## Théorie des groupes

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

Le cours de cette année a eu pour objet *Le groupe de GRIESS-FISCHER : constructions et « Moonshine » ;* l'étude de ces questions sera poursuivie l'an prochain.

### 1. *Le module du « Moonshine », d'après FRENKEL-LEPOWSKY-MEURMAN*

Cette partie du cours était basée sur les travaux de I. FRENKEL, J. LEPOWSKY et A. MEURMAN concernant le « Monstre », et notamment sur leur communication aux *Proceedings Nat. Acad. Sci.* 81 (1984), 3256-3260, désignée ci-dessous par le sigle [FLM].

Soient $\Lambda$ le réseau de LEECH, doté de son produit scalaire naturel $< , >$, $< \epsilon > = \{1, \epsilon\}$ un groupe d'ordre deux et

$$(*) \qquad 1 \to < \epsilon > \to \tilde{\Lambda} \xrightarrow{\pi} \Lambda \to 1$$

une extension centrale telle que le commutateur de deux éléments quelconques $\lambda$ et $\lambda'$ de $\tilde{\Lambda}$ soit égal à $\epsilon^{< \pi(\lambda), \pi(\lambda') >}$ : les extensions ayant cette propriété sont toutes isomorphes entre elles et l'on en choisit une (dans le cours, on a systématiquement évité de faire le choix — non invariant — d'un cocyle décrivant l'extension). Le sous-groupe de $\tilde{\Lambda}$ engendré par les carrés des éléments $\lambda$ tels que $< \pi(\lambda), \pi(\lambda) >$ soit divisible par 4 est appliqué bijectivement sur $2\Lambda$ par $\pi$ ; on le désignera aussi, abusivement, par $2\Lambda$. On a $\mathrm{Int}\, \tilde{\Lambda} = \tilde{\Lambda} / (2\Lambda + < \epsilon >) = \Lambda / 2\Lambda$, quotient qui sera noté $M$. Le quotient $Q = \tilde{\Lambda} / 2\Lambda$ est un groupe extra-spécial d'ordre $2^{1+24}$, extension centrale de $M$ par un groupe $< q_0 >$ d'ordre deux.

Soit $C_1$ le groupe des automorphismes de (*) qui induisent sur $\Lambda$ une isométrie (c'est-à-dire un élément du groupe de CONWAY $\cdot 0$, que nous noterons plutôt $\widetilde{\mathrm{Co}}_1$) ; il est extension de $\widetilde{\mathrm{Co}}_1$ par $M$. Le sous-groupe $\overline{C}$ de Aut $Q$ induit par $C_1$ est extension du groupe de CONWAY $\mathrm{Co}_1$ ($= \cdot 1$) par $M$ et $C_1$ est extension de $\overline{C}$ par un groupe $< z_1 >$ d'ordre deux.

Choisissons une fois pour toutes un corps $K$ de caractéristique différente de 2. On sait que le groupe extra-spécial $Q$ possède une et, à équivalence près, une seule représentation linéaire fidèle absolument irréductible sur $K$, dont le degré est $2^{12}$. Soient $T$ l'espace de cette représentation et $\overline{T}$ l'espace projectif de $T$. L'unicité de la représentation en question implique l'existence d'un plongement de Aut $Q$, donc aussi de $\overline{C}$, dans le groupe projectif PGL $(\overline{T})$. Soit $C_2$ le groupe dérivé de l'image réciproque de $\overline{C}$ dans GL $(T)$ ; c'est à nouveau une extension centrale de $\overline{C}$ par un groupe $< z_2 >$ d'ordre 2.

On note encore $\tilde{C}$ le « produit fibré » de $C_1$ et $C_2$ au-dessus de $\overline{C}$, $\tilde{z}$ l'élément $(z_1, z_2)$ de ce produit, $C$ le quotient $C / < \tilde{z} >$ et $z$ l'image commune de $(z_1, 1)$ et $(1, z_2)$ dans le quotient ; ainsi, le groupe $C$ est, lui aussi, extension centrale de $\overline{C}$ par un groupe d'ordre deux $< z >$.

Soit $t$ une indéterminée. Si $X$ est un espace vectoriel sur $K$, on note $X[t]$ l'espace vectoriel $X \otimes K[t]$ doté de sa graduation naturelle, et, pour tout espace vectoriel gradué $Y$, ce même espace $Y$ dont la graduation est augmentée d'un nombre rationnel $a$ est noté $t^a Y$. Désignons par $K[\tilde{\Lambda}]^{\cdot}$ le quotient de l'algèbre de groupe $K[\tilde{\Lambda}]$ par l'idéal principal $(1 + \epsilon)$ ; ainsi, $\tilde{\Lambda}$ s'applique bijectivement sur une *double base* (réunion d'une base et de son opposée) de l'espace vectoriel $K[\tilde{\Lambda}]^{\cdot}$, et sera identifié avec elle. On gradue $K[\tilde{\Lambda}]^{\cdot}$ en attribuant à tout élément $\lambda$ de $\tilde{\Lambda}$ le degré $< \pi(\lambda), \pi(\lambda) > / 2$. Posons $\mathfrak{h} = \Lambda \underset{\mathbf{Z}}{\otimes} K$ et

$$(1) \qquad W = t^{-1} S(t \cdot \mathfrak{h}[t]) \otimes K[\tilde{\Lambda}]^{\cdot} \oplus t^{1/2} S(t^{1/2} \cdot \mathfrak{h}[t]) \otimes T,$$

où $S$ désigne le foncteur « algèbre symétrique ». L'espace $W$ est, de façon naturelle, un $C$-module gradué, car $C_1$ opère sur $K[\tilde{\Lambda}]^{\cdot}$ et sur $\mathfrak{h}$ (à travers $\widetilde{\mathrm{Co}}_1$), tandis que $C_2$ opère sur $T$. L'espace, noté $V$, des points fixes de $z$ dans $W$, est un $C$-module gradué *à degrés entiers* ; en effet, l'intersection de $V$ avec le deuxième terme de (1) est la somme des composantes homogènes de degré entier de ce terme.

A tout endomorphisme $g$ de degré zéro d'un espace vectoriel gradué $Y$ dont les composantes homogènes sont de dimension finie est naturellement associée une série formelle que l'on peut appeler sa *trace (graduée)*, à savoir la série $\Sigma\, (\mathrm{tr}_i\, g)\, \xi^i$, où $\mathrm{tr}_i\, g$ désigne la trace de la restriction de $g$ à la composante homogène de $Y$ de degré $i$ ; on la notera $\tau_Y(g)$, ou encore $\tau_Y(g, \xi)$.

Rappelons que le groupe sporadique de GRIESS-FISCHER, ou « Monstre », noté $F$, est un groupe fini simple contenant $C$ comme centralisateur d'une involution [1] et que la conjecture de CONWAY-NORTON (« Monstrous Moon-

(1) Un groupe fini simple ayant cette propriété est dit « of Monster type ». Son unicité à isomorphisme près n'est guère douteuse, mais n'est pas encore entièrement démontrée (bien qu'un progrès essentiel ait été fait récemment par S. NORTON dans cette direction). Pour éviter toute ambiguïté, il convient donc de préciser que, dans ce résumé, $F$ désigne le groupe « of Monster type » particulier construit par R. GRIESS dans son article « The Friendly Giant », dont la référence est rappelée plus loin.

shine », *Bull. London Math. Soc.*, 11 (1979), 308-339) concerne l'existence d'un $F$-module gradué tel que les traces (graduées) des divers éléments de $F$ soient les développements à l'infini de fonctions modulaires (pour des sous-groupes de $\mathrm{PSL}_2(\mathbf{R})$ commensurables au groupe modulaire mais en général distincts de lui) spécifiées par la conjecture.

Supposons provisoirement que la caractéristique de $K$ est nulle. L'espace vectoriel gradué $V$ décrit plus haut est, sous cette hypothèse, le support du « module du Moonshine » proposé par FRENKEL, LEPOWSKY et MEURMAN. Ceux-ci montrent que l'action de $C$ sur $V$ s'étend en une action de $F$ et conjecturent que, pour $f \in F$, $\tau_v(f)$ est la série prescrite par la conjecture de CONWAY-NORTON. Cependant, jusqu'ici, $\tau_v(f)$ n'a pu être calculé que pour $f \in C$ : ce calcul est alors facile, comme on va le voir, mais, même dans ce cas, l'égalité de $\tau_v(f)$ avec la série conjecturée n'a pas été vérifiée en général.

Soient $c$ un élément de $C$, $(c_1, c_2)$ avec $c_1 \in C_1$ et $c_2 \in C_2$, un représentant de $c$ dans $C$, $c_0$ la projection de $c_1$ dans $\widetilde{\mathrm{Co}}_1$ identifié à son image dans $\mathrm{GL}(\mathfrak{h})$, $\varphi(c_0, \xi)$ le polynôme dét $(1 - \xi c_0)$ et $\mathrm{H}(c_0, \xi)$ la série formelle $\xi \prod_{i=1}^{\infty} \varphi(\xi^i)$. Un calcul immédiat montre que la trace de $c_1$ dans $t^{-1}S(t \cdot \mathfrak{h}[t])$ est égale à $\mathrm{H}(c_0, \xi)^{-1}$ et, observant que $t \cdot \mathfrak{h}[t] + t^{1/2} \cdot \mathfrak{h}[t] = t^{1/2} \cdot \mathfrak{h}[t^{1/2}]$, on en déduit que la trace de $c_1$ dans $t^{1/2}S(t^{1/2} \cdot \mathfrak{h}[t])$ est $\mathrm{H}(c_0, \xi) \cdot \mathrm{H}(c_0, \xi^{1/2})^{-1}$. Notons $\Theta(c_1, \xi)$ la trace de $c_1$ dans $K[\tilde{\Lambda}]^{\cdot}$ ; c'est une série que l'on peut exprimer à l'aide de « séries thêta » de translatés de sous-réseaux de $\Lambda$, dépendant de $c_1$ ; par exemple, $\Theta(1, \xi)$ n'est autre que la série thêta du réseau de LEECH lui-même. Désignant encore par $\chi_T$ le caractère de la représentation de $C_2$ dans $T$, on trouve finalement que

$$(2) \quad \tau_W(c_1, c_2) = \Theta(c_1, \xi) \cdot \mathrm{H}(c_0, \xi)^{-1} + \chi_T(c_2) \cdot \mathrm{H}(c_0, \xi) \cdot \mathrm{H}(c_0, \xi^{1/2})^{-1},$$

et, comme $(c_1, c_2)$ et $(c_1 z_1, c_2 z_2)$ coïncident sur $V$ et sont opposés sur un complémentaire de $V$ dans $W$,

$$(3) \quad \tau_V(c) = \frac{1}{2}(\tau_W(c_1, c_2) + \tau_W(c_1 z_1, c_2 z_2)).$$

Calculons en particulier la série $\tau_V(1)$, qui fournit les dimensions des composantes homogènes du module gradué $V$. Utilisant les formules de transformation bien connues des séries $\Theta$ et $\eta$, on vérifie immédiatement que la fonction $\tau_V(1, \exp 2\pi i \xi)$, qui est invariante par $\xi \mapsto \xi + 1$ (puisque $\tau_V(1)$ est une série de puissances entières), l'est aussi par $\xi \mapsto -\xi^{-1}$ ; c'est donc une fonction modulaire (pour le groupe modulaire lui-même). De plus, $\tau_V(1) = \xi^{-1} +$ des termes de degrés strictement positifs (car $V$ n'a manifestement pas d'élément homogène non nul de degré zéro). Donc $\tau_V(1, \exp 2\pi i \xi) = j - 744$, où $j$ est l'invariant modulaire ; ainsi, $\tau_V(1)$ est bien, comme le veut la conjecture de CONWAY-NORTON, le développement à l'infini de $j - 744$.

La formule suivante, conséquence immédiate de (2) et (3), s'avère utile :

(4) $\tau_V(c) + \tau_V(cz) = \Theta(c_1, \xi) \cdot \mathrm{H}(c_0, \xi)^{-1} + \Theta(c_1 z_1, \xi) \cdot \mathrm{H}(-c_0, \xi)^{-1}$.

Pour $c = 1$, on en déduit :

(5) $$\tau_V(z) = \Theta(z_1, \xi) \cdot \mathrm{H}(-1, \xi)^{-1} = \Delta(\xi) \cdot \Delta(2\xi)^{-1},$$

où $\Delta(\xi) = \xi \cdot \prod_{i=1}^{\infty} (1 - \xi^i)^{24}$ ; ceci est, à nouveau, conforme à la conjecture de CONWAY-NORTON. La deuxième égalité (5) s'établit par un argument très simple qui m'a été fourni par J.-P. SERRE : appelant $G(\xi)$ la différence des deux membres, on note que $g(\xi) = G(\exp 2\pi i \xi)$ est invariante par le groupe $\Gamma_0(2)$ ; il suffit alors de vérifier que $g$ est « holomorphe à distance finie » et nulle en $\xi = 0$ (c'est-à-dire que $G$ n'a pas de terme en $\xi^{-1}$ ni de terme constant), et que la fonction $g(-1/\xi)$ (que l'on calcule en utilisant les formules de transformation connues de $\Theta$ et $\eta$) n'a pas de pôle à l'origine.

2) *La composante homogène de degré un du module $V$ : formes invariantes*

Désormais, $K$ est à nouveau un corps quelconque de caractéristique différente de deux. Soient $\Lambda_2$ l'ensemble $\{\lambda \in \Lambda \mid <\lambda, \lambda> = 4\}$, $\tilde{\Lambda}_2$ son image réciproque dans $\tilde{\Lambda}$ et $Q_2 = (\tilde{\Lambda}_2 + 2\Lambda / 2\Lambda)$ la projection canonique de $\tilde{\Lambda}_2$ dans $Q$ (qui est aussi l'image réciproque dans $Q$ de la projection canonique de $\tilde{\Lambda}_2$ dans $M$). Chaque élément $q$ de $Q_2$ a pour image réciproque dans $\tilde{\Lambda}_2$ une paire d'éléments dont la somme dans $K[\tilde{\Lambda}]^{\cdot}$, notée $\upsilon(q)$, appartient à $V$ (on identifie ici $K[\tilde{\Lambda}]^{\cdot}$ au sous-espace $1 \otimes K[\tilde{\Lambda}]^{\cdot}$ de $W$). Le sous-espace vectoriel de $V$ engendré par $\upsilon(Q_2)$, et dont $\upsilon(Q_2)$ forme une double base, sera noté $K[Q_2]^{\cdot}$.

On vérifie aisément que la composante $V_1$ de degré un de $V$ s'identifie à la somme directe

(6) $$S(\mathfrak{h}) \oplus K[Q_2]^{\cdot} \oplus \mathfrak{h} \otimes T.$$

Pour $K = \mathbf{Q}$, ceci n'est autre que le $C$-module utilisé par R. GRIESS (*Inventiones Math.*, 69 (1982), 1-102) pour construire le « Friendly Giant » $F$. Le renseignement essentiel, fourni par S. NORTON, qui sert de point de départ à GRIESS, est l'existence de deux applications bilinéaires invariantes par $F$, une forme bilinéaire symétrique $<\ ,\ >$ : $V_1 \times V_1 \to K$ (2) et une loi de produit $\mu$ : $V_1 \times V_1 \to V_1$ bilinéaire commutative et « autoadjointe par rapport à $<\ ,\ >$ », c'est-à-dire telle que

(7) $$<v, \mu(v', v'')> = <\mu(v, v'), v''> \quad (v, v', v'' \in V_1).$$

(2) Toute confusion étant exclue par le contexte, nous utilisons la même notation $<\ ,\ >$ pour désigner le produit scalaire canonique dans $\Lambda$, son « image » dans $\mathfrak{h}$ (par tensorisation avec $K$) et la forme bilinéaire dont il est question ici.

Une étape, facile mais importante, de sa recherche est donc la détermination de tous les couples $< , >$, $\mu$ de ce type invariants de $C$. Il était intéressant de refaire ce travail sous les hypothèses un peu plus générales du cours, le but étant d'obtenir des « formules universelles », à coefficients dans $\mathbb{Z}[1/2]$ (on aurait d'ailleurs pu, moyennant quelques précautions de langage, travailler directement sur cet anneau plutôt que sur un corps $K$). Le résultat est énoncé ci-après.

Nous identifions désormais $S(\mathfrak{h})$ et l'espace $\mathrm{End}^{aa}(\mathfrak{h})$ des endomorphismes autoadjoints de $\mathfrak{h}$ : le carré $h^2$ d'un élément $h$ de $\mathfrak{h}$ est identifié à l'endomorphisme $x \mapsto < h, x > \cdot h$ de $\mathfrak{h}$. La trace d'un élément $b$ de $\mathrm{End}\,\mathfrak{h}$ est notée $\mathrm{tr}\, b$ ; en particulier, $\mathrm{tr}\, h^2 = < h, h >$. Nous désignons par $\mathrm{tr}_{V_1}$ la forme linéaire sur $V_1$ égale à tr sur $S(\mathfrak{h}) = \mathrm{End}^{aa}(\mathfrak{h})$ et nulle sur les autres termes de la somme (4), et par $V_1^\circ$ le noyau de cette forme. Pour $q \in Q_2$, il y a deux éléments opposés de $\Lambda_2$, soient $\lambda$ et $-\lambda$, dont l'image dans $M = Q / < q_0 > = \Lambda / 2\Lambda$ est égale à $q$ ; l'élément $(\lambda \otimes 1)^2$ de $S(\mathfrak{h}) = \mathrm{End}^{aa}(\mathfrak{h})$, élément qui ne dépend que de $q$, sera noté $b_q$. Pour $q, q' \in Q_2$, nous désignons par $\delta_{qq'}$ (« symbole de KRONECKER ») l'élément de $K$ égal à 1 si $q' = q$, à $-1$ si $q' = qq_0$ et à 0 sinon. Soient $d$ un élément non nul de $K$ et $< , >_T$ une forme bilinéaire symétrique non dégénérée sur $T$ invariante par $Q$. Munissons $V_1$ du produit scalaire $< , >$ tel que les trois termes de la somme (6) soient deux à deux orthogonaux et que l'on ait :

$$< b, b' > = d \cdot \mathrm{tr}\, bb' \qquad \text{pour } b, b' \in S(\mathfrak{h}) = \mathrm{End}^{aa}(\mathfrak{h}) ;$$
$$< \upsilon(q), \upsilon(q') > = \delta_{qq'} \qquad \text{pour } q, q' \in Q_2 ;$$
$$< h \otimes t, h' \otimes t' > = < h, h' > \cdot < t, t' >_T \qquad \text{pour } h, h' \in \mathfrak{h} \text{ et } t, t' \in T.$$

On note que le choix de $d$ et de $< , >_T$ n'est pas indifférent car si on les multiplie par des éléments de $K$ non carrés, la forme $< , >$ est remplacée par une autre qui n'est généralement pas équivalente à un multiple de la première. Il est facile de voir que toute forme bilinéaire symétrique non dégénérée sur $V_1$ invariante par $C$ est combinaison linéaire de $< , >$ (pour un choix approprié de $d$ et $< , >_T$) et de la forme $(v, v') \mapsto \mathrm{tr}_{V_1} v \cdot \mathrm{tr}_{V_1} v'$. Pour ne pas compliquer inutilement les formules nous nous abstiendrons d'ajouter à $< , >$ un multiple indéterminé de $\mathrm{tr}_{V_1} v \cdot \mathrm{tr}_{V_1} v'$ ; on peut d'ailleurs se convaincre que cela serait sans intérêt pour l'étude du « Monstre ».

Enfin, *les lois bilinéaires* $\mu : V_1 \times V_1 \to V_1$ *commutatives, satisfaisant à (7) et invariantes par C sont toutes données par les formules suivantes,* où $k_1$, $k_1'$, $k_1''$, ..., $k_6$ sont dix constantes arbitraires, éléments de $K$, et où $b$, $b' \in S(\mathfrak{h}) = \mathrm{End}^{aa}(\mathfrak{h})$ ; $q, q' \in Q_2$ ; $h, h' \in \mathfrak{h}$ ; $t, t' \in T$ ; et 1 désigne l'élément unité de $\mathrm{End}\,\mathfrak{h}$ :

$$\mu(b, b') = k_1 \cdot (bb' + b'b) + k_1' \cdot (\mathrm{tr}\, b \cdot b' + \mathrm{tr}\, b' \cdot b + \mathrm{tr}\, bb' \cdot 1) + k_1'' \cdot (\mathrm{tr}\, b \cdot \mathrm{tr}\, b' \cdot 1) ;$$

$$\mu\,(b,\ \upsilon\,(q)) = \mu\,(\upsilon\,(q),\ b) = d \cdot (k_2 \cdot \operatorname{tr} bb_q + k_2' \cdot \operatorname{tr} b) \cdot \upsilon\,(q)\ ;$$

$$\mu\,(\upsilon\,(q),\ \upsilon\,(q')) = \delta_{qq'} \cdot (k_2 \cdot b_q + k_2' \cdot 1) + \begin{cases} k_3 \cdot \upsilon\,(qq') \text{ si } qq' \in Q_2, \\ 0 \text{ sinon}\ ; \end{cases}$$

$$\mu\,(b,\ h \otimes t) = \mu\,(h \otimes t,\ b) = d \cdot (k_4 \cdot b\,(h) + k_4' \cdot \operatorname{tr} b \cdot h) \otimes t\ ;$$

$$\mu\,(\upsilon\,(q),\ h \otimes t) = \mu\,(h \otimes t,\ \upsilon\,(q)) = (k_5 \cdot h + k_6 \cdot b_q\,(h)) \otimes q\,(t)\ ;$$

$$\begin{aligned} \mu\,(h \otimes t,\ h' \otimes t') = {} & < t,\ t' >_T \cdot (k_4 \cdot hh' + k_4' \cdot < h,\ h' > \cdot 1) \\ & + (k_5 / 2) \cdot < h,\ h' > \cdot \sum_{q \in Q_2} < q\,(t),\ t' >_T \cdot \upsilon\,(q) \\ & + (k_6 / 2) \cdot \sum_{q \in Q_2} < b_q\,(h),\ h' > \cdot < q\,(t),\ t' >_T \cdot \upsilon\,(q). \end{aligned}$$

3) *Trialité*

Pour construire le groupe $F$ à la façon de GRIESS, il faut trouver un automorphisme $g$ de $V_1$ qui, avec $C$, engendre un groupe fini simple dans lequel $C$ soit le centralisateur de $z$. Ensuite, pour faire de $V$ un $F$-module gradué, on doit prolonger l'automorphisme $g$ en un automorphisme de degré zéro $\tilde{g}$ de $V$ et montrer que le groupe d'automorphismes de $V$ engendré par $C$ et $\tilde{g}$ opère fidèlement sur $V_1$ (donc est isomorphe à $F$ lui aussi).

Une même observation heuristique, appliquée à $V_1$ et à $V$, permet d'orienter la recherche de $g$ et $\tilde{g}$ et même, s'aidant d'hypothèses naturelles basées sur des propriétés de $F$ connues *a priori*, de les *déterminer sans tâtonnement*, à un certain groupe de symétries près. Expliquons d'abord dans les grandes lignes le principe général de la méthode.

On appelle *croix* tout ensemble de 48 éléments de $\Lambda$, de carré scalaire 8, deux à deux orthogonaux ou opposés (donc formant une « double base orthogonale » de $\Lambda \otimes \mathbf{Q}$). On sait qu'il existe des croix et qu'elles sont permutées transitivement par le groupe de CONWAY $\widetilde{\mathrm{Co}}_1$ (cela résulte par exemple de la jolie preuve d'unicité du réseau de LEECH donnée par J.H. CONWAY : *Inventiones Math.*, 7 (1969), 137-142). L'observation à laquelle il a été fait allusion plus haut consiste en ceci : *si l'on distingue une croix*, on « brise » évidemment la symétrie des modules $V$ et $V_1$ — le groupe $C$ étant remplacé par un sous-groupe $D$, extension du groupe de MATHIEU $\mathrm{M}_{24}$ par un groupe d'ordre $2^{36}$ —, mais une *nouvelle symétrie d'ordre 3 apparaît*, symétrie que, suivant [FLM] nous appelons la *trialité* ; elle a d'ailleurs des liens avec la trialité du groupe $\mathrm{D}_4$. Notre formulation est volontairement vague : on peut, si l'on veut, la préciser en introduisant un groupe de symétries $\hat{D}$ dont $D$ est un sous-groupe d'indice trois (voir p. ex. l'*Annuaire du Collège de France* de 1982-1983, pp. 89-103, ou l'exposé n° 620 du *Séminaire BOURBAKI* de novembre 1983, exposé cité [SB] ci-après, en prenant toutefois garde aux différences

de notations [3]), mais cela n'est pas indispensable. Il s'avère en effet possible, par de simples considérations heuristiques, de transformer « par trialité » une certaine classe de conjugaison de $D$ et d'obtenir, de la sorte, *une famille* d'éléments $g$ ou $\tilde{g}$ qui, avec $C$, engendrent le groupe $F$ cherché. Le cas de $V$, esquissé dans [FLM], fait appel à la théorie de KAC-MOODY ; on y reviendra dans le cours de l'an prochain. Dans le cas de $V_1$, qui a été traité cette année, des raisonnements plus élémentaires conduisent, comme on va le voir, à des formules explicites pour $g$.

Choisissons donc une croix, appelée $8E$ et que, par abus de notation, nous identifierons à son image canonique $8E \otimes 1$ dans $\mathfrak{h}$. Ainsi, $E$ désignera, selon les circonstances, une double base de $\Lambda \otimes \mathbf{Q}$ ou une double base de $\mathfrak{h}$, dont les éléments sont de carré scalaire $1/8$. Posons $S = \{e^2 \mid e \in E\}$ ; c'est un ensemble (partie de $S(\mathfrak{h})$) à 24 éléments.

Le choix de $E$ détermine une partition de $\Lambda_2$ en trois sous-ensemble $\Lambda_2^4$, $\Lambda_2^2$, $\Lambda_2^1$ : un élément $\lambda$ de $\Lambda_2$ appartient à $\Lambda_2^4$ (resp. $\Lambda_2^2$ ; resp. $\Lambda_2^1$) s'il est de la forme $4(e_1 + e_2)$ (resp. $2(e_1 + \ldots + e_8)$ ; resp. $-4e_1 + \sum_{i=1}^{24} e_i$), où les $e_i$ appartiennent à une base de $\Lambda$ extraite de $E$ ; on pose alors $\operatorname{supp} \lambda = \{e_1^2, e_2^2\}$ (resp. $\operatorname{supp} \lambda = \{e_1^2, \ldots, e_8^2\}$ ; resp. $\sigma(\lambda) = e_1^2$). Ici, « supp » se lit « support de ». À cette partition correspond de façon évidente une partition $Q_2^4 \cup Q_2^2 \cup Q_2^1$ de $Q_2$. Si $q$ est un élément de $Q_2^4 \cup Q_2^2$ (resp. $Q_2^1$) et si $\lambda$ est un élément de $\Lambda_2$ ayant même projection que $q$ dans $\Lambda / 2\Lambda = Q / < q_0 >$, on pose $\operatorname{supp} q = \operatorname{supp} \lambda$ (resp. $\sigma(q) = \sigma(\lambda)$).

L'image de $E$ dans $M = \Lambda / 2\Lambda$ se compose d'un seul élément dont l'image réciproque dans $Q$ est notée $\{q_1, q_2\}$. *On se propose de faire jouer un rôle symétrique aux trois éléments* $q_0$, $q_1$, $q_2$ ; c'est un premier aspect du principe de trialité dont vont découler tous les autres.

Pour $j = 0, 1, 2$, notons $\mathcal{U}_j$ l'espace des classes latérales de $q_j$ dans $Q_2^4$. Nous allons définir des injections, notées $\upsilon$, des $\mathcal{U}_j$ dans $V_1$. Soit $u = \{r; rq_j\}$ un élément de $\mathcal{U}_j$. Si $j = 1$ ou 2, on pose simplement $\upsilon(u) = \upsilon(r) + \upsilon(rq_j)$. Si $j = 0$, l'image de $q$ dans $M$ coïncide avec celle d'un élément de $\Lambda_2^4$ de la forme $4e - 4e'$, où $e, e' \in E$, et l'on prend pour $\upsilon(u)$ l'élément $16\, ee'$ de $S(\mathfrak{h})$. (Le coefficient 16 pourrait ici être remplacé par une constante $c$ quelconque : cela entraînerait seulement une modification de la forme des énoncés des propositions 1 et 2 ci-dessous. Par exemple, la condition $d = 1$ de la proposition 1 deviendrait $d = 16 / c$.)

---

(3) Par exemple, les groupes notés ici $D$ et $\hat{D}$ s'appelaient respectivement $\bar{D}$ et $\check{D}$ dans le Résumé de cours de 1982-1983. Profitons de l'occasion pour corriger une erreur qui s'est glissée à la p. 93, ligne 24, de ce Résumé : $\bar{D}$ n'est évidemment pas extension de $M_{24}$ par $Q$, mais par un groupe d'ordre $2^{36}$ contenant $Q$, comme on l'a rappelé ici.

Soit $R$ le sous-groupe de $Q$ engendré par $Q_2^4$ ; c'est un 2-groupe abélien élémentaire d'ordre $2^{13}$ et un sous-groupe abélien maximal de $Q$. Pour $j = 0$, 1, 2, soit $\Psi_j$ l'ensemble des caractères irréductibles de $R$ valant $-1$ sur $q_i$ pour $i \neq j$ (donc valant 1 sur $q_j$). Soit $\mathcal{T}$ une double base de $T$, stable par $Q$ et formée de vecteurs propres pour $R$ : on sait qu'une telle double base existe (et est d'ailleurs unique à un facteur près). Chaque élément de $\mathcal{T}$ est transformé par $R$ selon un caractère appartenant à $\Psi_1 \cup \Psi_2$, d'où l'on déduit une partition $\mathcal{T}_1 \cup \mathcal{T}_2$ de $\mathcal{T}$. Posons $\mathcal{X}_0 = Q_2^1$ et, pour $j = 1$, 2, donnons-nous une « copie » $\mathcal{X}_j$ du sous-ensemble $E \otimes \mathcal{T}_j$ de $\mathfrak{h} \otimes T$, la bijection canonique $\mathcal{X}_j \to E \otimes \mathcal{T}_j$ étant, une fois encore, notée $\upsilon$. Chacun des ensembles $\mathcal{X}_j$ est doté d'applications naturelles $\sigma : \mathcal{X}_j \to S$ et $\psi : \mathcal{X}_j \to \Psi_j$. Pour $x \in \mathcal{X}_0$, $\sigma(x)$ a été défini plus haut et l'on prend pour $\psi(x)$ le caractère de $R$ dont le noyau est le centralisateur de $x$ dans $R$ ; pour $x \in \mathcal{X}_1 \cup \mathcal{X}_2$ et $\upsilon(x) = e \otimes t \in E \otimes \mathcal{T}$, on pose $\sigma(x) = e^2$ et $\psi(x)$ est défini comme le caractère par lequel $R$ opère sur $t$.

Pour tout $x \in \mathcal{X}_j$ et tout $r \in Q_2^4$ tel que $\sigma(x) \in \operatorname{supp} r$ et $\psi(x)(r) = 1$, on définit canoniquement un « produit » $rx$, élément de $\mathcal{X}_j$ tel que $\{\sigma(x), \sigma(rx)\} = \operatorname{supp} r$ et $\psi(rx) = \psi(x)$ (on note que ces relations caractérisent déjà $rx$ « au signe près »). Pour $j = 0$, $rx$ est simplement le produit de $r$ et $x$ dans $Q$. Pour $j = 1$ ou 2, il existe $e, e' \in E$ et $t \in \mathcal{T}_j$ — uniques à la multiplication *simultanée* par $-1$ près — tels que $r$ et $4e + 4e'$ aient même image dans $M = Q / < q_0 > = \Lambda / 2\Lambda$, et que $\upsilon(x) = e \otimes t$ ; on pose alors $\upsilon(rx) = e' \otimes t$, ce qui définit $rx$.

On note que *la réunion de* $\pm S$, *des* $\upsilon(\mathcal{U}_j)$, *de* $\upsilon(Q_2^2)$ *et des* $\upsilon(\mathcal{X}_j)$ *est une double base de* $V_1$.

Les notations choisies ont fait apparaître une certaine symétrie entre les $q_j$, les $\mathcal{U}_j$ et les $\mathcal{X}_j$ pour $j = 0$, 1, 2. *La trialité consiste à ériger cette symétrie en principe,* principe qui va nous fournir les automorphismes de $V_1$ dont nous avons besoin pour engendrer le groupe $F$ (avec $C$).

Puisque les éléments de $Q$, et en particulier ceux de $\mathcal{X}_0$, opèrent sur $V_1$, cela doit aussi être vrai des éléments de $\mathcal{X}_1 \cup \mathcal{X}_2$. Soit $x$ un élément de $\mathcal{X}_1$, pour fixer les idées. Partant des formules décrivant l'action (connue) d'un élément de $\mathcal{X}_0$ sur $S$ et les $\upsilon(\mathcal{U}_j)$, on en déduit, par une simple permutation d'indices, quelle doit être l'action de $x$ sur ces mêmes ensembles. Il vient :

(8) $$xs = s \qquad \text{pour } s \in S ;$$

(9) $$x\,\upsilon(u) = \upsilon(u) \qquad \text{pour } u \in \mathcal{U}_j ;$$

(10) $$\text{si } \{j, k\} = \{0, 2\} \text{ et } u = \{r, rq_j\} \in \mathcal{U}_j, \quad \text{alors } x\,\upsilon(u) = \psi(x)(r) \cdot \upsilon(r, rq_k).$$

Pour $x' \in \mathcal{X}_0$, il existe $x'' \in \mathcal{X}_2$ tel que $\upsilon(x'') = x'\,\upsilon(x)$, et l'on a $\sigma(x'') = \sigma(x)$ et $\psi(x'') = \psi(x) \cdot \psi(x')$. Par symétrie, il doit exister $x_1'' \in \mathcal{X}_2$

tel que $\upsilon(x_1'') = x\,\upsilon(x')$, et l'on doit avoir $\sigma(x_1'') = \sigma(x')$ et $\psi(x_1'') = \psi(x) \cdot \psi(x')$. Malheureusement, ces deux dernières conditions ne déterminent $\upsilon(x_1'')$ qu'à un facteur $\pm 1$ près, mais lorsque $\sigma(x') = \sigma(x)$, il y a un *choix naturel évident* (qui est d'ailleurs, en un sens que l'on peut préciser, le seul choix « cohérent » possible), à savoir $x_1'' = x''$. Ce choix signifie que l'on pose

(11) $x\,\upsilon(x') = x'\,\upsilon(x)$ pour $x' \in \mathscr{X}_0$ tel que $\sigma(x) = \sigma(x')$.

L'action de $x$ sur $\upsilon(\mathscr{X}_0)$ tout entier s'en déduit aussitôt car on exige évidemment que

(12) si $x' \in \mathscr{X}_0$ et $\sigma(x) \neq \sigma(x')$, et si $r$ est un élément de $Q_2^4$ tel que $\operatorname{supp} r = \{\sigma(x), \sigma(x')\}$ et $\psi(x)(r) = 1$, alors $x\,\upsilon(x') = r\,(x'\,\upsilon(rx))$ ;

en effet, le deuxième membre de cette égalité est égal à $r\,((rx)\,\upsilon(x'))$, vu (11). L'action de $x$ sur $\mathscr{X}_2$ résulte à présent de ce que $x$, comme les éléments de $\mathscr{X}_0$, doit être involutif :

(13) si $x' \in \mathscr{X}_2$, $x\,\upsilon(x')$ est l'élément $\upsilon(x'')$ de $\upsilon(\mathscr{X}_0)$ dont le transformé $x\,\upsilon(x'')$ (déterminé par (11) et (12)) est $\upsilon(x')$.

Reste à déterminer l'action de $x$ sur $\upsilon(Q_2^2)$. Pour cela, on utilise l'existence d'une loi de produit $\mu$ invariante par $x$, donnée par les formules du n° 2 avec $k_3 = 1$. (L'existence d'un produit invariant est, rappelons-le, une donnée essentielle de la méthode de GRIESS. La condition $k_3 = 1$ n'est évidemment pas une restriction si $k_3$ est non nul. L'hypothèse $k_3 \neq 0$ peut être prise comme une hypothèse de travail naturelle, mais, en fait, des calculs élémentaires, assez analogues à ceux esquissés ci-dessous pour le calcul de $k_6$, montrent que si $k_3 = 0$, l'invariance de $\mu$ par $x$ implique sa nullité sur $V_1^\circ \times V_1^\circ$.) Enonçons d'emblée le résultat :

(14) pour $y \in Q_2^2$, on a $x\,\upsilon(y) = 2^{-4} \cdot \gamma \cdot \Sigma\,(\rho\,\psi(x))\,(yq) \cdot \upsilon(q)$, où $q$ parcourt les éléments de $Q_2^2$ de support $\operatorname{supp} y$, où $\rho$ désigne le caractère de $R$ égal à $-1$ sur tous les éléments de $Q_2^4$ et où $\gamma = 1$ ou $-1$ selon que $\sigma(x) \notin$ ou $\in \operatorname{supp} y$.

Esquissons-en la preuve en supposant d'abord que $\sigma(x) \notin \operatorname{supp} y$. Soient $x'$, $x''$ des éléments de $Q_2^1 = \mathscr{X}_0$ tels que $y = x'x''$ et $\sigma(x') \in \operatorname{supp} y$ (d'où aussi $\sigma(x'') \in \operatorname{supp} y$). Comme $\upsilon(y) = \mu(\upsilon(x'), \upsilon(x''))$, on doit aussi avoir $x\,\upsilon(y) = \mu(x\,\upsilon(x'), x\,\upsilon(x''))$, expression que l'on peut calculer à l'aide de (12) et des formules donnant $\mu$. On obtient ainsi le résultat annoncé, à ceci près que le coefficient $2^{-4}$ de (14) est remplacé par $-(k_6/2)$. On doit donc encore déterminer $k_6$. Pour cela, considérons un élément $u = \{r, rq_1\}$ de $\mathscr{U}_1$ et un élément $x_0$ de $\mathscr{X}_0$ tels que $\operatorname{supp} r = \{\sigma(x), \sigma(x_0)\}$ et $\psi(x)(r) = \psi(x_0)(r) = 1$. On a $\mu(\upsilon(u), \upsilon(x_0)) = \upsilon(rx_0)$, d'où, transformant par $x$ et tenant compte de (9), (12) et (11), $\mu(\upsilon(\mathrm{u}), (rx_0)\,\upsilon(rx)) = (rx_0)\,\upsilon(x)$. Développant les deux

membres, il vient, tous calculs faits, $k_6 = -(1/4)$, d'où (14) lorsque $\sigma(x) \in \operatorname{supp} y$. (N.B. Le calcul de $\mu(x \upsilon (x'), x \upsilon (x''))$ est plus commode lorsqu'on choisit $x'$, $x''$ satisfaisant à $\sigma(x') = \sigma(x'') = \sigma(x)$, mais il n'existe pas alors, semble-t-il, de procédé aussi simple pour déterminer le coefficient qui est, dans ce cas, $k_5 / 2$.)

Le cas où $\sigma(x) \in \operatorname{supp} y$ se ramène aussitôt au précédent en posant $x = r_1 x_1$, où $r_1 \in Q_2^4$ est choisi de telle sorte que $\psi(x)(r_1) = 1$ et $\sigma(x) \in \operatorname{supp} r_1 \not\subset \operatorname{supp} y$. En effet, la trialité impose alors que $x \upsilon (y) = r_1((r_1 x) \upsilon (y))$, et il suffit de remarquer que $r_1$ transforme en son opposé tout $\upsilon(q)$ pour $q \in Q_2^4$ tel que $\operatorname{supp} q = \operatorname{supp} y$.

*Les formules* (8) *à* (14) *décrivent explicitement l'action de* $\mathscr{X}_1$ *sur* $V_1$. On en déduit aussitôt, par symétrie, l'action de $\mathscr{X}_2$ sur ce même espace.

4) *Récolte*

PROPOSITION 1. - *La « trace »* $\mathrm{tr}_{V_1}$ *est invariante par* $\mathscr{X}_1 \cup \mathscr{X}_2$. *Pour qu'un élément donné quelconque de* $\mathscr{X}_1 \cup \mathscr{X}_2$ *conserve le produit scalaire* $< , >$ *(dans* $V_1$*), il faut et il suffit que* $d = 1$ *et que les éléments de la double base* $\mathscr{T}$ *choisie dans* $T$ *soient de carré scalaire* 8 *(pour* $< , >_T$*).*

L'invariance de $\mathrm{tr}_{V_1}$ et la nécessité des conditions pour l'invariance de $< , >$ résultent des formules (8) à (14). Un calcul facile montre la réciproque. Observons que l'existence d'une double base $\mathscr{T}$ possédant la propriété requise impose une restriction à la forme $< , >_T$.

*Dorénavant, nous supposerons que* $< , >$ *est invariant par* $\mathscr{X}_1 \cup \mathscr{X}_2$ *donc, en particulier, que* $d = 1$.

PROPOSITION 2. - *Pour que le produit* $\mu$ *donné par les formules du n° 2 soit invariant par un élément donné quelconque de* $\mathscr{X}_1 \cup \mathscr{X}_2$, *il faut et il suffit qu'il existe des constantes* $k$, $k' \in \mathrm{K}$ *telles que l'on ait*

$$k_1 = 2k,\ k_2 = k_3 = k_4 = k,\ k_5 = k/8,\ k_6 = -k/4,\ k'_1 = k'_2 = k',$$
$$k'_4 = (k/8) + k'.$$

La nécessité des conditions n'est pas difficile à établir (cf. [SB], § 4 : la preuve indiquée là reste valable, *mutatis mutandis*, sous les hypothèses un peu plus générales du présent résumé). La réciproque (« il suffit ») se montre par des calculs de routine, sans difficulté mais assez longs.

*Dans la suite, nous supposons le produit* $\mu$ *invariant par* $\mathscr{X}_1 \cup \mathscr{X}_2$ *et non identiquement nul sur* $V_1^\circ \times V_1^\circ$ (ce qui signifie que la constante $k$ de la proposition 2 n'est pas nulle).

THÉORÈME. - *Le sous-groupe $F$ de* GL $(V_1)$ *engendré par $C$ et l'un quelconque des éléments de $\mathcal{X}_1 \cup \mathcal{X}_2$ est indépendant du choix de cet élément et est aussi le groupe de tous les automorphismes du système* $(V_1, \mathrm{tr}_{V_1}, <\ ,\ >, \mu)$ *(il est même, « en général », le groupe de tous les automorphismes de l'algèbre* $(V_1, \mu)$ : *voir la remarque ci-dessous). C'est un groupe fini simple et le centralisateur de $z$ dans $F$ est le groupe $C$.*

En caractéristique zéro, ce résultat est démontré dans un article paru aux *Inventiones Math.* 78 (1984), 491-499, article cité [IM] ci-après. Pour étendre la preuve au cas général, on a eu besoin du fait suivant.

LEMME. - *Les seules isométries de $\mathfrak{h} = \Lambda \otimes K$ stabilisant l'ensemble $\Lambda_2 \otimes 1$ sont les éléments du groupe de* CONWAY $\widetilde{\mathrm{Co}}_1$ *(tensorisés par $id_K$).*

Il suffit de faire voir que le produit scalaire de deux éléments $\lambda$, $\lambda'$ de $\Lambda_2$ est entièrement déterminé par leurs images $\lambda \otimes 1$ et $\lambda' \otimes 1$ dans l'espace « métrique » $\mathfrak{h}$, et cela résulte aussitôt des observations suivantes :

on a $< \lambda, \lambda' > = \pm 4$ si et seulement si $\lambda \otimes 1 = \pm \lambda' \otimes 1$ ;

on a $< \lambda, \lambda' > = \pm 2$ si et seulement si $< \lambda \otimes 1, \lambda' \otimes 1 > = \pm 2$ et $< \lambda, \lambda' > \neq \pm 4$ ;

on a $< \lambda, \lambda' > = -1$, 0 ou 1 si et seulement si $< \lambda \otimes 1, \lambda' \otimes 1 > = -1$, 0 ou 1 respectivement et si, en outre, $< \lambda, \lambda' > \neq \pm 2$ et $\pm 4$.

Les deux dernières assertions sont évidemment fausses en caractéristique deux ; j'ignore si le lemme, lui, reste vrai.

La proposition suivante est conséquence facile de la définition de $F$.

PROPOSITION 3. - *Les seuls sous-$F$-modules de $V_1$ sont* 0, $K \cdot 1$ *(où* 1 *est l'élément unité de* $\mathrm{End}^{aa}(\mathfrak{h})$), $V_1^\circ$ et $V_1$.

Comme $\mathrm{tr}_{V_1} 1 = 24$, cela revient à dire que le $F$-module $V_1^\circ$ est simple sauf en caractéristique 3, cas où $K \cdot 1 \subset V_1^\circ$ et $V_1^\circ / K \cdot 1$ est un $F$-module simple de dimension 196882.

L'« universalité » des formules donnant $C$ et $\mathcal{X}_1 \cup \mathcal{X}_2$ (comme ensembles d'automorphismes de l'espace vectoriel $V_1$) montre que le groupe $F$ est « le même » quel que soit le corps $K$ ; plus exactement, on peut définir un $\mathbb{Z}[1/2][F]$ -module qui devienne le module $V_1$ par tensorisation avec $K$, pour tout $K$.

*Remarque.* - Il est facile de voir que les multiples de 1 (l'élément unité de $\mathrm{End}^{aa}(\mathfrak{h})$) sont les seuls éléments $v$ de $V_1$ tels que, pour tout $x \in V_1$, $\mu(v, x)$ soit combinaison linéaire de $v$ et $x$. Un raisonnement analogue à la preuve de la proposition 2 de [IM] (voir aussi le bas de la page 498 du même article) montre alors que si $\mu(V_1 \times \{1\})$ ne s'annule pas identiquement (ce qui signifie, avec les notations du n° 2 et de la proposition 2, que l'on n'a pas

$k = -6k' = 72\,k_1''$), on a $F = \mathrm{Aut}\,(V_1, \mu)$ sauf peut-être si car $K = 3$, 13 ou 41. (Il me paraît d'ailleurs très improbable que ces cas fassent réellement exception.)

J. T.

Trois séances de séminaire, préambules au cours de l'an prochain, ont été consacrées aux représentations linéaires des algèbres de KAC-MOODY de type $\tilde{A}_1$.

## PUBLICATIONS

A. COHEN and J. TITS, *On generalized hexagons and a near octagon whose lines have three points* (*European J. of Combinatorics,* 6, 1985, 13-27).

J. TITS, *Avatars des grands théorèmes de classification d'Elie Cartan* (court résumé d'une conférence au colloque : « Elie Cartan et les mathématiques d'aujourd'hui », Lyon, juin 1984, *in Astérisque*, numéro hors série, 1985, 439-440).

— , *Buildings of spherical type and finite* BN-*pairs* (*Springer Lecture Notes in Math.* n° 386 (1974), réimpression augmentée de quatre pages de compléments, Springer-Verlag, 1986).

— , *Immeubles de type affine* (*in* Buildings and the geometry of diagrams, Como 1984, *Springer Lecture Notes in Math.* n° 1181, 1986, 159-190).

## MISSIONS

*Exposés*

— *Über vier ähnlich aussehende Gruppen, von denen zwei arithmetisch sind und zwei nicht*, Hambourg, juillet 1985.

— *Building buildings*, 10th British Combinatorial Conference, Glasgow, juillet 1985.

— *Buildings and group amalgamations*, cinq exposés à la Conférence *Groups-Saint Andrews 1985*, Saint Andrews, août 1985.

— *On Griess' construction of the Monster*, I.H.E.S., Bures-sur-Yvette, novembre 1985.

— *Buildings, amalgams and simple connectedness*, Workshop on « Geometries and groups, finite and algebraic », Noordwijkerhout, mars 1986.

— *Rational unipotent elements in semi-simple groups over non-perfect fields*, Symposium on algebraic groups (conférence en l'honneur de T.A. Springer), Utrecht, avril 1986.

— *L'œuvre mathématique de Claude Chevalley*, Séminaire d'Histoire des Mathématiques, Paris, mai 1986.

— *Générateurs et relations pour les groupes de Kac-Moody*, Société Mathématique Suisse, Berne, mai 1986.