Astérisque

JACQUES TITS

Le module du « Moonshine »

Astérisque, tome 152-153 (1987), Séminaire Bourbaki,
exp. nº 684, p. 285-303

<http://www.numdam.org/item?id=SB_1986-1987__29__285_0>

© Société mathématique de France, 1987, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI
39ème année, 1986-87, n° 684

Juin 1987

LE MODULE DU "MOONSHINE"

[d'après I. Frenkel, J. Lepowsky et A. Meurman]

par Jacques TITS

1. INTRODUCTION : LE "MOONSHINE"

Cet exposé a pour objet le groupe fini simple d'ordre

$$2^{46} . 3^{20} . 5^{9} . 7^{6} . 11^{2} . 13^{3} . 17 . 19 . 23 . 29 . 31 . 41 . 47 . 59 . 71$$

construit par R. Griess en 1981 (cf. [Gr], article exposé au Séminaire Bourbaki de novembre 1983 [Ti 1]), huit ans après que son existence ait été prévue simultanément par B. Fischer et R. Griess. Ici, ce groupe sera appelé "Monstre", ou "groupe de Griess - Fischer", et noté $\mathbb{M}$. Il est plus que probable que c'est le seul groupe fini simple ayant l'ordre indiqué, mais cela n'est "pas tout à fait démontré". Ce qui le rend particulièrement intéressant n'est pas seulement qu'il soit le plus gros des groupes finis simples sporadiques (c'est-à-dire n'appartenant pas aux séries infinies bien connues) mais, plus encore, un ensemble de propriétés arithmétiques assez mystérieuses, collectivement baptisées "Moonshine" (= "fariboles", selon Harrap's) par J.H. Conway. Rappelons en quoi consiste ce phénomène, en renvoyant à [CN] et [Br] pour plus de détails.

La plus petite représentation linéaire fidèle de $\mathbb{M}$ en caractéristique zéro a pour degré 196883 , ce qui est, à une unité près, le coefficient de q dans l'invariant modulaire

$$j(z) = q^{-1} + 744 + 196884\, q + \dots \qquad (q = e^{2\pi i z}) .$$

Inspiré par cette remarque, due à McKay, J. Thompson observe que les deux ou trois coefficients suivants sont, eux aussi, sommes d'un petit nombre de degrés de représentations irréductibles de $\mathbb{M}$ (par exemple, le coefficient de q^2 est la somme des dimensions des trois plus petits $\mathbb{M}$-modules simples), ce qui l'amène à conjecturer l'existence d'un $\mathbb{M}$-module gradué $V = \sum_{i=-1}^{\infty} V_i$ "naturel" dont la série de Poincaré $\Sigma \dim V_i . q^i$ serait $j - 744$. Pour caractériser un tel module gradué V à isomorphisme près, il suffit de donner, pour chaque élément g de $\mathbb{M}$, la série $\Sigma(\mathrm{Tr}\, g|_{V_i}) . q^i$ (dont la série de Poincaré ci-dessus est le cas particulier pour $g = 1$), série que nous noterons $\mathrm{Tr}(g \mid V ; q)$ ou, plus simple-

ment, $\mathrm{Tr}(g \mid V)$, ou encore, s'il n'y a pas d'hésitation possible sur le module gradué que l'on considère, $\mathrm{Tr}(g\,;q)$. A chaque élément g de $\mathbb{M}$ devrait donc, selon Thompson, être naturellement associée une série $\mathrm{Tr}(g \mid V)$, qui ne dépend que de la classe de conjugaison de g . Si les premières composantes V_i de V n'ont qu'un petit nombre de composantes irréductibles, la relation $\mathrm{Tr}(1 \mid V\,; e^{2\pi i z}) = j - 744$ détermine (ou, au pire, ne laisse que très peu de choix pour) les V_i en question, donc aussi les premiers coefficients de la série $\mathrm{Tr}(g \mid V)$ pour tout g . Partant de là, de la table des caractères du Monstre (cf. [ATLAS], p. 220) et de l'idée préconçue, fortifiée par les premiers essais, que les $\mathrm{Tr}(g \mid V)$ doivent être les développements à l'infini de fonctions modulaires simples, J.H. Conway et S. Norton ([CN]) parviennent à déterminer pour tout $g \in \mathbb{M}$ une fonction modulaire candidate, notons-la μ_g . Ces fonctions μ_g ont des propriétés remarquables, qui sont l'essence du "Moonshine" : par exemple, elles sont toutes des uniformisantes de courbes modulaires de genre zéro, et l'on a une description assez satisfaisante des courbes modulaires qui correspondent effectivement à des classes de conjugaison de $\mathbb{M}$; en particulier, les résultats obtenus donnent de la substance (sans toutefois l'expliquer vraiment) à une remarque ancienne de A. Ogg sur les nombres premiers qui interviennent dans l'ordre du Monstre (cf. [CN], p. 308). Reste à vérifier que les relations

$$\mathrm{Tr}(g \mid V\,; e^{2\pi i z}) = \mu_g \tag{1}$$

définissent bien un $\mathbb{M}$-module gradué. Cela a été fait par A. Atkin, P. Fong et S. Smith suivant une méthode imaginée, elle aussi, par J. Thompson, utilisant le critère de Brauer pour qu'une fonction centrale donnée sur un groupe soit un caractère virtuel, ainsi que des relations de congruence satisfaites par les coefficients des fonctions modulaires considérées. Ces résultats sont jusqu'ici restés inédits et peut-être même non écrits ; on trouvera cependant un bref exposé de la méthode dans [Fo].

Cela établit l'existence d'un module V satisfaisant à (1), mais n'en donne pas une construction "naturelle". Dans [FLM 1], qui fait l'objet du présent exposé, I. Frenkel, J. Lepowsky et A. Meurman (appelés FLM dans la suite) construisent *effectivement* un $\mathbb{M}$-module gradué, que nous noterons encore V , tel que $\mathrm{Tr}(1 \mid V\,; e^{2\pi i z}) = j - 744$. La définition tout à fait explicite de ce module permet de calculer facilement la série $\mathrm{Tr}(g \mid V)$ *pour certains éléments* g *de* $\mathbb{M}$, à savoir ceux qui appartiennent à un certain sous-groupe C (voir plus loin) ; les expressions que l'on trouve représentent bien des fonctions modulaires mais diffèrent dans la forme de celles proposées par [CN]. Leur égalité, que l'on conjecture évidemment, implique des identités non triviales entre fonctions modulaires. A ma connaissance, ces identités n'ont pas été vérifiées (sauf pour quel-

ques éléments g très particuliers : cf. [FLM 2], p. 268 et [Ti 2], p. 104) et, par ailleurs, on ne sait rien des séries $\mathrm{Tr}(g \mid V)$ lorsque g n'appartient pas à C, pas même si ce sont des fonctions modulaires. Si la construction de FLM a, jusqu'ici, apporté peu de lumière sur les aspects purement arithmétiques du "Moonshine" (notamment sur le rôle surprenant joué par les courbes modulaires de genre zéro), en revanche, elle fournit une approche intéressante, plus conceptuelle, de la preuve d'existence du Monstre due à R. Griess (et déjà quelque peu simplifiée entretemps : cf. [Ti 1], [Co]).

2. INTRODUCTION (SUITE) : LES GRANDES LIGNES DE LA CONSTRUCTION

Nous utiliserons l'abus de notation suivant, en usage dans la théorie des groupes finis : $G \cong X_1 . X_2 \ldots X_m$ signifie que G est un groupe possédant une suite de composition distinguée $(G = G_m, G_{m-1}, \ldots, G_0 = \{1\})$ dont le quotient G_i / G_{i-1} est isomorphe à X_i pour $i = m, m-1, \ldots, 1$; dans cette écriture, $(\mathbb{Z}/n\mathbb{Z})^s$ est souvent remplacé par n^s et $p^{s+s'+s''+\ldots}$ est synonyme de $p^s . p^{s'} . p^{s''} \ldots$ (ainsi, il ne faut pas confondre 2^3, groupe abélien élémentaire d'ordre 8, et 2^{1+2}, qui représente n'importe quel groupe non cyclique d'ordre 8 et même presque toujours, par convention tacite, un groupe non abélien). Soient Λ le réseau de Leech, doté de son produit scalaire naturel, et $Co_1 = \mathrm{Aut}\,\Lambda / \{\pm 1\}$ (resp. M_{24}) le plus grand des groupes simples de Conway (resp. Mathieu).

Dans [FLM 1], comme dans l'article original de Griess [Gr], $\mathbb{M}$ est obtenu comme le groupe engendré par un sous-groupe $C \cong 2^{1+24} . Co_1$ et un élément σ d'ordre 2. Dans la variante de [Gr] proposée à ce même Séminaire ([Ti 1]), σ a été remplacé par un groupe de type $2^{2+11+22} . (\mathfrak{S}_3 \times M_{24})$, où $\mathfrak{S}_3$ est le groupe symétrique d'ordre 6 ; ce groupe, noté $\hat{D}$ dans [Ti 1], sera ici désigné par D. Cette présentation, plus symétrique, débarrasse la construction de certains choix arbitraires ou non expliqués, ce qui met en évidence son unicité et simplifie les formules. Pour l'exposé de [FLM 1], nous suivrons la même démarche avec, espérons-le, des effets analogues (dans [FLM 1], l'unicité de la construction, à isomorphisme près, est loin de sauter aux yeux[1]).

Il s'agit donc de construire un certain $\langle C,D \rangle$-module gradué V. Il s'avère que les actions de C et D sur V se voient mieux dans des extensions conve-

---

[1] Le point de vue de [FLM 3] est plus invariant et, à certains égards, plus proche de celui adopté ici. Je remercie J. Lepowsky de m'avoir communiqué, au fur et à mesure de sa progression, le manuscrit de [FLM 3]. Les chapitres qui concernent le plus le présent exposé me sont parvenus trop tard pour que je puisse en tenir pleinement compte, mais ils m'ont néanmoins permis de mieux comprendre certains aspects de la construction, et notamment l'action du groupe $\tilde{D}$ sur l'espace ${}_0V''$ (cf. §8).

nables V' et V'' de V, où $V \subset V' \subset V''$. Plus exactement, V' est un $\tilde{C}$-module gradué, où $\tilde{C}$ est extension centrale de C par un groupe $\langle\tilde{z}\rangle$ d'ordre 2, et V est l'espace des points fixes de $\tilde{z}$ dans V' (espace sur lequel opère donc $\tilde{C}/\langle\tilde{z}\rangle = C$). Quant à V'', c'est un $\tilde{D}$-module gradué, où $\tilde{D}$ est un groupe de type $2^{3+3+12+24}.(\mathfrak{S}_3 \times M_{24})$ possédant un sous-groupe abélien élémentaire Z d'ordre 4 dont V est l'espace des points fixes et tel que le quotient par Z du normalisateur de Z dans $\tilde{D}$, quotient qui opère fidèlement sur V, possède D comme sous-groupe (aisément caractérisable) d'indice 16. Dans V'', V' est l'espace des points fixes d'un élément d'ordre 2 de Z et Z induit $\langle\tilde{z}\rangle$ sur V'.

Le groupe $\tilde{D}$ est extension de $\mathfrak{S}_3$ par un groupe $\tilde{D}_0 \cong 2^{3+3+12+24}.M_{24}$, et le module V'' se décompose naturellement en une somme directe de quatre facteurs ${}_jV''$ $(j = 0,1,2,3)$, stables par $\tilde{D}_0$: ${}_0V''$ est stable par $\tilde{D}$ tandis que ${}_1V''$, ${}_2V''$ et ${}_3V''$ sont permutés symétriquement par $\tilde{D}$ (ou, si l'on peut dire, par son quotient $\mathfrak{S}_3$). La description des espaces gradués V'' et V' est aisée (§ 4) et leurs structures respectives de $\tilde{C}$- et de $\tilde{D}_0$-modules sont assez évidentes (§§ 7 et 8). Mais il reste, et c'est là le point difficile de la construction, à prolonger l'action de $\tilde{D}_0$ sur V'' en une action de $\tilde{D}$. C'est ici qu'interviennent les "opérateurs de sommet" ("vertex operators" : cf. § 5) et la théorie de Kac-Moody. L'idée est la suivante : on considère quatre algèbres de Lie de dimension infinie ${}_j\hat{\mathfrak{G}}$ $(j = 0,1,2,3)$ opérant respectivement sur les ${}_jV''$ (cf. § 5) et permutées entre elles (vues comme algèbres d'opérateurs) par le groupe $\tilde{D}$. Les ${}_j\hat{\mathfrak{G}}$ sont des algèbres de Kac-Moody de type affine (en un sens un peu élargi), extensions centrales de $\mathfrak{sl}_2(\mathbb{C}[t,t^{-1}])^{24}$ par $\mathbb{C}$. Leur action sur les ${}_iV''$ s'obtient par application de deux procédés de construction, dus à J. Lepowsky, R. Wilson ([LW]), I. Frenkel et V. Kac ([FK]) des représentations "de base" de l'algèbre de Kac-Moody de type $\tilde{A}_1$. Pour $j = 1,2,3$, la composante ${}_jV''_{\frac{1}{2}}$ de degré $\frac{1}{2}$ de ${}_jV''$ est un espace vectoriel de dimension 2^{12} qui engendre ${}_jV''$ en tant que ${}_j\hat{\mathfrak{G}}$-module (de la même façon qu'un module simple à poids minimum pour une algèbre de Kac-Moody est engendré par les vecteurs non nuls de poids minimum). Pour décrire l'opération de $\tilde{D}$ sur ${}_1V'' \oplus {}_2V'' \oplus {}_3V''$, il suffit donc de donner son action sur l'espace ${}_1V''_{\frac{1}{2}} \oplus {}_2V''_{\frac{1}{2}} \oplus {}_3V''_{\frac{1}{2}}$, laquelle est de nature essentiellement combinatoire (cf. § 8), et son action sur l'algèbre ${}_1\hat{\mathfrak{G}} \oplus {}_2\hat{\mathfrak{G}} \oplus {}_3\hat{\mathfrak{G}}$. L'opération de $\tilde{D}$ sur ${}_0V''$ se décrit par un procédé assez différent (bien qu'utilisant aussi l'action de ${}_0G$ sur ${}_0V''$), plus malaisé à esquisser en quelques mots, mais en fait plus élémentaire (cf. §8, remarque 2)).

Une fois obtenues (par restriction à partir de V' et V'') les opérations des groupes C et D sur V, on doit encore montrer que le sous-groupe $\langle C,D\rangle$ de $GL(V)$ engendré par C et D est bien le groupe de Griess-Fischer. Pour cela, on constate d'abord que la composante homogène V_1 de degré 1 de V se

décompose sous l'action de $\langle C,D\rangle$ en somme directe de $\mathbb{C}$ et d'un espace vectoriel B de dimension 196883, lequel s'identifie canoniquement à l'espace noté B dans [Ti 1], tensorisé par $\mathbb{C}$. On vérifie en outre que les groupes C et D induisent sur B les groupes notés C et $\hat{D}$ dans [Ti 1]. Il s'ensuit, d'après le théorème fondamental de Griess (sous la forme exposée dans [Ti 1], § 5), que la restriction de $\langle C,D\rangle$ à V_1 est bien le groupe $\mathbb{M}$ voulu. Considérant alors l'"affinisé" de V_1, c'est-à-dire l'espace $\hat{V}_1 = V_1 \otimes \mathbb{C}[t,t^{-1}] \oplus \mathbb{C}$, FLM montrent qu'il "opère" sur V, c'est-à-dire qu'il existe une application linéaire $\rho : \hat{V}_1 \longrightarrow \mathrm{End}\, V$ compatible avec les opérations de C et D sur V_1 (donc $\hat{V}_1$) et V ; de plus, ρ est irréductible, c'est-à-dire que $\rho(\hat{V}_1)$ ne laisse stable aucun sous-espace propre non nul de V. Cela implique manifestement que $\langle C,D\rangle$ opère fidèlement sur V_1, donc est isomorphe à $\mathbb{M}$. Signalons qu'à nouveau, la construction de ρ fait intervenir de façon essentielle les opérateurs de sommet.

En fait, FLM considère $\hat{V}_1$ non seulement en tant qu'espace vectoriel mais comme une algèbre non associative graduée, dont ils démontrent que ρ est une "représentation", en un sens précisé dans [FLM 1], § 4. L'algèbre en question est, à peu de chose près, l'"affinisée" de l'algèbre de Griess-Norton, jouant un rôle important dans la preuve par Griess de l'existence du Monstre. (La notion d'"affinisée" d'une algèbre non associative provient de la théorie de Kac-Moody ; on en trouve la définition - sans toutefois que l'expression soit explicitement utilisée - dans les premières lignes du § 4 de [FLM 1]. Le cas particulier de l'algèbre $\mathfrak{G}$ définie au § 6 ci-dessous laisse deviner la définition générale. Pour l'algèbre $\hat{V}_1$, voir par exemple [FLM 2], § 13, ou [Ti 1], p. 119, lignes 4 à 9.) Je ne sais pas si la structure d'algèbre de $\hat{V}_1$ est indispensable pour prouver l'existence d'un homomorphisme ρ ayant les propriétés requises.

Malgré son importance pour la démonstration du résultat final (i.e. le fait que $\langle C,D\rangle$ opère fidèlement sur V_1, donc est isomorphe à $\mathbb{M}$), cette dernière partie de la construction de FLM, à savoir l'existence de ρ, ne sera pas développée plus avant dans cet exposé : outre que cela aurait pour effet de l'allonger au-delà du raisonnable, les indications fournies par [FLM 1] et [FLM 2] sur ce point sont peu détaillées et je n'ai pas fait l'effort d'en déduire une démonstration complète.

Pour conclure cette introduction, signalons que, comme on a d'ailleurs déjà pu s'en rendre compte, les notations utilisées ici ne sont pas toujours conformes à celles de [Ti 1], et encore moins à celles de [FLM 1].

Je remercie M. Broué et R. Griess pour des remarques qui m'ont été très utiles dans la mise au point de ce texte.

3. RÉSEAUX, EXTENSIONS CENTRALES ET 2-GROUPES

Soit S un ensemble à 24 éléments ; dans l'espace vectoriel $\mathbb{F}_2^S$, identifié à l'ensemble des parties de S, on se donne un sous-espace G de dimension 12 tel que le cardinal (comme partie de S) de tout élément de G soit égal à 0, 8, 12, 16 ou 24. On sait qu'un tel sous-espace G, appelé "code de Golay", existe et est unique à une permutation de S près.

Soient $\mathcal{H}$ un espace vectoriel complexe de dimension 24, E une double base de $\mathcal{H}$ (c'est-à-dire une partie de $\mathcal{H}$ de cardinal 48, contenant une base de $\mathcal{H}$ et égale à son opposée $-E$) et $\sigma : E \longrightarrow S$ une application telle que, pour tout $s \in S$, $\sigma^{-1}(s)$ soit une paire d'éléments opposés de E. Le groupe $\mathbb{F}_2^S$, donc aussi G, opère sur E de façon évidente : si $T \in \mathbb{F}_2^S$ et $e \in E$, on pose $Te = -e$ ou e selon que $\sigma(e)$ appartient ou non à T. Chaque orbite de G dans l'ensemble des bases de $\mathcal{H}$ extraites de E est un espace homogène principal sous G ; on en choisit une que l'on note $\mathcal{B}$ (elles sont toutes conjuguées sous l'action de $\mathbb{F}_2^S$). Pour toute famille F d'éléments de E, nous désignons par ΣF la somme dans $\mathcal{H}$ des éléments de F. Notons $\langle\ ,\ \rangle$ la forme bilinéaire symétrique dans $\mathcal{H}$ définie par $\langle e,e\rangle = 2$ et $\langle e,e'\rangle = 0$ pour $e \in E$ et $e' \in E - \{\pm e\}$. (On prendra garde au fait que le symbole $\langle\ \rangle$ signifie tantôt "produit scalaire", tantôt "groupe engendré par" ; le contexte devrait écarter toute possibilité de confusion.) Pour tout réseau $X \subset \mathcal{H}$ (sous-groupe de $\mathcal{H}$ engendré par une base), l'ensemble $X^{\perp} = \{h \in \mathcal{H} \mid \langle h,X\rangle \subset \mathbb{Z}\}$ est un réseau qui s'identifie au $\mathbb{Z}$-dual de X.

Notons $\mathcal{B}'$ l'ensemble des éléments de $\mathcal{H}$ de la forme $\frac{1}{4}\Sigma b$ avec $b \in \mathcal{B}$, et définissons K (lire : "kappa") comme le réseau engendré par E et $\mathcal{B}'$. On vérifie aisément que $K/K^{\perp}$ est un groupe abélien élémentaire d'ordre 4 engendré par l'image commune ε des éléments de E et l'image commune β des éléments de $\mathcal{B}'$. L'image réciproque de $\langle\varepsilon\beta\rangle$ dans K est un sous-réseau d'indice 2 de K que nous notons Λ ; c'est le *réseau de Leech*. On a $\Lambda^{\perp} = \Lambda$. L'intersection de K avec le réseau engendré par $\frac{1}{2}E$ est aussi un sous-réseau d'indice 2 de K, noté K_0. Soit K_1 la classe latérale non triviale de K_0 dans K ; on a donc $K = K_0 \cup K_1$ et $K_1 = K_0 + b$ pour tout $b \in \mathcal{B}'$.

Il existe une et une seule forme alternée $K \times K \longrightarrow \langle i\rangle$ (où i est la racine carrée de -1 bien connue, d'où $\langle i\rangle \cong \mathbb{Z}/4\mathbb{Z}$) telle que $[k,k'] = (-1)^{\langle k,k'\rangle}$ si $\langle k,k'\rangle$ est entier et $[e,b] = i^{\langle e,b\rangle}$ si $e \in E$ et $b \in \mathcal{B}'$. Soit

$$1 \longrightarrow \langle i\rangle \longrightarrow \tilde{K} \xrightarrow{\pi} K \longrightarrow 1$$

l'extension centrale définie par cette forme alternée, c'est-à-dire telle que le commutateur de deux éléments k et k' de K soit $[\pi(k), \pi(k')]$. [N.B. Les groupes $\tilde{K}$ et K sont respectivement notés multiplicativement et additivement,

d'où certaines bizarreries dans les formules que nous allons écrire.] Le centre de K est le groupe $\pi^{-1}(2K^{\perp}) = \langle i\rangle \times (2K^{\perp})$. On a un homomorphisme canonique $\pi' : 4K \longrightarrow \pi^{-1}(4K)$, section (c'est-à-dire, inverse à droite) de la restriction de π à $\pi^{-1}(4K)$, homomorphisme défini par $\pi'(k) = \tilde{k}^4 . (-1)^{\langle k,k\rangle}$, où $\tilde{k}$ est un élément quelconque de $\pi^{-1}(k)$. Il peut être prolongé en un homomorphisme $2K^{\perp} \longrightarrow \pi^{-1}(2K^{\perp})$, section de la restriction de π au centre de $\tilde{K}$, et deux tels prolongements sont conjugués par un automorphisme de $\tilde{K}$ fixant $\langle i\rangle$ et K . Choisissons-en un et notons-le encore π' . Ce choix "épingle" $\tilde{K}$ au sens suivant : les automorphismes de $\tilde{K}$ fixant $\langle i\rangle$ et $\pi'(2K^{\perp})$ sont exactement les automorphismes intérieurs.

Faisons encore le choix d'un prolongement de π' en un homomorphisme - lui aussi noté π' - de 2Λ dans $\pi^{-1}(2\Lambda)$, section de la restriction de π à $\pi^{-1}(2\Lambda)$: il y a deux tels prolongements, conjugués l'un de l'autre par n'importe quel élément de $\tilde{K} - \pi^{-1}(\Lambda)$. Il est immédiat que l'ensemble $\tilde{\Lambda}$ des éléments $\tilde{k}$ de $\pi^{-1}(\Lambda)$ tels que, posant $k = \pi(\tilde{k})$, on ait $\tilde{k}^2 = \pi'(2k) . (-1)^{\langle k,k\rangle}$ est un sous-groupe de $\tilde{K}$, et que la restriction de π à $\tilde{\Lambda}$ définit une extension centrale

$$1 \longrightarrow \langle -1\rangle \longrightarrow \tilde{\Lambda} \longrightarrow \Lambda \longrightarrow 1$$

correspondant à la forme alternée $[\ell,\ell'] = (-1)^{\langle \ell,\ell'\rangle}$ sur Λ ; le centre de $\tilde{\Lambda}$ est $\pi^{-1}(2\Lambda) \cap \tilde{\Lambda} = \pi'(2\Lambda) \times \langle -1\rangle$.

Nous aurons à considérer les groupes $P = \tilde{K}/\pi'(2K^{\perp})$ et $Q = \tilde{\Lambda}/\pi'(2\Lambda)$, qui sont respectivement extensions centrales de $\bar{K} = K/2K^{\perp} \cong 4^2 \times 2^{22}$ par $\langle i\rangle$ et de $\bar{\Lambda} = \Lambda/2\Lambda \cong 2^{24}$ par $\langle -1\rangle$ (groupe extraspécial). La projection canonique d'un élément x de P ou de K (resp. de Q ou de Λ) dans $\bar{K}$ (resp. $\bar{\Lambda}$) est notée $\bar{x}$; comme $\Lambda \subset K$, il y a ambiguïté lorsque $x \in \Lambda$, mais on s'arrangera pour la lever par le contexte. Le groupe Q s'identifie à un sous-quotient de P , à savoir, le quotient $\tilde{Q}/\langle q_1\rangle$ de l'image $\tilde{Q}$ de $\tilde{\Lambda}$ dans P par le sous-groupe d'ordre 2 engendré par l'image commune q_1 de tous les éléments de $\pi'(2E + 2B')$ dans P . Notons que le groupe P et l'élément q_1 ne déterminent pas Q canoniquement : tout ce que l'on peut dire, c'est que $\tilde{Q}$ est un sous-groupe d'indice 2 du centralisateur de q_1 dans P ne contenant pas i , mais on ne peut préciser lequel sans faire intervenir $\tilde{\Lambda}$.

L'image dans P de $\pi^{-1}(2E)$ est une classe latérale de $\langle i\rangle$, formée de deux éléments d'ordre 2 que nous notons p_2 et p_3 (donc $p_3 = (-1) . p_2$) et de deux éléments de carré -1 . On en déduit une partition de l'ensemble $\pi^{-1}(E)$ en deux sous-ensembles $\tilde{E}_2$ et $\tilde{E}_3$ définis de la façon suivante : pour $j = 2,3$, $\tilde{E}_j$ est l'ensemble des $x \in \pi^{-1}(E)$ tels que l'image de x^2 dans P soit l'élément p_j . On a donc $\tilde{E}_3 = i . \tilde{E}_2$. Pour des raisons qui apparaîtront plus loin, l'élément -1 de P sera parfois noté p_1 ; ainsi, $\{1 , p_1 , p_2 , p_3\}$ est un

2-groupe abélien élémentaire.

4. LES ESPACES VECTORIELS GRADUÉS V" , V' ET V

Soit T l'espace d'une représentation linéaire complexe, fidèle et irréductible de P , telle que l'élément i de P soit représenté par le scalaire i . Une telle représentation est unique à équivalence près et de dimension 2^{13} . Tout élément de P n'appartenant pas à $\tilde{Q}.\langle i\rangle$ conjugue q_1 en $(-1).q_1$, donc permute les espaces propres T_+ et T_- de q_1 dans T correspondant aux valeurs propres $+1$ et -1 ; il s'ensuit que $\dim T_+ = \dim T_- = 2^{12}$. Comme $\tilde{Q}$ centralise q_1 , il laisse invariants T_+ et T_- . En particulier, l'espace T_+ est un Q-module (car $Q = \tilde{Q}/\langle q_1\rangle$) , qui ne peut être, évidemment, que l'unique module fidèle pour le groupe extra-spécial Q .

Posons $\mathbb{C}[K]^{\sim} = \mathbb{C}[K] \otimes_{\mathbb{C}[\langle i\rangle]} \mathbb{C}$, où $\mathbb{C}$ est considéré comme $\mathbb{C}[\langle i\rangle]$-module pour l'action évidente : $i \longmapsto$ multiplication par i . Ainsi, $\mathbb{C}[K]^{\sim}$ est l'algèbre du groupe $\tilde{K}$ dans laquelle "l'élément i du groupe est identifié à la constante i ". (Le choix de la notation a pour but de suggérer que $\mathbb{C}[K]^{\sim}$ est "l'algèbre du groupe K tordue" : le choix d'une section $K \longmapsto \tilde{K}$ détermine une base de $\mathbb{C}[K]^{\sim}$ indexée par K .) De même, nous notons $\mathbb{C}[\Lambda]^{\sim}$ l'algèbre $\mathbb{C}[\tilde{\Lambda}] \otimes_{\mathbb{C}[\langle -1\rangle]} \mathbb{C}$, qui s'identifie naturellement à une sous-algèbre de $\mathbb{C}[K]^{\sim}$. Identifions aussi $\tilde{K}$ et $\tilde{\Lambda}$ avec leurs images canoniques dans $\mathbb{C}[K]^{\sim}$ et $\mathbb{C}[\Lambda]^{\sim}$; ainsi, le groupe $\tilde{K}$ (resp. $\tilde{\Lambda}$) opère sur $\mathbb{C}[K]^{\sim}$ (resp. $\mathbb{C}[\Lambda]^{\sim}$) par conjugaison, et cette opération se factorise à travers P (resp. Q) et même à travers $\bar{K}$ (resp. $\bar{\Lambda}$). On gradue $\mathbb{C}[K]^{\sim}$, donc aussi $\mathbb{C}[\Lambda]^{\sim}$, en attribuant à tout élément k de $\tilde{K}$ le degré $\frac{1}{2}\langle\pi(k),\pi(k)\rangle$; ainsi la graduation de $\mathbb{C}[K]^{\sim}$ est à valeurs dans $\frac{1}{2}\mathbb{N}$ et celle de $\mathbb{C}[\Lambda]^{\sim}$ dans $\mathbb{N}$.

Nous sommes à présent en mesure de définir les espaces gradués V" , V' et V . Ecrivons

$$V'' = t^{-1}S(t\mathcal{H}[t]) \otimes \mathbb{C}[K]^{\sim} \oplus t^{\frac{1}{2}}S(t^{\frac{1}{2}}\mathcal{H}[t]) \otimes T , \tag{2}$$

avec les conventions (un peu osées) suivantes : t est une "indéterminée de degré 1 " , $t\mathcal{H}[t] = t\mathcal{H} \oplus t^2\mathcal{H} \oplus \ldots$ désigne une somme directe de copies de $\mathcal{H}$ dotées de degrés $1, 2, 3, \ldots$, $t^{-1}S(t\mathcal{H}[t])$ est l'algèbre symétrique graduée de cette somme directe dont tous les degrés sont diminués d'une unité (ses composantes homogènes de degrés $-1, 0, 1, 2, \ldots$ sont donc respectivement les espaces $\mathbb{C}, \mathcal{H}, S^2(\mathcal{H}), S^3(\mathcal{H}) \oplus \mathcal{H} \otimes \mathcal{H}, \ldots$), $t^{\frac{1}{2}}S(t^{\frac{1}{2}}\mathcal{H}[t])$ s'interprète de façon analogue (ses composantes de degrés $\frac{1}{2}, 1, \frac{3}{2}, 2, \ldots$ sont $\mathbb{C}, \mathcal{H}, S^2(\mathcal{H}), \mathcal{H}, \ldots$) , $\mathbb{C}[K]^{\sim}$ est gradué de la façon prescrite plus haut et T reçoit le degré 0 . On trouvera à la fin du § 6 (remarque 4) une explication partielle des motifs ayant conduit FLM à poser la formule (2). L'espace gradué V' est défini par une expression analogue :

$$V' = t^{-1}S(t\mathbb{H}[t]) \otimes \mathbb{C}[\Lambda]^{\sim} \oplus t^{\frac{1}{2}}S(t^{\frac{1}{2}}\mathbb{H}[t]) \otimes T_+ \ ;$$

c'est l'espace des points fixes de q_1 dans V'' (le groupe P opère sur $\mathbb{C}[K]^{\sim}$ et sur T, donc sur V''). Enfin, on note V l'espace des points fixes de l'automorphisme ω d'ordre 2 de V' induit par :

l'automorphisme -1 de $\mathbb{H}$,

l'automorphisme de $\mathbb{C}[\Lambda]^{\sim}$ induit par l'élément central d'ordre 2 de $\mathrm{Aut}\,\tilde{\Lambda}$ (i.e. $\lambda \longmapsto \lambda^{-1} . (-1)^{\frac{1}{2}<\pi(\lambda),\pi(\lambda)>}$ pour $\lambda \in \tilde{\Lambda}$),

l'automorphisme -1 de T_+.

[N.B. La graduation adoptée par FLM pour V'' est l'opposée de la nôtre. Cela s'explique sans doute par des raisons liées à l'origine physique de certaines notions utilisées et aussi par le fait qu'en théorie de Kac-Moody, la tradition veut que l'on considère plus volontiers des représentations à poids maximum que des représentations à poids minimum (comme ici, au § 6). Dans cet exposé, un emploi systématique de graduations négatives aurait cependant paru quelque peu artificiel. Ce changement de signe en entraîne beaucoup d'autres dans les formules ; j'espère m'être le plus souvent trompé un nombre pair de fois.]

Calculons la série de Poincaré de V. Elle est manifestement égale à la demi-somme de $\mathrm{Tr}(1 \mid V' ; q)$ et de $\mathrm{Tr}(\omega \mid V' ; q)$. On a successivement $\mathrm{Tr}(1 \mid S(\mathbb{C}t^i) ; q) = 1 + q^i + q^{2i} + \ldots = \frac{1}{1-q^i}$, d'où $\mathrm{Tr}(1 \mid S(\mathbb{H}t^i) ; q) = \frac{1}{(1-q^i)^{24}}$, puis $\mathrm{Tr}(1 \mid t^{-1}S(t\mathbb{H}[t]) ; q) = q^{-1}\left(\prod_{i=1}^{\infty} (\frac{1}{1-q^i})\right)^{24}$, série que l'on note $H(q)^{-1}$ (où H se lit "êta"). Comme $t^{\frac{1}{2}}\mathbb{H}[t] = t^{\frac{1}{2}}\mathbb{H}[t^{\frac{1}{2}}] / t\mathbb{H}[t]$, on en déduit que $\mathrm{Tr}(1 \mid t^{\frac{1}{2}}S(t^{\frac{1}{2}}\mathbb{H}[t]) ; q) = H(q) / H(q^{\frac{1}{2}})$. D'autre part, $\mathrm{Tr}(1 \mid \mathbb{C}[\Lambda]^{\sim} ; q)$ n'est autre que la série thêta du réseau Λ (en variable q) ; nous la noterons $\Theta(q)$. On a donc

$$\mathrm{Tr}(1 \mid V' ; q) = \Theta(q) . H(q)^{-1} + 2^{12} . H(q).H(q^{\frac{1}{2}})^{-1} .$$

Un calcul analogue fournit la relation

$$\mathrm{Tr}(\omega \mid V' ; q) = H(q) . H(q^2)^{-1} + 2^{12} . H(q^2) . H(q^{\frac{1}{2}}) . H(q)^{-2} ,$$

d'où, finalement,

$$\mathrm{Tr}(1 \mid V ; q) = \frac{1}{2}(\Theta(q) . H(q)^{-1} + H(q) . H(q^2)^{-1} + 2^{12}(H(q) . H(q^{\frac{1}{2}})^{-1} + H(q^2) . H(q^{\frac{1}{2}}) . H(q)^{-2})) .$$

Désignons (abusivement) par $J'(q)$ le second membre de cette égalité. C'est *a priori* une série en $q^{\frac{1}{2}}$, mais on sait que l'espace V n'a que des composantes de degré entier (car ω vaut -1 sur les autres) ; donc J' est en fait une série à coefficients entiers, c'est-à-dire que la fonction $J'(e^{2\pi i z})$ est invariante par $z \longmapsto z+1$. Elle l'est aussi par $z \longmapsto -z^{-1}$ comme on le déduit

facilement des formules de transformation classiques des fonctions thêta et êta. Ainsi, $J'(e^{2\pi iz})$ est une fonction modulaire (pour le groupe $SL_2(\mathbb{Z})$). De plus, $J'(q) = q^{-1}$ + des termes de degrés strictement positifs. Donc, $J' = J - 744$, où J est l'invariant modulaire (en variable q).

Considéré comme $\{1, p_1 = -1, p_2, p_3\}$-module, V'' est somme directe de quatre composantes isotypiques, à savoir, l'espace ${}_0V''$ des points fixes simultanés des p_j et, pour $j = 1, 2, 3$, l'espace ${}_jV''$ des points v fixes par p_j et transformés en $-v$ par $p_{j'}$ pour $j' \neq j$. Pour $j = 0$ ou 1 , on a ${}_jV'' = (t^{-1}S(t\mathbb{H}[t])) \otimes \mathbb{C}[K]^{\sim}_j$, où l'on note $\mathbb{C}[K]^{\sim}_j$ le sous-espace de $\mathbb{C}[K]^{\sim}$ engendré linéairement par les éléments de $\pi^{-1}(K_j)$; de même, pour $j = 2$ ou 3 , ${}_jV'' = (t^{\frac{1}{2}}S(t^{\frac{1}{2}}\mathbb{H}[t])) \otimes T_j$, où T_j est l'espace des points fixes de p_j dans T .

5. DESCRIPTION DE CERTAINES FAMILLES D'OPÉRATEURS

Pour $h \in \mathbb{H}$ et $n \in \mathbb{N}^*$ (resp. $\mathbb{N}+\frac{1}{2}$), l'élément ht^n de $t\mathbb{H}[t]$ (resp. $t^{\frac{1}{2}}\mathbb{H}[t]$), c'est-à-dire la réplique de degré n de h dans l'espace gradué en question, sera aussi noté $h(n)$. Remarquons que $S(t\mathbb{H}[t])$ (resp. $S(t^{\frac{1}{2}}\mathbb{H}[t])$) est une algèbre de polynômes en les $h_i(n)$, où (h_i) désigne une base de $\mathbb{H}$ et n parcourt $\mathbb{N}^*$ (resp. $\mathbb{N}+\frac{1}{2}$) . Pour $h \in \mathbb{H}$ et $n \in \frac{1}{2}\mathbb{Z}$, on désignera par une notation unique $\underline{h}(n)$ les divers opérateurs suivants :

pour $n > 0$, la multiplication par $h(n)$ dans $S(t\mathbb{H}[t])$ ou $S(t^{\frac{1}{2}}\mathbb{H}[t])$, selon que $n \in \mathbb{Z}$ ou $\mathbb{Z}+\frac{1}{2}$;

pour $n \leq 0$, la dérivation de l'algèbre de polynômes $S(t\mathbb{H}[t])$ ou $S(t^{\frac{1}{2}}\mathbb{H}[t])$ qui envoie $h'(n')$ sur $n . \langle h,h'\rangle . \delta_{n',-n}$ ("dérivée partielle par rapport à $n^{-1} . \langle h,h\rangle^{-1} . h(-n)$" si $n \neq 0$, et opérateur nul sinon) ;

pour $n \neq 0$, les opérateurs nuls de $\mathbb{C}[K]^{\sim}$ et T ;

pour $n = 0$, l'opérateur $k \longmapsto \langle\pi(k),h\rangle . k$ (pour $k \in \tilde{K}$) dans $\mathbb{C}[K]^{\sim}$;

enfin, pour tout $n \in \frac{1}{2}\mathbb{Z}$, l'endomorphisme de V'' induit par les opérateurs qui viennent d'être décrits.

Pour $k \in \tilde{K}$ et $n \in \frac{1}{2}\mathbb{Z}$, notons $\underline{\mu}_k(n)$ la composante de degré n de l'endomorphisme $k' \longmapsto kk'$ (pour $k' \in \tilde{K}$) de $\mathbb{C}[K]^{\sim}$ (autrement dit, $\underline{\mu}_k(n)k' = kk'$ ou 0 selon que $n =$ ou $\neq \frac{1}{2}\langle\pi(k), \pi(k)\rangle + \langle\pi(k), \pi(k')\rangle$), et $\underline{x}_k(n)$ l'endomorphisme de degré n de $t^{-1}S(t\mathbb{H}[t]) \otimes \mathbb{C}[K]^{\sim}$ défini par l'égalité entre séries formelles suivante, où l'on pose $h = \pi(k)$:

$$\sum_{n\in\frac{1}{2}\mathbb{Z}} \underline{x}_k(n)\zeta^n = \exp(-\sum_{n\in\mathbb{N}^*} \underline{h}(n)\zeta^n/n) . \exp(-\sum_{n\in-\mathbb{N}^*} \underline{h}(n)\zeta^n/n)$$

$$\otimes (\sum_{n\in\frac{1}{2}\mathbb{N}} \underline{\mu}_k(n)\zeta^n) .$$

Cette définition a un sens car on constate aisément que si l'on applique le second membre à un élément donné de $t^{-1}S(t\mathbb{H}[t]) \otimes \mathbb{C}[K]^{\sim}$, le résultat est une

somme finie. Si l'on veut expliciter $\underline{x}_k(n)$, il est commode de considérer l'espace $t^{-1}S(t\mathfrak{H}[t]) \otimes \mathbb{C}[K]^{\sim}$ comme une somme directe de copies de l'algèbre de polynômes $S(t\mathfrak{H}[t])$ indexées par K et d'écrire $\underline{x}_k(n)$ sous forme de matrice $(\underline{x}_k(n)_{k_1k_2})$, avec $k_1,k_2 \in K$. Les coefficients de cette matrice sont des séries d'opérateurs différentiels à coefficients polynomiaux, séries dont il n'est pas difficile d'écrire autant de termes que l'on souhaite pour n, k, k_1, k_2 donnés, et qui convergent (en tant que séries d'opérateurs dans l'algèbre de polynômes) parce que les degrés des dérivations qui y interviennent croissent indéfiniment.

Pour $k \in \tilde{K}$, $h = \pi(k)$ et $n \in \frac{1}{2}\mathbb{Z}$, on note encore $\underline{y}_k(n)$ l'endomorphisme de degré n de $t^{\frac{1}{2}}S(t^{\frac{1}{2}}\mathfrak{H}[t]) \otimes T$ défini par l'égalité

$$\sum_{n\in\frac{1}{2}\mathbb{Z}} \underline{y}_k(n)\zeta^n = \exp(-\sum_{n\in\mathbb{N}^*+\frac{1}{2}} \underline{h}(n)\zeta^n/n).\exp(-\sum_{n\in-\mathbb{N}^*-\frac{1}{2}} \underline{h}(n)\zeta^n/n)$$
$$\otimes\, 2^{-\langle h,h\rangle}.k$$

(il faut se rappeler que T est un $\tilde{K}$-module). Comme les opérateurs $\underline{x}_k(n)$, les $\underline{y}_k(n)$ peuvent être représentés par des matrices dont les coefficients sont des séries convergentes d'opérateurs différentiels à coefficients polynomiaux (dans l'algèbre de polynômes $S(t^{\frac{1}{2}}\mathfrak{H}[t])$), mais il s'agit cette fois de matrices d'ordre fini 2^{13} . Observons que, pour $j = 2$ ou 3 et $e \in \tilde{E}_j$ (cf. § 3), les restrictions des opérateurs $\underline{y}_e(n)$ et $\underline{y}_{e^{-1}}(n)$ à V''_j (resp. V''_{5-j}) sont égales ou opposées (resp. opposées ou égales) selon que n appartient à $\mathbb{Z}$ ou à $\mathbb{Z}+\frac{1}{2}$.

Les formules qui nous ont permis de définir les $\underline{x}_k(n)$ et les $\underline{y}_k(n)$ s'appliquent *mutatis mutandis* à des situations beaucoup plus générales (cf. par exemple [Bo], [FLM 2], [KP], [Le], [V0]). Les séries formelles d'opérateurs figurant aux seconds membres de ces formules - ou d'autres relations analogues - portent le nom d'"opérateurs de sommet" ("vertex operators") ; nous dirons plus loin (§ 6) quelques mots de leur origine.

6. LES ALGÈBRES DE LIE $\mathfrak{G}$, $\hat{\mathfrak{G}}$ ET ${}_j\hat{\mathfrak{G}}$

Notons $\mathfrak{G}$ l'algèbre de Lie isomorphe à $(\mathfrak{sl}_2(\mathbb{C}))^{24}$ et "rigidement épinglée" à $(\mathfrak{H},\tilde{K})$ de la façon suivante : l'espace $\mathfrak{H}$ est identifié à une sous-algèbre de Cartan de $\mathfrak{G}$ de telle façon que E soit le système des coracines et l'on se donne une application $e \longmapsto \underline{x}_e$ de $\pi^{-1}(E)$ dans $\mathfrak{G}$ telle que

$\mathbb{C}\underline{x}_e$ soit la sous-algèbre radicielle de G correspondant à la racine associée à la coracine $\pi(e)$,

$i\underline{x}_e = \underline{x}_{ie}$ (rappelons que $i \in \tilde{K}$),

$[\underline{x}_e , \underline{x}_{e^{-1}}] = \pi(e)$.

Soit $\hat{\mathfrak{G}}$ l'affinisée $\frac{1}{2}\mathbb{Z}$-graduée de $\mathfrak{G}$, c'est-à-dire l'espace vectoriel somme directe de $\mathfrak{G}[t^{\frac{1}{2}}, t^{-\frac{1}{2}}]$ et d'un espace $\mathbb{C}c$ de dimension 1 , doté de la loi

d'algèbre de Lie définie par les relations de commutation

$$[c,\hat{\mathfrak{G}}] = \{0\} ,$$

$$[xt^m, yt^n] = [x,y]t^{m+n} + m\,\delta_{m,-n}\langle x,y\rangle c \qquad (x,y \in \mathfrak{G} \; ; \; m,n \in \tfrac{1}{2}\mathbb{Z}) ,$$

où $\langle\ ,\ \rangle$ est la forme bilinéaire symétrique invariante sur $\mathfrak{G}$ qui prolonge la forme $\langle\ ,\ \rangle$ sur $\mathfrak{H}$. L'algèbre de Lie $\hat{\mathfrak{G}}$ est graduée de façon évidente : on pose $\deg \mathfrak{G}t^n = n$ et $\deg c = 0$. On s'intéressera à quatre sous-algèbres de $\hat{\mathfrak{G}}$, à savoir :

l'algèbre ${}_0\hat{\mathfrak{G}}$ engendrée linéairement par $\mathfrak{H}[t,t^{-1}] + \mathbb{C}c$ et les $\underline{x}_e \cdot t^n$ pour $e \in \pi^{-1}(E)$ et $n \in \mathbb{Z}$) ;

l'algèbre ${}_1\hat{\mathfrak{G}}$ engendrée par $\mathfrak{H}[t,t^{-1}] + \mathbb{C}c$ et les $\underline{x}_e t^n$ pour $e \in \pi^{-1}(E)$ et $n \in \mathbb{Z} + \frac{1}{2}$) ;

pour $j = 2,3$, l'algèbre ${}_j\hat{\mathfrak{G}}$ engendrée par $\mathbb{C}c$, les $\mathfrak{H}t^m$ $(m \in \mathbb{Z} + \frac{1}{2})$ et les éléments $(\underline{x}_e + \underline{x}_{e^{-1}})t^n$ et $(\underline{x}_e - \underline{x}_{e^{-1}})t^{n+\frac{1}{2}}$ pour $n \in \mathbb{Z}$ et $e \in \tilde{E}_j$ (cf. § 3).

Pour $j = 0, 1, 2, 3$, les opérateurs définis au § 5 fournissent une représentation linéaire graduée de l'algèbre ${}_j\hat{\mathfrak{G}}$ dans l'espace ${}_jV''$:

PROPOSITION.- *L'application linéaire de* ${}_j\hat{\mathfrak{G}}$ *dans* $\mathrm{End}({}_jV'')$ *définie par*

$$c \longmapsto -\mathrm{Id} ,$$

$$ht^n \longmapsto \underline{h}(n) \quad \textit{pour } h \in \mathfrak{H} \textit{ et } n \in \mathbb{Z} \textit{ ou } \mathbb{Z} + \tfrac{1}{2} \textit{ selon que } j \in \{0,1\} \textit{ ou } \{2,3\} ,$$

$$\underline{x}_e t^n \longmapsto \underline{x}_e(n) \quad \textit{pour } e \in \pi^{-1}(E) \textit{ et } n \in \mathbb{Z} + \tfrac{j}{2} \textit{ si } j \in \{0,1\} ,$$

$$(\underline{x}_e + \underline{x}_{e^{-1}})t^n \longmapsto \underline{y}_e(n) + \underline{y}_{e^{-1}}(n) \quad \textit{et} \quad (\underline{x}_e - \underline{x}_{e^{-1}})t^{n+\frac{1}{2}} \longmapsto \underline{y}_e(n+\tfrac{1}{2}) - \underline{y}_{e^{-1}}(n+\tfrac{1}{2})$$

pour $e \in \tilde{E}_j$ *et* $n \in \mathbb{Z}$ *si* $j \in \{2,3\}$,

est une représentation linéaire fidèle.

Remarques.- 1) Il résulte des observations faites à la fin du § 5 que, pour $e \in \tilde{E}_j$ et $n \in \mathbb{Z}$, les opérateurs $\underline{y}_e(n) + \underline{y}_{e^{-1}}(n)$ et $\underline{y}_e(n+\frac{1}{2}) - \underline{y}_{e^{-1}}(n+\frac{1}{2})$ de l'énoncé précédent s'annulent sur ${}_{j'}V''$ pour $j' = 5-j$. De même, $\underline{x}_e(n)$ s'annule sur ${}_0V''$ (resp. ${}_1V''$) si $n \in \mathbb{Z}+\frac{1}{2}$ (resp. $\mathbb{Z}$).

2) Soit G "le" groupe simplement connexe d'algèbre de Lie $\mathfrak{G}$, groupe isomorphe à $(SL_2(\mathbb{C}))^{24}$. C'est un groupe algébrique complexe et l'on peut donc parler du groupe $G(\mathbb{C}[t^{\frac{1}{2}}, t^{-\frac{1}{2}}])$. Celui-ci opère sur $\hat{\mathfrak{G}}$, et la restriction de cette opération à $G = G(\mathbb{C})$ respecte la graduation. Pour $j = 1, 2, 3$, les algèbres ${}_j\hat{\mathfrak{G}}$ sont conjuguées entre elles par des éléments de $G(\mathbb{C})$ (en particulier, elles sont isomorphes comme algèbres de Lie graduées), et elles sont conjuguées à ${}_0\hat{\mathfrak{G}}$ par des éléments de $G(\mathbb{C}[t^{\frac{1}{2}}, t^{-\frac{1}{2}}])$.

3) En tant qu'algèbre de Lie non graduée, $\hat{\mathfrak{G}}$ est produit central d'algèbres de Kac-Moody $\hat{\mathfrak{G}}^{(s)}$ de type $\tilde{A}_1$ indexées par les éléments s de S. Posant ${}_j\hat{\mathfrak{G}}^{(s)} = \hat{\mathfrak{G}}^{(s)} \cap {}_j\hat{\mathfrak{G}}$, on observe que les ${}_j\hat{\mathfrak{G}}^{(s)}$ sont isomorphes, comme algèbres de Lie non graduées, à l'algèbre $\tilde{A}_1$, mais qu'elles ne portent la graduation naturelle (dite aussi "principale") des algèbres de Kac-Moody que si $j \neq 0$.

4) La proposition ci-dessus est l'extension immédiate à $\hat{\mathfrak{G}}$ de deux procédés de construction à l'aide d'opérateurs différentiels de la représentation dite "de base" de l'algèbre $\tilde{A}_1$, procédés dus respectivement à J. Lepowsky et R. Wilson [LW] et à I. Frenkel et V. Kac [FK] (voir aussi [Se] pour une approche différente, plus géométrique). La généralisation esquissée dans [KP] met ces deux constructions en bijection avec les deux classes de conjugaison du groupe de Weyl de A_1 (d'où le titre de [KP]). C'est H. Garland qui a remarqué l'analogie des opérateurs intervenant dans [LW] avec certains opérateurs connus des physiciens sous le nom de "vertex operators". L'isomorphisme entre les $\tilde{A}_1$-modules obtenus par les deux procédés en question, isomorphisme qui joue ici un rôle essentiel (cf. § 8), a des implications arithmétiques remarquables ; il est une des expressions de la "correspondance boson-fermion".

7. LES GROUPES $\tilde{C}$ ET C

Soit C_0 le groupe des automorphismes de Λ qui induisent sur $\Lambda = \Lambda/\langle -1\rangle$ un élément du groupe de Conway $Co_0 = \mathrm{Aut}(\Lambda, \langle\ ,\ \rangle)$. Il laisse invariante la section $\pi'(2\Lambda)$ du § 3, donc opère sur Q, et son image dans $\mathrm{Aut}\, Q$, que nous notons $\bar{C}$, est une extension de $Co_1 = Co_0/\langle -1\rangle$ par $\Lambda/2\Lambda = (\mathbb{Z}/2\mathbb{Z})^{24}$. Le groupe C_0 opère sur Λ, par l'intermédiaire de Co_0, donc sur H.

Soient X un groupe irréductible d'automorphismes d'un espace vectoriel Y sur un corps quadratiquement clos conservant une forme bilinéaire non nulle, et A un groupe d'automorphismes de X laissant invariant le caractère de la représentation $X \hookrightarrow GL(Y)$. A ces données correspond canoniquement un sous-groupe $\tilde{A}$ de $GL(Y)$, extension centrale de A par $\mathbb{Z}/2\mathbb{Z}$, à savoir le groupe des transformations linéaires de Y normalisant X, induisant sur X un élément de A et induisant l'identité sur l'espace (à une dimension, vu l'irréductibilité) des formes bilinéaires invariantes par X. Appliquant cette remarque en prenant pour X, Y, A, le groupe Q, l'espace T_+ et $\bar{C}$, on trouve une extension centrale C_1 de $\bar{C}$ par $\mathbb{Z}/2\mathbb{Z}$ contenue dans $GL(T_+)$.

On note $\tilde{C}$ le produit fibré de C_0 et C_1 au-dessus de $\bar{C}$, c'est-à-dire le groupe des éléments de $C_0 \times C_1$ dont les deux projections ont même image dans $\bar{C}$. Soit $\tilde{z}$ l'élément central d'ordre 2 de $\tilde{C}$ dont les projections dans C_0 et C_1 sont les éléments non triviaux des noyaux de $C_0 \longrightarrow \bar{C}$ et $C_1 \longrightarrow \bar{C}$.

Le groupe $\tilde{C}$ opère sur H et $\mathbb{C}[\Lambda]^{\sim}$ par l'intermédiaire de C_0 et sur

T_+ par l'intermédiaire de C_1 . De la sorte, il opère sur V' , et $\tilde{z}$ induit sur V' l'involution ω du § 4. Ainsi, le groupe $C = \tilde{C}/\langle\tilde{z}\rangle$ opère sur V .

8. LES GROUPES $\tilde{D}$ ET D

Le groupe P opère naturellement sur V'' (il opère *ex officio* sur T , via les automorphismes intérieurs de $\tilde{K}$ sur $\mathbb{C}[K]^{\sim}$ et trivialement sur $\mathcal{H}$) ; nous l'identifions à son image dans $GL(V'')$. Soit E^* (resp. $\mathcal{B}'^*$) l'image dans P de $\pi^{-1}(E)$ (resp. $\pi^{-1}(\mathcal{B}')$). Pour $j = 1,2,3$, notons i_j (resp. $(-1)_j$) la transformation linéaire de V'' égale à i (resp. -1) sur ${}_jV''$ et à 1 sur les autres ${}_kV''$; on a donc $p_j = (-1)_{j'} \cdot (-1)_{j''}$ pour $\{j,j',j''\} = \{1,2,3\}$, et i_2i_3 engendre le centre de P . Soit R le sous-groupe de $GL(V'')$ engendré par E^* et les i_j : c'est un groupe abélien isomorphe à $(\mathbb{Z}/4\mathbb{Z})^3 \times (\mathbb{Z}/2\mathbb{Z})^{12}$ dont une vertu essentielle, pour nous, est que les éléments p_j y jouent des rôles symétriques. (On pourrait sans doute, dans la suite, le remplacer plus économiquement par un sous-groupe d'indice 2 possédant aussi cette propriété, à savoir le groupe engendré par E^* et les éléments i_1i_2 et i_2i_3 .)

Pour $j = 1,2,3$, soit X_j l'ensemble des caractères de R valant i sur i_j et 1 sur les autres i_k ; ce sont les 2^{12} caractères de R intervenant dans ${}_jV''$ et aussi (avec multiplicité 1) dans ${}_jV''_{\frac{1}{2}}$. Dans T , identifié à ${}_2V''_{\frac{1}{2}} + {}_3V''_{\frac{1}{2}}$, choisissons une orbite de P formée de vecteurs propres de R (ces orbites sont toutes proportionnelles entre elles) et notons Δ_2 et Δ_3 ses intersections avec ${}_2V''_{\frac{1}{2}}$ et ${}_3V''_{\frac{1}{2}}$. L'espace à 2^{12} dimensions ${}_1V''_{\frac{1}{2}}$ est contenu dans $1 \otimes \mathbb{C}[K]^{\sim}$; il s'identifie donc à un sous-espace de $\mathbb{C}[K]^{\sim}$ et, comme tel, intersecte $\tilde{K}$ suivant l'ensemble $\pi^{-1}(\mathcal{B}')$. Vu comme partie de ${}_1V''_{\frac{1}{2}}$, cet ensemble sera noté Δ_1 ; c'est aussi une orbite de P formée de vecteurs propres de R . On observe que, pour $j = 1,2,3$, l'ensemble Δ_j , de cardinal $4 \cdot 2^{12}$, est une "quadruple base" de ${}_jV''_{\frac{1}{2}}$, c'est-à-dire une base multipliée par $\{1,i,-1,-i\}$, et que l'ensemble des quadruples de points proportionnels dans Δ_j est en bijection canonique avec X_j .

Soit D_* le groupe des automorphismes de $\tilde{K}$ qui fixent i , induisent sur $K = \tilde{K}/\langle i\rangle$ un élément de $\mathrm{Aut}(K,\langle,\rangle)$ et conservent la section $\pi'(2K^{\perp})$ du § 3. Par contraste avec ce qui se passait pour C_0 au § 7, ce groupe opère *fidèlement* sur P ; il opère aussi sur K , donc sur $\mathcal{H}$, sur l'algèbre de Lie $\mathfrak{G}$ (qui est, rappelons-le, canoniquement attachée à $(\mathcal{H},\tilde{K})$) et, par transport de structure, sur l'algèbre de Lie $\hat{\mathfrak{G}}$.

Comme T est, à isomorphisme près, le seul P-module fidèle simple sur lequel le centre de P opère de la façon prescrite (*cf.* § 4), le groupe des automorphismes de P fixant le centre, et en particulier D_* , opère sur l'espace projectif $\mathrm{Pr}\,T$ de T . Soit $\tilde{D}_*$ le groupe des transformations linéaires de T

conservant $\Delta_2 \cup \Delta_3$ et induisant sur $\mathrm{Pr}\, T$ un élément de D_* ; c'est une extension centrale de D_* par $\langle i \rangle$ que nous identifions à son image dans $GL(V'')$ par l'injection évidente (il opère sur $\mathbb{C}[K]^{\sim}$ par l'intermédiaire de D_* et sur $\mathbb{H}$ trivialement). Notons encore $\tilde{D}_1$ le groupe engendré par $\tilde{D}_*$ et les i_j $(j = 1,2,3)$, et étendons à $\tilde{D}_1$ l'action de D_* sur $\tilde{K}, P, R, \mathfrak{C}, \hat{\mathfrak{C}}$ en convenant que l'action des i_j y est triviale.

Pour rendre les choses plus concrètes, donnons la structure des groupes qui viennent d'être introduits. Dans l'énoncé des résultats, nous utiliserons la convention suivante : tous les groupes en question étant des extensions du groupe de Mathieu M_{24} par des 2-groupes, nous représentons par 2^{12} (resp. $2^{12'}$) les sous-quotients du 2-groupe qui sont isomorphes comme M_{24}-module au code de Golay (resp. à son dual). Plus loin, nous utiliserons aussi la notation 2^{11} (resp. $2^{11'}$) pour désigner le M_{24}-module simple quotient de 2^{12} par son sous-module d'ordre 2 (resp. le dual de 2^{11}, sous-module d'indice 2 de $2^{12'}$). (Je dois à R. Griess l'idée, heuristiquement très utile, d'expliciter ces structures de M_{24}-modules.) On a

$$D_* = 2^{1+12'+12+1} \,.\, 2^{12} \,.\, M_{24}$$

(où le premier facteur représente le groupe, isomorphe à $\bar{K}$, des automorphismes intérieurs de P)

$$\tilde{D}_* = 4 \,.\, 2^{1+12'+12+12+1} \,.\, M_{24} \,,$$

$$\tilde{D}_1 = 4^3 \,.\, 2^{12'+12+12+1} \,.\, M_{24} \,.$$

Le groupe $\tilde{D}_1$ contient R et P , donc q_1 . Nous y distinguerons aussi deux éléments q_2 et q_3 , appelés à jouer avec q_1 des rôles symétriques dans un groupe plus grand, et que nous allons définir à présent. Pour $j = 2,3$, il existe un automorphisme α_j de $\tilde{K}$, évidemment unique, qui prolonge l'élément central d'ordre 2 de $\mathrm{Aut}\, \tilde{\Lambda}$ (voir p. 293, ligne 7), fixe le centre de $\tilde{K}$ et transforme tout élément de $\tilde{E}_j$ (cf. § 3) en son inverse ; on note que α_j induit sur K la multiplication par -1 . Cela dit, nous définissons q_j comme l'élément de $GL(V'')$ induit par l'automorphisme de $\mathbb{C}[K]^{\sim}$ prolongeant α_j , l'automorphisme -1 de $\mathbb{H}$ et l'automorphisme de T égal à $1, 1, 1, -1$ respectivement sur l'espace propre du couple (q_1, p_j) correspondant au couple de valeurs propres $(1,1)$, $(1,-1)$, $(-1,1)$ et $(-1,-1)$ (autrement dit, la restriction de q_j à T est égale dans $\mathrm{End}\, T$ à $\frac{1}{2}((q_1 - 1)(p_j - 1) + 1))$; on vérifie que q_j appartient effectivement à $\tilde{D}_1$.

L'ensemble $Z = \{1, q_1, q_2, q_3\}$ est un groupe abélien élémentaire, et il engendre avec $\{1, p_1, p_2, p_3\}$ un sous-groupe distingué $\hat{Z}$ de $\tilde{D}_1$ qui est abélien élémentaire d'ordre 16 . (N.B. FLM ne considèrent pas explicitement $\hat{Z}$ mais utilisent la décomposition de V'' en les seize sous-espaces propres correspondant

aux seize caractères irréductibles de Z .) Il est utile de comprendre l'action sur $\hat{Z}$ des automorphismes intérieurs de $\tilde{D}_1$: la restriction à $\hat{Z}$ de l'automorphisme intérieur correspondant à un élément de E^* (resp. B'^*) (voir le début du § 8 pour ces notations) est l'involution définie par $q_j \longmapsto p_j q_j$ (resp. $p_2 \longmapsto p_3$, $q_2 \longmapsto p_3 q_3$) ; de plus, modulo le centralisateur de $\hat{Z}$, E^* et B'^* engendrent $\tilde{D}_1$, ce qui revient à dire, vu ce qu'on vient de voir, que le groupe des restrictions à $\hat{Z}$ des automorphismes intérieurs de $\tilde{D}_1$ est abélien élémentaire d'ordre 4 .

Posons $H_1 = H$ et, pour $j = 2,3$, notons H_j la sous-algèbre de Cartan de $\mathfrak{G}$ engendrée par les $\underline{x}_e + \underline{x}_{e^{-1}}$ avec $e \in \tilde{E}_j$. Soit D_0 ($= 4^3 . 3^{12'+12+12} . M_{24}$) le centralisateur de p_2 (ou p_3) dans $\tilde{D}_1$; c'est aussi le sous-groupe d'indice 2 de $\tilde{D}_1$ formé des éléments qui laissent invariants chaque X_j , chaque Δ_j , chaque paire $\{q_j , p_j q_j\}$, chaque H_j , chaque ${}_j\hat{\mathfrak{G}}$ et chaque ${}_jV''$. Le groupe $\tilde{D}_1$, dont la structure peut s'écrire $\tilde{D}_0 . 2$, est engendré par $\tilde{D}_0$ et B'^* ; les éléments de B'^* stabilisent $X_1 , \Delta_1 , p_1 , \{q_1 , p_1 q_1\}, H_1 ,$ ${}_0\hat{\mathfrak{G}} , {}_1\hat{\mathfrak{G}} ,$ ${}_0V''$ et ${}_1V''$, et ils permutent X_2 et X_3 , Δ_2 et Δ_3 , p_2 et $p_3 , \ldots ,$ ${}_2V''$ et ${}_3V''$. Une étape essentielle de la construction consiste à étendre cette symétrie d'ordre 2 , entre les valeurs 2 et 3 de l'indice, en une symétrie d'ordre 3 (incluant $j = 1$). Plus précisément :

Le groupe $\tilde{D}_1$, *considéré en tant que groupe de permutations de* $\Delta_1 \cup \Delta_2 \cup \Delta_3$, *se plonge de façon unique comme sous-groupe d'indice* 3 *dans un groupe de permutations* $\tilde{D}$ *de ce même ensemble, permutant symétriquement* Δ_1 , Δ_2 *et* Δ_3 *et ayant les sous-groupes* $\tilde{D}_0$, R , $\hat{Z}$, *et* $\{1,p_1,p_2,p_3\}$ *comme sous-groupes distingués ; on a* $\tilde{D} \cong \tilde{D}_0 . \mathfrak{S}_3 \cong 4^3 . 2^{12'+2.12} (M_{24} \times \mathfrak{S}_3)$ *et les automorphismes intérieurs de* $\tilde{D}$ *permutent symétriquement les* X_j , *les* p_j *et les paires* $\{q_j , p_j q_j\}$. *Les opérations de* $\tilde{D}_1$ *sur* $\mathfrak{G}$, $\hat{\mathfrak{G}}$ *et* V'' *se prolongent naturellement à* $\tilde{D}$ *de telle sorte que* $\tilde{D}$ *permute symétriquement les* H_j , *les* ${}_j\hat{\mathfrak{G}}$ *et les* ${}_jV''$ *et normalise* ${}_0\hat{\mathfrak{G}}$ *et* ${}_0V''$.

Supposons cet énoncé établi (nous y reviendrons), et V'' doté par conséquent d'une structure de $\tilde{D}$-module. L'espace V' du § 4 est alors l'espace des points fixes de q_1 dans V'' et V est l'espace des points fixes de $Z = \{1,q_1,q_2,q_3\}$ (comme l'élément $\tilde{z}$ de $\tilde{C}$, q_2 et q_3 induisent sur V' l'involution ω du § 4). Soit $N(Z)$ le normalisateur de Z dans $\tilde{D}$. D'après ce que l'on a vu plus haut, c'est un sous-groupe d'indice 2 de $\tilde{D}$, de type $4^3 . 2^{11'+2.12} . (M_{24} \times \mathfrak{S}_3)$ (le groupe $\tilde{D}$ est engendré par $N(Z)$ et E^*). Le quotient $N(Z)/Z = 4^3 . 2^{11'+2.11} . (M_{24} \times \mathfrak{S}_3)$ opère *fidèlement* sur V . Ce n'est malheureusement pas encore le groupe D que l'on a en vue (cf. § 2) car il contient des éléments "parasites", à savoir les i_j : plus exactement, l'intersection de D avec le groupe $\langle i_j \rangle \cong 4^3$ est le sous-groupe $\{1,p_1,p_2,p_3\}$, d'ordre 4 . Mais

il est facile de caractériser D à l'intérieur de $N(Z)/Z$, par exemple de la façon suivante : le plus grand sous-groupe distingué de $N(Z)/Z$ dont l'indice est une puissance de 2 est un sous-groupe d'indice 32 qui engendre D avec n'importe quel élément de $E^*\mathcal{B}'^* \cap \tilde{G}$ (cf. § 3 ; comme on l'a vu plus haut, les éléments de E^* et de $\mathcal{B}'^*$ ne normalisent pas Z).

Revenons comme promis à l'énoncé ci-dessus. Bien qu'élémentaire dans son principe, la preuve de l'existence et de l'unicité de $\tilde{D}$ est trop longue pour être exposée ici ; disons seulement que $\tilde{D}$ "devrait" pouvoir être défini assez simplement comme groupe des automorphismes d'une structure combinatoire portée par $\Delta_1 \cup \Delta_2 \cup \Delta_3$. (Dans [FLM 1], il n'est pas question de $\tilde{D}$ mais on peut y trouver la description, à partir d'un épinglage de toute la situation, d'*une* permutation σ de $\Delta_1 \cup \Delta_2 \cup \Delta_3$ qui appartient à $\tilde{D}$ et telle que $\sigma(\Delta_2) = \Delta_2$ et $\sigma(\Delta_1) = \Delta_3$, de sorte que $\tilde{D}$ est engendré par σ et $\tilde{D}_1$.) En revanche, nous allons voir que, une fois le groupe $\tilde{D}$ connu *en tant que groupe de permutations de* $\Delta_1 \cup \Delta_2 \cup \Delta_3$, il est possible de décrire en quelques lignes la façon dont il opère sur V''. Pour $j = 1,2,3$, le ${}_j\hat{\mathfrak{G}}$-module ${}_jV''$ est engendré par Δ_j ; par conséquent, pour connaître l'action de $\tilde{D}$ sur ${}_1V'' + {}_2V'' + {}_3V''$, il suffit de savoir comment il opère sur les ${}_j\hat{\mathfrak{G}}$ ou, plus simplement, sur l'algèbre $\mathfrak{G}$. Reste donc à décrire les actions de $\tilde{D}$ sur $\mathfrak{G}$ et ${}_0V''$. On bénéficie pour cela de la circonstance favorable que, sur $\mathfrak{G}$ et ${}_0V''$, l'action de $\tilde{D}$ se factorise à travers le groupe quotient $\bar{D} = \tilde{D}/\langle i_j \mid j = 1,2,3\rangle$, plus commode à manier que $\tilde{D}$. On a vu plus haut qu'à chaque élément de X_1 est canoniquement associé un quadruple d'éléments de $\mathcal{B}'^*$ permutant Δ_2 et Δ_3 ; ce quadruple a pour image dans $\bar{D}$ un unique élément qui est d'ordre 4. Par symétrie, on en déduit qu'à tout caractère $\chi \in X_j$, pour $j = 2$ ou 3, doit correspondre un élément d'ordre 4 bien déterminé δ_χ de $\bar{D}$ dont les images réciproques dans $\tilde{D}$ permutent Δ_1 et Δ_{5-j}, et qui engendre donc $\bar{D}$ avec le sous-groupe (connu) $\tilde{D}_1/\langle i_j\rangle$. Pour décrire le groupe $\bar{D}$ et son action sur $\mathfrak{G}$ et ${}_0V''$, il suffit donc de donner l'action de δ_χ sur ceux-ci. Cela se fait simplement en se souvenant que le groupe de Lie $G \cong (SL_2(\mathbb{C}))^{24}$ (cf. § 6) opère sur $\mathfrak{G}$ par la représentation adjointe et sur ${}_0V''$ par intégration de la représentation de $\mathfrak{G}$ (on a $\mathfrak{G} \subset {}_0\hat{\mathfrak{G}}$ et l'on a vu au § 6 que ${}_0\hat{\mathfrak{G}}$ opère sur ${}_0V''$), et en exhibant un élément de G ayant sur $\mathfrak{G}$ et ${}_0V''$ la même action que δ_χ : c'est le cas de l'élément $\tilde{\delta}_\chi$ donné par la formule

$$\tilde{\delta}_\chi = \Pi \exp((\pi i/4)(\underline{x}_e + \underline{x}_{e^{-1}})),$$

où le produit est étendu aux paires $\{e, e^{-1}\}$ d'éléments de $\tilde{E}_j$, inverses l'un de l'autre et dont les images dans P appartiennent au noyau de χ.

Remarques.- 1) L'ordre de $\tilde{\delta}_\chi$ n'est pas 4, comme celui de δ_χ, mais 8. Cela s'explique de la façon suivante. Le centre de G s'identifie de façon évidente à

$(\mathbb{Z}/2\mathbb{Z})^S$, de sorte que le code de Golay G se plonge naturellement dans G. On vérifie alors que G n'opère sur ${}_oV''$ (et évidemment sur $\mathbb{C}$) qu'à travers son quotient G/G, or il est clair que $(\tilde{\delta}_\chi)^4 \in G$. En fait, on peut montrer que $\bar{D}$ peut être plongé dans un groupe de Lie L extension non scindée de M_{24} par G/G qui opère sur ${}_oV''$ et $\mathbb{C}$ de façon compatible avec les opérations de $\bar{D}$ et G/G, et qu'au sein de L, l'élément δ_χ de $\bar{D}$ s'identifie à l'image canonique de $\tilde{\delta}_\chi$ dans G/G.

2) L'opération de $\tilde{D}$ sur ${}_oV''$ est, à certains égards, plus élémentaire que son opération sur la somme des autres ${}_jV''$ puisqu'elle peut être décrite sans faire usage de la correspondance boson-fermion (*cf.* § 6, *remarque* 4)).

9. CONCLUSION

Il est facile de voir que la composante homogène V_1 de degré 1 de V s'identifie au produit direct de $\mathbb{C}$ et du tensorisé par $\mathbb{C}$ de l'espace à 196883 dimensions noté B dans [Ti 1]. De plus, les groupes C et D stabilisent les deux facteurs du produit et induisent sur le second les groupes notés C et $\hat{D}$ dans *loc. cit.* (pour C c'est immédiat, pour D ce l'est beaucoup moins !). Il résulte donc du théorème de Griess (*cf.* [Ti 1], § 5) que $\langle C,D\rangle$ induit le groupe $\mathbb{M}$ sur V_1. Par un procédé brièvement esquissé à la fin du § 2, et sur lequel nous ne revenons pas, on en déduit le résultat final :

THÉORÈME.- *Le sous-groupe de* $GL(V)$ *engendré par* C *et* D *est un groupe fini simple dans lequel* C *est le centralisateur de son élément central d'ordre* 2.

Rappelons que cela implique que l'ordre de $\langle C,D\rangle$ est le nombre figurant à la première page de cet exposé.

[D'après les derniers paragraphes de [FLM 3], dont j'ai eu connaissance après que le présent exposé ait été rédigé et que le Séminaire ait eu lieu, il apparaît que, pour achever leur programme, FLM sont amenés à considérer, outre les réseaux Λ et K et les espaces vectoriels correspondants V' et V'', un troisième réseau contenant K comme sous-réseau d'indice 2, une extension centrale de ce réseau par $\langle i\rangle$ et l'espace vectoriel contenant V'' qui se déduit de ces données par une formule analogue à la formule (2) du § 4.]

BIBLIOGRAPHIE

[ATLAS] *Atlas of finite groups*, by J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson - Clarendon Press, Oxford, 1985.

[Bo] R.E. BORCHERDS - *Vertex algebras, Kac-Moody algebras and the Monster*, Proc. Nat. Acad. Sci. USA, 83 (1956), 3068-3071.

[Br] M. BROUÉ - *Groupes finis, séries formelles et fonctions modulaires*, in Séminaire sur les Groupes finis, Tome 1, Publ. Math. Univ. Paris VII, 1983, 105-127.

[Co] J.H. CONWAY - *A simple construction for the Fischer - Griess monster group*, Invent. Math. 79 (1985), 513-540.

[CN] J.H. CONWAY and S.P. NORTON - *Monstrous Moonshine*, Bull. London Math. Soc., 11 (1979), 308-339.

[FH] I.B. FRENKEL and V.G. KAC - *Basic representations of affine Lie algebras and dual resonance models*, Invent. Math. 62 (1980), 23-66.

[FLM 1] I.B. FRENKEL, J. LEPOWSKY and A. MEURMAN - *A natural representation of the Fischer - Griess Monster with the modular function* J *as character*, Proc. Nat. Acad. Sci. USA 81 (1984), 3256-3260.

[FLM 2] I.B. FRENKEL, J. LEPOWSKY and A. MEURMAN - *A Moonshine module for the Monster*, [VO] (référence ci-dessous), 231-273.

[FLM 3] I.B. FRENKEL, J. LEPOWSKY and A. MEURMAN - *A book on affine Lie algebras, vertex operators representations and the Moonshine*, en préparation.

[Fo] P. FONG - *Characters arising in the monster-modular connection*, in The Santa Cruz conference on Finite Groups, Proc. Symp. Pure Math. A.M.S., 37 (1980), 557-559.

[Gr] R.L. GRIESS Jr. - *The friendly giant*, Invent. Math. 69 (1982), 1-102.

[KP] V.G. KAC and D.H. PETERSON - *112 constructions of the basic representations of the loop group of* E_8, in Proc. Symposium on Anomalies, Geometry, Topology, Singapore 1985, ed. W.A. Bardeen and A.R. White, 276-298.

[Le] J. LEPOWSKY - *Calculus of twisted vertex operators*, Proc. Nat. Acad. Sci. USA 82 (1985), 8295-8299.

[LW] J. LEPOWSKY and R.L. WILSON - *Construction of the affine Lie algebra* $A_1^{(1)}$, Comm. Math. Phys. 62 (1978), 43-53.

[Se] G. SEGAL - *Unitary representations of some infinite-dimensional groups*, Comm. Math. Phys. 80 (1981), 301-342.

[Ti 1] J. TITS - *Le Monstre (d'après R. Griess, B. Fischer et al.)*, Sém. Bourbaki, exposé n° 620, novembre 1983, Astérisque 121-122 (1985), 105-122.

[Ti 2] J. TITS - *Résumé de cours*, Annuaire du Collège de France, 86e année (1985-1986), 101-112.

[VO] *Vertex operators in mathematics and physics*, edited by J. Lepowsky, S. Mandelstam and I.M. Singer, Math. Sci. Res. Inst. Publications n° 3, Springer-Verlag, 1985.

Jacques TITS

Collège de France
11 place Berthelot
F-75231 PARIS CEDEX 05