2
ETUDES

Du nouveau en algèbre : La classification des groupes finis simples

par Daniel LIGNON, IUT, Université d'Angers

L'été 1980 a vu s'achever une recherche mathématique très importante : la classification complète des groupes finis simples.

C'est ce résultat fondamental — le journal LE MONDE y a même consacré un article le 11 février 1981 — que l'on va tenter d'expliquer.

1. Qu'est-ce qu'un groupe fini simple ?

Un groupe fini est, bien sûr, un groupe qui n'a qu'un nombre fini d'éléments. Ce nombre d'éléments s'appelle, en général, l'ordre du groupe.

Donnons des exemples de groupes finis :

• $\mathbb{Z}/n\mathbb{Z}$, muni de l'addition, pour n entier est un groupe commutatif d'ordre n.

• S_n, l'ensemble des permutations d'un ensemble de n éléments, muni de la composition des applications, est un groupe d'ordre n !, non commutatif pour $n \geqslant 3$.

• Si k est un corps fini d'ordre q, alors l'ensemble des automorphismes d'espaces vectoriels de k^n, muni de la composition, est un groupe fini non commutatif d'ordre $q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (q^i - 1)$. On le note GL (n,k).

On peut remarquer que tous les corps finis d'ordre q sont isomorphes : il n'y a qu'un seul modèle que l'on appelle alors corps de Galois et que l'on note F_q où $q = p^n$, p étant la caractéristique du corps. Il est commutatif d'après le théorème de Wedderburn. *(Voir [1], [2], ou [9])*

Par suite, le groupe GL(n,k) peut être aussi noté GL(n,q) ou GL$_n(q)$ puisque l'ordre caractérise le corps.

Pour terminer avec cet exemple, qui est très important car beaucoup de groupes finis simples en sont des sous-groupes, on peut remarquer qu'il peut être représenté par l'ensemble des matrices carrées inversibles de dimension n, à coefficients dans k, muni de la multiplication des matrices.

Dans un groupe G où la loi est notée multiplicativement, un sous-groupe H de G qui vérifie la condition :

pour tout x de G et tout y de H, on a $xyx^{-1} \in H$

s'appelle un *sous-groupe distingué*, ou normal, de G. On note alors : $H \lhd G$ ou $G \rhd H$.

Donnons des exemples :

• Il est évident que dans un groupe commutatif, tout sous-groupe est distingué.

• Dans $G = GL(2, \mathbb{Z}/2\mathbb{Z})$, l'ensemble $H = \{I, A\}$ où $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est un sous-groupe mais il n'est pas distingué dans G. (Prendre $x = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et $y = A$).

L'intérêt des sous-groupes distingués est qu'ils permettent de construire des relations d'équivalence compatibles avec la loi de groupe de G — ce qui n'est pas toujours possible avec un sous-groupe quelconque —, et de définir une structure de groupe sur l'ensemble des classes d'équivalence, groupe que l'on appelle le groupe-quotient de G par H et que l'on note G/H.

De ce point de vue, les sous-groupes distingués jouent le même rôle que les idéaux dans les anneaux, ou les sous-espaces vectoriels dans les espaces vectoriels : ils permettent de construire une structure-quotient.

Un groupe G est *simple* s'il ne contient pas d'autres sous-groupes distingués que le sous-groupe réduit à l'élément neutre $\{e\}$ et G, c'est-à-dire s'il ne contient pas de sous-groupes distingués non triviaux.

Les groupes simples ont été introduits par Evariste Galois (1811-1832) dans ses études sur la résolution des équations algébriques par radicaux.

Donnons un exemple de groupe simple :

Soit G un groupe fini d'ordre p premier. D'après le théorème de Lagrange selon lequel l'ordre d'un sous-groupe divise l'ordre du groupe, G ne peut admettre d'autres sous-groupes que $\{e\}$ et G ; donc G est simple.

En conséquence $\mathbb{Z}/p\mathbb{Z}$ pour p premier, muni de l'addition, est simple (en fait, il n'y a pas d'autres groupes d'ordre premier).

2. Quel est l'intérêt des groupes simples ?

Commençons par une analogie :

Considérons dans l'ensemble des entiers naturels non nuls $\mathbf{N}^*$ la relation "divise" notée $|$, c'est-à-dire :

$$m \mid n \quad \text{si il existe} \quad q \in \mathbf{N}^* \quad \text{tel que} \quad n = m.q$$

C'est une relation d'ordre dans $\mathbf{N}^*$.

Les entiers les "plus simples" vis à vis de cette relation sont les nombres premiers. L'importance de ces nombres résulte du théorème fondamental de l'arithmétique qui dit que tout entier $n \geqslant 2$ peut s'écrire sous la forme :

$$n = p_1^{\alpha_1} \ldots\ldots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

où les p_i sont premiers et les α_i des entiers non nuls.

De plus, à l'indexation près, cette écriture est unique : c'est la décomposition de n en produit de facteurs premiers.

On peut énoncer ce théorème sous une autre forme qui est équivalente :

Pour tout entier $n \geqslant 2$, il existe une suite d'entiers :

$$n = n_0 \geqslant n_1 \ldots\ldots \geqslant n_{k-1} \geqslant n_k = 1 \quad \text{telle que} \quad n_{i+1} \mid n_i$$

et que $\dfrac{n_i}{n_{i+1}} = q_i$ soit un entier premier pour tout i variant de 0 à $k-1$.

Il est presque évident qu'il n'y a pas unicité de la suite $(n_i)_i$ ni de la suite $(q_i)_i$ mais on a la propriété suivante :

S'il y a deux suites $(q_i)_{i=0}^{k-1}$ et $(q'_i)_{i=0}^{l-1}$ ainsi définies, on a :

- $k = l$, c'est-à-dire que les deux suites ont même longueur.
- il existe une bijection σ de $\{0, \ldots\ldots, k-1\}$ dans lui-même telle que $q_{\sigma(i)} = q'_i$ pour $i = 0, \ldots\ldots, k-1$;
  c'est-à-dire que les termes des deux suites sont égaux à l'indexation près.

Prenons un exemple : soit $n = 30$.

On peut définir la suite : $30 \geqslant 10 \geqslant 5 \geqslant 1$

et $q_0 = \dfrac{30}{10} = 3$, $q_1 = \dfrac{10}{5} = 2$, $q_2 = \dfrac{5}{1} = 5$.

Ils sont bien entiers.

On peut aussi définir la suite : $30 \geqslant 6 \geqslant 2 \geqslant 1$

et $q'_0 = \dfrac{30}{6} = 5$, $q'_1 = \dfrac{6}{2} = 3$, $q'_2 = \dfrac{2}{1} = 2$.

Ces deux suites ont bien même longueur et, à l'indexation près, ce sont les mêmes termes, 2, 3 et 5 (qui sont, bien sûr, les facteurs premiers de 30) qui apparaissent dans les deux suites $(q_i)_i$ et $(q'_i)_i$.

Maintenant, nous pouvons dire que les groupes finis simples jouent le même rôle vis-à-vis des groupes finis que les nombres premiers vis-à-vis des entiers naturels. De manière plus précise, on a le théorème suivant dû à Camille Jordan (1838-1922) et au mathématicien allemand Otto Hölder (1859-1937) :

Pour tout groupe fini G, il existe une suite de sous-groupes :
$G = G_0 \rhd G_1 \rhd \ldots \rhd G_{k-1} \rhd G_k = \{e\}$ telle que le groupe quotient $H_i = G_i/G_{i+1}$ soit un groupe simple pour tout i de 0 à $k-1$.

De plus, la suite des groupes H_i vérifie les propriétés suivantes :

- la longueur de la suite est définie par G et est donc déterminée.
- les groupes H_i sont uniques à l'indexation près (voir [2]).

Au-delà de cette décomposition, on peut montrer que l'on peut construire tous les groupes finis à partir des groupes finis simples (voir [7] ou [8]).

Remarques :

- Dans le cas des groupes finis abéliens, on a un théorème plus simple et plus puissant donnant la décomposition d'un groupe fini abélien en groupes cycliques :

Tout groupe fini abélien d'ordre n est isomorphe à :

$$\mathbf{Z}/m_1\mathbf{Z} \times \mathbf{Z}/m_2\mathbf{Z} \times \ldots \times \mathbf{Z}/m_{k-1}\mathbf{Z} \times \mathbf{Z}/m_k\mathbf{Z}$$

où la suite $(m_i)_{i=1}^{k}$ est unique et vérifie $m_i | m_{i+1}$ et $\prod_{i=1}^{k} m_i = n$ (voir [2]).

- Dans tout ceci, il ne faut pas oublier que deux groupes isomorphes définissent la même structure de groupe. En conséquence, tous les groupes sont définis à isomorphisme près.

Par exemple, le groupe additif $\mathbf{Z}/6\mathbf{Z}$ est isomorphe au groupe additif $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ et au groupe multiplicatif des éléments inversibles de $\mathbf{Z}/9\mathbf{Z}$. De même, le groupe des permutations S_3 est isomorphe au groupe des isométries du triangle équilatéral.

Par contre, $\mathbf{Z}/6\mathbf{Z}$ n'est pas isomorphe à S_3, le premier étant abélien, le second ne l'étant pas.

- Le théorème de Jordan-Hölder est à la base de l'algorithme de reconstitution du cube hongrois proposé par E. Halberstadt (voir POUR LA SCIENCE, août 1980).

3. Quels sont les groupes finis simples ?

La liste complète des groupes finis simples est la suivante : il y a 18 familles infinies de groupes et 26 groupes isolés qui, pour cette raison, sont appelés groupes sporadiques.

Donnons le détail de cette liste :

a) Groupes finis simples abéliens :

Il est facile de voir, avec le théorème de Lagrange, qu'un groupe fini simple abélien est d'ordre premier, donc cyclique, donc isomorphe au groupe additif $\mathbf{Z}/p\mathbf{Z}$ pour p premier.

b) Groupes alternés :

Le groupe alterné A_n est défini comme l'ensemble des permutations paires du groupe S_n : c'est le noyau de l'application signature de S_n dans $\{-1, +1\}$.

Evariste Galois a montré que, pour $n \geqslant 5$, A_n est un groupe fini simple non abélien (voir [2]). Ce résultat lui a permis de montrer que les équations de degré $n \geqslant 5$ ne sont pas résolubles, en général, par radicaux (voir [6]).

Remarque : $A_2 = \{e\}$ et A_3 isomorphe à $\mathbf{Z}/3\mathbf{Z}$ sont aussi des groupes simples mais A_4 ne l'est pas car le sous-groupe d'ordre 4 des permutations qui échangent les éléments 2 par 2 est isomorphe au groupe de Klein $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et est distingué dans A_4.

c) Groupes classiques :

Ces groupes ont été ainsi nommés par Hermann Weyl (1885-1955) et leur simplicité dans le cas fini a été prouvée d'abord par Jordan dans certains cas puis de manière complète par Dickson dans les années 1900.

Dieudonné, en 1948, a simplifié les démonstrations initiales et en a donné une exposition plus rigoureuse.

Il y a 6 familles de groupes classiques.

La famille la plus simple à définir est celle des groupes projectifs unimodulaires notés $PSL_n(q)$ et définis à partir du groupe $GL_n(q)$ de la manière suivante :

Le sous-groupe de $GL_n(q)$ constitué des endomorphismes de déterminant égal à 1 est noté $SL_n(q)$: sauf pour $n = q = 2$, c'est le groupe dérivé ou groupe des commutateurs de $GL_n(q)$, engendré par les éléments de la forme $aba^{-1}b^{-1}$ où a et b appartiennent à $GL_n(q)$. On montre que le groupe dérivé d'un groupe G est un sous-groupe distingué H et que c'est le plus petit sous-groupe H tel que le groupe-quotient G/H soit commutatif.

Le groupe $PSL_n(q)$ est alors le quotient de $SL_n(q)$ par son centre Z_0 qui est l'ensemble des éléments qui commutent avec tous les éléments de

$SL_n(q)$: ce sont les homothéties de l'espace vectoriel k^n de déterminant égal à $+1$; Z_0 est donc isomorphe à l'ensemble des éléments a du corps k tel que $a^n = +1$. $PSL_n(q)$ est un groupe fini simple pour $n > 2$ ou bien pour $n = 2$ et $q \geqslant 4$.

Son ordre est : $$\frac{1}{d} q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n} (q^i - 1)$$

où d est le p.g.c.d de n et $q-1$ (d est l'ordre de Z_0).

Remarquons que : $PSL_2(2)$ est isomorphe à S_3 qui n'est pas simple car il contient le sous-groupe distingué A_3.

$PSL_2(3)$ est isomorphe à A_4 qui n'est pas simple d'après le paragraphe précédent.

(Voir [1] ou [4]).

Les autres groupes classiques sont des groupes d'isométries de certaines formes non dégénérées sur k^n :

• Si c'est une *forme bilinéaire symétrique*, le groupe des isométries s'appelle le *groupe orthogonal*.

Si la dimension de l'espace vectoriel k^n est impaire, alors deux formes bilinéaires symétriques non dégénérées donnent des groupes orthogonaux isomorphes qui seront notés, après changement d'indice, $O_{2n+1}(q)$.

Si la dimension de l'espace vectoriel est paire, alors il y a deux modèles de formes bilinéaires symétriques non dégénérées, ce qui donne deux groupes orthogonaux : $O_{2n}(q, -)$ et $O_{2n}(q, +)$.

• Si c'est une *forme bilinéaire alternée*, le groupe des isométries s'appelle le *groupe symplectique*.

Un espace vectoriel muni d'une forme bilinéaire alternée non dégénérée étant nécessairement de dimension paire et deux telles formes donnant naissance à des groupes symplectiques isomorphes, il n'y a qu'un seul modèle noté $Sp_{2n}(q)$.

• On peut aussi considérer une *forme sesquilinéaire*, analogue au cas complexe où on utilise l'automorphisme de conjugaison $z \mapsto \bar{z}$ qui est involutif.

Dans le cas des corps finis Fq, on a besoin d'un automorphisme involutif ; par exemple :

$$x \mapsto \bar{x} = x^{p^n} \quad \text{si} \quad q = p^{n^2}$$

Et les formes sesquilinéaires sont alors définies, comme dans $\mathbf{C}$, par :

$f(x,y) = \overline{f(y,x)}$ | pour tous les y et y appartenant
$f(\lambda x, y) = \lambda f(x,y)$ | à k^n et $\lambda \in F_q$

et l'additivité sur les deux variables.

Comme dans le cas d'une forme bilinéaire alternée, il n'y a qu'un seul modèle de groupe associé appelé *groupe unitaire* et noté $U_n(q)$.

La procédure pour construire des groupes simples à partir de ces groupes classiques est la même que celle pour passer de $GL_n(q)$ à $PSL_n(q)$: si on appelle G le groupe classique, soient D(G) son groupe dérivé et Z_0 le centre de D(G) qui est donc distingué dans D(G). (On peut remarquer que Z_0 est isomorphe à un sous-groupe de k ; dans beaucoup de cas, c'est même $\{1, -1\}$ ou $\{1\}$). Alors, en général, c'est-à-dire sauf pour de petites valeurs de n et de q, le groupe-quotient $D(G)/Z_0$ est simple.

On a ainsi 5 familles de groupes finis simples, qui avec $PSL_n(q)$ ont été découvertes avant 1900 (voir [1] ou [4]).

d) Groupes de Mathieu :

En 1861 et en 1873, E. Mathieu, à propos de travaux sur les permutations, introduisit 5 groupes qui, maintenant, portent son nom :

M_{11} d'ordre $7920 = 2^4.3^2.5.11$
M_{12} d'ordre $95040 = 2^6.3^3.5.11$
M_{22} d'ordre $443\,520 = 2^7.3^2.5.7.11$
M_{23} d'ordre $10\,200\,960 = 2^7.3^2.5.7.11.23$
M_{24} d'ordre $244\,823\,040 = 2^{10}.3^3.5.7.11.23$

Les indices 11, 12,... proviennent du fait que ce sont des sous-groupes de S_{11}, S_{12},... c'est-à-dire que ce sont des groupes de permutations sur 11, 12,... objets.

En 1900, d'autres mathématiciens montrèrent que ces 5 groupes étaient simples. Or, ils ne rentraient pas dans une famille infinie déjà connue. Aussi, Burnside, spécialiste des groupes finis, proposa en 1911 de les appeler groupes sporadiques ; et ce nom est maintenant employé pour désigner tous les groupes simples n'appartenant pas à une famille infinie.

Les groupes de Mathieu possèdent une propriété remarquable ; pour l'énoncer, donnons une définition :

Un groupe G de permutations sur un ensemble E de cardinal supérieur ou égal à n est dit n-fois transitif si, pour tous les n-uplets $(x_1,...,x_n)$ et $(y_1,...,y_n)$ de E^n, il existe une permutation Π de G telle que :

$$\Pi(x_i) = y_i \text{ pour tout } i \text{ de } 1 \text{ à } n.$$

Donnons des exemples :

- le groupe symétrique S_n est n-fois transitif.
- le groupe alterné A_n est $(n-2)$-fois transitif pour $n \geqslant 3$.
- il y a beaucoup de groupes 3-fois transitifs mais peu sont 4-fois transitifs :

il y a les groupes S_n pour $n \geqslant 4$, les groupes A_n pour $n \geqslant 6$ et les groupes de Mathieu M_{11}, M_{12}, M_{23} et M_{24}.
On démontre que ce sont les seuls groupes 4-fois transitifs.

• les seuls groupes 5-fois transitifs sont :
les groupes S_n pour $n \geqslant 5$, les groupes A_n pour $n \geqslant 7$ et les groupes M_{12} et M_{24}.

• on conjecture que les seuls groupes 6-fois transitifs (ou plus) sont du type S_n ou A_n.

Pour en terminer avec les groupes de Mathieu, on peut remarquer qu'ils sont utilisés dans la théorie du codage : par exemple, M_{23} et M_{24} sont liés aux codes correcteurs d'erreurs employés pour la restitution d'un message brouillé par un bruit.

e) Groupes de Chevalley et variantes :

En 1901 et en 1905, Dickson, qui avait déjà prouvé la simplicité de certains groupes classiques, trouva d'autres familles infinies de groupes simples.

Pour expliquer cela, revenons en arrière : nous avons vu que les groupes simples classiques sont des groupes classiques au sens de H. Weyl définis sur des corps finis. On peut se demander quelle est la structure de ces groupes classiques définis sur les corps "de nos grands-pères", selon l'expression de Conway, c'est-à-dire $\mathbf{R}$ ou $\mathbf{C}$: ce sont alors des groupes de Lie, c'est-à-dire pour schématiser des groupes où la notion de différentiabilité a un sens.

Une classification analogue à celle des groupes finis simples est celle des groupes de Lie complexes de dimension finie et simples (pour les définitions précises, voir CHEVALLEY ou DIEUDONNE [2]).

Cette classification, qui a été faite par W. Killing de 1888 à 1890 et par E. Cartan en 1894, comprend :

• 4 familles infinies qui ne sont autres que les groupes classiques définis sur $\mathbf{C}$: les groupes unimodulaires $SL(n+1,\mathbf{C})$
les groupes spéciaux-orthogonaux $SO(2n+1,\mathbf{C})$
les groupes spéciaux-orthogonaux $SO(2n,\mathbf{C})$
les groupes symplectiques $Sp(n,\mathbf{C})$
Ils sont simples pour n assez grand ($n \geqslant 4$ en général).

• 5 groupes isolés :
E_8 de dimension 248
E_7 de dimension 139
E_6 de dimension 78
F_4 de dimension 52
G_2 de dimension 14

Dans le cas réel, la classification analogue est celle des groupes de Lie réels de dimension finie, simples, compacts et elle a été faite par E. Cartan en 1914. On y retrouve, bien sûr, les groupes classiques.

Maintenant nous pouvons revenir aux groupes finis car les familles que Dickson trouva sont liées aux groupes de Lie G_2 et E_6.

Cela n'eut pas d'autres conséquences à ce moment-là et il n'y eut pas de découverte de nouveaux groupes simples jusqu'en 1955, année où le mathématicien C. Chevalley publia un article très important : il introduisait un point de vue général permettant de définir toutes les familles connues de groupes finis simples à partir des groupes de Lie ; de plus, il en donnait 3 nouvelles familles, correspondant à E_7, E_8 et F_4. On peut aussi remarquer que ses démonstrations de simplicité sont similaires pour toutes les familles, ce qui n'était absolument pas le cas avec les démonstrations de Dickson, Artin et Dieudonné.

Dans les 6 années qui suivirent, les méthodes de Chevalley furent encore généralisées et on put ainsi trouver 5 autres familles infinies de groupes finis simples, toujours définies à partir des groupes de Lie :

- les 2 familles de groupes de Steinberg-Tits
- la famille des groupes de Suzuki
- les 2 familles de groupes de Ree.

On pensait alors qu'il n'y avait pas d'autres groupes finis simples que ceux déjà cités, c'est-à-dire les 16 familles et les 5 groupes de Mathieu, mais aucune démonstration n'en avait été donnée... et pour cause...

f) Groupes sporadiques :

La découverte par S. Janko, en 1964, d'un groupe simple d'ordre $2^3.3.5.7.11.19 = 175\,560$ non isomorphe aux groupes déjà connus, provoqua une certaine surprise. On le nomma J_1. Janko construisit ce groupe comme sous-groupe de matrices carrées inversibles de dimension 7 à coefficients dans $\mathbb{Z}/11\mathbb{Z}$.

Depuis, de nombreux groupes finis simples sporadiques ont été découverts : il y en a 26 en tout, y compris les groupes de Mathieu. Ils furent construits, en général, comme sous-groupes de permutations ou comme groupes d'automorphismes dans un espace bien choisi. Citons parmi tous ces groupes :

* *Les 3 groupes notés .1 ou Co_1, .2 ou Co_2, .3 ou Co_3*, découverts par Conway en 1968. Cette découverte repose sur un travail sur les empilements compacts d'hypersphères dans un espace à 24 dimensions.
Co_1 est d'ordre $2^{21}.3^9.5^4.7^2.11.13.23 = 4\,157\,771\,806\,543\,360\,000$.
Co_2 et Co_3 en sont des sous-groupes (Co_3 est en rapport avec le problème de mathématiques générales de l'agrégation 1979).

* *Le groupe Ly ou Ly-S* dont l'existence fut annoncée en 1970 par Lyons. Il fut construit par Sims, avec l'aide d'un ordinateur, comme sous-groupe de permutations sur un ensemble d'environ 8 millions d'éléments.
Ce groupe est d'ordre $2^8.3^7.5^6.7.11.31.37.67 = 51\,765\,179\,004\,000\,000$.

* *Le groupe F_2*, conjecturé par Fisher en 1973 et construit par Léon et Sims en 1976 comme groupe de permutations.

Son ordre est : $2^{41}.3^{13}.5^6.7^2.11.13.17.19.23.31.47$ =
4 154 781 481 226 426 191 177 580 544 000 000.
Ce groupe s'appelle aussi B car Conway lui a donné le surnom de *bébé-monstre* ; il est en effet isomorphe à un sous-groupe du suivant...

* Le fameux *monstre noté* F_1 ou M, conjecturé par Fisher en 1974 et dont un exemplaire a été construit "à la main" par Griess en janvier 1980 comme sous-groupe de rotations dans un espace à 196 883 dimensions (!!!).
Son ordre est : $2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71$ =
808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000
(ouf !) c'est-à-dire environ 8.10^{53}.

On peut deviner pourquoi Conway lui a donné le surnom de monstre. Bien qu'on en soit pratiquement sûr, on n'a peut-être pas encore démontré l'unicité d'un groupe vérifiant les conditions que Fischer donna en 1974. (Aschbacher, dans [A], indique que c'est fait, et Broué et Puig, dans un article [B] postérieur, ne le signalent pas...)

M pose un certain nombre de problèmes : par exemple, certains de ses invariants sont les mêmes nombres que ceux apparaissant dans la théorie des fonctions elliptiques et remarqués par Jacobi en 1829 ; on ne connaît pas, à l'heure actuelle, l'explication de cette coïncidence.

* *Le groupe* J_4, conjecturé par Janko en 1975 et construit en février 1980 par un groupe de mathématiciens de Cambridge autour de Conway, avec l'aide d'un ordinateur. Il a été construit comme groupe de matrices carrées inversibles de dimension 112 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.
Son ordre est : $2^{21}.3^3.5.7.11^3.23.29.31.37.43$ = 86 775 571 046 077 562 880 (quantité négligeable à côté de l'ordre de M !).

C'est le 26ème groupe sporadique et le dernier.

A l'exception de J_1, Ly-S, J_4 et de 3 autres groupes, tous les groupes sporadiques sont isomorphes à des sous-groupes du monstre M.

4. Pourquoi n'y a-t-il pas d'autres groupes finis simples ?

Cette classification qui s'est achevée en août 1980 a consisté à énumérer tous les groupes simples et à démontrer que tout autre groupe fini simple était isomorphe à un des groupes cités.

Cette dernière partie est en fait un travail gigantesque qui s'est déroulé depuis les premières découvertes avant 1900 jusqu'à maintenant. Il n'est pas question de citer toutes les étapes ou tous les résultats, car cela représente environ 10 000 pages de démonstration !!!

Dans un premier temps, à la fin du 19e siècle, on a essayé de déterminer tous les groupes finis simples d'ordre donné ; par exemple O. Hölder, en 1892, a montré que les seuls groupes simples non abéliens dont l'ordre est compris entre 1 et 200 sont : A_5 d'ordre 60 et $PSL_2(7)$ d'ordre 168.

En 1900, on connaissait tous les groupes simples d'ordre inférieur ou égal à 2000 et les techniques utilisées permirent de mettre au point des critères indiquant si un groupe dont on ne connaît que l'ordre n est simple ou non. Par exemple, Burnside, en 1904, a montré que l'ordre d'un groupe fini simple non abélien possède au moins 3 facteurs premiers.

Le résultat le plus frappant dans cette direction fut obtenu en 1963 quand Feit et Thompson, après une démonstration par l'absurde de 255 pages (!!!), démontrèrent que tout groupe simple fini non abélien est nécessairement d'ordre pair. Ce théorème et d'autres travaux sur les groupes finis valurent à Thompson la médaille Fields en 1970. Rappelons que cette médaille est l'équivalent pour les mathématiques du prix Nobel.

Une technique très importante dans la démonstration du théorème de Feit-Thompson et dans toute la théorie des groupes simples est la théorie de la représentation.

On peut dire, en restant très superficiel, qu'une représentation du groupe G est un homomorphisme injectif du groupe G dans le groupe $GL_n(K)$ des matrices carrées inversibles de dimension n à coefficients dans un corps K. L'étude de l'ensemble image de G dans $GL_n(K)$ permet de tirer des informations sur le groupe G.

On peut donner, avec ces techniques, des conditions nécessaires très précises sur l'existence d'un groupe simple d'un ordre donné. Il ne reste plus alors (!!!) qu'à démontrer l'existence en construisant un groupe vérifiant ces conditions ; puis l'unicité à isomorphisme près.

C'est ce qui s'est souvent passé pour les groupes sporadiques (on peut citer parmi ceux que l'on a vus : B, M et J_4) où la prédiction a parfois précédé la construction effective de plusieurs années : M prédit en 1974 et J_4 prédit en 1975 ont été construits en 1980.

On retrouve là des faits analogues à ce qui se passe quelquefois en physique où certaines particules élémentaires ont été prédites bien avant leur découverte matérielle.

Suite au théorème de Feit-Thompson et à d'autres travaux, on aboutit à la classification des groupes finis simples dont certains sous-groupes possèdent des propriétés particulières (par exemple sont des groupes de symétrie d'un polygone régulier à n côtés, sont abéliens,...). Tout comme celle de Feit-Thompson, certaines de ces démonstrations sont très longues : entre 100 et 200 pages de revues !!!

La voie vers la classification complète était ouverte et beaucoup de mathématiciens travaillaient sur le sujet. Cela prit une ampleur encore plus grande quand, au début des années 1970, un programme détaillé pour résoudre ce problème fut mis au point par plusieurs mathématiciens parmi lesquels il faut citer les américains M. Aschbacher et D. Gorenstein et l'anglais J. Conway. Les différentes étapes furent réparties entre les chercheurs intéressés.... En fait, cela constituait un vrai plan de bataille avec l'état-major, l'armée de chercheurs,... Il est exceptionnel en mathé-

matiques de planifier ainsi un programme de recherche, situation qui pourtant est courante dans d'autres disciplines.

Les spécialistes s'attendaient à l'aboutissement durant la décade 80, mais cela a été plus rapide et la victoire est intervenue dans le mois d'août 1980, après avoir reçu l'aide d'un non-spécialiste des groupes finis, E. Bombieri, médaille Fields en 1974 pour ses travaux en théorie des nombres et en géométrie différentielle, qui a résolu un problème sur lequel Thompson et d'autres "séchaient" depuis une dizaine d'années.

La classification est donc terminée : il y a 18 familles infinies et 26 groupes sporadiques. Mais il ne faut pas croire que le travail est fini. Il reste à simplifier les démonstrations, à les rendre cohérentes (car chaque mathématicien a appliqué ses propres techniques, parfois fort dissemblables), à éliminer les erreurs (il est vraisemblable qu'il y en ait sur la masse d'articles consacrés à la classification : les spécialistes les plus pessimistes pensent que les erreurs éventuelles ne feront apparaître qu'un nombre fini de nouveaux groupes alors que les plus optimistes pensent que la liste est définitivement close) et puis aussi à comprendre tous les résultats et toutes les découvertes qu'elles ont amenés. Une page est tournée mais les problèmes posés à cette occasion sont encore plus nombreux.

Pour terminer, on peut remarquer que, pour résoudre ce problème purement algébrique, on a fait appel à de nombreux domaines des mathématiques : la géométrie, l'analyse par l'intermédiaire des groupes de Lie, l'arithmétique,...

C'est, sans doute, cela, l'unité de la mathématique.

Bibliographie :

L'essentiel de cet article est tiré de :

[a] J.A. GALLIAN, *The search for finite simple groups,* Mathematics Magazine, vol. 49, p. 163-179, septembre 1976.

[b] J.F. HURLEY and A. RUDVALIS, *Finite simple groups,* American Monthly Magazine, vol. 84, p. 693-714, novembre 1977.

On peut trouver un exposé plus mathématique des problèmes généraux posés par la classification dans :

[A] M. ASCHBACHER, *The classification of the finite simple groups,* The mathematical intelligencer, vol. 3, p. 59-65, 1981.

[B] M. BROUE et L. PUIG, *Classification des groupes finis simples : bref aperçu et quelques conséquences internes,* Séminaire Bourbaki, n° 584, novembre 1981.

[C] J.H. CONWAY, *Monsters and moonshine,* The mathematical intelligencer, vol. 2, p. 165-171, 1980.

Les livres cités dans le cours de l'article sont :

[1] ARTIN : *Algèbre géométrique,* Gauthier-Villars, 1972.

[2] BOUVIER-RICHARD : *Groupes,* Collection Formation des enseignants Hermann, 1974.

[3] CHEVALLEY : *Theory of Lie groups,* Princeton University Press, 1946.

[4] DIEUDONNE [1] : *La géométrie des groupes classiques,* 2ème édition, Springer Verlag, 1963.

[5] DIEUDONNE [2] : *Eléments d'analyse,* volumes 1 à 8, Gauthier-Villars.

[6] MUTAFIAN : *Equations algébriques et théorie de Galois,* Vuibert, 1980.

[7] ROTMAN : *The theory of groups : an introduction,* Allyn and Bacon, 1968.

[8] SCOTT : *Group theory,* Prentice Hall, 1964.

[9] WARUSFEL : *Structures algébriques finies,* Hachette, 1971.

* * *

Depuis la rédaction de cet article, d'autres références sont parues :

[10] G. GLAESER, *Chasse aux groupes finis : avec un revolver à bouchons,* L'Ouvert n° 24, IREM Strasbourg.

[11] P. BOREL, *Groupes finis : la chasse est finie,* L'Ouvert n° 25, IREM Strasbourg.

[12] F. BUEKENHOUT, *Les groupes sporadiques,* La Recherche n° 131, mars 1982.

LES 18 FAMILLES INFINIES DE GROUPES FINIS SIMPLES

nom du groupe et type	date	découvert par	ordre du groupe
$\mathbf{Z}/p\mathbf{Z}$ abélien			p (p premier)
A_n $n \geqslant 5$ alterné	1832	Galois	$\frac{1}{2}\, n\,!$
$PSL_n(q)$ $n \geqslant 2$ spécial linéaire classique	1870/ 1897	Jordan/Dickson	$\frac{1}{d}\, q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n} (q^i - 1)$ où d est le pgcd de n et de $q-1$.
$PSp_{2n}(q)$ $n \geqslant 2$ symplectique classique	1870/ 1897	Jordan/Dickson	$\frac{1}{d}\, q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1)$ où d est le pgcd de 2 et de $q-1$
$PSU_n(q)$ $n \geqslant 3$ unitaire classique	1870/ 1898	Jordan/Dickson	$\frac{1}{d}\, q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n} (q^i - (-1)^i)$ où d est le pgcd de n et de $q+1$.
$P\Omega_{2n}(q,+)$ $n \geqslant 4$ orthogonal classique	1870/ 1898	Jordan/Dickson	$\frac{1}{d}\, q^{n(n-1)} (q^n - 1) \prod_{i=1}^{n-1} (q^{2i} - 1)$ où d est le pgcd de 4 et de $q^n - 1$
$P\Omega_{2n}(q,-)$ $n \geqslant 4$ orthogonal classique	1870/ 1898	Jordan/Dickson	$\frac{1}{d}\, q^{n(n-1)} (q^n + 1) \prod_{i=1}^{n-1} (q^{2i} - 1)$ où d est le pgcd de 4 et de $q^n + 1$
$P\Omega_{2n+1}(q)$ $n \geqslant 3$ orthogonal classique	1870/ 1898	Jordan/Dickson	$\frac{1}{d}\, q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1)$ où d est le pgcd de 2 et de $q-1$
$G_2(q)$ groupe de Lie	1901	Dickson	$q^6(q^6-1)(q^2-1)$

$E_6(q)$ groupe de Lie	1905	Dickson	$\frac{1}{d} q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)$ où d est le pgcd de 3 et de $q-1$
$F_4(q)$ groupe de Lie	1955	Chevalley	$q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$
$E_7(q)$ groupe de Lie	1955	Chevalley	$\frac{1}{d} q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1)$ où d est le pgcd de 2 et de $q-1$
$E_8(q)$ groupe de Lie	1955	Chevalley	$q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1)$
${}^3D_4(q)$ groupe de Lie	1959	Steinberg-Tits	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$
${}^2E_6(q)$ groupe de Lie	1959	Steinberg-Tits	$\frac{1}{d} q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1)$ où d est le pgcd de 3 et de $q+1$
${}^2B_2(q)$ $q=2^{2n+1}$ groupe de Lie	1960	Suzuki	$q^2(q^4+1)(q-1)$
${}^2G_2(q)$ $q=3^{2n+1}$ groupe de Lie	1961	Ree	$q^3(q^3+1)(q-1)$
${}^2F_4(q)$ $q=2^{2n+1}$ groupe de Lie	1961	Ree	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$

Remarques :

* Dans l'ordre des groupes, la valeur q est égale à $q=p^m$ où p est premier et $m \geqslant 1$.
* Dans cette liste, il y a quelques exceptions :
  $PSL_2(2)$, $PSL_2(3)$, $PSU_3(2)$, ${}^2B_2(2)$, $PSp_4(2)$, $G_2(2)$, ${}^2F_4(2)$ et ${}^2G_2(3)$ ne sont pas simples.
* Les dates ne sont qu'approximatives et concernent la preuve de la simplicité, en particulier pour les groupes classiques.
* Dans le cas des groupes classiques, la simplicité fut démontrée par Jordan pour $m=1$, c'est-à-dire pour $q=p$ premier.
* Les groupes classiques, depuis les travaux de Chevalley, sont considérés comme groupes de Lie.

LES 26 GROUPES SPORADIQUES

Nom du groupe	date	découvert par	ordre du groupe
M_{11}	1861/ 1895	Mathieu/Cole	$2^4.3^2.5.11 = 7\,920$
M_{12}	1861/ 1899	Mathieu/Miller	$2^6.3^3.5.11 = 95\,040$
M_{22}	1873/ 1900	Mathieu/Miller	$2^7.3^2.5.7.11 = 443\,520$
M_{23}	1873/ 1900	Mathieu/Miller	$2^7.3^2.5.7.11.23 = 10\,200\,960$
M_{24}	1873/ 1900	Mathieu/Miller	$2^{10}.3^3.5.7.11.23 = 244\,823\,040$
J ou J_1	1964	Janko	$2^3.3.5.7.11.19 = 175\,560$
H_i-S	1967	Higman-Sims	$2^9.3^2.5^3.7.11 = 44\,352\,000$
H_a-J-W ou J_2	1967	Hall-Janko-Wales	$2^7.3^3.5^2.7 = 604\,800$
M_c L	1968	Mc Laughlin	$2^7.3^6.5^3.7.11 = 898\,128\,000$
S_z	1968	Suzuki	$2^{13}.3^7.5^2.7.11.13 = 448\,345\,497\,600$
H-J-M_cK ou J_3	1968	Janko Higman-Mc Kay	$2^7.3^5.5.17.19 = 50\,232\,960$
.1 ou Co_1	1968	Conway	$2^{21}.3^9.5^4.7^2.11.13.23$
.2 ou Co_2	1968	Conway	$2^{18}.3^6.5^3.7.11.23 = 42\,305\,421\,312\,000$
.3 ou Co_3	1968	Conway	$2^{10}.3^7.5^3.7.11.23 = 495\,766\,656\,000$

H_e ou H-H-M_cK	1968	Held/ Higman-Mc Kay	$2^{10}.3^3.5^2.7^3.17 = 4\ 030\ 387\ 200$
F_{i22} ou M(22)	1969	Fisher	$2^{17}.3^9.5^2.7.11.13 = 64\ 561\ 751\ 654\ 400$
F_{i23} ou M(23)	1969	Fisher	$2^{18}.3^{13}.5^2.7.11.13.17.23$
F_{i24} ou M(24)	1969	Fisher	$2^{21}.3^{16}.5^2.7^3.11.13.17.23.29$
Ly ou Ly-S	1970	Lyons/Sims	$2^8.3^7.5^6.7.11.31.37.67$
R_v ou R-C-W	1972	Rudvalis/ Conway-Wales	$2^{14}.3^3.5^3.7.13.29 = 145\ 926\ 144\ 000$
O'N ou O'N-S	1973	O'Nan/Sims	$2^9.3^4.5.7^3.11.19.31 = 460\ 815\ 505\ 920$
T	1974	Thompson/ Smith	$2^{15}.3^{10}.5^3.7^2.13.19.31 = 90\ 745\ 943\ 887\ 872\ 000$
H_a-N ou H_a-C-N-S	1974	Harada-Norton/ Conway-Smith	$2^{14}.3^6.5^6.7.11.19 = 273\ 030\ 912\ 000\ 000$
B ou F_2 ou F-L-S	1973/ 1976	Fisher/ Leon-Sims	$2^{41}.3^{13}.5^6.7^2.11.13.17.19.23.31.47$
M ou F_1	1974/ 1980	Fisher-Griess/ Griess	$2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71$
J_4	1975/ 1980	Janko/ Norton-Parker-Benson-Conway-Thackray	$2^{21}.3^3.5.7.11^3.23.29.31.37.43$

Remarques :

* Les dates ne sont qu'approximatives, la publication d'un article annonçant une découverte se faisant plusieurs mois après son annonce.
* Pour les groupes de Mathieu, la date et le nom avant / concernent la découverte du groupe et la date et le nom après / concernent la preuve de la simplicité.
* Pour les autres groupes, quand la prédiction est antérieure à la construction, la date et les noms avant / concernent la prédiction et la date et les noms après / concernent la construction.