Théorie des groupes

M. Jacques TITS, membre de l'Institut
(Académie des Sciences), professeur

Le cours de cette année a été consacré au *groupe sporadique de Griess-Fischer.*

1. *Introduction*

Il s'agit d'un groupe fini simple, que l'on notera F, d'ordre

$$2^{46}.3^{20}.5^{9}.7^{6}.11^{2}.13^{3}.17.19.23.29.31.41.47.59.71 \approx 8.10^{53},$$

appelé aussi « Monstre », ou encore, suivant R. Griess, « Friendly Giant » (son ordre n'excède d'ailleurs pas celui de « petits » groupes classiques, tels que $PSL_9(\mathbf{F}_5)$ par exemple !). Son existence a été conjecturée presque simultanément, au mois de novembre 1973, par B. Fischer et R. Griess qui, bien entendu, partaient non pas de l'ordre du groupe mais de la forme de certains centralisateurs (d'éléments d'ordre 2 et 3). En 1981, Griess est parvenu à prouver l'existence de F, sans ordinateur. Ce résultat remarquable a fait l'objet d'un article paru aux *Inventiones Mathematicae* (vol. 69, 1982, 1-102), désigné ci-dessous par [Gr]. Le but principal du cours a été de reprendre le contenu de cet article et d'y apporter un certain nombre de simplifications. Mais avant d'en venir à ces résultats, nous commencerons, comme dans le cours, par évoquer quelques autres aspects des recherches récentes concernant le « Monstre ».

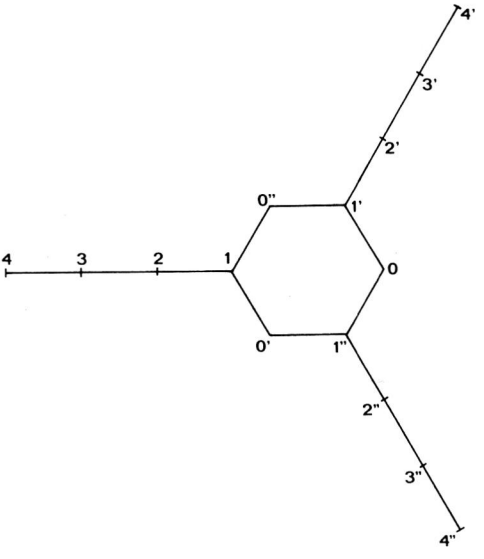
Selon la classification des groupes finis simples, réputée complète, ce groupe [1] est le plus grand des 26 groupes sporadiques. Il « implique » (comme quotients de sous-groupes) 20 de ces derniers : les 12 groupes

(1) L'unicité du groupe simple ayant l'ordre indiqué, qui ne fait guère de doute, est « presque établie » par des résultats de J. Thompson et S. Norton. Pour la commodité de l'exposé, je m'exprime comme si elle l'était effectivement.

sporadiques impliqués dans le groupe de Conway (groupes de Mathieu, His, McL, J_2, Suz, ·3, ·2, ·1 : cf. le résumé de cours de 1976-1977), les trois groupes de Fischer, trois groupes (Har, Th, BM) découverts au sein du « Monstre » — alors même que son existence n'était pas encore prouvée —, le groupe de Held et F lui-même ; des six groupes sporadiques restants, cinq ne sont certainement pas impliqués dans F (cf. [Gr], § 14) ; le cas de J_1 n'est pas décidé, à ma connaissance.

Ce rôle exceptionnel de F suffirait à justifier l'intérêt qu'il suscite, mais cet intérêt a encore été accru par la découverte, due à A. Ogg, J. McKay, J. Thompson, J. Comway et S. Norton, de coïncidences numériques reliant notamment les dimensions et, plus généralement, les valeurs des caractères, d'une suite infinie de représentations linéaires de F avec les coefficients de certaines formes modulaires (c'est le « Monstrous Moonshine » : cf. J. Conway et S. Norton, *Bull. London Math. Soc.*, 11, 1979, 308-339). Jusqu'à présent, il s'agit encore, essentiellement, de constatations expérimentales (voir cependant M. Broué, Groupes finis, séries formelles et fonctions modulaires, Sém. Gr. Finis, I, *Publ. Math. Univ. Paris VII*, 1983, 105-127), mais des recherches en cours (I. Frenkel, J. Lepowsky, A. Meurman et al.) tendent à obtenir une preuve d'existence de F plus conceptuelle que celle de Griess et qui expliquerait le « Moonshine ».

Pour terminer cette introduction, j'évoquerai encore une autre voie d'approche de F, par générateurs et relations. Dès 1976, B. Fischer a observé que ce groupe possède un système générateur d'involutions $(r_i \mid i \in I)$, avec $I = \{0, 1, 2, 3, 4, 0', \ldots, 4', 0'', \ldots, 4''\}$, représentable par le diagramme de Coxeter suivant :



avec les conventions habituelles. Bien entendu, les relations exprimées par le diagramme ne suffisent pas à définir le groupe ; d'ailleurs, le système générateur (r_i) n'est même pas minimal : on peut en effacer les éléments r_0, $r_{4'}$, et $r_{4''}$ sans modifier le groupe engendré. Pour $J \subset I$, soit $G(J)$ le sous-groupe de F engendré par les r_i $(i \notin J \cup \{0, 4', 4''\})$. En faisant varier J, Fischer obtient plusieurs sous-groupes intéressants de F : $G(3') \cong 2.\mathbf{BM}$ (le centre est $<r_{4'}>$), $G(4) \cong 3.\mathrm{Fi}_{24}$ (le sous-groupe distingué d'ordre trois, central dans $3.\mathrm{Fi}'_{24}$ mais non dans $G(4)$, s'aperçoit bien sur le système générateur de Conway, décrit plus bas), $G(3, 4) \cong \mathrm{O}_{10}(2)$ (contient encore $r_{4'}$ et $r_{4''}$), $G(3', 3'') \cong (2 \times 2).({}^2\mathrm{E}_6(2))$, $G(2', 3') \cong \mathrm{Fi}_{23}$, $G(2', 3', 3'') \cong 2.\mathrm{Fi}_{22}$.

Récemment, J. Conway a découvert (résultat inédit à ma connaissance) un système générateur de F encore plus symétrique que le précédent : plus exactement, il décrit le produit en couronne $\tilde{F} = (F \times F) \rtimes (\mathbf{Z}/2\mathbf{Z})$ comme quotient du groupe de Coxeter Γ dont le diagramme est le graphe d'incidence du plan projectif Π sur $\mathbf{F}_3$. Le système générateur de Fischer se déduit de celui de Conway de la façon suivante. Si x est un point ou une droite de Π, notons r_x l'élément du système générateur distingué de Γ qui lui correspond. Soient D une droite de Π, que nous prenons comme « droite à l'infini », et X l'ensemble formé des six points de $\Pi - D$ appartenant à un triangle affine et des neuf droites affines distinctes des côtés du triangle. Alors, on vérifie aussitôt que les quinze éléments $r_x r_D$ $(x \in X)$ de Γ sont des involutions satisfaisant aux relations décrites par le graphe ci-dessus. L'homomorphisme $\Gamma \to \tilde{F}$ applique le centralisateur de r_D dans Γ sur un « sous-groupe diagonal » de $F \times F$ (le graphe de la conjugaison par r_D) et le système $(r_x r_D \mid x \in X)$ sur le système générateur de Fischer.

On souhaiterait compléter ces systèmes générateurs en des présentations tout aussi élégantes.

2. *Le groupe C et son module B ; groupes de type* **M**

Soient Λ le réseau de Leech, M le quotient $\Lambda/2\Lambda$, qui est un espace vectoriel de dimension 24 sur $\mathbf{F}_2$, doté d'une forme quadratique $\varkappa$,

$$1 \to \mathbf{Z}/2\mathbf{Z} \to Q \xrightarrow{\pi} M \to 1$$

la suite exacte non scindée correspondant à $\varkappa$ (i.e. définie par $q^2 = \varkappa(\pi(q))$ pour $q \in Q$), V l'espace de l'unique $\mathbf{Q}$-représentation irréductible fidèle de Q (espace vectoriel de dimension 2^{12} sur $\mathbf{Q}$) et A le groupe dérivé du normalisateur de Q dans $\mathrm{GL}(V)$. On a des homomorphismes évidents

$$A \to \mathrm{Aut}\ Q \to \mathrm{Aut}\,(M, \varkappa) = \mathrm{O}(\varkappa).$$

D'autre part, le groupe $\cdot 1$ de Conway ($= \cdot 0/\{\pm 1\}$, où $\cdot 0$ est le groupe des isométries de Λ) est contenu dans $O(\varkappa)$. Soient $\bar{C}$ et C_1 les images réciproques de $\cdot 1$ dans $\mathrm{Aut}\, Q$ et dans A (C_1 est donc extension de $\bar{C}$ par $\mathbf{Z}/2\mathbf{Z}$), $\tilde{C}$ le produit fibré de $\cdot 0$ et C_1 au-dessus de $\cdot 1$ — on montre que c'est l'extension centrale universelle de $\bar{C}$ — et C le quotient de $\tilde{C}$ par le sous-groupe d'ordre deux, « diagonal » dans le noyau (isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$) de l'homomorphisme $\tilde{C} \to \bar{C}$. Le centre de C est un groupe d'ordre deux, noté $<z>$ (avec $z^2 = 1$). On identifie Q avec son image canonique dans C.

On appelle « *groupe de type* **M** » (« of Monster type ») tout groupe fini simple possédant une involution z dont le centralisateur est isomorphe à C. L'ordre d'un tel groupe est le nombre écrit au début de ce résumé : cela a été prouvé par Griess et Conway-Norton sous des hypothèses supplémentaires dont des travaux ultérieurs de F. Timmesfeld, S. Smith et al. ont permis de se débarrasser. Comme toujours pour ce genre de résultat, ces auteurs imposent en fait beaucoup moins que la simplicité ; le théorème qu'ils établissent implique par exemple l'assertion suivante, dont nous aurons besoin :

(*) si un groupe fini sans sous-groupe abélien distingué non trivial possède une involution dont le centralisateur est isomorphe à C, il est simple (donc de type **M**).

Le résultat central de [Gr], qui a été l'objet principal du cours, est l'existence d'un groupe de type **M**.

Posons $L = \Lambda \otimes \mathbf{Q}$. Le groupe C opère fidèlement, de façon évidente, sur l'espace vectoriel $B_1 = L \otimes V$, de dimension $24.2^{12} = 98304$.

Soient Λ_2 l'ensemble des vecteurs de Λ de norme 4, M_2 l'image de Λ_2 dans M et $Q_2 \subset Q$ l'image réciproque de M_2 par π. On a $|Q_2| = |\Lambda_2| = 2.98280$. Appelons *double base* d'un espace vectoriel, la réunion d'une base et de son opposée, et soit B_2 un $\mathbf{Q}$-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 $v(zq) = -v(q)$. Le groupe C opère sur Q_2 (par conjugaison) donc sur B_2 ; le noyau de cette action est $<z>$.

Sous l'action de $\cdot 1$, et même du groupe orthogonal qui le contient, le carré symétrique S^2L se décompose en un espace B_* de dimension 299 (à savoir, le noyau de la forme quadratique fondamentale sur L, considérée comme forme linéaire sur S^2L) et un espace de dimension un. Il est commode, pour certains calculs, de doter L du produit scalaire $(\ ,\ )_L$ égal à *huit fois* le produit scalaire naturel (i.e. faisant de Λ un réseau unimodulaire). Identifions L à son dual (à l'aide de $(\ ,\ )_L$) et, par voie de conséquence, S^2L à l'espace ${}^{aa}\mathrm{End}\, L$ des endomorphismes autoadjoints de L ; l'espace B_* est alors formé des endomorphismes autoadjoints de trace nulle.

La construction de Griess a pour point de départ les faits suivants, où F désigne un groupe de type **M** :

toute représentation linéaire fidèle de F est de dimension au moins égale à 196883 [1], et la restriction à C (supposé contenu dans F comme centralisateur d'involution) de toute représentation fidèle de cette dimension est isomorphe à la représentation de C dans le module $B = B_* \oplus B_2 \oplus B_1$;

si le groupe F est contenu dans $\mathrm{GL}(B)$, il laisse invariantes une forme quadratique et une forme cubique non nulles, donc aussi une loi d'algèbre commutative $\tau : B \otimes B \to B$ (résultat obtenu par S. Norton, avant même que la table des caractères de F n'ait été connue).

La méthode de Griess est alors celle-ci : le C-module B étant connu, on cherche à construire simultanément une loi d'algèbre $\tau : B \otimes B \to B$ stable par C et un automorphisme σ de (B, τ) n'appartenant pas à C, puis on montre que le groupe $F = <C, \sigma>$ est fini et que $C_F(\sigma) = C$. Le problème étant posé de cette façon, la recherche de τ et σ implique des tâtonnements assez considérables, mais on va voir comment une variante de cette méthode, utilisée dans le cours, permet de les éviter.

3. *Le groupe $\check{D}$ et son action sur B ; énoncé du théorème principal*

Choisissons une double base E de L, contenue dans $\frac{1}{8}\Lambda$ et formée de vecteurs deux à deux orthogonaux ou opposés, de carré scalaire 1 (pour la forme $(\ ,\ )_L$). L'image de $8E$ dans M est réduite à un seul élément dont les images réciproques dans Q sont notées z_1, z_2. On pose $z = z_0$ et l'on note D (resp. $\tilde{D}$) le centralisateur (resp. le normalisateur) de $\{z_0, z_1, z_2\}$ dans C. Le groupe $\tilde{D}$ est une extension du groupe de Mathieu M_{24} par Q et l'on a $[\tilde{D} : D] = 2$.

On montre que $\tilde{D}$ se plonge de façon unique dans un groupe $\check{D}$ tel que D soit distingué dans $\check{D}$, que $\check{D}/D \cong \mathfrak{S}_3$ et que les automorphismes intérieurs de $\check{D}$ permutent symétriquement les z_i. D'autre part, il n'est pas difficile de décomposer les D-modules B_*, B_2, B_1 en leurs composantes irréductibles : on trouve :

$$B_* = T \oplus U_0, \quad B_2 = U_1 \oplus U_2 \oplus Y \oplus X_0, \quad B_1 = X_1 \oplus X_2$$

avec $\dim T = 23$, $\dim U_i = 276$, $\dim Y = 759.2^6$, $\dim X_i = 24.2^{11}$. Nous donnerons au § 8 une description plus précise des modules T, U_i, Y et X_i ;

(1) L'observation de J. McKay rapprochant ce nombre du coefficient 196884 de q dans l'invariant modulaire j est à l'origine du « Monstrous Moonshine ».

bornons-nous pour l'instant à signaler que tout automorphisme de D (nécessairement induit par un automorphisme intérieur de $\check{D}$) permute les U_i et les X_i de la même façon que les z_i, et normalise le module Y. On en déduit aisément la

PROPOSITION 1. *La structure de D-module de B se prolonge en une structure de $\check{D}$-module qui est unique à un automorphisme de B centralisant C près (c'est-à-dire un automorphisme stabilisant B_*, B_1, B_2 et induisant sur chacun d'eux une homothétie).*

Autrement dit, on a ainsi défini un $(C, \check{D})$-module B, unique à isomorphisme près. Le théorème principal s'énonce alors :

THÉORÈME. *Le sous-groupe F de $\mathrm{GL}(B)$ engendré par C et $\check{D}$ est un groupe fini simple, et l'on a $C_F(z) = C$ (donc F est de type* **M**).

Remarque. Les considérations précédentes ont été inspirées par la lecture de [Gr], mais sont en fait très proches de la preuve d'unicité du « Monstre » (sous certaines conditions) dues à J.G. Thompson (*Bull. London Math. Soc.*, 11, 1979, 340-346).

4. *Réduction à trois propositions auxiliaires*

Les trois étapes de la preuve du théorème exposée dans le cours (à quelques calculs près) sont résumées par les énoncés suivants.

PROPOSITION 2. *Soit G un sous-groupe irréductible de $\mathrm{GL}(B)$, contenant C et fermé dans $\mathrm{GL}(B)$ pour la topologie de Zariski. Alors, G contient le groupe spécial orthogonal d'une forme quadratique, ou bien il est fini, ou extension d'un groupe fini par le groupe de toutes les homothéties. De plus, tout sous-groupe abélien distingué de G est contenu dans le groupe des homothéties.*

Disons qu'un sous-groupe de $\mathrm{GL}(B_1) = GL(L \otimes V)$ est « factorisable » s'il est produit tensoriel (en un sens évident) d'un sous-groupe de $\mathrm{GL}(L)$ et d'un sous-groupe de $\mathrm{GL}(V)$.

PROPOSITION 3. *Tout sous-groupe fini de $\mathrm{GL}(B_1)$ contenant proprement C est factorisable.*

PROPOSITION 4. (i) *Dans B, il existe une forme bilinéaire symétrique β et une forme cubique γ non nulles, stables par C et $\check{D}$; ces formes sont uniques à un facteur près. Choisissons-les, identifions B à son dual à l'aide*

de β *et notons* $\tau : B \otimes B \to B$ *la loi d'algèbre commutative déduite de* γ *par cette identification.*

(ii) *On a* $\tau(B_1 \otimes B_1) = B_* \oplus B_2$.

(iii) *L'application linéaire* $B_1 \otimes B_2 \to B_1$ *déduite de* τ *par restriction et projection n'est pas le produit tensoriel de* id_L *par une application :*

$$V \otimes B_2 \to V.$$

Montrons que ces propositions impliquent le théorème du § 3. Soit G un sous-groupe fermé de $\mathrm{Aut}(B, \tau)$ contenant $F = <C, \check{D}>$. Il est clair que $\mathrm{Aut}(B, \tau)$ ne peut contenir un groupe spécial orthogonal tout entier, ni aucune homothétie non triviale. Il s'ensuit (proposition 2) que G est un groupe fini sans sous-groupe abélien distingué non trivial. Comme z a la valeur propre -1 sur B_1 et la valeur propre 1 sur $B_* \oplus B_2$, le centralisateur $C_G(z)$ stabilise B_1. En vertu de la proposition 4 (ii) il opère fidèlement sur B_1 et on déduit aisément de la proposition 4 (iii) qu'il n'est pas factorisable. Donc (proposition 3), $C_G(z) = C$. Compte tenu de l'assertion (*) du § 2, cela prouve le théorème et aussi la :

PROPOSITION 5. *Le groupe* F *est le groupe de tous les automorphismes de l'algèbre* (B, τ).

(N.B. : Griess prouve tout autrement la finitude de son groupe $F = <C, \sigma>$: observant que les formules donnant C, τ et σ ne contiennent pas d'autre facteur premier en dénominateur que 2 et 3, il réduit F modulo un nombre premier p quelconque, distinct de 2 et 3, et montre, en faisant appel à des résultats profonds de la théorie des groupes finis, que la réduction est un groupe de type **M** ; en particulier, l'ordre de cette réduction est indépendant de p et l'on en déduit que F est fini. Ce raisonnement ne donne pas de renseignement sur $\mathrm{Aut}(B, \tau)$.)

5. *Schéma de preuve de la proposition 2*

Pour établir cette proposition, on commence par montrer que :

l'espace vectoriel B *ne peut être décomposé en somme directe de sous-espaces propres de même dimension, permutés par* C.

C'est un exercice d'autant plus facile que les facteurs premiers de $\dim B = 47.59.71$ ne divisent pas C .

L'assertion précédente entraîne aussitôt la deuxième partie de la proposition et permet, par des arguments standard, de ramener la preuve du

restant de l'énoncé au cas où la composante neutre G° de G est un groupe absolument quasi-simple irréductible (comme sous-groupe de $\mathrm{GL}(B)$), ce que nous supposons désormais. Soient $\tilde{G}^\circ$ le revêtement universel de G° et $\varrho : \tilde{G}^\circ \to \mathrm{GL}(B')$ une représentation linéaire complexe non triviale de $\tilde{G}^\circ$ de dimension $d = \dim B'$ minimum. Le groupe C opère fidèlement sur G° (par conjugaison dans G), donc sur $\tilde{G}^\circ$, et cette opération se fait par automorphismes intérieurs, car $[\mathrm{Aut}\,\tilde{G}^\circ : \mathrm{Int}\,\tilde{G}^\circ] \leqslant 6$ tandis que C n'a pas de sous-groupe propre d'indice $\leqslant 6$. Par conséquent, ϱ induit une représentation projective fidèle de C dans $\mathrm{PGL}(B')$. Mais on montre que le degré d'une telle représentation est $> 2^{12}$ (la valeur minimum exacte est $2^{12} + 24$). Donc $d > 2^{12}$; en particulier, $\tilde{G}^\circ$ est nécessairement de type classique. Selon que $\tilde{G}^\circ$ est isomorphe sur $\mathbf{C}$ à SL_d, $\mathrm{Spin}\,d$ ou Sp_{2d}, le plus petit entier $> d$ qui soit dimension d'une représentation irréductible de $\tilde{G}^\circ$ est $\frac{1}{2}d\,(d-1)$, $\frac{1}{2}d\,(d-1)$ ou $\frac{1}{2}d\,(d-1)-1$. Comme $\dim B < 2^{11}\,(2^{12}-1)-1$, on doit avoir $\dim B = d$, c'est-à-dire que l'inclusion $G^\circ \to \mathrm{GL}(B)$ est la « représentation standard » du groupe classique G°. La dimension de B étant impaire, on ne peut avoir $G^\circ = \mathrm{Sp}_d$, et la proposition s'ensuit, puisque SL_d contient SO_d.

6. *Sur la preuve de la proposition 3*

La démonstration qu'on a donnée dans le cours suit dans les grandes lignes les raisonnements du § 12 de [Gr]. En particulier, elle utilise les résultats fondamentaux de D. Goldschmidt sur la 2-fusion dans les groupes finis (*Ann. of Math.*, 99, 1974, 70-117). (On a cependant pu simplifier quelque peu la présentation de [Gr], notamment en remplaçant le lemme 2.14 de [Gr] par un lemme plus fort, implicite dans l'article cité de Goldschmidt, et en utilisant le lemme très facile — et sans doute bien connu — repris ci-dessous au lieu de la proposition 2.21 de [Gr], sensiblement plus compliquée.) Ceci est le seul point de l'exposé où on a dû faire appel à des résultats profonds de la théorie des groupes finis, et il serait souhaitable de donner de cette proposition 3 une démonstration plus élémentaire, par exemple sur le modèle de la preuve du lemme suivant.

LEMME. *Le groupe* $\cdot 0$ *est un sous-groupe fini maximal de* $\mathrm{GL}_{24}(\mathbf{Q})$.

Tout sous-groupe fini de $\mathrm{GL}_{24}(\mathbf{Q})$ stabilisant un réseau, il suffit de montrer que tout réseau $\Lambda' \subset \mathbf{Q}^{24}$, stable par $\cdot 0$, est multiple de Λ. Quitte à multiplier Λ' par une constante, on peut supposer que $\Lambda' \subset \Lambda$ et que Λ' contient un vecteur primitif de Λ. Si $\Lambda' \neq \Lambda$ et si p est un nombre premier divisant $[\Lambda : \Lambda']$, l'image de Λ' dans $\Lambda/p\Lambda \cong \mathbf{F}_p^{24}$ est un sous-espace propre non nul, stable par $\cdot 0$. Or il est facile de voir que $\cdot 0$ n'a pas de représentation

irréductible non triviale de degré < 24 sur $\mathbf{F}_p$, d'où l'on déduit aussitôt qu'il n'a pas non plus de représentation réductible non triviale de degré 24. Ainsi, 0 devrait fixer Λ modulo $p\Lambda$, ce qui est manifestement absurde. La contradiction provient de ce que l'on a supposé $\Lambda' \neq \Lambda$, et le lemme est démontré.

Bien entendu, une démonstration éventuelle de la proposition 3 basée sur un principe analogue serait beaucoup plus compliquée, notamment du fait que la représentation de C dans B_1 ne reste *pas irréductible en caractéristique 2.*

7. *Les formes cubiques C-invariantes*

Choisissons dans V un produit scalaire $(\ ,\ )_V$ défini positif et stable par Q et dotons les espaces B_*, B_2, B_1 et B des produits scolaires $(\ ,\ )_B$, etc. suivants : pour $x, y \in B_* \subset \mathrm{End}\ V$, on pose $(x, y)_{B_*} = 4\ \mathrm{Tr}\ xy$; pour $q, q' \in Q$, on pose $(v(q), v(q'))_{B_2} = 1$, -1 ou 0 selon que $q' = q$, $q' = qz$ ou $q' \notin \{q, qz\}$; la forme $(\ ,\ )_{B_1}$ est le produit tensoriel des formes $(\ ,\ )_L$ et $(\ ,\ )_V$; enfin, la forme $(\ ,\ )_B$, qui sera aussi notée β, est la somme directe des trois précédentes. Nous identifierons souvent les espaces V, B_*, B_2, B_1, B à leurs espaces duaux à l'aide des formes ainsi définies.

Le produit de Jordan dans ${}^{aa}\mathrm{End}\ L$ composé avec la projection canonique ${}^{aa}\mathrm{End}\ L \to B_*$ définit une application $\tau_1 : B_* \otimes B_* \to B_*$. Soit $\tau_2 : B_2 \otimes B_2 \to B_*$ l'application définie comme suit : si $q \in Q_2$, si λ est l'un des deux éléments de Λ_2 dont l'image dans M_2 coïncide avec l'image de q et si $q' \notin Q_2 - \{q, qz\}$, on pose $\tau_2(v(q) \otimes v(q)) = \lambda^2$ et $\tau_2(v(q) \otimes v(q')) = 0$. Moyennant les identifications annoncées, τ_2 donne lieu à une forme $B_2 \otimes B_2 \otimes B_* \to \mathbf{Q}$, puis à une fonction $B_* \otimes B_2 \to B_2$, que nous noterons également τ_2. Soit encore $\tau_3 : B_2 \otimes B_2 \to B_2$ l'application définie par :

$$\tau_3(v(q) \otimes v(q')) = v(qq') \text{ ou } 0 \text{ selon que } qq' \in \text{ ou } \notin Q_2\ (q, q' \in Q_2).$$

Le groupe Q est contenu dans $\mathrm{End}\ V$ et forme une double base de cet espace ; cela nous permet d'identifier B_2 et $\mathbf{Q}$ à des facteurs directs de $\mathrm{End}\ V$ (par $v(q) \mapsto q$ et $1 \mapsto 1$). Soient $\pi_1 : \mathrm{End}\ L \to \mathbf{Q}.1 = \mathbf{Q}$, $\pi_2 : \mathrm{End}\ L \to B_*$, $\pi_3 : \mathrm{End}\ V \to \mathbf{Q}$ et $\pi_4 : \mathrm{End}\ V \to B_2$ les projections canoniques. Observons que $B_1 \otimes B_1 = (L \otimes L) \otimes (V \otimes V) = (\mathrm{End}\ L) \otimes (\mathrm{End}\ V)$ et posons :

$$\begin{aligned}
\tau_4 = \pi_2 \otimes \pi_3 \quad &: B_1 \otimes B_1 \to B_*, \\
\tau_5 = \pi_1 \otimes \pi_4 \quad &: B_1 \otimes B_1 \to B_2, \\
\tau_6 = \tau_2 \circ (\pi_2 \otimes \pi_4) \quad &: B_1 \otimes B_1 \to B_2.
\end{aligned}$$

Moyennant l'identification de B_*, B_1, B_2 avec leurs espaces duaux, chacune

des fonctions τ_i $(1 \leqslant i \leqslant 6)$ définit une fonction trilinéaire sur l'une des 27 composantes du produit $B \times B \times B$, fonction qui est symétrique par rapport aux facteurs égaux de cette composante. Nous notons γ_i la forme trilinéaire symétrique sur $B \times B \times B$ (et aussi la forme cubique correspondante), obtenue à partir de cette fonction-là par l'extension évidente : par exemple, $\gamma_1(x, y, z) = (\tau_1(x \otimes y), z)_{B_*}$ — fonction symétrique en x, y, z — si $(x, y, z) \in B_* \times B_* \times B_*$ et $= 0$ si (x, y, z) appartient à l'une des 26 autres composantes de $B \times B \times B$; $\gamma_2(x, y, z) = (\tau_2(x \otimes y), z)_{B_*}$ — fonction symétrique en x, y — si $(x, y, z) \in B_2 \times B_2 \times B_*$ et $= 0$ si (x, y, z) appartient à l'une des 24 composantes de $B \times B \times B$ distinctes de $B_2 \times B_2 \times B_*$, $B_* \times B_2 \times B_2$ et $B_2 \times B_* \times B_2$; etc.

PROPOSITION 6. *Les* γ_i $(i = 1, ..., 6)$ *forment une base de l'espace des formes cubiques C-invariantes sur B.*

Cette proposition n'est pas nécessaire à la preuve d'existence du groupe F mais elle a un intérêt heuristique : elle indique que la forme γ de la proposition 3 doit être cherchée parmi les combinaisons linéaires $\Sigma c_i \gamma_i$.

8. *Composantes irréductibles du D-module B*

Les notations E et z_i sont celles du § 3. Soient S l'ensemble des 24 paires d'éléments opposés de E (c'est le support du *système de Steiner* sur lequel opère M_{24}), $\mathbf{Q}[S]$ l'espace des combinaisons linéaires formelles des éléments de S à coefficients dans $\mathbf{Q}$ et T le sous-espace $\{\Sigma t_s s \in \mathbf{Q}[S] \mid \Sigma t_s = 0\}$. Soit encore $\mathcal{U}$ (resp. $\mathcal{Y}_0$; resp. $\mathcal{X}_0$) l'image réciproque dans Q_2 de l'ensemble des éléments de M_2 possédant un représentant dans Λ_2 de la forme $4e_1 + 4e_2$ (resp. $2e_1 + ... + 2e_8$; resp. $3e_1 + e_2 + ... + e_{24}$) avec $e_1, e_2, ... \in E$. Pour $i = 0, 1, 2$, soient $\mathcal{U}_i$ l'ensemble des classes latérales du groupe $<z_i>$ dans $\mathcal{U}$, $\mathcal{Y}_i$ (resp. $\mathcal{X}_i$) le transformé de $\mathcal{Y}_0$ (resp. $\mathcal{X}_0$) par un automorphisme intérieur quelconque de $\check{D}$ transformant z_0 en z_i et U_i (resp. Y_i ; resp. X_i) un espace vectoriel de dimension 276 (resp. 759.2^6 ; resp. 24.2^{11}) doté d'une double base $(v(u))$ (resp. $(v(q))$) indexée par $\mathcal{U}_i$ (resp. $\mathcal{Y}_i$; resp. $\mathcal{X}_i$) de telle sorte que $v(uz_j) = -v(u)$ pour $j \neq i$ (resp. $v(qz_i) = -v(q)$). Les espaces T, U_i, X_i, Y_i sont, de façon évidente, des D-modules (le groupe D a été défini au § 3).

On montre que les D-modules Y_0, Y_1, Y_2 sont isomorphes. De façon plus précise, on peut les identifier de telle façon que, si (i, j, k) désigne une permutation quelconque de $(0, 1, 2)$ et si $y \in \mathcal{Y}_i$, alors $v(y)$ s'identifie à $2^{-3}.\Sigma y'$ où y' parcourt l'ensemble des éléments de $\mathcal{Y}_j$ tels que $yy' \in \mathcal{Y}_k$ (ces éléments sont au nombre de 2^6). On note Y le D-module résultant de cette

identification. C'est manifestement un $\check{D}$-module, de même que T (par l'intermédiaire du quotient M_{24} de $\check{D}$), $\bigoplus_i U_i$ et $\bigoplus_i X_i$.

Les D-modules T, U_i, Y, X_i ne sont autres que ceux du § 3. Pour le montrer, on exhibe des isomorphismes de D-modules $\psi_* : T \oplus U_0 \to B_*$, $\psi_2 : U_1 \oplus U_2 \oplus Y \oplus X_0 \to B_2$, $\psi_1 : X_1 \oplus X_2 \to B_1$, que nous allons décrire à présent.

Pour $s = \{\pm e\} \in S$, soit $\psi_*(s) \in {}^{aa}\mathrm{End}\, L$ le projecteur de L qui fixe $\pm e$ et annule les autres éléments de E. L'application de S dans ${}^{aa}\mathrm{End}\, V$ ainsi obtenue se prolonge par linéarité en une injection $\mathbf{Q}[S] \to {}^{aa}\mathrm{End}\, V$. Si $u = q\langle z_0\rangle \in \mathscr{U}_0$ et si l'image réciproque dans Λ_2 de la projection canonique de q dans M_2 est $\{\pm (4e - 4e')\}$, avec $e, e' \in E$, on pose $\psi_*(u) = ee' \in S^2L = {}^{aa}\mathrm{End}\, L$. Nous avons ainsi défini un isomorphisme $\psi_* : \mathbf{Q}[S] \oplus U_0 \to {}^{aa}\mathrm{End}\, L$ dont la restriction à $T \oplus U_0$, notée aussi ψ_*, est l'isomorphisme $T \oplus U_0 \to B_*$ annoncé.

Si $u = q\langle z_i\rangle \in \mathscr{U}_i$ avec $i = 1$ ou 2, alors $\psi_2(u) = v(q) + v(qz_i)$. Si $q \in \mathscr{Y}_0 \cup \mathscr{X}_0$, l'isomorphisme ψ_2 applique $v(q)$ sur l'élément de B_2 de même nom.

L'isomorphisme ψ_1 ne peut pas être décrit de façon aussi explicite. Pour $q \in \mathscr{X}_0$, l'image de q dans M_2 a dans Λ_2 un représentant de la forme $3e_1 + e_2 \ldots + e_{24}$ avec $e_1, e_2, \ldots \in E$; posons alors $\sigma(q) = \{\pm e_1\} \in S$ et notons également σ les applications $\mathscr{X}_i \to S$ ($i = 1, 2$) déduites de $\sigma : \mathscr{X}_0 \to S$ par l'action de D (opérant par conjugaison sur la réunion des $\mathscr{X}_i$ et par l'intermédiaire de M_{24} sur S). Soit Q^+ le sous-groupe de Q engendré par $\mathscr{U}$: c'est un groupe abélien élémentaire d'ordre 2^{13}. Pour $q \in \mathscr{X}_i$ (i = 1, 2), le centralisateur de q dans Q^+ est un sous-groupe d'indice deux de Q^+ ne contenant pas z_0, donc le noyau d'un caractère non-trivial sur z_0, et il existe une unique droite V_q de V stable par Q^+ et sur laquelle Q^+ opère par ce caractère. Finalement, pour $q \in \mathscr{X}_i$, on a $\psi_1(q) = e \otimes v$ où e est l'un des deux éléments de $\sigma(q)$ et v et l'un des deux vecteurs unitaires de V_q. Cette propriété et le fait que ψ_1 est un isomorphisme de $\tilde{D}$-module caractérisent ψ_1 à la multiplication par — 1 près. (La non-unicité de ψ_1 sera sans conséquence, et est d'ailleurs inévitable puisque z induit sur B_1 la multiplication par — 1 et respecte par ailleurs tous les choix qu'on a fait.)

9. *La forme cubique γ. Comment on vérifie la proposition 4*

Chacune des formes γ_i du § 7 peut être réécrite dans les « coordonnées » adaptées au groupe $\check{D}$, c'est-à-dire au moyen du système générateur $S \cup \bigcup_i (v(\mathscr{U}_i) \cup v(\mathscr{Y}_i) \cup v(\mathscr{X}_i))$ du $\mathbf{Q}$-module B. Il est alors facile, du

moins en principe, de trouver les conditions nécessaires et suffisantes d'invariance par $\check{D}$ de la forme $\sum_1^6 c_i\gamma_i$. Le résultat est le suivant :

PROPOSITION 4′. *La forme cubique* $\sum_1^6 c_i\gamma_i$ *est invariante par* $\check{D}$ *si et seulement si elle est proportionnelle à la forme :*

$$\gamma = 2^7\gamma_1 + \gamma_2 + 2^4\gamma_3 + 2^{15}\gamma_4 + 2^{17}\gamma_5 - 2^9\gamma_6.$$

La proposition 4 s'en déduit aisément. L'assertion (iii) de cette proposition est équivalente à la non-nullité du coefficient de γ_6 dans γ.

On a vu dans le cours que pour prouver l'assertion « il faut » de la proposition 4′, on doit seulement calculer les γ_i sur certains éléments appartenant à la réunion de T, des U_i et des X_i ; cela permet de déterminer assez simplement les coefficients de la forme invariante γ (car Y est la composante du D-module B la plus difficile à manier). Cependant, c'est l'assertion « il suffit » de la proposition 4′ dont on a besoin pour prouver l'existence du groupe de Griess-Fischer. On établit cette assertion en calculant γ sur les diverses composantes du produit $B \times B \times B$ et en *constatant* l'invariance par D. Pour ce calcul, on doit seulement considérer les composantes $T \times T \times T$, $T \times U_i \times U_i$, $T \times Y \times Y$, $T \times X_i \times X_i$, $U_i \times U_i \times U_i$, $U_0 \times U_1 \times U_2$, $U_i \times Y \times Y$, $U_i \times X_i \times X_i$, $U_i \times X_j \times X_j$ $(i \neq j)$, $Y \times Y \times Y$, $Y \times X_i \times X_i$, $X_0 \times X_1 \times X_2$, car il est facile de voir que l'invariance de γ par Q impose sa nullité sur toutes les composantes de $B \times B \times B$ qui ne se déduisent pas de l'une de celles-là par une permutation des facteurs. Nous nous bornerons ici à écrire, à titre d'exemples, quelques-unes des douze formules que l'on obtient ; on verra ainsi de quelle façon l'invariance par $\check{D}$ découle de la forme même des relations.

Etablissons d'abord quelques conventions de langage et de notations. Les formules donnant la forme γ se simplifient lorsqu'on étend celle-ci à l'espace $Q.1 \oplus B = {}^{aa}\mathrm{End}\, L \oplus B_2 \oplus B_1 = \mathbf{Q}[S] \oplus (\bigoplus_i U_i) \oplus Y \oplus (\bigoplus_i X_i)$ (on identifie $\mathbf{Q}[S] \oplus U_0$ à ${}^{aa}\mathrm{End}\, L$ par ψ_* : cf. § 8) en posant $\gamma(1, 1, B) = \{0\}$, $\gamma(1, b, b') = 2^7\beta(b, b')$ pour $b, b' \in B$ et $\gamma(1, 1, 1) = 24.2^9$; la restriction de γ à l'espace ${}^{aa}\mathrm{End}\, L$ est alors la forme $(x, y, z) \mapsto 2^8\,\mathrm{Tr}\,(xyz + zyx)$. Si $u = q\langle z_i\rangle$ et si l'image de q dans M_2 a pour représentant dans Λ_2 le vecteur $4e—4e'$, avec $e, e' \in E$, nous appelons *support* de u le couple $\mathrm{supp}\, u = \{(\pm e), (\pm e')\} \subset S$. On définit de façon analogue le support $\mathrm{supp}\, y$ d'un élément y de $\mathscr{Y}_0$, support qui est un bloc (octade) du système de Steiner ; utilisant l'action de $\check{D}$ sur la réunion des $\mathscr{Y}_i$ (par conjugaison) et sur S (par M_{24}), on étend cette notion de support à tout $y \in \mathscr{Y}_i$, $i = 0, 1, 2$. Rappelons qu'au § 8, on a défini des applications $\sigma : \mathscr{X}_i \to S$. Pour $u \in \mathscr{U}_i$,

$y \in \mathscr{Y}_i$, $x \in \mathscr{X}_i$, convenons de poser $-u = uz_j$ $(j \neq i)$, $-y = yz_i$ et $-x = xz_i$.

Dans les relations suivantes, s, s', s'' désignent des éléments de S, x_i, x'_i, x''_i des éléments de $\mathscr{X}_i$, et y_i, y'_i, y''_i des éléments de $\mathscr{Y}_i$; des expressions telles que $\gamma(s, x_i, x'_i)$, $\gamma(y_i, y'_i, y''_i)$, ... signifient $\gamma(s, v(x_i), v(x'_i))$, $\gamma(v(y_i), v(y'_i), v(y''_i))$, ... ; les éléments i, j de $\{0, 1, 2\}$ sont supposés *distincts*. On a :

$$\gamma(s, s', s'') = \begin{cases} 2^9 & \text{si } s = s' = s'', \\ 0 & \text{sinon ;} \end{cases}$$

$$\gamma(s, x_i, x'_i) = \begin{cases} \pm 36 & \text{si } x'_i = \pm x_i \text{ et } \sigma(x_i) = s, \\ \pm 4 & \text{si } x'_i = \pm x_i \text{ et } \sigma(x_i) \neq s, \\ 0 & \text{sinon ;} \end{cases}$$

si $u = q\langle z_i \rangle$, alors

$$\gamma(u, x_i, x'_i) = \begin{cases} \pm 12 & \text{si } x'_i = x_i \text{ et } \sigma(x_i) \in \operatorname{supp} u, \text{ le signe } + \text{ correspondant au cas où } qx_i \in \mathscr{X}_i, \\ \pm 4 & \text{si } x'_i = x_i \text{ et } \sigma(x_i) \notin \operatorname{supp} u, \text{ le signe } + \text{ correspondant au cas où } q \text{ et } x_i \text{ commutent}, \\ 0 & \text{si } x'_i \neq \pm x_i, \end{cases}$$

et

$$\gamma(u, x_j, x'_j) = \begin{cases} \pm 2^4 & \text{si } \pm x'_j \in ux_j = \{qx_j, qz_ix_j\} \text{ (ce qui implique que } \operatorname{supp} u = \{\sigma(x_j), \sigma(x'_j)\}), \\ 0 & \text{sinon ;} \end{cases}$$

$$\gamma(y_i, y'_i, y''_i) = \begin{cases} \pm 2^4 & \text{si } \pm y''_i = y_iy'_i, \\ 0 & \text{sinon ;} \end{cases}$$

etc.

On voit que, comme il a été dit plus haut, la fonction γ définie par de telles relations est manifestement invariante par $\check{D}$.

Remarques. a) Bien entendu, la preuve des relations précédentes doit être faite *séparément* pour les diverses valeurs des indices i et j (c'est seulement en comparant les résultats obtenus qu'on établit l'invariance). Ainsi, le calcul de $\gamma(y_i, y'_i, y''_i)$ est très différent selon que $i =$ ou $\neq 0$. Cependant, on sait *a priori* que γ est invariant par $\tilde{D}$, de sorte que les indices 1 et 2 sont interchangeables. Au total, les calculs à effectuer sont au nombre de 22 :

un seul pour $T \times T \times T$, $U_0 \times U_1 \times U_2$ et $X_0 \times X_1 \times X_2$, trois pour $U_i \times X_j \times X_j$ et deux pour chacun des autres produits énumérés plus haut.

b) Il est relativement facile de montrer que pour chacun des produits $T \times T \times T$, $T \times Y \times Y$, $Y \times Y \times Y$, $U_0 \times U_1 \times U_2$ et $X_0 \times X_1 \times X_2$, l'espace K des formes trilinéaires D-invariantes est de dimension un. Le groupe $\check{\mathrm{D}}$ opère sur K par l'intermédiaire de $\check{D}/D \cong \mathfrak{S}_3$, mais comme $\tilde{D}$ opère trivialement sur K (puisque la restriction de γ au produit considéré est non nulle et fixe par $\tilde{D}$), il doit en être de même de $\check{D}$. On peut donc, du moins pour la preuve de la $\check{D}$-invariance, se dispenser de calculer la restriction de γ à ces cinq produits. Cela évite sept des 22 calculs en question ci-dessus, et notamment trois des moins immédiats.

c) La fonction $B \otimes B \to B$ déduite de γ par l'identification de B avec son dual est égale à $-\frac{4}{9}$ fois la loi de produit de [Gr], table 6.1, p. 40. Les 22 calculs dont on vient de parler correspondent en gros aux calculs des §§ 10 et 11 de [Gr]. Les formules et les calculs de [Gr] sont sensiblement plus compliqués que les nôtres notamment à cause des problèmes de signes que nous avons réussi à éviter ici, dans une large mesure, grâce à l'emploi systématique de doubles bases.

J. T.

Séminaire

Le séminaire a été consacré à quelques applications des algèbres et groupes de Kac-Moody.

J. Tits, *Rappels sur les algèbres et groupes de Kac-Moody ; modèles de résonance duaux (introduction)* (2 exposés).

B. Julia, *Algèbres de type affine et supergravité* (2 exposés).

G. Segal, *Representations of loop groups* (2 exposés).

A. Neveu, *Introduction aux modèles de cordes duales et origine physique des opérateurs de vertex* (2 exposés).

J.-L. Verdier, *Symétrie des équations de Kadomcev-Petviašvili* (4 exposés).

Missions et conférences

Exposés

— *Über die Griess'sche Konstruktion der sporadischen Gruppe von Fischer-Griess,* Bielefeld, février 1983, Bâle, avril 1983.

— *Gebäude und endliche Geometrien vom affinen Typ,* Giessen, février 1983.

— *Sur la construction du « Monstre » de Griess-Fischer,* Groupe de contact « Algèbre » du F.N.R.S., Mons, mars 1983.

Conférences sur invitation de la London Mathematical Society comme « Hardy Lecturer 1983 », mai-juin 1983

— *The Leech lattice,* Durham ; Edinburgh Mathematical Society.

— *The principle of inertia in relativity theory,* Aberdeen.

— *Buildings and incidence geometries with diagrams,* Liverpool.

— *Free geometries and Coxeter diagrams,* Aberystwyth.

— *On Griess' construction of the Monster,* Birmingham, London Algebra Colloquium.

— *Algebras and groups of Kac-Moody : a survey,* Warwick ; Symposium « Algebra in Physics », Manchester ; Edinburgh ; London Mathematical Society (« Hardy Lecture »).

— *Maximal subgroups of linear groups,* Oxford ; Queen Mary College, Londres.

— *Reductive groups over local fields,* Manchester.

— *Chevalley groups and Kac-Moody groups : an axiomatic approach,* Cambridge.