JOURNAL OF ALGEBRA 77, 552–576 (1982)

Sur les multiplicateurs de Schur des groupes de Mathieu

PIERRE MAZET

Mathématiques, Université de Paris VI,
4, Place Jussieu, 75230 Paris Cedex 05, France

Communicated by J. Tits

Received October 14, 1980

INTRODUCTION

Le calcul des multiplicateurs de Schur des groupes de Mathieu a été fait par Burgoyne et Fong dans un article au *Nagoya Mathematical Journal* de 1966 [1] rectifié en 1968 [2]. Cependant ce rectificatif comporte encore un résultat erronné en ce qui concerne M_{22}; en outre il fait un large usage de la théorie des blocs de caractères. Aussi, nous nous sommes attachés ici, en raffinant les méthodes de [1], à reprendre le calcul de ces multiplicateurs en rectifiant le résultat sur M_{22} et en n'utilisant que la théorie des caractères ordinaires.

Par ailleurs, le groupe $PSL(3, 4)$, que l'on peut considérer comme le groupe de Mathieu M_{21}, est connu pour avoir un "gros" multiplicateur de Schur (d'ordre 48). Cependant il semble impossible de trouver une référence écrite de ce résultat dû à N. Burgoyne et J.-G. Thompson. Pour cette raison, quitte à compliquer légèrement les méthodes, nous avons donné également le calcul du multiplicateur de Schur de ce groupe.

Nous prouvons ici que les multiplicateurs des groupes M_{11}, M_{12}, M_{22}, M_{23}, M_{24} sont cycliques d'ordres respectivement 1, 2, 12, 1, 1 tandis que celui de $PSL(3, 4)$ est le produit de deux composantes cycliques d'ordres respectifs 12 et 4.

L'existence d'une extension centrale propre de M_{22} par $\mathbb{Z}/4\mathbb{Z}$ peut se déduire de la table des caractères d'une extension centrale $\overline{M_{22}}$ de M_{22} par $\mathbb{Z}/2\mathbb{Z}$. Cela a été remarqué par W. Feit qui a calculé explicitement cette table et constaté qu'elle fait apparaître des caractères réels dont le degré est congru à 2 modulo 4; on en déduit aisément une extension centrale propre de $\overline{M_{22}}$ par $\mathbb{Z}/2\mathbb{Z}$ qui s'interprète aussi comme extension centrale propre de M_{22} par $\mathbb{Z}/4\mathbb{Z}$.

0021-8693/82/080552-25$02.00/0

I. Rappels sur le multiplicateur de Schur

On introduit le multiplicateur de Schur d'un groupe G lorsque l'on étudie les extensions centrales de G, c'est-à-dire les suites exactes $1 \to N \to \bar{G} \xrightarrow{s} G \to 1$ où N est contenu dans le centre de G. On sait que les classes d'isomorphismes de telles extensions sont repérées par les éléments du groupe de cohomologie $H^2(G, N)$ où N est muni de la structure de G-module triviale. Parmi ces extensions on distingue les *extensions quasitriviales*, ce sont celles pour lesquelles le groupe dérivé $[\bar{G}, \bar{G}]$ a une trace triviale sur N. Lorsque G est abélien, ce sont celles pour lesquelles $\bar{G}$ est abélien, elles sont donc repérées par les éléments de $\mathrm{Ext}^1(G, N)$; dans le cas général les classes d'extension quasi-triviales forment un sous-groupe de $H^2(G, N)$ isomorphe à $\mathrm{Ext}^1(G/[G, G], N)$.

Pour G fixé $H^2(G, N)$ et $\mathrm{Ext}^1(G/[G, G], N)$ sont fonctoriels en N; on montre que le foncteur quotient $H^2(G, \cdot)/\mathrm{Ext}^1(G/[G, G], \cdot)$ est représentable et l'on appelle multiplicateur de Schur de G un groupe $\Sigma(G)$ qui représente ce foncteur quotient. On a donc pour tout groupe abélien N une suite exacte:

$$0 \to \mathrm{Ext}^1(G/[G, G], N) \to H^2(G, N) \to \mathrm{Hom}[\Sigma(G), N] \to 0. \qquad \text{(E)}$$

A une extension centrale $1 \to N \to \bar{G} \to G \to 1$ est donc associé un morphisme $\varphi: \Sigma(G) \to N$. Par définition φ est nul si et seulement si l'extension est quasi-triviale, c'est-à-dire si $[\bar{G}, \bar{G}] \cap N = \{1\}$. Dans le cas général on prouve que l'image de φ est la trace de $[\bar{G}, \bar{G}]$ sur N. Le morphisme φ est donc surjectif si et seulement si $[\bar{G}, \bar{G}]$ contient N; on dit alors que l'*extension* considérée est *propre*.

Pour N fixé, $H^2(G, N)$ et $\mathrm{Ext}^1(G/[G, G], N)$ sont contrafonctoriels en G, il en va donc de même du quotient; il s'ensuit que $\Sigma(G)$ est fonctoriel en G.

En particulier, si H est un sous-groupe de G, l'injection canonique de H dans G définit, pour tout groupe abélien N, un morphisme de restriction $\rho: H^2(G, N) \to H^2(H, N)$. Lorsque l'indice $[G : H]$ est fini on sait également définir un morphisme $t: H^2(H, N) \to H^2(G, N)$ et l'on prouve que $t \circ \rho$ est la multiplication par $[G : H]$. On en déduit en particulier:

Proposition I.1. *Soient G un groupe, H un sous-groupe, N un groupe abélien et p un nombre premier. On suppose que l'indice $[G : H]$ est fini et non divisible par p; alors le morphisme de restriction $H^2(G, N) \to H^2(H, N)$ est injectif sur la p-composante de $H^2(G, N)$.*

De même, en utilisant le cas où H est le sous-groupe trivial, on montre, lorsque G est fini, que $H^2(G, N)$ est de torsion; plus précisément $H^2(G, N)$ est alors la somme directe de ses p-composantes pour p divisant $|G|$.

Lorsque $N = \mathbb{C}^*$, comme $\mathbb{C}^*$ est divisible, on a $\mathrm{Ext}^1(G/[G, G], \mathbb{C}^*) = 0$:

la suite (E) fournit donc un isomorphisme de $H^2(G, \mathbb{C}^*)$ sur le groupe dual $\widehat{\Sigma(G)}$. Par ailleurs la suite exacte

$$1 \to R_n \to \mathbb{C}^* \to \mathbb{C}^* \to 1$$
$$z \mapsto z^n$$

(où R_n est le groupe des racines n-ièmes de l'unité) fournit en cohomologie la suite exacte $H^2(G, R_n) \to H^2(G, \mathbb{C}^*) \to H^2(G, \mathbb{C}^*)$ qui montre, lorsque $|G| = n$, que $H^2(G, \mathbb{C}^*)$ est l'image de $H^2(G, R_n) \simeq H^2(G, \mathbb{Z}/n\mathbb{Z})$. Lorsque G est fini on conclut que $H^2(G, \mathbb{C}^*)$ est fini; il s'ensuit qu'alors $\Sigma(G)$ est également fini et donc isomorphe à $H^2(G, \mathbb{C}^*)$.

PROPOSITION I.2. *Lorsque G est fini, $H^2(G, \mathbb{C}^*)$ et $\Sigma(G)$ sont des groupes finis duaux l'un de l'autre.*

Ainsi, pour G fini, $\Sigma(G)$ est la somme directe de ses p-composantes notées $\Sigma_p(G)$. La proposition I.1 a alors un énoncé dual:

PROPOSITION I.3. *Soient G un groupe fini, H un sous-groupe de G et p un nombre premier ne divisant pas $[G : H]$; alors le morphisme canonique $\Sigma_p(H) \to \Sigma_p(G)$ est surjectif.*

En ce qui concerne la valeur du multiplicateur de Schur de certains groupes nous utiliserons les résultats classiques suivants:

— pour $n \geqslant 4$, $\Sigma_2(A_n) \simeq \mathbb{Z}/2\mathbb{Z}$ (cf. [7]),
— pour tout groupe semi-diédral G, $\Sigma(G) = 0$ (cf. [8]),
— pour tout entier n $\quad \Sigma(\mathbb{Z}/n\mathbb{Z}) = 0$, $\Sigma(\mathbb{Z}/n\mathbb{Z})^2 \simeq \mathbb{Z}/n\mathbb{Z}$,
— $\Sigma(\mathbb{Z}/2\mathbb{Z})^4 \simeq (\mathbb{Z}/2\mathbb{Z})^6$.

Ces deux derniers résultats sont en fait des cas particuliers de l'isomorphisme $\Sigma(G) \simeq \Lambda^2(G)$ valable pour tout groupe commutatif G de type fini.

Terminons ce chapitre par une remarque importante: Pour qu'un groupe fini G admette une extension centrale propre par le groupe $\mathbb{Z}/n\mathbb{Z}$ il faut et il suffit que son multiplicateur de Schur contienne un élément d'ordre n. En effet c'est là une condition nécessaire et suffisante pour qu'il existe une injection de $\mathbb{Z}/n\mathbb{Z}$ dans $\Sigma(G)$ donc, dualement, un morphisme surjectif de $\Sigma(G)$ dans $\mathbb{Z}/n\mathbb{Z}$.

II. Rappels sur les groupes de Mathieu

A. *Systèmes de Steiner*

Soient E un ensemble fini et S un ensemble de parties de E appelées blocs; on dit que S est un système de Steiner de type (p, q, r), ou un $S(p, q, r)$, sur E si l'on a:

$$|E| = r, \qquad \text{tout bloc est de cardinal } q,$$

toute partie de E de cardinal p est contenue dans un bloc et un seul.

Un isomorphisme de E muni d'un $S(p, q, r)$ sur E' muni d'un $S(p, q, r)$ est une bijection de E sur E' qui envoie les blocs de E sur les blocs de E'.

Trace d'un système de Steiner. Soit E un ensemble muni d'un $S(p, q, r)$; si A est une partie de E telle que $|A| = s \leqslant p$, notons E' le complémentaire de A dans E. Les traces sur E' des blocs de E qui contiennent A forment alors un système de Steiner de type $(p - s, q - s, r - s)$; c'est la trace sur E' du système de Steiner donné sur E.

B. *Les grands groupes de Mathieu*

On prouve (cf. [9]) que, sur un ensemble E de cardinal 24, il existe un système de Steiner de type $(5, 8, 24)$ et un seul à isomorphisme près. Le groupe des automorphismes de ce système de Steiner est, par définition, le groupe de Mathieu M_{24}, son action sur E est 5 fois transitive. Le fixateur de 1 (resp. 2, 3) point(s) de E est, par définition, le groupe de Mathieu M_{23} (resp. M_{22}, M_{21}).

Fixons n dans $\{21, 22, 23, 24\}$; en considérant la trace du $S(5, 8, 24)$ sur une partie de E à n éléments on constate que M_n est un sous-groupe (d'indice $(24 - n)!$) du groupe des automorphismes d'un $S(n - 19, n - 16, n)$ et qu'il est $n - 19$ fois transitif. Le système $S(n - 19, n - 16, n)$ est encore unique à isomorphisme près; en particulier, pour $n = 21$, le $S(2, 5, 21)$ peut s'obtenir en prenant pour blocs les droites d'un plan projectif construit sur le corps $\mathbb{F}_4$, on en déduit que M_{21} est isomorphe à $PSL(3, 4)$. Ces 4 groupes sont simples, leur ordre est donné par le tableau suivant:

$$|M_{21}| = \quad 20{,}160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7,$$
$$|M_{22}| = \quad 443{,}520 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11,$$
$$|M_{23}| = 10{,}200{,}960 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23,$$
$$|M_{24}| = 244{,}823{,}040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23.$$

Interprètons M_n comme groupe d'automorphismes d'un $S(n - 19, n - 16, n)$

sur un ensemble E'. L'action de M_n sur l'ensemble des blocs de ce système de Steiner est transitive; si X est un tel bloc notons S_X (resp. F_X) le sous-groupe des éléments de M_n qui stabilisent globalement (resp. fixent points par points) X. On montre que l'action de S_X sur X induit toutes les permutations paires de X, on en déduit une suite exacte $1 \to F_X \to S_X \to A_X \to 1$. Le groupe F_X est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^4$ et opère de façon simplement transitive sur $E' - X$; il s'ensuit que la suite exacte précédente est scindée. Plus précisément, si $a \in E' - X$, le sous-groupe $S_{X,a}$ des éléments de S_X qui fixent a est un complément de F_X dans S_X, il est donc isomorphe à A_{n-16}. L'indice de S_X dans M_n (qui est le nombre de blocs du système de Steiner) est un nombre impair. Les éléments des différents F_X, autres que l'identité, forment une classe d'involutions de M_n; pour $n \in \{21, 22, 23\}$, c'est la seule classe d'involutions tandis que, pour $n = 24$, il y a une autre classe formée d'involutions sans points fixes.

C. *Les petits groupes de Mathieu*

Dans un système de Steiner de type (5, 8, 24) il existe des parties de cardinal 12 appelées dodécades qui ont la propriété de rencontrer tous les blocs du $S(5, 8, 24)$ suivant un ensemble de cardinal 2, 4, ou 6. Le groupe de Mathieu M_{24} opère transitivement sur l'ensemble des dodécades. Soit D une telle dodécade, le stabilisateur de D est, par définition, le groupe de Mathieu M_{12}. L'action de M_{12} sur D est strictement 5 fois transitive, le fixateur d'un point de D dans M_{12} est, par définition, le groupe de Mathieu M_{11} qui est strictement 4 fois transitif sur le complémentaire du point dans la dodécade. L'action de M_{11} sur le complémentaire D' de D (qui est encore une dodécade) est 3 fois transitive, le sous-groupe des éléments de M_{11} qui fixent un point de D' est isomorphe à $PSL(2, 11)$. Les groupes M_{11} et M_{12} sont simples, leur ordre est:

$$|M_{11}| = 7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11,$$

$$|M_{12}| = 95{,}040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11.$$

Parmi les traces sur D des blocs du $S(5, 8, 24)$, celles qui sont de cardinal 6 forment un système de Steiner de type $S(5, 6, 12)$ dont la trace sur le complémentaire d'un point est un $S(4, 5, 11)$. On montre que ces systèmes de Steiner sont uniques à isomorphisme près et ont pour groupe d'automorphismes respectivement M_{12} et M_{11}.

On utilisera enfin le fait que les 2-groupes de Sylow de M_{11} sont semi-diédraux d'ordre 16.

III. Majoration de $\Sigma(G)$

Dans ce chapitre nous nous proposons, pour G groupe de Mathieu et p nombre premier, de trouver des groupes contenant la p-composante de $H^2(G, \mathbb{C}^*)$ ou, dualement, des groupes dont $\Sigma_p(G)$ est quotient.

A. *Majorations relatives*

Ce sont celles que l'on obtient en prouvant que, pour un sous-groupe H de G, le morphisme canonique $\Sigma_p(H) \to \Sigma_p(G)$ est surjectif.

1. *Le cas où p ne divise pas $|G : H|$*

Nous avons vu (cf. proposition I.3) que si p ne divise pas $|G : H|$, $\Sigma_p(H) \to \Sigma_p(G)$ est surjectif. Voici quelques exemples d'utilisation de ce résultat:

Exemple 1.

$$\Sigma_3(M_{11}) \to \Sigma_3(M_{23}), \qquad \Sigma_3(M_{12}) \to \Sigma_3(M_{24}), \qquad \Sigma_3(M_{21}) \to \Sigma_3(M_{22})$$

sont surjectifs.

Un cas particulier d'application de ce principe est celui où H est un groupe de Sylow de G; on obtient par exemple:

Proposition III.1. *Soient G un groupe et p un nombre premier alors*:

— *si p^2 ne divise pas $|G|$, $\Sigma_p(G)$ est trivial,*

— *si p^3 ne divise pas $|G|$, $\Sigma_p(G)$ est trivial ou isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration. Soit S un p-groupe de Sylow de G; $\Sigma_p(G)$ est donc un quotient de $\Sigma_p(S)$. Dans le cas considéré S est soit trivial soit isomorphe à $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z}$ ou $(\mathbb{Z}/p\mathbb{Z})^2$; $\Sigma(S)$ est alors trivial sauf dans le dernier cas où l'on a $\Sigma(S) \simeq \mathbb{Z}/p\mathbb{Z}$ (cf. I). Le résultat en découle.

Exemple 2. Pour tout groupe de Mathieu G, $\Sigma_p(G)$ est trivial si $p \notin \{2, 3\}$, $\Sigma_3(M_{21})$ et $\Sigma_3(M_{22})$ sont triviaux ou isomorphes à $\mathbb{Z}/3\mathbb{Z}$.

Exemple 3. On sait (cf. II.C et I) que les 2-groupes de Sylow de M_{11} sont semi-diédraux d'ordre 16 et que de tels groupes ont un multiplicateur de Schur trivial; il s'ensuit que $\Sigma_2(M_{11})$ est trivial.

2. *L'argument d'induction*

Il s'agit d'une technique utilisant la théorie des caractères pour prouver,

dans certains cas, la surjectivité de $\Sigma_p(H) \to \Sigma_p(G)$. Cette technique est particulièrement adaptée au cas où G est un groupe au moins 3-transitif et donc au cas des groupes de Mathieu.

a. *Un lemme.*

LEMME. *Soit G un groupe opérant de façon 3 fois transitive sur un ensemble X. Notons H le fixateur d'un point de X. Pour qu'un caractère φ de degré 1 sur H se prolonge à G il faut et il suffit que le caractère φ^* induit sur G vérifie $\langle \varphi^* \mid \varphi^* \rangle = 2$.*

Démonstration. Notons 1_H le caractère trivial sur H; le caractère induit 1_H^* est alors le caractère de l'action de G sur X. Comme cette action est 2 fois transitive on a $\langle 1_H^* \mid 1_H^* \rangle = 2$. Alors si φ admet un prolongement $\tilde{\varphi}$ on vérifie immédiatement $\varphi^* = \tilde{\varphi} \cdot 1_H^*$ et donc $\langle \varphi^* \mid \varphi^* \rangle = \langle 1_H^* \mid 1_H^* \rangle = 2$.

Réciproquement, on a $|\varphi| \leqslant 1_H$, il s'ensuit, pour $g \in G$, $|\varphi^*(g)| \leqslant 1_H^*(g)$; en outre l'inégalité obtenue est stricte sauf si, dans la somme qui définit $\varphi^*(g)$, tous les termes sont égaux. Alors $\langle \varphi^* | \varphi^* \rangle = 2$ implique $(\forall\, g \in G)$ $(|\varphi^*(g)| = 1_H^*(g))$ et donc, pour $h \in H$, tous les termes de la somme qui définit $\varphi^*(h)$ sont égaux à $\varphi(h)$; on a alors $\varphi^*(h) = \varphi(h) \cdot 1_H^*(h)$, soit $\varphi^*|_H = \varphi \cdot 1_H^*|_H$. Comme G est 3 fois transitif le caractère $1_H^*|_H$ se décompose en $1_H + 1_H + \psi$ où ψ est irréductible. Par ailleurs φ^* se décompose en 2 composantes irréductibles θ_1 et θ_2 et, d'après le théorème de Frobénius, chaque $\theta_i|_H$ contient le caractère φ. On a alors $\varphi^*|_H = \theta_1|_H + \theta_2|_H = \varphi \cdot 1_H^*|_H = \varphi + \varphi + \varphi \cdot \psi$. Comme ψ et donc $\varphi \cdot \psi$ sont irréductibles il existe i dans $\{1, 2\}$ tel que $\theta_i|_H = \varphi$.

b. *Application aux multiplicateurs de Schur.*

PROPOSITION III.2. *Soient G un groupe opérant de façon 3 fois transitive sur un ensemble X et p un nombre premier. Notons H le fixateur d'un point de X, Π le caractère de l'action de G sur X et δ_p la somme $(1/|G|) \sum |\Pi(g)|^2$ étendue aux éléments g de G dont l'ordre est divisible par p. Alors, si $\delta_p < 1$, le morphisme $\Sigma_p(H) \to \Sigma_p(G)$ est surjectif.*

Démonstration. Soit N le quotient de $\Sigma_p(G)$ par l'image de $\Sigma_p(H)$. On peut alors définir une surjection $\sigma: \Sigma(G) \to N$ qui est triviale sur l'image de $\Sigma(H)$. A cette surjection correspond donc une extension centrale propre $1 \to N \to \bar{G} \xrightarrow{s} G \to 1$ dont la restriction à H vérifie $N \cap [\bar{H}, \bar{H}] = \{1\}$ (où $\bar{H} = s^{-1}(H)$).

Soit φ un élément du groupe dual $\hat{N}$; comme N est un p-groupe φ est à valeurs dans la p-composante de $\mathbb{C}^*$. Par ailleurs l'égalité $N \cap [\bar{H}, \bar{H}] = \{1\}$ prouve que N s'injecte dans $\bar{H}/[\bar{H}, \bar{H}]$; cela permet de prolonger φ à $\bar{H}/[\bar{H}, \bar{H}]$ et par conséquent à $\bar{H}$ en un caractère, encore noté φ, de degré 1, à valeurs dans la p-composante de $\mathbb{C}^*$.

Montrons que le lemme précédent permet de prolonger φ à $\bar{G}$. Nous considérons donc l'action de $\bar{G}$ sur X par l'intermédiaire de G, elle est encore 3 fois transitive et $\bar{H} = s^{-1}(H)$ est le fixateur d'un point de X. Nous devons donc évaluer $\langle \varphi^* \mid \varphi^* \rangle$.

Comme N est contenu dans $\bar{H}$ et dans le centre de $\bar{G}$, pour $n \in N$, $g \in \bar{G}$, $x \in \bar{G}$, on a $xgx^{-1} \in \bar{H} \Leftrightarrow xngx^{-1} \in \bar{H}$ et $\varphi(xngx^{-1}) = \varphi(xgx^{-1})\varphi(n)$ si $xgx^{-1} \in \bar{H}$. On en déduit $\varphi^*(ng) = \varphi(n) \cdot \varphi^*(g)$. Ainsi $|\varphi^*(g)|$ ne dépend que de la classe de g modulo N, ce qui permet de définir une fonction centrale $\hat{\varphi}$ sur G par $|\varphi^*| = \hat{\varphi} \circ s$. On a alors $\langle \varphi^* \mid \varphi^* \rangle = \langle \hat{\varphi} \mid \hat{\varphi} \rangle$.

Dans le cas particulier où φ est le caractère trivial 1_H on a $\hat{1}_H = \Pi$ et, comme nous l'avons remarqué dans le lemme, $\langle \hat{\varphi} \mid \hat{\varphi} \rangle \leqslant \langle \Pi \mid \Pi \rangle$; $\Delta(\varphi) = \langle \Pi \mid \Pi \rangle - \langle \hat{\varphi} \mid \hat{\varphi} \rangle$ est donc un entier positif. Par ailleurs, soit g dans G dont l'ordre n'est pas divisible par p; comme N est un p-groupe, g admet un relèvement $\bar{g}$ dans $\bar{G}$ ayant le même ordre.

Alors, pour tout x de $\bar{G}$, $x\bar{g}x^{-1}$ a un ordre non divisible par p; en particulier, si $x\bar{g}x^{-1} \in \bar{H}$, $\varphi(x\bar{g}x^{-1})$ est d'ordre non divisible par p et appartient à la p-composante de $\mathbb{C}^*$, on a donc $\varphi(x\bar{g}x^{-1}) = 1$.

On en déduit $\varphi^*(\bar{g}) = 1_H^*(\bar{g})$ et donc $\hat{\varphi}(g) = \Pi(g)$. Dans le calcul de $\Delta(\varphi) = (1/|G|) \sum |\Pi(g)|^2 - |\hat{\varphi}(g)|^2$ on peut donc n'étendre la sommation qu'aux éléments d'ordre divisible par p; on en déduit $\Delta(\varphi) \leqslant \delta_p$. Ainsi, si $\delta_p < 1$, comme $\Delta(\varphi) \in \mathbb{N}$, on a $\Delta(\varphi) = 0$, soit $\langle \varphi^* \mid \varphi^* \rangle = \langle \hat{\varphi} \mid \hat{\varphi} \rangle = \langle \Pi \mid \Pi \rangle = 2$ (puisque l'action de G est 2-fois transitive). Le lemme s'applique donc et assure l'existence de $\tilde{\varphi}$ caractère de degré 1 sur $\bar{G}$ prolongeant φ. Cependant, $\tilde{\varphi}$ étant de degré 1 est trivial sur $[\bar{G}, \bar{G}]$ donc sur N (puisque l'extension est propre); il s'ensuit que φ est trivial sur N. Nous avons ainsi montré que $\hat{N}$ ne contient que le caractère trivial, ce qui prouve bien que N est trivial et donc que $\Sigma_p(H) \to \Sigma_p(G)$ est surjectif.

c. *Le cas des groupes de Mathieu.* La proposition III.2 s'applique dans les 4 cas repérés par le tableau suivant:

G	M_{22}	M_{24}	M_{12}	M_{11}
H	M_{21}	M_{23}	M_{11}	$PSL(2, 11)$
p	2	2	3	3
δ_p	$\frac{15}{32}$	$\frac{11}{16}$	$\frac{1}{3}$	$\frac{2}{3}$

Pour le calcul de δ_p on pourra consulter les tables données en appendice. Les trois premiers cas correspondent à l'action 3 fois transitive évidente du groupe de Mathieu, le quatrième cas correspond à l'action de M_{11} sur la dodécade complémentaire (cf. II.C).

Remarque (due au referee). Avec les notations de la proposition III.2, si K est le fixateur d'un couple de points de X, on peut exprimer δ_p à l'aide de H et de K. En effet, les théorèmes de Frobenius et Mackey prouvent: $\delta_p = \alpha_p(H)/|H| + \alpha_p(K)/|K|$ où l'on a noté α_p le nombre d'éléments dont l'ordre est divisible par p.

B. *Majorations directes*

1. *Le cas de* M_{21}, M_{22}, M_{23}

Prenons n dans $\{21, 22, 23\}$; nous avons vu au chapitre II que M_n est un groupe d'automorphismes d'un système de Steiner de type $(n-19, n-16, n)$. Si X est un bloc de ce système son stabilisateur S_X est d'indice impair dans M_n et il se décompose en un produit semi-direct $F_X \rtimes S_{X,a}$ avec

$$F_X \simeq (\mathbb{Z}/2\mathbb{Z})^4 \qquad \text{et} \qquad S_{X,a} \simeq A_{n-16}.$$

Considérons un groupe abélien N que l'on munit de structures de module triviales; on a alors des morphismes de restrictions:

$$\begin{array}{ccccc} & & & \xrightarrow{\beta} & H^2(F_X, N) \\ H^2(M_n, N) & \xrightarrow{\alpha} & H^2(S_X, N) & & \\ & & & \xrightarrow{\gamma} & H^2(S_{X,a}, N) \end{array}$$

Par ailleurs l'isomorphisme entre $S_{X,a}$ et le quotient S_X/F_X fournit un morphisme d'inflation $\delta: H^2(S_{X,a}, N) \to H^2(S_X, N)$.

Les propriétés fonctorielles de la cohomologie donnent les relations: $\beta \circ \delta = 0$ et $\gamma \circ \delta = \mathrm{Id}$, d'où l'on déduit la décomposition: $\mathrm{Ker}\,\beta = \mathrm{Im}\,\delta \oplus (\mathrm{Ker}\,\beta \cap \mathrm{Ker}\,\gamma)$. D'autre part la suite exacte: $1 \to F_X \to S_X \to S_{X,a} \to 1$ fournit (par exemple à l'aide de la suite spectrale de Hochschild–Serre) une injection de $\mathrm{Ker}\,\beta/\mathrm{Im}\,\delta$ dans $H^1[S_{X,a}, H^1(F_X, N)]$ (c'est même un isomorphisme puisque la suite est scindée et le module N est trivial); il s'ensuit que $\mathrm{Ker}\,\beta \cap \mathrm{Ker}\,\gamma$ (qui est isomorphe à $\mathrm{Ker}\,\beta/\mathrm{Im}\,\delta$) s'injecte dans $H^1[S_{X,a}, H^1(F_X, N)]$.

Supposons tout d'abord $N = \mathbb{C}^*$. On a $H^1(F_X, \mathbb{C}^*) \simeq \mathrm{Hom}(F_X, \mathbb{C}^*) = \hat{F}_X \simeq (\mathbb{Z}/2\mathbb{Z})^4$; il existe donc un entier p tel que $H^1[S_{X,a}, H^1(F_X, \mathbb{C}^*)] \simeq (\mathbb{Z}/2\mathbb{Z})^p$.

Par ailleurs on a $H^2(F_X, \mathbb{C}^*) \simeq \mathrm{Hom}[\Sigma(F_X), \mathbb{C}^*] \simeq \Sigma(F_X) \simeq \Sigma(\mathbb{Z}/2\mathbb{Z})^4$ et,

de même, $H^2(S_{X,a}, \mathbb{C}^*) \simeq \Sigma(A_{n-16})$; or on sait (cf. I) $\Sigma(\mathbb{Z}/2\mathbb{Z})^4 \simeq (\mathbb{Z}/2\mathbb{Z})^6$ et $\Sigma_2(A_{n-16}) \simeq \mathbb{Z}/2\mathbb{Z}$. De cela on déduit que la multiplication par 2 est le morphisme nul sur $\operatorname{Ker}\beta \cap \operatorname{Ker}\gamma$, sur $\operatorname{Im}\beta$ et sur la 2-composante de $\operatorname{Im}\gamma$; on en tire immédiatement que, sur la 2-composante de $H^2(S_X, \mathbb{C}^*)$, la multiplication par 4 est le morphisme nul.

Remarquons alors que, l'indice de S_X dans M_n étant impair, α est injectif sur la 2-composante de $H^2(M_n, \mathbb{C}^*)$; il s'ensuit que, sur cette 2-composante, la multiplication par 4 est encore le morphisme nul.

Supposons maintenant $N = \mathbb{Z}/2\mathbb{Z}$. Un élément de $H^2(M_n, \mathbb{Z}/2\mathbb{Z})$ correspond à une extension centrale

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \bar{M}_n \xrightarrow{s} M_n \longrightarrow 1.$$

Une involution θ de M_n se relève alors dans $\bar{M}_n$ soit en deux involutions soit en deux éléments d'ordre 4. Cependant, comme M_n ne possède qu'une classe d'involutions (ce point empêche la généralisation à $n = 24$), le cas qui se présente pour θ se présente pour toutes les involutions. Supposons que l'on soit dans le deuxième cas, $\bar{G}$ ne possède alors qu'une involution (celle qui engendre N) et un 2-groupe de Sylow est cyclique ou quaternionnien; on conclut à l'existence dans $\bar{G}$ d'un élément d'ordre 64 (et même 128 si $n \neq 21$) et donc dans G d'un élément d'ordre 32, ce qui est absurde ($32 > n$). Ainsi les involutions de M_n se relèvent en involutions. Appliquons cela aux éléments de $F_X \simeq (\mathbb{Z}/2\mathbb{Z})^4$ on conclut $\bar{F}_X = s^{-1}(F_X) \simeq (\mathbb{Z}/2\mathbb{Z})^5$; l'extension est donc triviale sur F_X. Par ailleurs on montre (cf. appendice A) que $S_{X,a}$ n'admet qu'une classe d'extension non triviale par $\mathbb{Z}/2\mathbb{Z}$ et que, pour celle-ci, les involutions se relèvent en éléments d'ordre 4; on conclut que l'extension de M_n est également triviale sur $S_{X,a}$.

Autrement dit $\beta \circ \alpha$ et $\gamma \circ \alpha$ sont des applications nulles, d'où $\operatorname{Im}\alpha \subset \operatorname{Ker}\beta \cap \operatorname{Ker}\gamma$. Cependant, l'indice de S_X dans M_n étant impair et $\mathbb{Z}/2\mathbb{Z}$ étant un 2-groupe, α est injective et, par conséquent, $H^2(M_n, \mathbb{Z}/2\mathbb{Z})$ s'injecte dans $\operatorname{Ker}\beta \cap \operatorname{Ker}\gamma$ et donc dans $H^1[S_{X,a}, H^1(F_X, \mathbb{Z}/2\mathbb{Z})]$.

Remarquons que l'on a encore $H_1(F_X, \mathbb{Z}/2\mathbb{Z}) \simeq \hat{F}_X$ et donc

$$H^1[S_{X,a}, H^1(F_X, \mathbb{Z}/2\mathbb{Z})] \simeq (\mathbb{Z}/2\mathbb{Z})^p.$$

Comme le groupe M_n est simple on a $H^2(M_n, N) \simeq \operatorname{Hom}[\Sigma(M_n), N]$. Si l'on décompose alors $\Sigma_2(M_n)$ en composantes cycliques, le résultat obtenu pour $N = \mathbb{C}^*$ prouve que ces composantes sont d'ordre au plus 4, le résultat obtenu pour $N = \mathbb{Z}/2\mathbb{Z}$ prouve qu'elles sont en nombre au plus p. Or un calcul cohomologique prouve (cf. appendice B) que, pour $n = 23$, on a $p = 0$ et, pour $n = 21$, on a $p \leqslant 2$ (les résultats du IV.B.4 impliquent a postériori $p = 2$). En conclusion nous avons obtenu:

— $\Sigma_2(M_{23})$ est trivial,

— $\Sigma_2(M_{21})$ est le produit d'au plus 2 groupes cycliques dont l'ordre est au plus 4.

Remarque. On peut également montrer $p = 1$ pour $n = 22$; cela prouve que $\Sigma_2(M_{22})$ est cyclique d'ordre au plus 4 mais nous obtiendrons ce résultat par un autre procédé.

2. *Le cas de* M_{12}

La proposition III.2 ne s'applique pas au cas $G = M_{12}$, $H = M_{11}$, $p = 2$; en effet on a alors $\delta_2 = 5/4 \geqslant 1$. On peut cependant obtenir une majoration de $\Sigma_2(M_{12})$ en raffinant l'argument d'induction.

Reprenons les notations générales de la proposition III.2 et de sa démonstration. Sans hypothèse sur la transitivité de G ni sur la valeur de δ_p on dispose encore d'une extension centrale propre $1 \to N \to \bar{G} \xrightarrow{s} G \to 1$ où N est le quotient de $\Sigma_p(G)$ par l'image de $\Sigma_p(H)$.

Tout élément φ de $\hat{N}$ se prolonge en un caractère φ sur $\bar{H}$ à valeurs dans la p-composante de $\mathbb{C}^*$ et l'on peut définir le caractère induit φ^*, la fonction $\hat{\varphi}$ et l'entier $\Delta(\varphi)$. C'est précisément en utilisant le fait que $\Delta(\varphi)$ est entier que l'on va obtenir des renseignements sur $\hat{N}$ et donc sur N; pour cela nous devons estimer $\hat{\varphi}(g)$ sans hypothèse sur l'ordre de g.

Soient g dans G et a sa classe de conjugaison; $s^{-1}(a)$ est alors la réunion disjointe de classes de conjugaison dans $\bar{G}$. Comme N est dans le centre de $\bar{G}$, N opère transitivement par multiplication sur l'ensemble de ces classes et, comme N est commutatif, elles ont toutes le même fixateur soit N_a. Alors, pour $\bar{g} \in s^{-1}(g)$ et $n \in N_a$, $n\bar{g}$ et $\bar{g}$ sont conjugués dans $\bar{G}$ d'où $\varphi^*(n\bar{g}) = \varphi^*(\bar{g})$. Par ailleurs on sait $\varphi^*(n\bar{g}) = \varphi(n)\,\varphi^*(\bar{g})$; il s'ensuit que si φ n'est pas trivial sur N_a $\varphi^*(\bar{g})$ et par conséquent $\hat{\varphi}(g)$ sont nuls.

Supposons maintenant φ trivial sur N_a. Si l'on a $\Pi(g) = 0$, la relation $0 \leqslant \hat{\varphi}(g) \leqslant \Pi(g)$ prouve $\hat{\varphi}(g) = 0$. Supposons donc $\Pi(g) \neq 0$; cela signifie que $a \cap H$ est non vide, c'est la réunion disjointe d'une famille $(a_i)_{i \in I}$ de classes de conjugaison dans H. Soient $\bar{g}$ un relèvement de g dans $\bar{G}$ et $\bar{a}$ sa classe de conjugaison. Pour chaque indice i posons $\bar{a}_i = \bar{a} \cap s^{-1}(a_i)$ et choisissons un élément α_i dans $\bar{a}_i$. Alors, pour $t \in \bar{a}_i$, $s(t)$ et $s(\alpha_i)$ sont conjugués dans H; il existe donc n dans N tel que t et $n\alpha_i$ soient conjugués dans $\bar{H} = s^{-1}(H)$ et donc dans $\bar{G}$. On a donc $n\alpha_i \in \bar{a}$ d'où $n \in N_a$ et $\varphi(n) = 1$. Par ailleurs on a $\varphi(t) = \varphi(n\alpha_i) = \varphi(n)\,\varphi(\alpha_i) = \varphi(\alpha_i)$. Ainsi φ est constant sur $\bar{a}_i$. On en déduit que $\varphi^*(\bar{g})$ s'écrit $\sum \lambda_i \varphi(\alpha_i)$ où les λ_i sont des coefficients proportionnels aux cardinaux des ensembles $\{x \in \bar{G} \mid x\bar{g}x^{-1} \in \bar{a}_i\}$ donc à ceux des ensembles $\bar{a}_i$. Posons $c_i = |a_i|$, on a $|\bar{a}_i| = |N_a| \cdot c_i$ d'où $\varphi^*(\bar{g}) = A \sum c_i \varphi(\alpha_i)$, où A ne dépend pas de φ. En utilisant cette formule pour $\varphi = 1_H$ on obtient $\varphi^*(\bar{g}) = (\sum c_i \varphi(\alpha_i)/\sum c_i)\, 1_H^*(\bar{g})$ et donc $\hat{\varphi}(g) = (|\sum c_i \varphi(\alpha_i)|/\sum c_i)\, \Pi(g)$.

En conclusion on a:

$$\begin{aligned}
&\text{— si } \Pi(g) = 0, \qquad \hat{\varphi}(g) = 0, \\
&\text{— si } \Pi(g) \neq 0, \qquad \hat{\varphi}(g) = 0 \qquad \text{lorsque } \varphi(N_a) \neq \{1\}, \\
&\qquad\qquad \hat{\varphi}(g) = \frac{|\sum c_i \varphi(\alpha_i)|}{\sum c_i} \Pi(g) \qquad \text{lorsque } \varphi(N_a) = \{1\}.
\end{aligned}$$

Remarques. Lorsque $a \cap H$ est une classe de conjugaison dans H la dernière relation s'écrit $\hat{\varphi}(g) = \Pi(g)$.

Comme nous l'avons vu la valeur de $\varphi(\alpha_i)$ ne dépend pas du choix de α_i dans $\bar{a}_i$. Par contre, si l'on remplace $\bar{g}$ par un autre relèvement $n\bar{g}$, $\bar{a}$ est remplacé par $n\bar{a}$ et en remplaçant les α_i par $n\alpha_i$ on voit que tous les $\varphi(\alpha_i)$ sont multipliés par $\varphi(n)$ ce qui, bien sûr, ne change pas la valeur de $|\sum c_i \varphi(\alpha_i)|$.

Comme φ^*, les $\varphi(\alpha_i)$ ne sont pas déterminés par $\varphi|_N$ mais dépendent du prolongement à $\bar{H}$ choisi.

Lorsque l'ordre de g n'est pas divisible par p on a toujours $\hat{\varphi}(g) = \Pi(g)$: dans ce cas N_a est trivial.

Afin d'utiliser les formules obtenues nous avons besoin d'estimer N_a; cela est possible grâce au lemme suivant:

LEMME. *Soient g dans G, a sa classe de conjugaison et $\bar{g}$ un relèvement de g dans $\bar{G}$. Notons C_g (resp. $C_{\bar{g}}$) le centralisateur de g (resp. $\bar{g}$) dans G (resp. $\bar{G}$). Alors N_a est isomorphe au quotient $C_g/s(C_{\bar{g}})$.*

Démonstration. Soient x dans C_g et $\bar{x}$ un relèvement de x dans $\bar{G}$. Comme x commute avec g le commutateur $\bar{x}\bar{g}\bar{x}^{-1}\bar{g}^{-1}$ appartient à N; par ailleurs comme les éléments de N commutent avec les éléments de $\bar{G}$, ce commutateur ne dépend pas du choix de $\bar{x}$, notons le $f(x)$.

Pour x et y dans C_g se relevant en $\bar{x}$ et $\bar{y}$ on a: $f(xy) = \bar{x}\bar{y}\bar{g}\bar{y}^{-1}\bar{x}^{-1}\bar{g}^{-1} = \bar{x}f(y)\,\bar{g}\bar{x}^{-1}\bar{g}^{-1}$ et, comme $f(y)$ appartenant à N commute avec $\bar{x}$, on obtient $f(xy) = f(x)f(y)$. Ainsi f est un morphisme de C_g dans N dont le noyau est évidemment formé par les x qui se relèvent dans $C_{\bar{g}}$, c'est donc $s(C_{\bar{g}})$. Par ailleurs, pour $x \in C_g$, $\bar{x}\bar{g}\bar{x}^{-1} = f(x) \cdot \bar{g}$ est conjugué de $\bar{g}$ donc $f(x) \in N_a$; réciproquement, si $n \in N_a$ il existe t dans $\bar{G}$ tel que $t\bar{g}t^{-1} = n\bar{g}$ d'où $n = t\bar{g}t^{-1}\bar{g}^{-1}$ et $s(n) = 1$ prouve $s(t) \in C_g$ donc $n = f(s(t))$. Ainsi N_a est l'image de f et le lemme en découle.

Remarquons que le groupe engendré par $\bar{g}$ est contenu dans $C_{\bar{g}}$, celui engendré par g est donc contenu dans $s(C_{\bar{g}})$; on en déduit

COROLLAIRE. *Si l'ordre de g est égal à $|C_g|$. N_a est trivial.*

Application à M_{12}. Nous considérons donc le cas $G = M_{12}$, $H = M_{11}$, $p = 2$. L'action de G est 3 fois transitive donc $\langle \Pi \mid \Pi \rangle = 2$ et le lemme de A.2.a s'applique. On conclut que si $\varphi \in \hat{N}$ vérifie $\Delta(\varphi) = 0$, φ se prolonge à $\bar{G}$; φ est alors trivial sur $[\bar{G}, \bar{G}]$ donc sur N. Par ailleurs, comme $\langle \varphi^* \mid \varphi^* \rangle$ est un entier non nul on a $0 \leqslant \Delta(\varphi) \leqslant \langle \Pi \mid \Pi \rangle - 1 = 1$. Ainsi pour φ non trivial la seule possibilité est $\Delta(\varphi) = 1$.

Les seuls éléments g pour lesquels on peut avoir $\hat{\varphi}(g) \neq \Pi(g)$ sont ceux d'ordre pair pour lesquels $\Pi(g) \neq 0$; la table de caractères de M_{12} montre (cf. appendice C) qu'ils se répartissent en 4 classes a, b, c, d, et l'on a

	a	b	c	d
Π	4	4	2	1
ω	2	4	8	6
h	192	32	8	6

où, pour une classe x, $\omega(x)$ désigne l'ordre des éléments de x, $h(x)$ désigne l'ordre des centralisateurs des éléments de x.

En outre a, b, et d rencontrent M_{11} suivant une seule classe de conjugaison tandis que $c \cap M_{11}$ se divise en deux classes de même cardinal (cf. table des caractères de M_{11}).

Enfin pour c et d on a $\omega = h$ le corollaire du lemme précédent assure donc que N_c et N_d sont triviaux.

En conclusion, sur a et b $\hat{\varphi}$ est nul ou coïncide avec Π, sur d $\hat{\varphi} = \Pi$, et sur c on a $\hat{\varphi} = |(\varphi(\alpha_1) + \varphi(\alpha_2))/2| \cdot \Pi = |1 + \varphi(\alpha)|$ si $\alpha = \alpha_1 \cdot \alpha_2^{-1}$. On en déduit $\Delta(\varphi) = (\lambda/192) + (\mu/32) + (4 - |1 + \varphi(\alpha)|^2)/8$ avec $\lambda = 0$ ou 16, $\mu = 0$ ou 16.

Pour φ non trivial on a vu $\Delta(\varphi) = 1$, d'où $|1 + \varphi(\alpha)|^2 = (\lambda/24) + (\mu/4) - 4$. Les seules possibilités qui donnent une valeur positive au deuxième membre sont

$$\lambda = 0, \qquad \mu = 16 \qquad \text{alors} \quad |1 + \varphi(\alpha)|^2 = 0$$

$$\lambda = 16, \qquad \mu = 16 \qquad \text{alors} \quad |1 + \varphi(\alpha)|^2 = \tfrac{2}{3}.$$

Comme $|\varphi(\alpha)| = 1$ on conclut $\varphi(\alpha) = -1$ dans le premier cas, $\varphi(\alpha) = z$ ou $\bar{z}$, avec $z = (-2 + i\sqrt{5})/3$, dans le deuxième cas.

Remarquons alors que $[M_{11}, M_{11}]$ étant égal à M_{11}, on a $N \simeq \bar{M}_{11}/[\bar{M}_{11}, \bar{M}_{11}]$ et tout caractère de degré 1 sur N se prolonge de façon unique à $s^{-1}(M_{11})$. On définit donc un morphisme $\hat{N} \xrightarrow{\phi} \mathbb{C}^*$ par $\varphi \to \varphi(\alpha)$. En tenant compte du cas ou φ est trivial nous avons prouvé $\operatorname{Im} \phi \subset X = \{1, -1, z, \bar{z}\}$. Comme $\operatorname{Im} \phi$ est un sous-groupe de $\mathbb{C}^*$, on ne peut avoir $z \in \operatorname{Im} \phi$ (car $z^2 \notin X$) ni $\bar{z} \in \operatorname{Im} \phi$, d'où $\operatorname{Im} \phi \subset \{1, -1\}$.

Par ailleurs on a vu φ non trivial $\Rightarrow \varphi(\alpha) \neq 1$; ainsi ϕ est injectif et l'on

conclut que $\hat{N}$ a au plus 2 éléments. Il en va donc de même de N. Dans le cas de M_{12}, N est le quotient de $\Sigma_2(M_{12})$ par l'image de $\Sigma_2(M_{11})$;

Nous avons vu (A.1, exemple 3) que $\Sigma_2(M_{11})$ est trivial, on conclut donc: $\Sigma_2(M_{12})$ est trivial ou isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

C. *Récapitulation des résultats*

Pour $p = 2$

$\Sigma_2(M_{11}) = 0$ (A.1, exemple 3),

$\Sigma_2(M_{12}) \subset \mathbb{Z}/2\mathbb{Z}$ (B.2), $\Sigma_2(M_{23}) = 0$ (B.1),

$\Sigma_2(M_{23}) \to \Sigma_2(M_{24})$ est surjectif (A.2.c), d'où

$\Sigma_2(M_{24}) = 0$,

$\Sigma_2(M_{21}) \to \Sigma_2(M_{22})$ est surjectif (A.2.c) et

$\Sigma_2(M_{21}) \subset (\mathbb{Z}/4\mathbb{Z})^2$ (B.1).

Pour $p = 3$

$\Sigma_3(PSL(2, 11)) \to \Sigma_3(M_{11})$ et $\Sigma_3(M_{11}) \to \Sigma_3(M_{12})$ sont surjectifs (A.2.c),

$\Sigma_3(M_{11}) \to \Sigma_3(M_{23})$ et $\Sigma_3(M_{12}) \to \Sigma_3(M_{24})$ sont surjectifs (A.1, exemple 1).

Or $|PSL(2, 11)| = 660$ n'est pas divisible par 9; de la proposition III.1 on conclut donc que $\Sigma_3(PSL(2, 11))$ et par conséquent $\Sigma_3(M_{11})$, $\Sigma_3(M_{12})$, $\Sigma_3(M_{23})$ et $\Sigma_3(M_{24})$ sont triviaux.

Enfin $\Sigma_3(M_{21}) \subset \mathbb{Z}/3\mathbb{Z}$, $\Sigma_3(M_{22}) \subset \mathbb{Z}/3\mathbb{Z}$ (A.1, exemple 2). Pour les autres nombres premiers les p-composantes sont triviales.

IV. Minoration de $\Sigma(G)$

A l'inverse de la démarche du chapitre précédent, nous nous proposons de montrer que, pour G groupe de Mathieu, $\Sigma(G)$ contient certains sous-groupes, ce qui revient à prouver l'existence de certaines extensions centrales propres de G. Pour cela nous pourrons soit expliciter une extension soit construire une extension sur un sous-groupe de G et montrer qu'elle se prolonge à G. Dans le deuxième cas l'outil fondamental est le critère de stabilité (cf. [3]).

A. *Critère de stabilité*

Soient G un groupe, H un sous-groupe et x un élément de G. Posons $K = H \cap xHx^{-1}$; on dispose alors de deux morphismes de K dans H, l'injection canonique et le morphisme $t \to x^{-1}tx$. Si N est un groupe abélien, le foncteur $H^2(\cdot, N)$ fournit donc deux morphismes de $H^2(H, N)$ dans $H^2(K, N)$; les images d'un élément Θ de $H^2(H, N)$ par ces morphismes sont d'une part la restriction de Θ à K notée $\Theta|_K$ et d'autre part une classe de cohomologie notée Θ_K^x.

DÉFINITION. Avec les notations ci-dessus, on dit que Θ est stable par x si l'on a $\Theta|_K = \Theta_K^x$.

Remarque. Lorsque x^2 est dans le normalisateur de H, la conjugaison par x^{-1} induit un automorphisme de K donc du groupe de cohomologie $H^2(K, N)$; la classe Θ_K^x est alors l'image par cet automorphisme de $\Theta|_K$. La classe Θ est donc stable par x si et seulement si sa restriction $\Theta|_K$ est invariante sous l'action de x; si $\Theta|_K$ représente l'extension $1 \to N \to \bar{K} \to K \to 1$ cela revient à dire qu'il existe un automorphisme de $\bar{K}$, trivial sur N et qui, par passage au quotient, donne l'automorphisme $t \to x^{-1}tx$ de K.

En particulier, lorsque $x \in H$, on a $K = H$ et tout élément $\bar{x}$ de $\bar{K}$ qui relève x fournit, par conjugaison, un automorphisme qui permet de conclure $\Theta_H^x = \Theta|_H = \Theta$. Plus généralement, si Θ est la restriction d'un élément $\tilde{\Theta}$ de $H^2(G, N)$, $\Theta|_K$ et Θ_K^x sont les restrictions à K de $\tilde{\Theta}$ et $\tilde{\Theta}_G^x$; comme l'on a $\tilde{\Theta}_G^x = \tilde{\Theta}$ on conclut que Θ est stable par x. Ainsi, pour qu'une extension centrale de H se prolonge à G il faut que sa classe soit stable par les éléments de G.

Une réciproque partielle de ce résultat est donnée par l'énoncé suivant (cf. [3]):

PROPOSITION IV.1 (Critère de stabilité). *Soient G un groupe, H un sous-groupe, N un groupe abélien et p un nombre premier. On suppose que l'indice $[G : H]$ est fini et non divisible par p; alors pour qu'un élément de la p-composante de $H^2(H, N)$ soit la restriction d'un élément de $H^2(G, N)$ il faut et il suffit qu'il soit stable par les éléments d'un système de représentants des doubles classes de G modulo H.*

B. *Application aux groupes de Mathieu*

1. *Le cas $p = 2$, $G = M_{12}$*

Le groupe de Mathieu M_{12} peut se plonger dans le groupe projectif $PSL(6, 3)$. On peut le voir en utilisant une réalisation du système de Steiner

$S(5, 6, 12)$ dans l'espace projectif de dimension 5 sur $\mathbb{F}_3$ (cf. [5]) ou en utilisant le code ternaire de Golay (cf. [4]).

L'extension centrale $1 \to \mathbb{Z}/2\mathbb{Z} \to SL(6, 3) \to PSL(6, 3) \to 1$ donne par restriction une extension $1 \to \mathbb{Z}/2\mathbb{Z} \to \bar{M}_{12} \to M_{12} \to 1$. On remarque alors que $\bar{M}_{12}$ contient un élément de carré $-\mathrm{Id}$ (avec les notations de [5], on peut prendre l'automorphisme de $(\mathbb{F}_3)^6$ qui envoie $1, 2, 3, 4, 5, f$ sur $a, b, c, d, e, -6$; avec les notations de [4] on peut prendre l'élément C). Il s'ensuit que l'extension de M_{12} obtenue n'est pas triviale et, puisque $[M_{12}, M_{12}] = M_{12}$, elle est donc propre. Ainsi $\Sigma_2(M_{12})$ n'est pas trivial; la majoration obtenue au chapitre III prouve donc $\Sigma_2(M_{12}) \simeq \mathbb{Z}/2\mathbb{Z}$.

2. *Les cas $p = 3$, $G = M_{21}$ et $G = M_{22}$*

On sait que M_{21} est isomorphe à $PSL(3, 4)$; on a donc une extension centrale propre $1 \to \mathbb{Z}/3\mathbb{Z} \to SL(3, 4) \to M_{21} \to 1$. Montrons que cette extension se prolonge à M_{22}. Comme $[M_{22} : M_{21}] = 22$ n'est pas divisible par 3 le critère de stabilité s'applique.

Interprétons M_{22} comme groupe de permutations sur 22 éléments; M_{21} est le fixateur d'un point a. Des éléments σ et τ de M_{22} sont alors dans la même double classe modulo M_{21} si et seulement $(a, \sigma(a))$ et $(a, \tau(a))$ sont dans la même orbite sous l'action de M_{22}. Comme l'action de M_{22} est deux fois transitive il y a deux orbites donc deux doubles classes.

Pour σ dans la première double classe on a $a = \sigma(a)$, c'est-à-dire $\sigma \in M_{21}$ et toute extension de M_{21} est stable par σ. Pour σ dans la deuxième double classe on a $a \neq \sigma(a) = b$ et $K = M_{21} \cap \sigma M_{21} \sigma^{-1}$ est le fixateur du couple (a, b). Ainsi K est isomorphe au groupe spécial affine du plan $(\mathbb{F}_4)^2$ donc au produit semi-direct $(\mathbb{F}_4)^2 \rtimes SL(2, 4)$. On en déduit $[K, K] = K$. Par ailleurs $|K| = 16 \times 60$ n'est pas divisible par 9 donc $\Sigma_3(K)$ est trivial (cf. proposition III.1); on a donc $H^2(K, \mathbb{Z}/3\mathbb{Z}) \simeq \mathrm{Hom}(\Sigma_3(K), \mathbb{Z}/3\mathbb{Z}) = 0$. Ainsi, pour $\Theta \in H^2[M_{21}, \mathbb{Z}/3\mathbb{Z}]$, $\Theta|_K$ et θ_K^σ sont triviaux donc égaux et Θ est stable par σ.

En conclusion toute extension centrale de M_{21} par $\mathbb{Z}/3\mathbb{Z}$ s'étend à M_{22}. En particulier l'extension propre $1 \to \mathbb{Z}/3\mathbb{Z} \to SL(3, 4) \to M_{21} \to 1$ est la restriction d'une extension de M_{22} qui, a fortiori, est propre. Ainsi $\Sigma_3(M_{21})$ et $\Sigma_3(M_{22})$ ne peuvent pas être triviaux. Les majorations du chapitre III prouvent donc $\Sigma_3(M_{21}) \simeq \Sigma_3(M_{22}) \simeq \mathbb{Z}/3\mathbb{Z}$.

3. *Construction d'une extension centrale propre de M_{22} par $\mathbb{Z}/4\mathbb{Z}$*

Considérons M_{22} comme un groupe de permutations d'un ensemble E de cardinal 22 qui conserve un système de Steiner de type (3, 6, 22). Nous avons vu au chapitre II que le stabilisateur d'un bloc X est un sous-groupe S_X d'indice impair dans M_{22}; tout revient donc à construire une extension centrale propre de S_X par $\mathbb{Z}/4\mathbb{Z}$ qui soit stable par les éléments de M_{22}.

Nous avons vu également qu'il existe une suite exacte,

$$1 \to F_X \to S_X \to A_X \to 1,$$

où F_X isomorphe à $(\mathbb{Z}/2\mathbb{Z})^4$ opère de façon régulière sur $E - X$ et A_X est le groupe des permutations paires de X.

a. *Action de M_{22} sur les couples de blocs.* Par des calculs d'analyse combinatoire élémentaire on montre aisément que, si (X, Y) est un couple de blocs on a $n = |X \cap Y| \in \{0, 2, 6\}$. En outre il y a 77 couples pour lesquels $n = 6$ (ce sont bien sur les couples (X, X)), 4620 couples pour lesquels $n = 2$ et 1232 couples pour lesquels $n = 0$.

Soit (X, Y) un couple de blocs tels que $n = 0$; le fixateur du couple (X, Y) est le groupe $S_X \cap S_Y$, son indice est donc inférieur à 1232 d'où $|S_X \cap S_Y| \geqslant 443{,}520/1232 = 360$. Par ailleurs, si $\sigma \in F_X \cap S_Y$, $\sigma|_Y$ est une permutation paire de Y de carré Id_Y, ainsi $\sigma|_Y$ possède un point fixe; comme l'action de F_X sur $E - X$ est régulière on conclut $\sigma = \mathrm{Id}_E$. Ainsi $F_X \cap S_Y = \{\mathrm{Id}_E\}$ et le morphisme $S_X \cap S_Y \to A_X$ est injectif. Comme l'on a $|A_X| = 360$, on en déduit $|S_X \cap S_Y| = 360$ et le morphisme $S_X \cap S_Y \to A_X$ est un isomorphisme. Il s'ensuit $[M_{22} : S_X \cap S_Y] = 1232$, l'action de M_{22} sur les couples de blocs vérifiant $n = 0$ est donc transitive; d'autre part $S_X \cap S_Y$ est un complément de F_X dans S_X, S_X est donc le produit semi-direct de F_X par $S_X \cap S_Y$.

Soit (X, Y) un couple de blocs tel que $n = 2$, le fixateur de ce couple est d'indice inférieur à 4620 d'où $|S_X \cap S_Y| \geqslant 443{,}520/4620 = 96$. Par ailleurs $F_X \cap S_Y$ conserve $Y \cap (E - X)$ qui est de cardinal 4; comme F_X agit de façon régulière sur $E - X$ on conclut $|F_X \cap S_Y| \leqslant 4$. L'image de $S_X \cap S_Y$ dans A_X conserve $X \cap Y$, c'est donc un groupe de cardinal inférieur à 24; on en déduit $|S_X \cap S_Y| \leqslant 96$. En conclusion on a $|S_X \cap S_Y| = 96$, d'où $|F_X \cap S_Y| = 4$ et $[M_{22} : S_X \cap S_Y] = 4620$; il s'ensuit que l'action de M_{22} sur les couples de blocs vérifiant $n = 2$ est transitive.

b. *Construction de l'extension sur S_X.* Considérons un bloc Z et une partie A de E de cardinal 2 disjointe de Z. Il y a $20/4 = 5$ blocs qui contiennent A parmi lesquels $6/2 = 3$ qui rencontrent Z, notons les T_1, T_2, T_3, les deux autres sont donc disjoints de Z, notons les X et Y. Notons t_i et t_i' les éléments de $Z \cap T_i$ $(i \in \{1, 2, 3\})$, on a $Z = \{t_1, t_1', t_2, t_2', t_3, t_3'\}$.

Nous avons vu au a que S_X est le produit semi-direct de F_X par $S_X \cap S_Z$. Nous allons construire l'extension de S_X comme un produit semi-direct par $S_X \cap S_Z$ d'une extension centrale de F_X par $\mathbb{Z}/4\mathbb{Z}$.

Considérons l'algèbre de Clifford de $\mathbb{R}^Z$; elle est engendrée par les 6 vecteurs $(e_z)_{z \in Z}$ qui vérifient $e_z e_{z'} = -e_{z'} e_z$ si $z \neq z'$ et $e_z^2 = -1$. Notons G (resp. Γ, N) le groupe engendré par les e_z (resp. les produits $e_z e_{z'}$, le produit des 6 vecteurs e_z). Le groupe G peut être défini par les générateurs e_z et

$\varepsilon = -1$ avec les relations: $e_z^2 = \varepsilon$, $\varepsilon^2 = 1$, $e_z e_{z'} = \varepsilon e_{z'} e_z$ si $z \neq z'$. Le produit des e_z dépend de l'ordre dans lequel on les compose, il prend l'une des deux valeurs ω ou $\varepsilon\omega$; en particulier $\omega^{-1} = \varepsilon\omega$ d'où $\omega^2 = \varepsilon$ et $N \simeq \mathbb{Z}/4\mathbb{Z}$. Par ailleurs on a $e_z \omega = \varepsilon \omega e_z$ ce qui prouve que N est distingué dans G et contenu dans le centre de Γ (c'est en fait le centre de Γ). En outre $S_X \cap S_Z$ opère sur Z par l'intermédiaire du morphisme $S_Z \to A_Z$; il opère donc sur l'algèbre de Clifford de $\mathbb{R}^Z$, sur G, sur Γ et sur N. Enfin comme l'opération sur Z se fait par des permutations paires, l'opération est triviale sur N. On en déduit une extension centrale:

$$1 \to N \to \Gamma \rtimes (S_X \cap S_Z) \to \Gamma/N \rtimes (S_X \cap S_Z) \to 1.$$

Si x et y sont dans $E - X$, notons $\langle x, y \rangle$ l'élément de F_X qui envoie y sur x. Fixons un élément m de $E - X$, on peut définir un morphisme Π' de G dans F_X par $\Pi'(e_x) = \langle m, x \rangle$ et $\Pi'(\varepsilon) = \mathrm{Id}$; ce morphisme dépend de m cependant on a $\Pi'(e_x e_y) = \langle x, y \rangle$, sa restriction à Γ est donc indépendante de m, notons la Π. En outre cette relation prouve que Π commute aux actions de $S_X \cap S_Z$ sur Γ et sur F_X, puisque l'on a clairement, pour $\varphi \in S_X$, et x, y dans $E - X$, $\varphi \circ \langle x, y \rangle \circ \varphi^{-1} = \langle \varphi(x), \varphi(y) \rangle$.

Il est aisé d'expliciter les éléments de Γ, il y en a 2 de degré 0, 30 de degré 2, 30 de degré 4 et 2 de degré 6; on constate ainsi que le noyau de Π est N et donc que $|\mathrm{Im}\,\Pi| = 64/4 = 16$. Il s'ensuit $\mathrm{Im}\,\Pi = F_X$ et donc F_X est isomorphe à Γ/N par Π; comme Π commute aux actions de $S_X \cap S_Z$ on en déduit:

$$S_X \simeq F_X \rtimes (S_X \cap Z_Z) \simeq \Gamma/N \rtimes (S_X \cap S_Z)$$

et donc l'extension centrale annoncée:

$$1 \to N \to \Gamma \rtimes (S_X \cap S_Z) \to S_X \to 1.$$

c. *Stabilité de l'extension par M_{22}.* D'après le critère de stabilité (proposition IV.1) nous devons vérifier cette stabilité pour les éléments d'un système de représentants des doubles classes modulo S_X. Raisonnant comme dans 2, nous voyons que la double classe d'un élément σ est caractérisée par l'orbite du couple $(X, \sigma(X))$; compte tenu des résultats du a cette orbite est caractérisée par l'entier $n = |X \cap \sigma(X)|$, il y a donc 3 doubles classes.

Le cas $n = 6$ correspond à la double classe S_X, la stabilité par ses éléments est toujours vérifiée.

Le cas $n = 0$. Il existe σ dans M_{22} qui envoie le couple (X, Z) sur le couple (Z, X); σ est alors dans la double classe caractérisée par $n = 0$. En outre $\sigma^2 \in S_X$, la stabilité par σ signifie donc que la restriction à $S_X \cap S_Z$ de l'extension construite est invariante par l'automorphisme de conjugaison par σ (cf. remarque du A). Par construction l'extension est triviale sur $S_X \cap S_Z$, son invariance est donc assurée.

Le cas $n = 2$. Soit σ l'élément de F_Z qui échange les points de A; σ est une involution dont l'ensemble des points fixes est exactement Z. Il est clair que σ conserve l'ensemble $\{X, Y\}$, cependant on ne peut pas avoir $\sigma(X) = X$ car $X \cap Z = \varnothing$ prouve $F_Z \cap S_X = \{\mathrm{Id}\}$ (cf. a), on a donc $\sigma(X) = Y$ et $\sigma(Y) = X$. Ainsi σ appartient à la double classe caractérisée par $n = 2$. Ici encore la stabilité par σ signifie que la restriction à $S_X \cap S_Y$ de l'extension construite est invariante par l'automorphisme de conjugaison par σ. Etudions donc le sous-groupe $S_X \cap S_Y$ et l'action de σ sur ce sous-groupe.

Soit $u \in S_X$, décomposons u en $v \cdot w$ avec $v \in F_X$ et $w \in S_X \cap S_Z$. Si $u \in S_Y$, u conserve $X \cap Y = A$ et, comme v conserve A, w conserve également A; alors w conserve l'ensemble $\{X, Y, T_1, T_2, T_3\}$, mais, comme il conserve Z, il conserve aussi l'ensemble $\{X, Y\}$ et, de $w \in S_X$ on déduit $w \in S_Y$ et, par conséquent, $v \in S_Y$. On a donc $u \in S_Y \Leftrightarrow (v \in S_Y$ et $w \in S_Y)$; il s'ensuit que $S_X \cap S_Y$ est le produit semi-direct de $F_X \cap S_Y$ par $S_X \cap S_Y \cap S_Z$. Comme le morphisme $S_X \cap S_Y \cap S_Z \to A_Z$ est injectif et σ fixe Z points par points on conclut que l'action de σ est triviale sur $S_X \cap S_Y \cap S_Z$. Par contre l'action de σ sur $F_X \cap S_Y$ fournit un morphisme $\lambda: F_X \cap S_Y \to S_X \cap S_Y$. Avec les notations du b, posons $H = \Pi^{-1}(F_X \cap S_Y)$; la restriction à $S_X \cap S_Y$ de l'extension construite est donc:

$$1 \to N \to H \rtimes (S_X \cap S_Y \cap S_Z) \to (F_X \cap S_Y) \rtimes (S_X \cap S_Y \cap S_Z) \to 1.$$

Montrer l'invariance de cette extension par l'action de σ revient à prouver l'existence d'un relèvement de cette action en un automorphisme de $H \times (S_X \cap S_Y \cap S_Z)$ trivial sur N. Pour cela il suffit d'expliciter un relèvement de λ en un morphisme $\bar{\lambda}: H \to H \rtimes (S_X \cap S_Y \cap S_Z)$ se réduisant à l'identité sur N et commutant à l'action de $S_X \cap S_Y \cap S_Z$; dans ce but nous allons expliciter λ.

Remarquons que $\lambda(F_X \cap S_Y) = S_X \cap F_Y$; les deux sous-groupes $F_X \cap S_Y$ et $S_X \cap F_Y$ sont distingués dans $S_X \cap S_Y$ et leur intersection, contenue dans $F_X \cap F_Y$, est triviale. Il s'ensuit que tout élément de $F_X \cap S_Y$ commute avec tout élément de $S_X \cap F_Y$. En particulier, prenons u dans $F_X \cap S_Y$, distinct de Id; u^{-1} et $\lambda(u)$ sont deux involutions qui commutent, en outre $u \notin S_X \cap F_Y$ prouve que $w = u^{-1}\lambda(u)$ est différent de Id. Ainsi w est une involution de $S_X \cap S_Y$. Par ailleurs $\sigma w = \sigma u^{-1} \sigma u \sigma^{-1}$ est, comme σ, une involution; il s'ensuit que σ et w commutent et donc que w conserve l'ensemble des points fixes de σ, c'est-à-dire Z. En conclusion $w \in S_X \cap S_Y \cap S_Z$ et $\lambda(u) = u \cdot w$. Les éléments σ et u agissent sur l'ensemble $\{X, Y, T_1, T_2, T_3\}$, σ fixe T_1, T_2 et T_3 et échange X et Y tandis que u fixe X et Y et conserve donc $\{T_1, T_2, T_3\}$. On en déduit que $w = u^{-1}\sigma u \sigma^{-1}$ fixe T_1, T_2 et T_3. L'image de w dans A_Z est donc une involution qui fixe chacun des ensembles $\{t_i, t_i'\}$ $(i \in \{1, 2, 3\})$, il s'agit par conséquent de l'une des trois permutations $\tau_i = (t_j, t_j')(t_k, t_k')$ $(\{1, 2, 3\} = \{i, j, k\})$. Notons Θ_i l'élément de $S_X \cap S_Z$ dont

l'image dans A_Z est τ_i $(i \in \{1, 2, 3\})$; w est donc l'un des éléments $\Theta_1, \Theta_2, \Theta_3$. Par ailleurs u est l'image par Π d'un élément de H qui n'appartient pas à N; modulo N on peut l'écrire $e_x e_y$ et l'on a donc $u = \langle x, y \rangle$. Mais alors $w = u^{-1}\sigma u \sigma^{-1}$ fixe les points x et y; on en déduit que, si $w = \Theta_i$, u est l'involution $\langle t_i, t_i' \rangle = \alpha_i$. Enfin on a vu (cf. a) que $|X \cap Y| = 2$ implique $|F_X \cap S_Y| = 4$; on conclut donc $F_X \cap S_Y = \{\mathrm{Id}, \alpha_1, \alpha_2, \alpha_3\}$ et λ est donné par $(\forall\, i \in \{1, 2, 3\})\ (\lambda(\alpha_i) = \alpha_i \cdot \Theta_i)$.

Ceci étant on conclut que le groupe H est défini par les générateurs $\varepsilon = -1$ et $a_i = e_{t_i} e_{t_i'}$ $(i \in \{1, 2, 3\})$ et les relations $a_i^2 = \varepsilon$, $\varepsilon^2 = 1$, $a_i a_j = a_j a_i$; le sous-groupe N étant engendré par $a_1 a_2 a_3$. On peut alors définir un morphisme $\bar{\lambda}$ de H dans $H \rtimes (S_X \cap S_Y \cap S_Z)$ par $\bar{\lambda}(\varepsilon) = \varepsilon$, $\bar{\lambda}(a_i) = \varepsilon a_i \Theta_i$ (il suffit de remarquer que Θ_i est une involution qui commute avec a_i et anticommute avec α_j pour $j \neq i$). On vérifie $\bar{\lambda}(a_1 a_2 a_3) = a_1 a_2 a_3$; il s'ensuit que $\bar{\lambda}$ coïncide avec l'identité sur N. Enfin il est clair que $\bar{\lambda}$ est un relèvement de λ qui commute à l'action de $S_X \cap S_Y \cap S_Z$. Ainsi $\bar{\lambda}$ possède toutes les propriétés voulues pour conclure à la stabilité de l'extension par σ et donc par M_{22}.

d. *L'extension est propre.* Prouvons que le groupe dérivé de $\Gamma \rtimes (S_X \cap S_Z)$ contient N; on a, si $x = e_{t_1'} e_{t_2}$: $x \Theta_2 x^{-1} \Theta_2^{-1} = -e_{t_1'} e_{t_2} e_{t_1} e_{t_2} = e_{t_1} e_{t_1'} = a_1$. On vérifie de même que a_2 et a_3 appartiennent au groupe dérivé ainsi donc que le produit $a_1 a_2 a_3$ qui engendre N.

4. *Conséquences pour $\Sigma_2(M_{21})$ et $\Sigma_2(M_{22})$*

Considérons le groupe de Mathieu $G = M_{23}$ comme groupe de permutations d'un ensemble de cardinal 23; soient a et b deux éléments distincts de cet ensemble et H (resp. K) le fixateur de a (resp. du couple (a, b)). On a donc $H \simeq M_{22}$ et $K \simeq M_{21}$. Notons σ un élément de G qui échange les points a et b; on a $K = H \cap \sigma H \sigma^{-1}$. Comme σ^2 fixe a, la conjugaison par σ^{-1} induit un automorphisme de K donc un automorphisme T du groupe de cohomologie $H^2(K, \mathbb{C}^*)$; en outre on a $\sigma^2 \in K$ et T vérifie donc $T^2 = \mathrm{Id}$.

Nous avons vu (cf. III.B.1) que la 2-composante de $H^2(G, \mathbb{C}^*)$ est triviale: par ailleurs l'indice $|G : H| = 23$ est impair. Il s'ensuit, d'après le critère de stabilité, qu'un élément non trivial de la 2-composante de $H^2(H, \mathbb{C}^*)$ n'est jamais stable par les éléments de G. Or, en répétant le raisonnement du 2, on constate, puisque G est deux fois transitif, qu'il y a deux doubles classes dans G modulo H; un système de représentants de ces doubles classes est donné par 1 et σ. Comme la stabilité par 1 est assurée on conclut que, pour Θ non trivial dans la 2-composante de $H^2(H, \mathbb{C}^*)$, on a $\Theta|_K \neq \Theta_K^\sigma$ c'est-à-dire $T(\Theta|_K) \neq \Theta|_K$.

Notons ρ le morphisme de restriction $H^2(H, \mathbb{C}^*) \to H^2(K, \mathbb{C}^*)$ et A (resp. B) la 2-composante de $H^2(H, \mathbb{C}^*)$ (resp. $H^2(K, \mathbb{C}^*)$). Nous avons vu

(cf. III.A.2.c) que $\Sigma_2(M_{21}) \to \Sigma_2(M_{22})$ est surjectif, cela prouve que ρ est injectif sur A. Par ailleurs nous savons (cf. III.B.1) que B est le produit d'au plus deux composantes cycliques, chacune étant d'ordre au plus 4.

Le résultat du 3 montre que A possède un élément Θ d'ordre 4; comme ρ est injectif sur A, $\rho(\Theta)$ est encore d'ordre 4. Enfin T induit un automorphisme involutif de B et nous venons de montrer que $\rho(A)$ ne possède aucun point fixe non trivial de cet automorphisme.

Notons C le sous-groupe de B engendré par $x = \rho(\Theta)$; on a $T(x^2) \neq x^2$, ce qui prouve $T(x^2) \notin C$ et donc, dans B/C l'image de $T(x)$ est d'ordre 4. Ainsi B/C est d'ordre au moins 4 et B d'ordre au moins 16. La seule possibilité est donc $B = C \times T(C) \simeq (\mathbb{Z}/4\mathbb{Z})^2$. Le groupe des points fixes de T est formé par les $(x, T(x))$ pour $x \in C$. Comme $\rho(A) \supset C$ et rencontre ce groupe de façon triviale on conclut $\rho(A) = C$ et donc, puisque ρ est injectif sur A, $A \simeq \mathbb{Z}/4\mathbb{Z}$. En passant aux groupes duaux on a donc $\Sigma_2(M_{21}) \simeq (\mathbb{Z}/4\mathbb{Z})^2$ et $\Sigma_2(M_{22}) \simeq \mathbb{Z}/4\mathbb{Z}$.

V. Récapitulation des Résultats

Nous pouvons récapituler les résultats dans le tableau suivant où nous donnons, pour G groupe de Mathieu, la décomposition en groupes cycliques de $\Sigma(G)$ (Nous avons noté (n) le groupe cyclique d'ordre n).

G	M_{11}	M_{12}	M_{21}	M_{22}	M_{23}	M_{24}
$\Sigma(G)$	(1)	(2)	(4)(4)(3)	(4)(3)	(1)	(1)

Appendices

A. *Extensions centrales de A_n par $\mathbb{Z}/2\mathbb{Z}$*

Considérons la représentation évidente du groupe alterné A_n dans le groupe orthogonal $O^+(n)$. Le groupe des spineurs fournit une extension centrale:

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \mathrm{Spin}(n) \to O^+(n) \to 1.$$

Par image réciproque on obtient donc une extension centrale de A_n.

Considérons $\mathrm{Spin}(n)$ comme plongé dans l'algèbre de Clifford de $\mathbb{R}^n$ et supposons $n \geqslant 4$. L'involution $(1, 2)(3, 4)$ de A_n peut alors se relever dans $\mathrm{Spin}(n)$ en $x = (e_1 - e_2)(e_3 - e_4)/2$ et l'on a $x^2 = -1$. Ainsi, pour l'extension de A_n obtenue, il y a des involutions qui se relèvent en élément d'ordre 4

(pour $n \leqslant 7$, c'est le cas de toutes les involutions puisqu'elles sont toutes conjuguées entre elles); il s'ensuit que cette extension n'est pas triviale.

Pour montrer que l'extension construite est la seule extension non triviale de A_n par $\mathbb{Z}/2\mathbb{Z}$ nous devons prouver $H^2(A_n, \mathbb{Z}/2) \simeq \mathbb{Z}/2\mathbb{Z}$. Comme l'on a $\mathrm{Ext}^1(A_n/[A_n, A_n], \mathbb{Z}/2\mathbb{Z}) = 0$ pour tout n (pour $n \neq 3, 4$ cela vient de $[A_n, A_n] = A_n$; pour $n = 3$ ou 4, cela vient de $A_n/[A_n, A_n] \simeq \mathbb{Z}/3\mathbb{Z}$), cet isomorphisme est une conséquence de la relation: $\Sigma_2(A_n) \simeq \mathbb{Z}/2\mathbb{Z}$ pour $n \geqslant 4$ (cf. [7]).

B. *Estimation de* $H^1[S_{X,a}, \mathrm{Hom}(F_X, \mathbb{C}^*)]$

L'étude de M_{21} et M_{23} nous a amenés à évaluer le groupe de cohomologie $H^1[S_{X,a}, \hat{F}_X]$ où l'on a $S_{X,a} \simeq A_5$ pour M_{21}, $S_{X,a} \simeq A_7$ pour M_{23} et $\hat{F}_X \simeq F_X \simeq (\mathbb{Z}/2\mathbb{Z})^4$. Nous avons donc à évaluer $H^1[A_n, M]$ où $n = 5$ ou $n = 7$, M est un A_n-module de groupe sous-jacent $(\mathbb{Z}/2\mathbb{Z})^4$; on a évidemment $H^1[A_n, M] \simeq (\mathbb{Z}/2\mathbb{Z})^p$ il s'agit d'évaluer p.

1. *Pour* $n = 5$ *on a* $p \leqslant 2$

Lorsque M est le module trivial (ce qui n'est d'ailleurs pas le cas dans la situation étudiée en III.B.1) on a $H^1[A_5, M] \simeq \mathrm{Hom}[A_5, (\mathbb{Z}/2\mathbb{Z})^4] = 0$, puisque A_5 est simple non commutatif. Nous pouvons donc supposer le module M non trivial; le morphisme $A_5 \to \mathrm{Aut}\, M \simeq GL(2, 4)$ est donc injectif.

Soit σ un élément d'ordre 5 de A_5. La décomposition du polynome $X^5 - 1$ sur le corps $\mathbb{F}_2$ est $(X-1)(X^4 + X^3 + X^2 + X + 1)$; comme l'action de σ est non triviale, son polynome minimal est $X^4 + X^3 + X^2 + X + 1$ et σ n'a donc aucun point fixe non trivial. Il s'ensuit que l'espace des cobords $\varphi(\alpha) = x - \alpha \cdot x$ est isomorphe à M par $\varphi \to \varphi(\sigma)$; ainsi tout cocycle est cohomologue à un cocycle et un seul qui s'annule sur σ. L'espace Z^1_σ de ces cocycles est donc isomorphe à $H^1[A_5, M]$. Soit τ un élément d'ordre 2 de A_5. Notons N_τ l'espace des x tels que $x + \tau \cdot x = 0$; il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^q$.

Comme, dans A_5, il n'y a qu'une classe d'involutions, l'entier q ne dépend pas de τ. Si l'on a $q \geqslant 3$, prenons deux involutions τ et τ' qui engendrent un élément d'ordre 5 (par exemple $(1, 2)(3, 4)$ et $(1, 3)(4, 5)$). L'intersection $N_\tau \cap N_{\tau'}$ n'est alors pas triviale; il existe donc un élément non nul de M invariant par τ et par τ' (la caractéristique est 2) donc par tous les éléments qu'elles engendrent. Cela contredit le résultat obtenu pour les éléments d'ordre 5; on a donc $q \leqslant 2$.

Raisonnons alors avec un couple (σ, τ), σ d'ordre 5, τ d'ordre 2, qui engendre A_5. Pour tout cocycle φ, la condition de cocycle $\varphi(\alpha\beta) = \varphi(\alpha) + \alpha\varphi(\beta)$ prouve que l'ensemble $\{\alpha \mid \varphi(\alpha) = 0\}$ est un sous-groupe de A_5. Il s'ensuit que le morphisme $\varphi \to \varphi(\tau)$ de Z^1_σ dans M est injectif. Or, comme τ

TABLE I

M_{11}	h	Π	M_{12}	h	Π	M_{22}	h	Π	M_{24}	h	Π
1	h_{11}	12	1	h_{12}	12	1	h_{22}	22	1	h_{24}	24
2^4	48	4	2^4	192	4	2^8	384	6	2^8	$21 \cdot 2^{10}$	8
4^2	8	0	4^2	32	4	3^6	36	4	3^6	1080	6
3^3	18	3	3^3	54	3	5^4	5	2	5^4	60	4
5^2	5	2	5^2	10	2	$4^4 \cdot 2^2$	16	2	$4^4 \cdot 2^2$	128	4
$8 \cdot 2$	8	0	$8 \cdot 2$	8	2	$4^4 \cdot 2^2$	32	2	7^3	42	3
$8 \cdot 2$	8	0	$6 \cdot 3 \cdot 2$	6	1	7^3	7	1	7^3	42	3
$6 \cdot 3 \cdot 2$	6	1	11	11	1	7^3	7	1	$8^4 \cdot 4 \cdot 2$	16	2
11	11	1	11	11	1	$8^2 \cdot 4 \cdot 2$	8	0	$6^2 \cdot 3^2 \cdot 2^2$	24	2
11	11	1	2^6	240	0	$6^2 \cdot 3^2 \cdot 2^2$	12	0	11^2	11	2
			$10 \cdot 2$	10	0	11^2	11	0	$15 \cdot 5 \cdot 3$	15	1
			$4^2 \cdot 2^2$	32	0	11^2	11	0	$15 \cdot 5 \cdot 3$	15	1
			3^4	36	0				$14 \cdot 7 \cdot 2$	14	1
			6^2	12	0				$14 \cdot 7 \cdot 2$	14	1
			$8 \cdot 4$	8	0				23	23	1
									23	23	1
									10 autres classes		0
$h_{11} = \|M_{11}\| = 7920$			$h_{12} = \|M_{12}\| = 95\,040$			$h_{22} = \|M_{22}\| = 443\,520$			$h_{24} = \|M_{24}\| = 244\,823\,040$		

est d'ordre 2, on a $0 = \varphi(\tau^2) = \varphi(\tau) + \tau \cdot \varphi(\tau)$ d'où $\varphi(\tau) \in N_\tau$. Ainsi $Z^1_\sigma \simeq H^1[A_5, M] \simeq (\mathbb{Z}/2\mathbb{Z})^p$ s'injecte dans $N_\tau \simeq (\mathbb{Z}/2\mathbb{Z})^q$; on a donc $p \leqslant q \leqslant 2$.

2. *Pour $n = 7$ on a $p = 0$*

Ici encore le résultat est évident lorsque M est le A_7-module trivial. Dans le cas général le résultat peut s'obtenir encore par des calculs de cocycles sur les générateurs de A_7. Nous allons ici utiliser une autre méthode consistant à interpréter géométriquement $H^1(A_7, M)$.

Posons $N = \mathbb{Z}/2 \times M$. Si φ est un cocycle dans $Z^1(A_7, M)$ on constate que l'on peut définir une structure de A_7-module sur N par $\sigma(\lambda, x) = (\lambda, \sigma \cdot x + \lambda\varphi(\sigma))$. L'action de A_7 laisse stable l'hyperplan $\lambda = 0$ ainsi donc que son complémentaire X qui est de cardinal 16. Soit σ un élément d'ordre 5 de A_7, l'ensemble des points de X fixés par σ a un cardinal qui est congru à 16 modulo 5 et qui est du type 2^n (puisque l'action de σ est linéaire). Si ce cardinal est 16 l'action de σ et donc de A_7 est triviale; sinon la seule possibilité pour ce cardinal est 1. Dans ce cas l'action de σ sur X fait alors apparaître un point fixe $(1, y)$ et 3 orbites de cardinal 5. L'orbite de $(1, y)$ sous l'action de A_7 est donc de cardinal 1, 6, 11 ou 16. Les possibilités 11 et 16 sont exclues car ces nombres ne divisent pas l'ordre de A_7; la possibilité 6 est exclue car elle donnerait un morphisme non trivial de A_7 dans S_6. En conclusion $(1, y)$ est fixé par tous les éléments de A_7 ce qui s'écrit: $(\forall\, \sigma \in A_7)$ $y = \sigma y + \varphi(\sigma)$ ou encore $\varphi(\sigma) = y - \sigma(y)$ ce qui prouve que φ est un cobord. Il s'ensuit $H^1(A_7, M) = 0$.

C. *Tables de caractères*

Pour les groupes M_{11}, M_{12}, M_{22} et M_{24} nous donnons, pour chaque classe de conjugaison, sur la première colonne le type de la décomposition en cycles d'un élément de la classe (pour la représentation usuelle du groupe comme groupe de permutations), sur la deuxième colonne l'ordre du centralisateur d'un élément de la classe (c'est-à-dire la valeur du caractère h de l'action du groupe sur lui-même par automorphismes intérieurs), sur la dernière colonne la valeur du caractère Π qui intervient dans l'utilisation de l'argument d'induction en III.

REFERENCES

1. N. BURGOYNE ET P. FONG, The Schur multipliers of the Mathieu groups, *Nagoya Math. J.* **27** (1966), 733–745.
2. N. BURGOYNE ET P. FONG, A correction to "The Schur multipliers of the Mathieu groups," *Nagoya Math. J.* **31** (1968), 297–304.
3. H. CARTAN ET S. EILENBERG, "Homological Algebra," Princeton Univ. Press, Princeton, N.J., 1956.

4. J. H. CONWAY, Three lectures on exceptional groups, *in* "Finite simple groups" (M. B. Powell et G. Higman, Eds.), Academic Press, New York, 1971.
5. H. S. M. COXETER, Twelve points in $PG(5, 3)$ with 95040 self-transformations, *Proc. Roy. Soc. A* **247** (1958), 279–293.
6. H. LÜNEBURG, "Transitive Enveiterungen endlicher Permutationsgruppen," Lecture Notes in Mathematics No. 84, Springer-Verlag, New York/Berlin, 1969.
7. I. SCHUR, Über die Darstellung des symetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen, *J. Math. (Crelle)* **139** (1911), 155–250.
8. I. SCHUR, Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, *J. Math. (Crelle)* **132** (1907), 85–137.
9. E. WITT, Über Steinersche System, *Abh. Math. Sem. Univ. Hamburg* **12** (1938), 265–274.