons maintenant la base $\{f_1, \ldots, f_n\}$ de E^* définie par $\forall_{i,j}\ f_i(b_j) = \delta_{ij}$. Montrons que $\{f_{r+1}, \ldots, f_n\}$ est une base de F°. On remarque d'abord que

$$\forall_{i \geqslant r+1, j \leqslant r}\ f_i(b_j) = \delta_{ij} = 0$$

et donc que $f_{r+1}, \ldots, f_n$ s'annulent sur $\{b_1, \ldots, b_r\}$ donc sur F, c'est-à-dire qu'ils sont dans F°.

On obtient l'indépendance linéaire des éléments $f_{r+1}, \ldots, f_n$ d'après leur construction.

Il reste à montrer que $f_{r+1},\ldots,f_n$ engendrent F°. Soit $f\in F^\circ$, comme $\{f_1,\ldots,f_n\}$ est une base de E^*, on peut trouver $\alpha_1,\alpha_2,\ldots,\alpha_n\in K$ telles que

$$f=\alpha_1 f_1+\ldots+\alpha_n f_n$$

Mais

$$f\in F^\circ \Rightarrow \forall_{i\leqslant r}\ 0=f(b_i)=\alpha_1 f_1(b_i)+\ldots+\alpha_i f_i(b_i)+\ldots+\alpha_n f_n(b_i)=\alpha_i f_i(b_i)=\alpha_i,$$

d'où $\alpha_1=\alpha_2=\ldots=\alpha_r=0$ et, alors, $f=\alpha_{r+1}f_{r+1}+\ldots+\alpha_n f_n$. L'ensemble $\{f_{r+1},\ldots,f_n\}$ engendre donc F° et

$$\dim F^\circ=n-r=\dim E-\dim F$$

□

Théorème C.2. *Soit E un espace vectoriel de dimension finie sur K. Soit φ une forme bilinéaire non dégénérée ($\forall_{x\in E}\ \varphi(x,y)=0\Rightarrow y=0$) et symétrique sur E. On définit pour $A\subset E$*

$$A^\perp:=\{x\in E|\forall_{a\in A}\ \varphi(x,a)=0\}.$$

Il est a noter que $A^\perp$ est toujours un sous-espace de E, même si A n'en est pas un. On a alors pour chaque sous-espace $F\subset E$

$$\forall_{F<E}\ \dim E=\dim F+\dim F^\perp.$$

PREUVE. Regardons l'application linéaire

$$\begin{array}{rccc}\psi: & E & \longrightarrow & E^*\\ & e & \longmapsto & \varphi(\cdot,e)\end{array}$$

En identifiant E^{**} à E de la façon suivante :

$$\begin{array}{rccc}\chi: & E & \longrightarrow & E^{**}\\ & e & \longmapsto & \chi_e\end{array}$$

où

$$\begin{array}{rccc}\chi_e: & E^* & \longrightarrow & K\\ & f & \longmapsto & f(e)\end{array}$$

on a

$$\begin{aligned}(Im(\psi|_F))^\circ &= \{\chi_v \in E^{**} | \forall_{f \in Im(\psi|_F)}\ \chi_v(f) = 0\} \\ &= \{v \in E | \forall_{f \in Im(\psi|_F)}\ f(v) = 0\} \\ &= \{v \in E | \forall_{w \in F}\ \varphi(v,w) = 0\} \\ &= F^\perp\end{aligned}$$

D'après le lemme C.1,

$$\begin{aligned}\dim E &= \dim(Im(\psi|_F))^\circ + \dim(Im(\psi|_F)) \\ &= \dim F^\perp + \dim(Im(\psi|_F))\end{aligned}$$

Or, on a $\dim F = \dim(Im(\psi|_F)) + \dim(ker(\psi|_F))$ et

$$\begin{aligned}ker(\psi|_F) &= \{e \in F | \varphi(\cdot, e) = 0\} \\ &= \{e \in F | \forall_{x \in E}\ \varphi(x,e) = 0\} \\ &= \{0\}, \text{ car } \varphi \text{ est non dégénérée.}\end{aligned}$$

Donc, $\dim F = \dim(Im(\psi|_F))$ et, ainsi, $\dim E = \dim F + \dim F^\perp$.

□

BIBLIOGRAPHIE

[Atlas] J.H. CONWAY, R.T. CURTIS, S.P. PARKER et R.A. WILSON, *Atlas of Finite Groups*, Oxford University Press, 1985.

[Broer] ABRAHAM BROER, *Introduction à la théorie des groupes*, Département de mathématiques et statistique, Université de Montréal, 1998.

[Camero] PETER J. CAMERON, *Finite permutation groups and fi nite simple groups*, Bull. London Math. Soc., 13, 1981, p. 1-22.

[Conway] J.H. CONWAY, *A group of order 8 315 553 613 086 720 000*, Bull. London Math. Soc., 1, 1969, p. 79-88.

[ConSlo] J.H. CONWAY et N.J.A. SLOANE, *Sphere packings, lattices and groups, 3^e édition*, Springer-Verlag, New York, 1999.

[Doyen] J. DOYEN et A. ROSA, *An updated bibliography and survey of Steiner system*, Ann. Discrete Math., 7, 1980, p. 317-349.

[Griess] ROBERT L. GRIESS, JR., *Twelve sporadic groups*, Springer-Verlag, New York, 1998.

[Grifon] JOSEPH GRIFONE, *Algèbre linéaire*, Cépaduès-Éditions, Toulouse, 1994.

[Leech1] JOHN LEECH, *Notes on sphere packings*, Canad. J. Math., 19, 1967, p. 251-267.

[Leech2] JOHN LEECH, *Some sphere packings in higher space*, Canad. J. Math., 16, 1964, p. 657-682.

[Mathieu1] ÉMILE MATHIEU, *Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables*, J. Math. Pures. Appl., Série II numéro 6, 1861, p. 241-274.

[Mathieu2] ÉMILE MATHIEU, *Sur la fonction cinq fois transitive de 24 quantités*, J. Math. Pures. Appl.,Série II numéro 18, 1873, p. 25-46.

[Rotman] JOSEPH J. ROTMAN, *An introduction to the theory of groups*, Springer-Verlag, New York, 1995.

[Suzuki] MICHIO SUZUKI, *Elementary proof of the simplicity of sporadic groups*, Proceedings of the Singapore group theory conference, de Gruyter, Berlin, 1989, p. 195-206.

[Thompson] THOMAS M. THOMPSON, *From error-correcting codes through sphere packings to simple groups*, The Mathematical Association of America, 1983.