Astérisque

JACQUES TITS

Le monstre

Astérisque, tome 121-122 (1985), Séminaire Bourbaki,
exp. n° 620, p. 105-122

<http://www.numdam.org/item?id=SB_1983-1984__26__105_0>

© Société mathématique de France, 1985, 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
36e année, 1983/84, n° 620 Novembre 1983

LE MONSTRE
[d'après R. Griess, B. Fischer et al.]

par Jacques TITS

Il existe un et, très probablement, à isomorphisme près, un seul groupe fini simple d'ordre

$$N = 808\ 017\ 424\ 794\ 512\ 875\ 886\ 459\ 904\ 961\ 710\ 757\ 005\ 754\ 368\ 000\ 000\ 000$$
$$= 2^{46}.3^{20}.5^{9}.7^{6}.11^{2}.13^{3}.17.19.23.29.31.41.47.59.71\ .$$

On l'appelle (assez injustement) *Monstre*, ou *Géant Amical* [Gr 2], ou encore *groupe sporadique de Griess-Fischer* ou *de Fischer-Griess* ; il est souvent noté F_1 ou, comme ici F . Selon la classification des groupes finis simples, réputée achevée (peut-être à l'unicité de F près : la tradition orale est fluctuante sur ce point) c'est le plus grand des groupes sporadiques. La "plupart" des 26 groupes sporadiques (cf. par ex. [Go], p. 134), sont impliqués dans F comme quotients de sous-groupes : seuls font exception les groupes de Rudvalis, de O'Nan, de Lyons, J_3 et J_4 de Janko et peut-être le Méchant Nain J_1 , d'ordre $2^3.3.5.7.11.19$. Cette circonstance peut expliquer, à elle seule, l'intérêt qu'on porte au groupe F , mais cet intérêt a été considérablement accru par la découverte des Miracles du Clair de Lune qui seront évoqués au § 6.

L'existence du groupe en question a été conjecturée presque simultanément, en novembre 1973, par B. Fischer et R. Griess. Leurs points de départ étaient des hypothèses "locales", sur la structure de certains centralisateurs d'éléments d'ordre 2 et 3 . Des techniques puissantes, développées au cours des 25 dernières années, permettent, à partir d'hypothèses de cette nature, d'obtenir une foule de renseignements - dont l'ordre du groupe est souvent l'un des plus accessibles - et, pour ainsi dire, de "cerner" le groupe cherché, dont ensuite il "n'y a plus qu'à" prouver l'existence. Pour 10 des 26 groupes sporadiques, cette dernière étape, toujours difficile, a, au moins dans un premier temps, nécessité l'utilisation d'un ordinateur et des techniques de programmation très élaborées, dues notamment à C. Sims. Pour ce qui est du Monstre, la réussite remarquable de R. Griess a été d'en prouver l'existence directement [Gr 2], sans recours à l'ordinateur ; du même coup, il délivrait de ce péché originel plusieurs autres groupes sporadiques impliqués dans F . La première partie du présent exposé donne les grandes lignes d'une preuve d'exis-

tence du Monstre, dérivée de celle de Griess mais qui en diffère par quelques aspects essentiels ; en particulier, elle est élémentaire en ceci qu'elle ne fait appel à aucun résultat difficile de la théorie des groupes finis (tels que les résultats de D. Goldschmidt sur la 2-fusion, utilisés dans [Gr 2]).

On verra plus loin le rôle essentiel joué, tant dans la preuve d'existence que pour la découverte du "Moonshine", par une certaine représentation irréductible ρ de dimension 196883. L'existence d'une telle représentation avait été conjecturée dès les premières recherches sur le Monstre ; elle était notamment suggérée par les résultats de [Gr 1]. Longtemps avant que l'existence de F ait été prouvée, B. Fischer, D. Livingston et M.P. Thorne ont réussi le tour de force de calculer entièrement la table des caractères de ce groupe en supposant seulement l'existence de ρ. Sous cette même hypothèse, en plus de quelques autres, J. Thompson [Th] a établi un théorème d'unicité dont le principe se retrouvera sous-jacent dans notre preuve d'existence.

I. EXISTENCE

1. Le groupe C. Groupes de type $\mathbb{M}$

Rappelons que dans $\mathbb{R}^{24}$ doté d'un produit scalaire euclidien $(\ , \ )$, il existe un et, à isométrie près, un seul réseau Λ de volume 1 tel que $(\Lambda,\Lambda) \subset \mathbb{Z}$ et que $\{(\lambda,\lambda) \mid \lambda \in \Lambda\} = 2\mathbb{N} - \{2\}$; c'est le *réseau de Leech*. Suivant Conway, on note $\cdot 0$ le groupe des isométries de Λ et $\cdot 1$ le groupe simple, quotient de $\cdot 0$ par $\{\pm 1\}$. Posons $M = \Lambda/2\Lambda$. C'est un espace vectoriel à 24 dimensions sur $\mathbb{F}_2$ doté d'une forme quadratique μ (réduction de $\lambda \longmapsto \frac{1}{2}(\lambda,\lambda)$) dont on se sert pour définir une extension

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow Q \xrightarrow{\pi} M \longrightarrow 1$$

par la relation $q^2 = \mu(\pi(q))$ $(\in \mathbb{Z}/2\mathbb{Z})$, pour $q \in Q$. L'élément non neutre du centre de Q sera noté z_0. On a une suite exacte évidente

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \operatorname{Int} Q & \longrightarrow & \operatorname{Aut} Q & \longrightarrow & \mathbb{O}(\mu) & \longrightarrow & 1 \ . \\ & & \| & & & & & & \\ & & M & & & & & & \end{array}$$

L'action de $\cdot 0$ sur Λ induit une inclusion $\cdot 1 \hookrightarrow \mathbb{O}(\mu)$ et l'on notera $\overline{C}$ l'image réciproque de $\cdot 1$ dans $\operatorname{Aut} Q$.

On sait que le groupe extraspécial Q possède une unique $\mathbb{Q}$-représentation linéaire fidèle irréductible ; cette représentation est absolument irréductible, de dimension 2^{12}, et sera notée $Q \longrightarrow GL(V)$ ($\dim_{\mathbb{Q}} V = 2^{12}$). On en déduit une représentation projective $\operatorname{Aut} Q \hookrightarrow PGL(V)$ et l'image réciproque de $\operatorname{Aut} Q$ dans $GL(V)$ a pour groupe dérivé une extension A de $\operatorname{Aut} Q$ par un groupe d'ordre 2. Soit C' l'image réciproque de $\overline{C}$ dans A ; c'est une extension de $\overline{C}$ par $\mathbb{Z}/2\mathbb{Z}$. Griess montre (sans difficulté) que l'extension centrale universelle $\widetilde{C}$ de

$\overline{C}$ est le produit fibré de $\cdot 0$ et C' au dessus de $\cdot 1$. Son centre est donc abélien élémentaire d'ordre 4 et le groupe C qui jouera ici un rôle fondamental est défini comme le quotient de $\widetilde{C}$ par le sous-groupe d'ordre 2 , "diagonal" dans le centre. Autrement dit, dans le groupe des extensions de $\overline{C}$ par $\mathbb{Z}/2\mathbb{Z}$, C est la somme des extensions $\cdot 0 \times_{\cdot 1} \overline{C}$ et C' . L'image réciproque de M ($\subset \overline{C}$) dans C est canoniquement isomorphe à Q et sera identifiée avec lui.

Disons qu'un groupe fini simple est *de type* $\mathbb{M}$ ("of Monster type") s'il possède une involution dont le centralisateur est isomorphe à C . Il ne fait guère de doute qu'il existe une seule classe d'isomorphisme de tels groupes. Cette unicité a été prouvée par Thompson [Th] moyennant un certain nombre d'hypothèses supplémentaires dont il paraît que S. Norton a pu se débarrasser, du moins pour ce qui concerne les plus substantielles d'entre elles, telles que l'existence d'une représentation linéaire fidèle de dimension 196883 (cf. l'introduction et le § 2). Quoi qu'il en soit, on sait que :

PROPOSITION 1.– *L'ordre d'un groupe fini simple de type* $\mathbb{M}$ *est le nombre* N *écrit au début de l'introduction.*

C'est une conséquence du Théorème C (ii) de [Sm] (résultat cumulatif des travaux de plusieurs auteurs), dans lequel l'hypothèse de simplicité est remplacée par des conditions beaucoup moins restrictives mais aussi moins agréables à formuler. On ne dira rien ici de la démonstration, très technique (et non élémentaire, au sens de l'introduction), de la proposition 1, qui ne sera d'ailleurs pas utilisée dans la preuve (élémentaire celle-là) que nous esquisserons du résultat principal de Griess, à savoir *l'existence d'un groupe fini simple de type* $\mathbb{M}$ (cf. § 5).

2. Le C-module B

On pose $L = \Lambda \otimes \mathbb{Q}$ et l'on note $(\ , \ )_L$ le produit scalaire sur L égal à *huit fois* le produit scalaire naturel (c'est-à-dire, faisant de Λ un réseau ayant les propriétés rappelées au § 1). La forme linéaire sur S^2L correspondant à $(\ , \ )_L$ possède un noyau B_* de dimension 299 que l'on peut, à l'aide de $(\ , \ )_L$, identifier à l'espace des endomorphismes autoadjoints de trace nulle de L .

On sait ([Co 1]) que Λ possède 196560 vecteurs de carré scalaire 4 (pour la forme *naturelle*) ; soit $\Lambda_2 = \{\lambda \in \Lambda \mid (\lambda,\lambda)_L = 32\}$ l'ensemble de ces vecteurs et soit Q_2 l'image réciproque dans Q de l'ensemble $(\Lambda_2 + 2\Lambda)/2\Lambda$ (partie de M). Appelons *double base* d'un espace vectoriel la réunion d'une base et de son opposée. Soit B_2 un $\mathbb{Q}$-espace vectoriel de dimension 98280 doté d'une double base $(v(q) \mid q \in Q_2)$ indexée par Q_2 de telle façon que $v(z_o q) = -v(q)$. (Si l'on préfère, B_2 est le quotient de $\coprod_{q \in Q_2} \mathbb{Q}q$ par le sous-espace engendré par les $q + z_o q$.)

Enfin posons $B_1 = L \otimes V$. C'est un espace de dimension 98304.

Le groupe C opère sur B_* par l'intermédiaire de son quotient $\cdot 1$ et sur B_2 par "conjugaison" (pour $c \in C$ et $q \in Q$, $c.v(q) = v({}^c q)$). D'autre part, $\cdot 0$

opère sur L et C' sur V, donc $\tilde{C} = \cdot 0 \times_{\cdot 1} C'$ opère sur B_1 et cette action se factorise à travers C, faisant aussi de B_1 un C-module qui est le C-module fidèle de plus petite dimension. Posons $B = B_* \oplus B_2 \oplus B_1$. C'est un C-module de dimension 196883.

Dès ses premières recherches sur le Monstre, Griess [Gr 1] avait montré que s'il existait un groupe F possédant les propriétés qu'il énoncait, la plus petite dimension possible d'un F-module fidèle était 196883 et que si F possédait une représentation fidèle de cette dimension, sa restriction à C ne pouvait être que la représentation $C \longrightarrow GL(B)$ décrite ici. Comme, d'autre part, il est facile de voir que C est un sous-groupe maximal de F, il "suffisait", pour construire F, de trouver un élément g de $GL(B)$ appartenant à $F - C$, puisqu'alors $F = \langle C, g \rangle$. L'idée de Griess dans [Gr 2] a été d'exploiter le fait, établi très tôt par S. Norton, que (toujours sous l'hypothèse de l'existence d'une représentation $F \hookrightarrow GL(B)$) le groupe F laisse invariant dans B une forme bilinéaire symétrique non nulle β et une loi d'algèbre non nulle $\tau : B \otimes B \longrightarrow B$. Sa méthode consiste à rechercher *simultanément* des formes β et τ stables par C et un automorphisme g de B n'appartenant pas à C et stabilisant ces mêmes formes, après quoi il reste à montrer que le groupe $F = \langle C, g \rangle$ est fini et que $C_F(z_0) = C$. Telle qu'elle est exposée dans [Gr 2], la recherche de τ et de g comporte pas mal de tâtonnements, mais ceux-ci peuvent être évités, comme on va le voir.

3. Le groupe D et son action sur B

Plutôt que de chercher *un élément* de F n'appartenant pas à C, il s'avère plus commode de construire un second *sous-groupe* de F, non contenu dans C (et qui, comme on le verra à la fin du § 5, engendre F avec C, ce qui n'aura d'ailleurs guère d'importance). C'est le groupe D dont il va maintenant être question.

Soit E une double base orthonormale de L (pour la forme $(\ ,\ )_L$) telle que $8E \subset \Lambda$, soit S l'ensemble des paires $\{\pm e \mid e \in E\}$ et soit $\sigma : E \to S$ la projection canonique. Il résulte de la description du réseau de Leech due à Conway [Co 1] que S est le support d'un *système de Steiner* $S(24,8,5)$. Le groupe $\underline{G}$ des "changements de signes" appartenant à $\cdot 0 = \mathrm{Aut}\,\Lambda$, c'est-à-dire des éléments de $\cdot 0$ représentés dans une base extraite de E par une matrice diagonale à coefficients ± 1, est canoniquement isomorphe au code de Golay ($\cong (\mathbb{Z}/2\mathbb{Z})^{12}$) et le stabilisateur $\mathrm{Stab}\,E$ de E dans $\cdot 0$ est produit semi-direct du groupe de Mathieu M_{24} par $\underline{G}$. On note $\hat{D}'$ et D' les images réciproques par $C \longrightarrow \cdot 1$ des images de $\mathrm{Stab}\,E$ et $\underline{G}$ dans $\cdot 1$. On voit que D' est un groupe d'ordre 2^{36}, extension de $\underline{G}/\{\pm 1\}$ par Q. L'image de $8E$ dans $M = \Lambda/2\Lambda$ est formée d'un seul élément dont l'image réciproque dans Q, notée $\{z_1, z_2\}$, est manifestement normalisée par $\hat{D}'$. Soient $\hat{D}^0$ et D^0 les sous-groupes d'indice deux de $\hat{D}'$ et D', centralisateurs dans ceux-ci de $\{z_1, z_2\}$. Le groupe $\hat{D}^0$ est aussi le centralisateur dans C, donc

dans le Monstre F s'il existe, du groupe abélien élémentaire $Z = \{1, z_0, z_1, z_2\}$. Les experts savaient, bien avant [Gr 2], que l'indice de $\hat{D}^0$ dans le normalisateur $\hat{D}$ de Z dans F "devait" être égal à 6, le quotient $\hat{D}/\hat{D}^0$ permutant symétriquement les z_i par conjugaison. Ce groupe $\hat{D}$, qui n'apparaît qu'incidemment dans [Gr 2], jouera ici un rôle primordial. En fait, nous nous intéresserons plutôt au sous-groupe distingué D de $\hat{D}$ engendré par Q et ses conjugués : c'est une extension de $\mathfrak{S}_3$ par le 2-groupe D^0, telle que le quotient D/D^0 permute symétriquement les z_i par conjugaison. Deux problèmes se posent :

(i) montrer l'existence d'une telle extension D ;

(ii) en décrire l'action sur B.

On va voir qu'il est commode de les résoudre simultanément.

Soit $\underline{R}$ (resp. $\underline{Y}_0$; resp. $\underline{X}_0$) l'ensemble des éléments q de Q_2 dont l'image dans M a un représentant de la forme $4e_1 - 4e_2$ (resp. $2e_1 + 2e_2 + \ldots + 2e_8$; resp. $-3e_1 + e_2 + \ldots + e_{24}$), où les e_i appartiennent à E ; pour un tel élément q, on pose $\operatorname{supp} q$ (= support de q) $= \sigma(\{e_1, e_2\})$ (resp. $\operatorname{supp} q = \sigma(\{e_1, \ldots, e_8\})$, un bloc du système de Steiner ; resp. $\varphi_0(q) = \sigma(e_1)$). On sait ([Co 1]) que $Q_2 = \underline{R} \cup \underline{X}_0 \cup \underline{Y}_0$. Les ensembles $\underline{X}_0$ et $\underline{Y}_0$ sont des classes de conjugaison de $\hat{D}'$. Le sous-groupe R de Q engendré par $\underline{R}$ est un groupe abélien élémentaire d'ordre 2^{13} contenant Z. Soit X_i ($i = 0,1,2$) l'ensemble des 2^{11} caractères de R qui valent -1 sur z_j pour $j \neq i$ et soit $\psi_0 : \underline{X}_0 \to X_0$ l'application définie par $\psi_0(q)(r) = 1$ ou -1 selon que le commutateur $(q,r) = 1$ ou z_0, pour $r \in R$. Rappelons que $v : Q \to B_2$ a été défini au § 2 et notons $\overline{\varphi}_0 : v(\underline{X}_0) \to S$ et $\overline{\psi}_0 : v(\underline{X}_0) \to X_0$ les applications composées de $v^{-1} : v(\underline{X}_0) \to \underline{X}_0$ avec φ_0 et ψ_0. L'application $(\overline{\varphi}_0, \overline{\psi}_0) : v(\underline{X}_0) \to S \times X_0$ est surjective et ses fibres sont les paires d'éléments opposés de $v(\underline{X}_0)$.

On sait que la représentation de Q dans V est induite par n'importe quel caractère de R valant -1 sur z_0 ; autrement dit, V possède une double base W invariante par Q et formée de vecteurs propres de R, et l'application $\chi : W \to X_1 \cup X_2$ qui envoie chaque élément de W sur le caractère correspondant est surjective et a pour fibres les paires d'éléments opposés de W. L'ensemble $E \otimes W$ est une double base de B_1. Notons $(\overline{\varphi}, \overline{\psi}) : E \otimes W \to S \times (X_1 \cup X_2)$ l'application $e \otimes w \to (\sigma(e), \chi(w))$; elle est surjective et a pour fibres les paires d'éléments opposés de $E \otimes W$.

Pour motiver les définitions qui seront données plus loin, supposons provisoirement les problèmes (i) et (ii) résolus. On peut voir que $\underline{R}$ est stable par les automorphismes intérieurs de D. Pour $i = 1,2$, soit $\underline{X}_i$ le transformé de $\underline{X}_0$ par n'importe quel élément de D conjuguant z_0 en z_i. Notons aussi $v : \underline{X}_i \to B$ la transformée de l'application $v|_{\underline{X}_0} : \underline{X}_0 \to B$ par un tel élément. Ce qui précède suggère - et l'on montre en effet - que $v(\underline{X}_1 \cup \underline{X}_2)$ ne peut être que l'ensemble $E \otimes W$, que l'on doit avoir $v(\underline{X}_i) = \overline{\psi}^{-1}(X_i)$ et que, si l'on pose

$P = v(\underline{X}_o) \cup (E \otimes W) = \bigcup_{i=o}^{3} v(\underline{X}_i)$ et si l'on prolonge $(\overline{\varphi},\overline{\Psi})$ à P tout entier par $(\overline{\varphi}_o,\overline{\Psi}_o)$, l'application $(\overline{\varphi},\overline{\Psi}) : P \longrightarrow S \times \left(\bigcup_{i=o}^{3} X_i\right)$ ainsi définie est stable par D (opérant sur S trivialement et sur $\bigcup X_i$ par le truchement des automorphismes intérieurs).

Soit $(\varphi,\psi) : \bigcup_{i=o}^{3} \underline{X}_i \longrightarrow S \times \left(\bigcup_{i=o}^{3} X_i\right)$ l'application composée de v^{-1} et de $(\overline{\varphi},\overline{\Psi})$. L'image réciproque d'un élément de $S \times X_i$ par (φ,ψ) est une classe latérale de $\langle z_i \rangle$ dans $\underline{X}_i$. Si (i,j,k) désigne une permutation de $(0,1,2)$ et si $x \in \underline{X}_i$, $x' \in \underline{X}_j$ et $\varphi(x) = \varphi(x')$, on montre facilement qu'on doit avoir ${}^{x}x' \in \underline{X}_k$, ${}^{x'}x \in \underline{X}_k$, $\varphi({}^{x}x') = \varphi({}^{x'}x) = \varphi(x)$ et $\psi({}^{x}x') = \psi({}^{x'}x) = \psi(x) + \psi(x')$, donc $(xx')^3 = {}^{x}x'.{}^{x'}x = 1$ ou z_k. De même, $(xx')^3 = ({}^{x}x'.x)^3 = 1$ ou z_j. Par conséquent,

(*) si $i \neq j$, $x \in \underline{X}_i$, $x' \in \underline{X}_j$ et $\varphi(x) = \varphi(x')$, alors ${}^{x}x' = {}^{x'}x$ et $(xx')^3 = 1$.

A tout couple $b = v(x)$, $b' = v(x')$ d'éléments de $v(\underline{X}_o)$ tels que $\overline{\varphi}(b) \neq \overline{\varphi}(b')$ et $\overline{\Psi}(b) = \overline{\Psi}(b')$ correspond naturellement un élément de $\underline{R} \cap \operatorname{Ker} \overline{\Psi}(b)$ de support $(\overline{\varphi}(b),\overline{\varphi}(b'))$, à savoir le produit xx' ; nous le notons $b.b'$. De même, à $b = e \otimes w$, $b' = e' \otimes w$, éléments de $v(\underline{X}_1 \cup \underline{X}_2)$ tels que $\overline{\varphi}(b) = \sigma(e) \neq \overline{\varphi}(b') = \sigma(e')$ (et $\overline{\Psi}(b) = \overline{\Psi}(b') = \chi(w)$) correspond un élément de $\underline{R} \cap \operatorname{Ker} \overline{\Psi}(b)$ de support $(\overline{\varphi}(b),\overline{\varphi}(b'))$, à savoir l'unique élément de $\underline{R} \cap \operatorname{Ker} \overline{\Psi}(b)$ dont l'image dans M est représentée dans Λ par $4e - 4e'$. On le note aussi $b.b'$. A nouveau, on devine, et l'on prouve sans peine, que les deux "produits" ainsi définis se correspondent sous l'action de D.

Rappelons que le code de Golay $\underline{G}$ peut être vu comme un groupe de parties de S de cardinalité 0, 8, 12, 16 ou 24. Il existe un isomorphisme canonique entre le groupe $\underline{G}/\langle S \rangle$ et le dual de R/Z défini comme suit : le caractère $\hat{r}$ de R trivial sur Z qui correspond à une paire S_1, $S - S_1$ de parties complémentaires de S appartenant à $\underline{G}$ prend sur tout $r \in \underline{R}$ la valeur $(-1)^{\operatorname{Card}((\operatorname{supp} r) \cap S_1)}$. Avec ces notations, posons $\varepsilon(\hat{r}) = (-1)^{\operatorname{Card} S_1/4}$. L'assertion suivante se vérifie immédiatement pour $i = 0$ et doit donc être vraie pour tout i :

(1) soient $x, x' \in \underline{X}_i$ tels que $\varphi(x) = \varphi(x')$ et posons $b = v(x)$, $b' = v(x')$; alors ${}^{x}b' = b'$ ou $-b'$ (i.e. ${}^{x}x' = x'$ ou $x'z_i$) selon que $\varepsilon(\overline{\Psi}(b)\overline{\Psi}(b')) = 1$ ou -1.

Pour $x \in \underline{X}_i$ et $r \in R$, posons ${}^{v(x)}r = {}^{x}r$. Autrement dit :

(2) pour $b \in v(\underline{X}_i)$ et $r \in R$, ${}^{b}r = r$ ou rz_i selon que $\overline{\Psi}(b)(r) = 1$ ou -1.

En conclusion de l'analyse qui précède, montrons que, *pour* $x \in \underline{X}_i$, *l'action de* x *sur l'ensemble* $P = v(\underline{X}_o) \cup (E \otimes W)$ *peut être décrite entièrement à partir de* $v(x)$, *de l'action de* Q *sur* P *et des fonctions* $\overline{\varphi}$, $\overline{\Psi}$. Pour $i = 0$ c'est clair. Supposons donc $i = 1$ (pour fixer les idées) et soit $b \in \overline{\Psi}^{-1}(X_j)$ $(= v(\underline{X}_j))$. Considérons d'abord le cas où $\overline{\varphi}(b) = \overline{\varphi}(v(x))$ $(= \varphi(x))$. Si $j = 1$, ${}^{x}b$ est défini

par (1). Si $j = 0$, il existe $x' \in \underline{X}_0$ tel que $b = v(x')$ et l'on a ${}^{x}b = {}^{x'}v(x)$ (par (*)). Enfin, le cas où $j = 2$ se ramène au précédent car ${}^{x}({}^{x}b)) = b$. Supposons à présent que $\overline{\varphi}(b) \neq \overline{\varphi}(v(x))$ et soit $b' \in \overline{\Psi}^{-1}(X_j)$ tel que $\overline{\varphi}(b') = \overline{\varphi}(v(x))$ et $\overline{\Psi}(b') = \overline{\Psi}(b)$; alors, ${}^{x}b'$ est déjà connu par ce qui précède et ${}^{x}b$ est caractérisé par les relations $\overline{\varphi}({}^{x}b) = \overline{\varphi}(b)$, $\overline{\Psi}({}^{x}b) = \overline{\Psi}({}^{x}b')$ et ${}^{x}b.{}^{x}b' = {}^{x}(b.b') = {}^{v(x)}(b.b')$ (cf. (2)).

Oublions à présent qu'on a supposé connu le groupe D. La description précédente associe à tout élément p ($= v(x)$) de P une permutation δ_p de P. On montre alors assez facilement le résultat suivant (pour plus de détails, cf. [Ti 2], IV) :

si l'on définit D *comme le groupe engendré par les* δ_p, *pour* $p \in P$, *le groupe* D', *identifié de façon évidente à un groupe de permutations de* P, *est un sous-groupe d'indice trois de* D *et, pour* $p \in \overline{\Psi}^{-1}(X_i)$, *l'automorphisme intérieur de* D *correspondant à* δ_p *fixe* z_i *et permute les deux autres* z_j.

On pose naturellement $\underline{X}_i = \{\delta_p | p \in \overline{\Psi}^{-1}(X_i)\}$ et $v(\delta_p) = p$.

Remarquons que nous connaissons déjà l'action de D sur un sous-espace de B de dimension $72.2^{11} = 147456$. Son action sur la "partie restante" de B se détermine par des considérations heuristiques du même ordre de difficulté que les précédentes. Bornons-nous à énoncer les résultats.

Soit $\underline{Y}_i$ ($i = 1,2$) la classe de conjugaison de D transformée de $\underline{Y}_0$ par n'importe quel élément de $\underline{X}_{3-i}$, définissons supp : $\underline{Y}_i \longrightarrow \underline{P}(S)$ par transport de structure ($\underline{X}_{3-i}$ opérant trivialement sur S). Pour $y \in \underline{Y}_i$, posons $v(y) = 2^{-3}.\Sigma v(y')$ où y' parcourt $\underline{Y}_0 \cap y\underline{Y}_{3-i}$ (on montre que ce dernier ensemble se compose de 2^6 éléments, un dans chaque paire d'éléments opposés de $\underline{Y}_0$ ayant même support que y). Soit $\underline{U}_i$ l'ensemble des classes latérales de $\langle z_i \rangle$ dans $\underline{R}$. Pour $u = r.\langle z_i \rangle \in \underline{U}_i$, définissons $v(u)$ comme suit : si $i = 1$ ou 2, $v(u) = v(r) + v(rz_i) \in B_2$; si $i = 0$ et si l'image de r dans $M = \Lambda/2\Lambda$ est représentée dans Λ par $4e - 4e'$, avec $e,e' \in E$, alors $v(u) = ee' \in B_*$ ($\subset S^2L$).

Finalement, on montre que *la seule action possible de* D *dans* B (*compatible avec l'existence de* F) *est la suivante, où l'on note* $e^2 - \frac{1}{24}$ *la projection canonique de* e^2 ($\in S^2L$) *dans* B_* :

pour $d \in D$, $e \in E$ *et* $h \in \bigcup_{i=0}^{3} (\underline{U}_i \cup \underline{Y}_i \cup \underline{X}_i)$, *on a* $d(e^2 - \frac{1}{24}) = e^2 - \frac{1}{24}$ *et* $d(v(h)) = v({}^{d}h)$.

4. L'algèbre (B,τ)

On a vu le rôle (avant tout heuristique) joué dans la construction de Griess par une certaine loi d'algèbre $\tau : B \otimes B \longrightarrow B$ invariante par F. Ici, nous n'avons pas eu besoin de cette loi pour trouver le groupe D. Par contre, nous *définirons* le groupe F comme le groupe des automorphismes d'une algèbre (B,τ). Il

est donc essentiel de déterminer l'application τ, dont nous savons qu'elle doit être invariante par C et D.

Dotons l'espace B du produit scalaire $(\ ,\ )_B$ pour lequel $v(Q_2) \cup v(\underline{X}_1 \cup \underline{X}_2) = v(Q_2) \cup (E \otimes W)$ est une double base orthonormale de $B_2 + B_1$, $(B_*, B_2 + B_1)_B = \{0\}$ et, pour $b,b' \in B_*$, $(b,b')_B = 4 \operatorname{Tr} bb'$ (rappelons que B_* a été identifié à un sous-espace de End L). On vérifie aussitôt que ce produit scalaire est invariant par C et D.

Soient $\tau_1 : B_* \otimes B_* \longrightarrow B_*$, $\tau_2 : B_* \otimes B_2 \longrightarrow B_2$, $\tau_3 : B_2 \otimes B_2 \longrightarrow B_2$, $\tau_4 : B_* \otimes B_1 \longrightarrow B_1$, $\tau_5 : B_2 \otimes B_1 \longrightarrow B_1$ et $\tau_6 : B_2 \otimes B_1 \longrightarrow B_1$ les applications définies par les relations ci-dessous, où $b,b' \in B_* \subset \operatorname{End} L$, $q,q' \in Q_2 \subset \operatorname{End} V$, $e \in E$, $v \in V$ (d'où $e \otimes v \in B_1$) et b_q est l'élément de B_* obtenu de la façon suivante : on considère un élément de Λ dont la projection dans $M = \Lambda/2\Lambda$ coïncide avec celle de q, son carré est un élément k_q de S^2L, identifié, à l'aide de $(\ ,\ )_L$, à l'espace des endomorphismes autoadjoints de L, et l'on pose $b_q = k_q - \frac{1}{24} \operatorname{Tr} k_q$. Voici alors les relations annoncées :

$$\tau_1(b \otimes b') = \frac{1}{2}(bb' + b'b) - \frac{1}{24} \operatorname{Tr} bb' \ ;$$

$$\tau_2(b \otimes v(q)) = \operatorname{Tr}(bb_q).v(q) \ ;$$

$$\tau_3(v(q) \otimes v(q')) = \begin{cases} v(qq') & \text{si } qq' \in Q_2 \ , \\ 0 & \text{sinon} \ ; \end{cases}$$

$$\tau_4(b \otimes (e \otimes v)) = b(e) \otimes v \ ;$$

$$\tau_5(v(q) \otimes (e \otimes v)) = e \otimes q(v) \ ;$$

$$\tau_6(v(q) \otimes (e \otimes v)) = b_q(e) \otimes q(v) \ .$$

Identifiant chacun des espaces B_*, B_2, B_1 à son dual à l'aide de la restriction de $(\ ,\ )_B$ à cet espace, on déduit de chaque τ_i une forme linéaire sur l'une des 27 composantes du produit $B \otimes B \otimes B$, dont on vérifie qu'elle est symétrique en les facteurs égaux de cette composante. En prolongeant cette forme par symétrie aux symétriques de la composante en question et par zéro ailleurs, on obtient une forme linéaire symétrique sur $B \otimes B \otimes B$ qui, moyennant identification de B à son dual par $(\ ,\ )_B$, fournit à son tour un élément de $\operatorname{Hom}(B \otimes B, B)$ prolongeant τ_i et que nous appelons encore τ_i. Notons $\operatorname{Hom}_s(B \otimes B, B)$ l'espace des applications $B \otimes B \longrightarrow B$ provenant, via $(\ ,\ )_B$, de formes $B \otimes B \otimes B \longrightarrow \mathbb{Q}$ *symétriques*.

PROPOSITION 2.– *Les* τ_i $(1 \leq i \leq 6)$ *forment une base de l'espace des points fixes de C dans* $\operatorname{Hom}_s(B \otimes B, B)$. *La fonction* $\tau' = \sum_{i=1}^{6} c_i \tau_i$ *est invariante par* D *si et seulement si elle est proportionnelle à*

$$\tau = 2^2\tau_1 + 2^{-3}\tau_2 + 2^{-1}\tau_3 + \tau_4 + 24^{-1}\tau_5 - 2^{-6}\tau_6 \ .$$

La première assertion (Lemme 5.4 de [Gr 2]) n'est pas nécessaire à la preuve d'existence du Monstre, mais elle donne confiance en la méthode suivie pour trouver

τ . En fait, on n'utilisera plus loin que l'invariance de τ par D , c'est-à-dire l'assertion "si" de la deuxième partie de l'énoncé. Pour l'établir, on calcule τ sur des produits tensoriels d'éléments de la forme $e^2 - \frac{1}{24}$ ou $v(h)$, où $e \in E$ et $h \in \bigcup_{i=0}^{2} (\underline{U}_i \cup \underline{Y}_i \cup \underline{X}_i)$ (cf. la dernière assertion du § 3) et l'on exprime que *la forme* du résultat est invariante par une permutation quelconque des indices 0 , 1 , 2 . Cela se traduit par des propriétés des sous-ensembles $\underline{R}$, $\underline{X}_i$, $\underline{Y}_i$ de D qui, une fois formulées, se démontrent sans grande peine. Les calculs correspondent en gros à ceux du § 11 de [Gr 2], mais ils sont plus courts et conduisent à des formules plus simples : cela tient notamment au fait que l'usage systématique de doubles bases élimine pour ainsi dire les complications de signes.

Cette démonstration (de l'assertion "si"), bien qu'élémentaire et assez facile, est trop longue pour être exposée ici. Au lieu de cela, donnons la preuve de l'assertion "seulement si", basée sur le même principe mais plus courte ; de cette façon, on verra aussi d'où sortent les coefficients de τ . Soient $e \in E$, $r \in \underline{R}$ et $x \in \underline{X}_i$ tels que $\varphi(x) = \sigma(e)$ et $rx \in \underline{X}_i$, d'où $\varphi(x) \subset \operatorname{supp} r$. Alors, il résulte immédiatement des définitions que l'on a

$$\tau'((e^2 - \tfrac{1}{24}) \otimes v(r\langle z_i\rangle)) = \begin{cases} (11/24)c_1.v(r\langle z_i\rangle) & \text{si } i = 0 , \\ (44/3)c_2.v(r\langle z_i\rangle) & \text{si } i = 1 \text{ ou } 2 ; \end{cases}$$

$$\tau'((e^2 - \tfrac{1}{24}) \otimes v(x)) = \begin{cases} (23/3)c_2.v(x) & \text{si } i = 0 , \\ (23/24)c_4.v(x) & \text{si } i = 1 \text{ ou } 2 ; \end{cases}$$

$$\tau'(v(r\langle z_j\rangle) \otimes v(x)) = \begin{cases} -3c_2.v(x) & \text{si } i = j = 0 , \\ c_3.v(rx) & \text{si } i = 0 \text{ et } j = 1 \text{ ou } 2 , \\ (1/2)c_4.v(rx) & \text{si } j = 0 \text{ et } i = 1 \text{ ou } 2 , \\ 2(c_5 + (44/3)c_6).v(x) & \text{si } i = j \in \{1,2\} , \\ -32c_6.v(rx) & \text{si } i,j \in \{1,2\} \text{ et } i \neq j . \end{cases}$$

L'invariance de τ' par D exige donc que $(11/24)c_1 = (44/3)c_2$, $(23/3)c_2 = (23/24)c_4$, $c_3 = \frac{1}{2} c_4 = -32c_6$ et $-3c_2 = 2(c_5 + (44/3)c_6)$, d'où $\tau' = c_4.\tau$.

Remarque.— La loi d'algèbre donnée par le Tableau 6.1 de [Gr 2] est (avec des équivalences de notations évidentes) -72τ . Signalons aussi que les notations utilisées ici diffèrent quelque peu de celles de [Ti 1] et [Ti 2] ; en particulier, les objets notés là D , $\check{D}$, τ_2 , τ_4 , τ_5 , τ_6 , τ et γ sont respectivement $\hat{D}^0$, $\hat{D}$, $4\tau_2$, $2^{-10}\tau_4$, $3^{-1}.2^{-15}\tau_5$, $2^{-10}\tau_6$, $2^5\tau$ et la forme cubique associée à $2^5\tau$ dans les notations du présent exposé.

5. Le groupe des automorphismes de l'algèbre (B,τ)

THÉORÈME.— *Le groupe* $\mathrm{Aut}(B,\tau)$ *est un groupe fini simple de type* $\mathbb{M}$.

Observons d'emblée que, comme aucune des trois composantes simples $B_* \otimes \mathbb{C}$, $B_2 \otimes \mathbb{C}$, $B_1 \otimes \mathbb{C}$ du C-module $B \otimes \mathbb{C}$ n'est stable par D ,

(*) *le* $<C,D>$*-module* $B \otimes \mathbb{C}$ *est simple.*

L'énoncé à établir peut se décomposer comme suit :

(i) $C_F(z_o) = C$;

(ii) F *est un groupe fini simple.*

Commençons par prouver

(ii') *tout sous-groupe abélien distingué* A *de* F *est réduit à l'élément neutre.*

De (*), il résulte que le A-module $B \otimes \mathbb{C}$ est somme directe de ses sous-modules simples, c'est-à-dire est semi-simple, puis que ses composantes isotypiques ont toutes même dimension. Mais il est facile de voir que $B \otimes \mathbb{C}$ ne peut être décomposé en somme directe de sous-espaces de même dimension permutés par C (on est aidé par le fait que $\dim B = 47.59.71$, et qu'aucun de ces facteurs ne divise $|C|$). Donc A est un groupe de matrices scalaires. Etant d'autre part contenu dans $\mathrm{Aut}(B,\tau)$, il est réduit à l'élément neutre, d'où (ii').

Supposons l'assertion (i) établie et montrons que (ii) en résulte.

Le groupe $C_F(z_o) = C$ étant fini, $\mathrm{Ad}\, z_o$ n'a, dans l'algèbre de Lie de F , d'autre point fixe que 0 ; donc $\mathrm{Ad}\, z_o = -1$. Il s'ensuit que la composante neutre de F est commutative, donc égale à $\{1\}$ (vu (ii')), c'est-à-dire que F est fini (puisque c'est un groupe algébrique).

Soit F_1 un sous-groupe distingué de F non réduit à l'élément neutre. On a $F_1 \cap C \neq \{1\}$, car s'il en était autrement, l'application $x \mapsto (z_o,x)$ de F_1 dans lui-même serait injective, donc surjective, tout élément de $F_1 = (z_o,F_1)$ serait inversé par z_o et le groupe F_1 serait commutatif, en contradiction avec (ii') (cet argument m'a été fourni par M. Broué). Il est facile de voir que les seuls sous-groupes distingués de C sont $\{1\}$, $<z_o>$, Q et C , et que le plus petit sous-groupe distingué de D contenant Q est D lui-même. Par conséquent, F_1 contient z_o , donc z_1 (car celui-ci est conjugué à z_o dans D), donc Q , donc D , donc aussi C . Soit $S_2(C)$ un 2-Sylow de C . On vérifie que son centre est engendré par z_o ; il s'ensuit que le normalisateur de $S_2(C)$ dans un 2-Sylow $S_2(F_1)$ de F_1 qui le contient centralise z_o , donc est contenu dans C (vu (i)). Ainsi, $S_2(C)$ est son propre normalisateur dans $S_2(F_1)$; cela implique que $S_2(C) = S_2(F_1)$, d'où $Z(S_2(F_1)) = <z_o>$. On conclut par l'"argument de Frattini" : pour $f \in F$, il existe $f' \in F_1$ tel que ${}^{f}S_2(F_1) = {}^{f'}S_2(F_1)$, d'où ${}^{f}z_o = {}^{f'}z_o$ et $f \in f'.C \subset F_1$. Ainsi, $F_1 = F$, et l'implication (i) $\Rightarrow$ (ii) est démontrée.

Il reste à faire voir que si $\alpha \in C_F(z_o)$, alors $\alpha \in C$.

Pour $b \in B$, soit $\tau_b \in \mathrm{GL}(B)$ la "translation" $x \mapsto \tau(b \otimes x)$. On a $\tau_{\alpha(b)} = {}^{\alpha}\tau_b$. Soient $\pi_1 : B \longrightarrow B_1$ la projection naturelle (de noyau $B_* + B_2$) et $\beta : B \times B \longrightarrow \mathbb{Q}$, $\beta' : (B_* + B_2) \times (B_* + B_2) \longrightarrow \mathbb{Q}$ les formes bilinéaires symétriques définies par $\beta(b,b') = \mathrm{Tr}(\tau_b.\tau_{b'})$ et $\beta'(b,b') = \mathrm{Tr}((\pi_1 \circ \tau_{b|B_1}).(\pi_1 \circ \tau_{b'|B_1}))$.

Etant invariante par C, la forme β' est combinaison linéaire des restrictions de $(\ ,\ )_B$ (cf. § 4) à $B_* \times B_*$ et $B_2 \times B_2$, restrictions que nous notons $(\ ,\ )_{B_*}$ et $(\ ,\ )_{B_2}$. Pour déterminer les coefficients, il suffit de calculer $\beta'(b,b)$ pour un élément $b \in B_* - \{0\}$ (par exemple $b = ee'$, avec $e,e' \in E$ et $e' \neq \pm e$: cf. § 3) et pour un élément $b \in B_2 - \{0\}$ (par exemple $b = v(q)$, avec $q \in Q_2$) ; on trouve

$$\beta' = 2^{10}.(\ ,\ )_{B_*} + 9.2^7.(\ ,\ )_{B_2} . \tag{1}$$

De même, β est invariant par $\langle C,D\rangle$, donc proportionnelle à $(\ ,\ )_B$ (vu (*)) et, calculant par exemple $\beta(ee',ee')$, on obtient

$$\beta = 3^{-1}.13^2.41.(\ ,\ )_B . \tag{2}$$

En particulier, on voit que

(3) *la forme* $(\ ,\ )_B$ *est invariante par* F

(ce qui est d'ailleurs évident sans cela). L'automorphisme α de (B,τ) laisse invariants les espaces propres $B_* + B_2$ et B_1 de z_o, donc les formes β et β' ; en vertu des relations (1) et (2), cela implique que

(4) α *stabilise* B_*, B_2 *et* B_1, *donc aussi les applications* τ_1, τ_2, τ_3, τ_4 *et* $24^{-1}\tau_5 - 2^{-6}\tau_6$.

Pour $\lambda \in \Lambda_2$, soit B_2^λ la droite de B_2 engendrée par $v(q)$, où $q \in Q_2$ a même image que λ dans $M = \Lambda/2\Lambda$. Il résulte de la définition de τ_2 que B_2^λ est une "droite propre" de B_* opérant sur B_2 par $b \mapsto \tau_b$, et que le "poids" (valeur propre) correspondant est la forme linéaire $\omega_\lambda : b \mapsto \mathrm{Tr}(\lambda^2.b)$ (où, comme précédemment, on identifie S^2L à un sous-espace de $\mathrm{End}\ L$ à l'aide de $(\ ,\ )_L$). Par conséquent,

(5) α *permute entre eux les* B_2^λ *et les* ω_λ.

Il est facile de voir (en réfléchissant quelques instants ou en se reportant à [Ja], p. 184) que tout automorphisme de l'algèbre de Jordan des endomorphismes autoadjoints de L est induit par une transformation orthogonale de L. On en déduit aussitôt que $\alpha_{|B_*}$ est lui aussi induit par une telle transformation, soit α_L. De la seconde partie de (5), il résulte que α_L conserve Λ_2, donc Λ, c'est-à-dire que $\alpha_L \in \cdot 0$. Quitte à multiplier α par un élément convenablement choisi de C, nous pouvons donc supposer - et nous le ferons - que α fixe B_*, donc stabilise B_2^λ pour tout $\lambda \in \Lambda_2$. Soit ε_λ la valeur propre correspondante. On a $\varepsilon_\lambda = \pm 1$ puisque α laisse invariante la forme $(\ ,\ )_B$. De l'invariance de τ_3 par α, il résulte que si $\lambda, \lambda', \lambda+\lambda' \in \Lambda_2$, on a $\varepsilon_{\lambda+\lambda'} = \varepsilon_\lambda.\varepsilon_{\lambda'}$. On en déduit qu'il existe $\lambda_o \in \Lambda$ tel que, pour $\lambda \in \Lambda_2$, on ait $\varepsilon_\lambda = (-1)^{(\lambda_o,\lambda)L/8}$: cela se voit facilement en utilisant une base de Λ contenue dans Λ_2 (l'existence d'une telle base se montre comme pour les systèmes de racines) et le fait que si deux éléments de Λ_2 ont un produit scalaire > 0, leur différence appartient aussi à Λ_2. En multi-

pliant α par un élément de Q dont l'image dans M est λ_0 mod. 2Λ, on se ramène au cas où α fixe B_2, ce que nous supposerons désormais.

Toute droite K de L est image de L par une somme d'éléments de B_* ($\subset$ End L). L'invariance de τ_4 par α implique donc que $K \otimes V$ (cf. § 2) est stable par α, d'où il résulte aussitôt que $\alpha_{|B_1}$ est produit tensoriel de Id_L et d'un automorphisme α_V de V. Pour $q \in Q_2$, $\tau_{V(q)}$ induit sur V la multiplication par q (rappelons que V est un Q-module absolument simple), laquelle commute donc avec α_V. Comme Q_2 engendre Q, α_V est un automorphisme de Q-module, donc est la multiplication par un scalaire qui ne peut être que ± 1 en raison de l'invariance de $(\ , \ )_B$ par α. Ainsi, $\alpha = 1$ ou z_0, et le théorème est démontré.

Remarques.— 1) Dans [Gr 2], Griess procède tout autrement. Observant que 2 et 3 sont les seuls nombres premiers apparaissant en dénominateur dans les formules donnant son groupe $F = \langle C, g \rangle$ et la loi de produit τ (notations du § 2 ci-dessus), il réduit la situation mod. $p \geq 5$. Il se sert ensuite de résultats profonds de théorie des groupes finis (et de l'existence de τ) pour montrer que le centralisateur de z_0 mod. p dans le groupe réduit F_p est l'image de C dans F_p. Les résultats de [Sm] (dont, rappelons-le, notre proposition 1 est un cas particulier) lui permettent de conclure que F_p est, pour tout $p \geq 5$, un groupe fini simple d'ordre N, donc qu'il en est de même de F. Cette méthode ne fournit pas de renseignement sur $Aut(B,\tau)$.

2) On peut aussi déduire le théorème des propositions suivantes :

(A) *Si un sous-groupe irréductible, infini et Zariski-fermé de* GL(B) *contient* C, *il est extension d'un groupe fini par le groupe de toutes les matrices scalaires, ou bien il contient la composante neutre du groupe orthogonal d'une forme quadratique dans* B (cf. [Ti 1] et [Ti 2], I).

(B) *Tout sous-groupe fini de* $GL(B_1)$ *contenant proprement* C *est produit tensoriel d'un sous-groupe de* GL(L) *et d'un sous-groupe de* GL(V).

La preuve de (A) donnée dans [Ti 2], I, utilise la classification des groupes de Lie semi-simples. L'assertion (B) peut se démontrer à peu près de la même façon que le Lemme 12.3 de [Gr 2], mais il serait agréable d'en avoir une preuve plus élémentaire (cf. [Ti 1], § 6).

3) Notre démonstration du théorème ci-dessus reste valable sans modification si l'on y remplace $F = Aut(B,\tau)$ par $\langle C, D \rangle$. Compte tenu de la proposition 1, on en déduit la

PROPOSITION 3.— *Le groupe* $F = Aut(B,\tau)$ *est engendré par* C *et* D.

II. ESSENCE

6. Le "Moonshine" ([CN])

(Moonshine = Foolish or visionary talk, plans or ideas [Shorter Oxford].)

On note $\underline{H}$ le demi-plan de Poincaré et, pour N entier ≥ 2, $\Gamma_0(N)$ le groupe $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N}\right\}$ et $\Gamma_0(N)^+$ le sous-groupe de $GL_2(\mathbb{Q})$ engendré par $\Gamma_0(N)$ et $\begin{pmatrix} 0 & N \\ -1 & 0 \end{pmatrix}$.

Le "Monstrous Moonshine" est inséparable de l'histoire de sa découverte ; rappelons-en les étapes principales.

En janvier 1975, A. Ogg observe qu'un nombre premier p divise l'ordre du Monstre si et seulement si la surface de Riemann $\underline{H}/\Gamma_0(p)^+$ (compactifiée) est de genre zéro. Cette remarque, à l'allure de plaisanterie, se révélera prophétique.

"Coïncidence" plus surprenante, mise en lumière par J. McKay (1977) : $\dim B = 196883$ (cf. § 2) n'est autre que le coefficient c_1 de l'invariant modulaire $j(z) = q^{-1} + 744 + \sum_{i\geq 1} c_i q^i$ (où $q = e^{2\pi i z}$), diminué d'une unité. Plus généralement, J.G. Thompson remarque peu après que les premiers coefficients de j (sauf 744) sont des combinaisons entières "simples" ($c_1 = f_1 + f_2$, $c_2 = f_1 + f_2 + f_3$, $c_3 = 2f_1 + 2f_2 + f_3 + f_4$, ...) de degrés f_i de représentations irréductibles du Monstre F ; autrement dit, ce sont les valeurs en l'élément neutre de certains caractères "simples" de F. Suivant une suggestion de Thompson, J.H. Conway et S. Norton remplacent les c_i par les valeurs de ces mêmes caractères en d'autres éléments du groupe et constatent qu'on obtient ainsi les débuts de développements en séries d'autres fonctions modulaires remarquables. La conjecture issue de ces étonnantes découvertes a finalement été prouvée (par les efforts conjugués de A. Atkin, J.H. Conway, P. Fong, S. Norton, S. Smith et J. Thompson) sous la forme du théorème suivant, cité ici d'après l'excellent exposé [Br] de M. Broué.

THÉORÈME.— *Il existe une série formelle* $J(X) = X^{-1} + \sum_{k\geq 1} C_k X^k$ *à coefficients dans l'ensemble des caractères "effectifs" du Monstre et, pour tout* $g \in F$ *d'ordre* $o(g)$, *un entier* $h(g)$ *divisant* 24 *et* $o(g)$ *et un sous-groupe* Γ_g *de* $GL_2(\mathbb{Q})$ *contenant et normalisant* $\Gamma_0(h(g).o(g))$ *tels que la surface* $\underline{H}/\Gamma_g$ *(compactifiée) soit de genre zéro et que la fonction* $j_g(z) = q^{-1} + \sum C_k(g) q^k$ *(pour* $q = e^{2\pi i z}$*) engendre le corps des fonctions de cette surface.*

En particulier, on a nécessairement $\Gamma_1 = SL_2(\mathbb{Z})$ (aux scalaires près), d'où $j_1 = j - 744$.

Les principaux ingrédients de la preuve de ce théorème sont des relations de congruence entre coefficients de formes modulaires et le théorème de Brauer sur la caractérisation des caractères par leurs restrictions aux sous-groupes élémentaires.

La remarque de Ogg prend à présent la forme plus précise suivante : pour tout p tel que $\underline{H}/\Gamma_0(p)^+$ soit de genre zéro, il existe un élément $g(p) \in F$ tel que

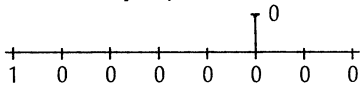
la fonction $j_{g(p)}$ engendre le corps des fonctions de cette surface.

Autre "miracle" : pour tout nombre premier p tel que $(p-1)|24$, d'où $24 = 2d(p-1)$, avec $d \in \mathbb{N}$, Conway exhibe un élément $g'(p) \in F$ (ou, plus exactement, une classe de conjugaison) d'ordre p et un automorphisme $\alpha(p)$ d'ordre p du réseau de Leech Λ tels que $C_F(g'(p))$ soit une extension de $C_{.0}(\alpha(p))$ par un groupe extra-spécial d'ordre p^{2d+1}, on a $j_{g'(p)}(z) = (\eta(z)/\eta(pz))^{2d} + 2d$, où $\eta(z) = q^{1/24}\prod_{k\geq 1}(1-q^k)$ est la fonction de Dedekind, et $j_{g'(p)}$ engendre le corps des fonctions méromorphes de $\underline{H}/\Gamma_0(p)$ (cf. [CN] et [Br], p. 107). L'élément $g'(2)$ n'est autre que notre z_0 (§ 2).

Lorsque $g \in C = C_F(z_0)$, on dispose de formules explicites (cf. [CN], [Ka 2] et [Br], 4.2) exprimant j_g à l'aide de fonctions thêta.

7. Modules et algèbres de dimension infinie

Le Moonshine suggère l'existence d'un F-module gradué *naturel* $M = (M_i)_{i\geq -1}$ dont le polynôme de Poincaré $\Sigma(\dim M_i)q^i$ serait $j(z) - 744$. On espère qu'une définition directe simple de ce module fournirait à la fois la clef du Moonshine et une construction plus conceptuelle du Monstre.

J. McKay avait découvert un phénomène analogue au Moonshine reliant une suite de représentations de l'algèbre de Lie E_8 et la fonction $(q.j(z))^{1/3}$. L'explication en a été donnée par V. Kac [Ka 1] et J. Lepowsky [Le]. On part de l'algèbre de Kac-Moody de type $E_8^{(1)}$, laquelle est, rappelons-le, une extension centrale par $\mathbb{C}$ de l'algèbre $E_8 \otimes \mathbb{C}[T,T^{-1}]$ et l'on considère le module gradué de la représentation fondamentale "basique", c'est-à-dire dont le poids dominant est donné par le diagramme 

. Son polynôme de Poincaré est précisément $(q.j(z))^{1/3}$, et E_8, sous-algèbre de $E_8^{(1)}$, opère de façon naturelle sur chaque composante homogène.

On dispose de constructions explicites du module de la représentation fondamentale basique des algèbres de Kac-Moody de type affine à l'aide d'"opérateurs de vertex" (cf. notamment [FK] et [KKLW]), et plusieurs auteurs ont cherché à s'en inspirer pour construire, par analogie, le "module du Moonshine".

A tout réseau entier pair Λ de volume impair, V. Kac [Ka 2] associe un module gradué que nous notons M_Λ. Lorsque Λ est le réseau de Leech, Kac observe que M_Λ est un C-module gradué (où C est le groupe du § 2) dont la série de Poincaré est $q.(j(z) + c^{te})$; il conjecture que la représentation de C dans le quotient $M_\Lambda/(M_\Lambda)_1$ se prolonge en une représentation graduée de F dont le caractère est donné par la série $X.J(X)$ (cf. § 6).

D'autres résultats ont été obtenus dans cette direction par I. Frenkel, J. Lepowsky et A. Meurman. Commençons par énoncer le plus récent, dont on verra qu'il se rapproche de l'objectif décrit au début de ce paragraphe. Reprenons les notations

du § 4 et considérons l'espace $\widetilde{B} = B + \mathbb{Q}.1$ doté du produit scalaire $(\ ,\ )_{\widetilde{B}}$ égal à la somme directe de $2^{-7}.(\ ,\ )_B$ et de trois fois le produit scalaire naturel sur $\mathbb{Q}$. Pour $\widetilde{b} = b + q.1$ et $\widetilde{b}' = b' + q'.1$, éléments de $\widetilde{B}$, posons $\widetilde{b} \times \widetilde{b}' = \frac{1}{8}\tau(b \otimes b') + qb' + q'b + \frac{1}{3}(\widetilde{b},\widetilde{b}')_{\widetilde{B}}.1$. Formons ensuite l'espace $\hat{B} = \widetilde{B}[T,T^{-1}] + \mathbb{Q}.e$ (on pose $\widetilde{B}[T,T^{-1}] = \widetilde{B} \otimes \mathbb{Q}[T,T^{-1}]$), que l'on dote à son tour d'un produit scalaire $(\ ,\ )_{\hat{B}}$ et d'une loi d'algèbre $\times$ définis par les formules suivantes, où $u,u' \in \widetilde{B}[T,T^{-1}]$ et où $(\ ,\ )_T$, $\times_T$ désignent les extensions naturelles de $(\ ,\ )_{\widetilde{B}}$ et $\times$ à $\widetilde{B}[T,T^{-1}]$:

$$(u + ke\ ,\ u' + k'e)_{\hat{B}} = \text{terme constant de } (u,u')_T\ ;$$

$$(u + ke) \times (u' + k'e) = u \times_T u' + \frac{1}{2}((T\frac{d}{dT})^2(u),u')_{\hat{B}}.e\ .$$

Le groupe F opère sur $\hat{B}$ de façon évidente en préservant le produit $\times$ et le produit scalaire $(\ ,\ )_{\hat{B}}$. Le résultat annoncé dans [FLM 2] est alors le suivant :

Il existe un F*-module gradué* $M = \coprod_{n \leq 1} M_n$ *et une "représentation"* $\pi : \hat{B} \longrightarrow \mathrm{End}\ M$ *compatible avec les actions de* F *sur* $\hat{B}$ *et* M, *telle que* $\pi(e) = \mathrm{Id}$.,

(1) $\quad \pi(u \times v) = \frac{1}{2}([\pi(Tu),\pi(T^{-1}v)] + [\pi(Tv),\pi(T^{-1}u)])$ *pour* $u,v \in B[T,T^{-1}]$,

$\pi(bT^n)$ *est homogène de degré* n *lorsque* $b \in \widetilde{B}$, $M_1 = \mathbb{Q}$, $M_0 = 0$, M_{-1} *est isomorphe à* $\widetilde{B}$ *(comme* F*-module) et* $\sum_{n \leq 1} (\dim M_n).q^{-n} = j(z) - 744$, *où, comme d'habitude,* $q = e^{2\pi i z}$.

Les auteurs conjecturent évidemment que le caractère du F-module gradué M est donné par la série $J(X^{-1})$ (cf. § 6).

Aucune indication n'est donnée dans [FLM 2] sur la façon de prouver ce résultat, mais un rapprochement avec [FLM 1] permet d'imaginer en gros ce qui se passe. A tout réseau entier, pair et unimodulaire Λ, [FLM 1] associe un espace vectoriel gradué ; appelons-le à nouveau M_Λ bien que, cette fois, les degrés parcourent $-\frac{1}{2}\mathbb{N}$. Pour tout $n \in \frac{1}{2}\mathbb{Z}$ et tout $\lambda \in \Lambda$, on définit, à l'aide d'un "opérateur de vertex", un opérateur $x_\lambda(n)$ de degré n dans M_Λ. Lorsque Λ est le réseau des racines de E_8, les auteurs montrent que l'algèbre de Lie engendrée par les opérateurs $x_\lambda(n)$ pour $n \in \frac{1}{2}\mathbb{Z}$ et $(\lambda,\lambda) = 2$ (i.e. λ parcourt l'ensemble des racines de E_8) est isomorphe à $E_8^{(1)}$ et que M_Λ est le module de la représentation basique, dont [FLM 1] fournit ainsi une nouvelle construction. La construction de l'algèbre $\hat{B}$ (à la place de $E_8^{(1)}$) et du "module" M (correspondant au module de la représentation basique) est un peu analogue mais nettement plus compliquée. On part ici du réseau Λ de Leech et l'on définit à nouveau des opérateurs $x_\lambda(n)$ (où cette fois $n \in Z$, $\lambda \in \Lambda$, $(\lambda,\lambda) = 4$) grâce à un "opérateur de vertex". Mais, outre que $\hat{B}$ n'est plus une algèbre de Lie, une différence importante avec le cas de $E_8^{(1)}$ est que les $x_\lambda(n)$ ne suffisent plus à l'"engendrer" (en un sens que l'on peut préciser) : il faut y adjoindre leurs transformés par une certaine

"trialité", à mettre en relation avec notre groupe D (§ 3). [Dans le texte primitif, distribué lors de l'exposé oral, la fin de cet alinéa, basée sur une information très fragmentaire, était assez vague et partiellement incorrecte. Plutôt que de chercher à la préciser, nous renvoyons le lecteur à la note, parue entretemps, de I. Frenkel, J. Lepowsky et A. Meurman, *A natural representation of the Fischer-Griess Monster with the modular function J as character*, Proc. Natl. Acad. Sci. USA 81(1984), 3256-3260.]

***

Dans un ordre d'idées assez différent, il y a lieu de mentionner ici une algèbre de Lie de dimension infinie construite par J. Conway, L. Queen et N. Sloane [CQS], et que ces auteurs espèrent mettre en relation avec le Monstre. Dans $\mathbb{R}^{26}$ doté du système de coordonnées $(x_0,x_1,\dots,x_{24},x_{70})$ et de la forme quadratique $\sum_{i=1}^{24} x_i^2 - x_{70}^2$, considérons le réseau Ξ formé des points dont les coordonnées appartiennent toutes à $\mathbb{Z}$ ou à $\mathbb{Z} + \frac{1}{2}$, et dont le produit scalaire avec $(\frac{1}{2},\dots,\frac{1}{2},\frac{1}{2})$ est un entier pair. Posons $w = (0,1,\dots,24,70)$ (un vecteur de longueur nulle !) et $\Phi = \{r \in \Xi \mid (r,r) = 2,\ (r,w) = -1\}$. L'ensemble Φ a des propriétés remarquables : il est isométrique au réseau de Leech ([CS]) et l'on a $\mathrm{Aut}\,\Xi = (\mathrm{Isom}\,\Phi \times \{\pm 1\}) \ltimes W_\Phi$, où $\mathrm{Isom}\,\Phi$ est le groupe des isométries de Φ (donc isomorphe à $\cdot 0$ étendu par les translations du réseau de Leech) et W_Φ est un groupe de Coxeter engendré par les réflexions par rapport aux éléments de Φ. L'algèbre de Lie en question est l'algèbre de Kac-Moody construite à partir du "système fondamental de racines" Φ, c'est-à-dire de la matrice de Cartan généralisée $((r,s))_{r,s\in\Phi}$.

8. Systèmes générateurs et sous-groupes

Appelons *ensemble de Fischer* toute partie d'un groupe formée d'involutions dont les produits deux à deux sont d'ordre 2 ou 3. Depuis longtemps, B. Fischer s'est intéressé aux systèmes générateurs de F possédant cette propriété, c'est-à-dire aux expressions de F comme quotient d'un groupe de Coxeter dont le graphe n'a que des liaisons simples. A défaut d'avoir jusqu'ici fourni de vraies présentations, de telles expressions ont au moins l'intérêt de permettre un repérage commode de certains sous-groupes remarquables de F. L'élégant énoncé qui suit, dû à Conway, redonne comme cas particuliers les systèmes générateurs obtenus par Fischer.

Le produit en couronne $(F \times F) \rtimes (\mathbb{Z}/2\mathbb{Z})$ *est un quotient du groupe de Coxeter* $\mathrm{Cox}\,\Gamma$ *associé au graphe d'incidence* Γ *du plan projectif* Π *sur* $\mathbb{F}_3$.

Soit Π' le dual de Π. Choisissons un épimorphisme $\varphi : \mathrm{Cox}\,\Gamma \longrightarrow (F \times F) \rtimes (\mathbb{Z}/2\mathbb{Z})$, pour $x \in \Pi \cup \Pi'$ soit s_x l'image par cet épimorphisme "du générateur" de $\mathrm{Cox}\,\Gamma$ correspondant et soit π la projection du produit $F \times F$ sur un de ses facteurs. Aucun des s_x n'appartient à $F \times F$, sinon ils lui appartiendraient tous (par conjugaison de proche en proche), donc, pour $x,y \in \Pi \cup \Pi'$, l'expression $\pi(\varphi(s_x s_y))$ a un sens et représente un élément de F. Fixons à présent une droite $d \in \Pi'$, prise comme "droite de l'infini", soient

$\Pi_d = \Pi - d$ le plan affine correspondant et $\Pi'_d = \Pi' - \{d\}$ l'ensemble de ses droites. Pour $x \in \Pi \cup \Pi'$, posons $r_x = \pi(\varphi(s_d s_x))$. On voit que $\{r_x | x \in \Pi_d \cup \Pi'_d\}$ est un ensemble de Fischer dans F, de sorte qu'à toute "configuration affine" $P \subset \Pi_d \cup \Pi'_d$ correspond un groupe $F_P = \langle r_x | x \in P \rangle$ doté d'un système générateur de Fischer. Donnons quelques exemples.

Soient $A_1, A_2, A_3 \in \Pi_d$ trois points formant triangle et, pour $i = 1,2,3$, notons A'_i le troisième point de la droite joignant les A_j ($j \neq i$), a_i la droite joignant les A'_j ($j \neq i$), a'_i la droite parallèle à cette dernière et passant par A_i, a''_i la droite joignant A_i et A'_i (cévienne du triangle) et $D \in d$ le point à l'infini commun aux droites a_1, a'_1 et A_2A_3. Posons $P_0 = \{A_i, A'_i, a_i, a'_i, a''_i | i = 1,2,3\}$ et $P_1 = P_0 - \{a_1, a'_2, a'_3\}$. *On a* $F_{P_0} = F_{P_1} = F$. Le lecteur est invité à dessiner les graphes de P_0 et P_1 et à constater que ce sont respectivement un hexagone doté de trois queues de longueur 3 et un arbre à trois branches de longueurs 3, 4 et 4. Fischer avait, dès avant 1976, découvert dans F des systèmes générateurs représentés par ces graphes.

Les résultats suivants, et beaucoup d'autres du même type, sont aussi dûs à Fischer. Pour $X \subset P_1$, posons $F(X) = F_{P_1 - X}$. Alors : $F(A_2)$ est extension centrale du Bébé-Monstre BM par le groupe $\langle r_{a'_2} \rangle$ d'ordre 2 ; $F(a'_1)$ (resp. son dérivé) est extension non centrale (resp. centrale) du groupe de Fischer Fi_{24} (resp. Fi'_{24}) par le groupe $\langle r_D \rangle$ d'ordre 3 ; $F(A_2, A_3)$ est extension centrale de ${}^2E_6(\mathbb{F}_2)$ par le groupe abélien élémentaire $\langle r_{a'_2}, r_{a'_3} \rangle$ d'ordre 4 ; on a $F(A_2, a''_2) \cong Fi_{23}$; $F(A_2, A_3, a''_2)$ est extension centrale de Fi_{22} par $\langle r_{a'_3} \rangle$. Observons que les graphes de Coxeter de ces groupes sont des arbres à trois branches de longueurs (3,3,4), (2,4,4), (3,3,3), (2,3,4) et (2,3,3) respectivement. On voit, par les exemples précédents, comment l'existence de certaines extensions centrales "exotiques" peut être mise en évidence au sein du Monstre.

Signalons encore, pour terminer, que [CN] contient une foule de renseignements sur les classes de conjugaison de F, les centralisateurs d'éléments d'ordre petit, etc.

BIBLIOGRAPHIE

[Br] M. BROUÉ - *Groupes finis, séries formelles et fonctions modulaires*, Sém. Groupes finis, tome I, Publ. Math. Univ. Paris VII, 1982, 105-127.

[Co 1] J.H. CONWAY - *A group of order* 8,315,553,613,086,720,000, Bull. Lond. Math. Soc. 1(1969), 79-88.

[Co 2] J.H. CONWAY - *The automorphism group of the 26-dimensional even unimodular Lorentzian Lattice*, preprint (non daté).

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

[CQS] J.H. CONWAY, L. QUEEN and N.J.A. SLOANE - *A Monster Lie algebra ?* , preprint (non daté).

[CS] J.H. CONWAY and N.J.A. SLOANE - *Lorentzian forms of the Leech lattice*, Bull. Amer. Math. Soc. 6(1982), 215-217.

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

[FLM 1] I.B. FRENKEL, J. LEPOWSKY and A. MEURMAN - *An E_8-approach to F_1* , à paraître dans les Proceedings of the 1982 Montreal conference on finite group theory.

[FLM 2] I.B. FRENKEL, J. LEPOWSKY and A. MEURMAN - Communication personnelle, octobre 1983.

[Go] D. GORENSTEIN - *Finite Simple Groups, An introduction to their classification*, The Univ. Series in Math., Plenum Press New York, 1982.

[Gr 1] R.L. GRIESS Jr. - *The structure of the "Monster" simple group*, Proc. Conf. Finite Groups, W. Scott and F. Gross eds., Academic Press, 1976, 113-118.

[Gr 2] R.L. GRIESS Jr. - *The Friendly Giant*, Inventiones Math. 69(1982), 1-102.

[Ja] N. JACOBSON - *Structure and representations of Jordan algebras*, Amer. Math. Soc. Colloquium Publ., vol. 39, 1968.

[Ka 1] V.G. KAC - *An elucidation of "Infinite dimensional algebras ... and the very strange formula", $E_8^{(1)}$ and the cube root of the modular invariant j* , Advances in Math. 35(1980), 264-273.

[Ka 2] V.G. KAC - *A remark on the Conway-Norton conjecture about the "Monster" simple group*, Proc. Nat. Acad. Sci. U.S.A., 77(1980), 5048-5049.

[KKLW] V.G. KAC, D.A. KAZHDAN, J. LEPOWSKY and R.L. WILSON - *Realization of the basic representation of the Euclidean Lie algebras*, Advances in Math. 42(1981), 83-112.

[Le] J. LEPOWSKY - *Euclidean Lie algebras and the modular function j* , Proc. Symp. Pure Math. 37(1980) (Santa Cruz Conference on Finite Groups), 567-570.

[Sm] S. SMITH - *Large extraspecial subgroups of widths 4 and 6* , Journal of Algebra 58(1979), 251-281.

[Th] J.G. THOMPSON - *Uniqueness of the Fischer-Griess Monster*, Bull. Lond. Math. Soc. 11(1979), 340-346.

[Ti 1] J. TITS - Résumé de cours, Annuaire du Collège de France 1982-1983.

[Ti 2] J. TITS - *Remarks on Griess' construction of the Griess-Fischer sporadic group*, I, II, III, IV, lettres polycopiées, 1983.

Jacques TITS

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