Tome 2, n° 1, Janvier-Février 1985

COMPTES RENDUS
DE L'ACADÉMIE DES SCIENCES

SÉRIE GÉNÉRALE

LA VIE DES SCIENCES

gauthier-villars

Symétries

Jacques TITS
Membre de l'Académie

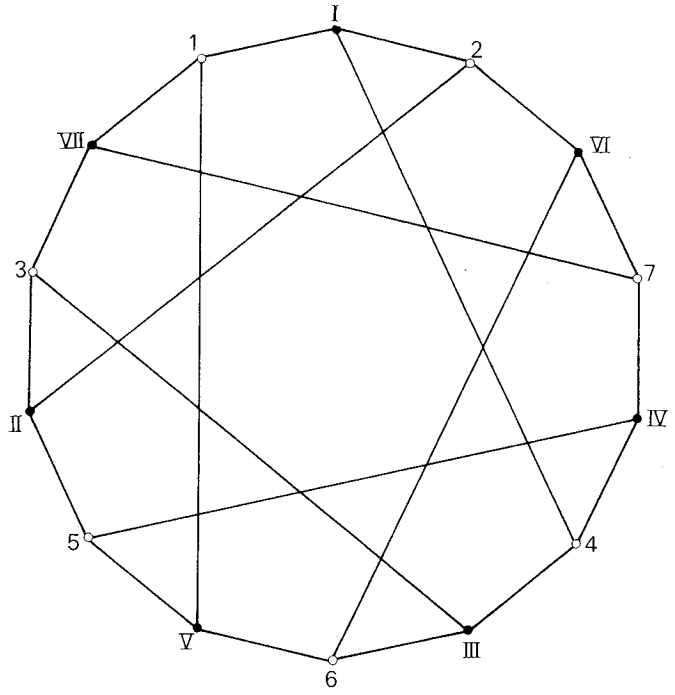
*Pour le mathématicien, la notion de symétrie ne se distingue guère de celle d'*automorphisme. *L'ensemble des symétries d'un objet est son* groupe d'automorphismes. *La notion de groupe « abstrait », due à Evariste Galois, répond à l'idée de « type de symétrie ». La théorie des groupes montre qu'il n'est pas raisonnable d'essayer de déterminer tous les types de symétrie possibles, mais elle permet de « décomposer » un type de symétrie en composants simples, et la* détermination de tous les groupes finis simples *a été achevée tout récemment, au terme d'un effort collectif sans précédent en mathématiques. Ces recherches ont entraîné la découverte de types de symétrie nouveaux, d'une grande beauté, les « groupes sporadiques », et notamment le très remarquable (et mal nommé) « Monstre » de Griess-Fischer.*

Symétries et groupes d'automorphismes

Les symétries que l'on attribue à un objet dépendent de façon essentielle des qualités de l'objet que l'on décide de prendre en compte à l'exclusion de toute autre. Sans ce processus d'abstraction, aucune symétrie (parfaite) n'est possible. Autrement dit, une *vraie* symétrie est l'apanage d'« objets » caractérisés par un système bien délimité de propriétés : c'est là le propre des « objets mathématiques ». En un sens, on peut donc affirmer qu'*il n'y a de symétrie absolue que mathématique.*

Les « objets mathématiques » dont il vient d'être question se présentent le plus souvent, dans les formulations actuellement les plus courantes, comme des *ensembles dotés de structures.* Lorsqu'on cherche à formaliser l'idée de symétrie, on est conduit à la notion d'*automorphisme* : un automorphisme d'un ensemble structuré est une permutation (on dit aussi « transformation », dans une acception du terme un peu éloignée de sa signification courante) de l'ensemble, qui préserve la structure envisagée (exemples 1 à 6). Ainsi, on retrouve les symétries du langage courant en considérant comme transformations la symétrie par rapport à un point (symétrie centrale), la réflexion dans un miroir (symétrie

La Vie des Sciences, *Comptes rendus*, série générale, tome 2, n° 1, p. 13-25



Exemple 1

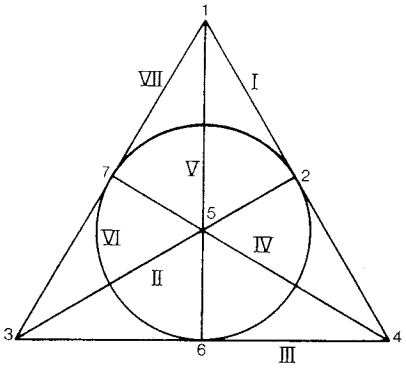
Cette figure a sept automorphismes (« symétries ») évidents.

Elle en acquiert quatorze si l'on « oublie » qu'il y a des points noirs et d'autres blancs. Elle en a cent soixante-huit si l'on distingue à nouveau ces deux couleurs mais si l'on fait abstraction de la longueur des segments pour ne retenir que la « structure de *graphe* », c'est-à-dire la distinction entre les couples de points liés par un segment et ceux qui ne le sont pas (noter par exemple que la permutation $1\to2\to3\to4\to5\to6\to7\to1$, $I\to II\to III\to IV\to V\to VI\to VII\to I$ respecte ces liaisons).

Enfin, elle en acquiert trois cent trente-six lorsqu'on ne considère plus que la structure de graphe. Ainsi, le groupe de tous les automorphismes de ce graphe est un groupe d'ordre 336.

bilatérale, ou énantiomorphie), les rotations d'un angle $2\pi/n$ autour d'un axe (symétrie axiale d'ordre n), les permutations d'une collection d'objets (sous-jacentes aux expressions « jouer un rôle symétrique », « avoir des relations symétriques »), etc.

Les automorphismes d'un objet donné jouissent évidemment des propriétés suivantes : la succession de deux automorphismes a pour résultat un automorphisme (appelé aussi *produit* des deux automorphismes en question); tout automorphisme possède un automorphisme *inverse* qui, effectué à sa suite, ramène l'objet à sa position initiale; il existe toujours au moins un automorphisme, à savoir l'*identité* (qui ne bouge rien). On exprime l'ensemble de ces propriétés en disant que les automorphismes d'un objet forment un *groupe* et, plus exactement, si l'objet en cause est un ensemble structuré, un *groupe de permutations* (ou de transformations) de cet ensemble. Ainsi, la théorie de la symétrie ne se distingue-t-elle guère de la théorie des groupes et, plus particulièrement, de la théorie



Exemple 2

Cette figure a six ou trois automorphismes « évidents » selon qu'on accepte ou non les retournements. Elle en a cent soixante-huit si l'on décide de n'y voir que sept points (1, 2, . . ., 7) dont certains triples sont « alignés » et d'autres ne le sont pas (« aligné » signifie « situés sur une même ligne », laquelle peut être droite ou circulaire : les points 2, 6, 7 sont alignés; 2, 6, 1 ne le sont pas).

Le groupe d'ordre 128 des permutations préservant l'alignement est « le même » que le groupe d'ordre 128 de la figure 1 (on dit qu'ils sont « isomorphes »); cela se voit en remarquant que si l'on met les points 1, 2, . . ., 7 et les lignes I, II, . . ., VII en correspondance avec les sommets de même nom du graphe de l'exemple 1, l'appartenance (ex. : le point 2 appartient aux lignes I, II, VI et à aucune autre) correspond, pour les sommets correspondants du graphe, à la propriété d'être liés (le sommet 2 de la figure 1 est lié aux sommets I, II, VI et à aucun autre).

des groupes de permutations. Rappelons que cette notion de groupe de permutations a été dégagée par E. Galois à l'occasion de ses travaux sur les équations algébriques : l'objet considéré est ici l'ensemble des solutions d'une telle équation [de la forme $P(x)=0$, où P est un polynome de degré quelconque], et la structure à laquelle on s'intéresse est constituée par toutes les relations *rationnelles* (c'est-à-dire, s'écrivant à l'aide des seules opérations élémentaires $+$, $-$, $\times$, :) existant entre ces solutions et les coefficients de l'équation (ou, plus généralement, un système de nombres que l'on considère comme donné) (exemples 3 et 4).

On a vu qu'un objet mathématique se présente le plus souvent comme un ensemble structuré. Lorsqu'on *enrichit* la structure (ce qui, dans des cas concrets, signifie que l'on décide de prendre en considération des qualités qu'on ignorait jusqu'alors), cela a pour effet de diminuer la symétrie de l'ensemble ou, en termes plus précis, de remplacer le groupe des automorphismes par un sous-groupe (exemples 1, 2, 3, 4). C'est le processus connu des physiciens sous le nom de *brisure de symétrie*. La théorie de Galois des équations algébriques peut être vue comme une application de cette idée. Résoudre *complètement* une équation algébrique revient à détruire totalement la symétrie de l'ensemble de ses solution : lorsque cet ensemble est entièrement dépourvu de symétrie (c'est-à-dire, n'a plus d'autre automorphisme que l'identité), chaque solution est différente de chaque autre, donc est connue ! Les critères de résolubilité des équations par extractions

Exemple 3

L'équation

$$x^5 - 6\,x^3 - x^2 + 4\,x - 1 = 0$$

a cinq solutions :

$x_1 = -2{,}132\ldots$, $x_2 = -1{,}127\ldots$, $x_3 = 0{,}330\ldots$, $x_4 = 0{,}552\ldots$, $x_5 = 2{,}407\ldots$

Considérés « avec toutes leurs propriétés », ces cinq nombres ne présentent *aucune symétrie* (le groupe d'automorphismes est réduit à la permutation identique). Mais lorsqu'on s'intéresse seulement aux *relations rationnelles* (relations s'exprimant à l'aide des quatre opérations élémentaires de l'arithmétique) entre eux, telles que

$$x_1 + x_2 + x_3 + x_4 + x_5 = 0,$$
$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 = 12,$$
$$x_1 x_2 x_3 x_4 x_5 = 1,$$

etc., toute permutation de $x_1, \ldots, x_5$ devient un automorphisme de la structure : le groupe des automorphismes est le « groupe symétrique », d'ordre 120, formé par ces permutations. Si, outre les opérations rationnelles, on s'autorise des extractions de racines carrées (en distinguant les deux racines opposées), de nouvelles relations apparaissent : on a

$$(x_2 - x_1)\,(x_3 - x_1)\,(x_4 - x_1)\,(x_5 - x_1)\cdot$$
$$(x_3 - x_2)\,(x_4 - x_2)\,(x_5 - x_2)\cdot$$
$$(x_4 - x_3)\,(x_5 - x_3)\cdot$$
$$(x_5 - x_4) = \sqrt{36497}.$$

Cette relation n'est plus conservée, par exemple, par la permutation $x_1 \leftrightarrow x_2$ (x_3, x_4, x_5 étant fixés). Le groupe des automorphismes devient ici le « groupe alterné » d'ordre 60.

Cet exemple et l'exemple 4 illustrent la *théorie de Galois* des équations algébriques.

(*N.B.* : Bien qu'une équation algébrique écrite « au hasard » ait « en général » le groupe symétrique comme groupe d'automorphismes, il n'est pas commode d'exhiber une équation simple dont toutes les racines soient réelles et dont le groupe est celui que l'on veut. L'exemple ci-dessus est dû à P. Cartier.)

de racines s'obtiennent comme cas particuliers de ce principe; chaque extraction de racine que l'on s'autorise « enrichit » la structure de l'ensemble des solutions et induit donc une « brisure de symétrie » de cet ensemble; l'équation est résoluble par radicaux si une succession de telles opérations permet de réduire « à néant » (plus exactement : à la seule transformation identique) le groupe de l'équation.

Types de symétrie et groupes « abstraits »

Quand peut-on dire que deux objets ont *les mêmes symétries*? Il est naturel de considérer que c'est le cas lorsque chacun d'eux peut se déduire de l'autre par une opération ne détruisant en rien la symétrie de ce dernier (le mathématicien dira : « invariante par son groupe d'automorphismes »). Ainsi, un dodécaèdre peut se déduire

Exemple 4

Les cinq racines de l'équation

$$x^5+x^4-4x^3-3x^2+3x+1=0,$$

sont

$$x_1=1{,}6825\ldots, \qquad x_2=0{,}8308\ldots$$
$$x_3=-0{,}2846\ldots, \qquad x_4=-1{,}3807\ldots, \qquad x_5=-1{,}9189\ldots,$$

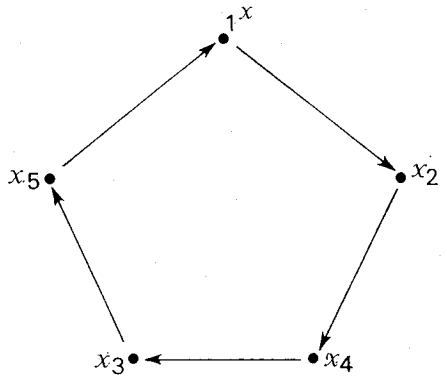
c'est-à-dire

$$x_1=2\cos\frac{2\pi}{11}, \qquad x_2=2\cos\frac{4\pi}{11},$$
$$x_3=2\cos\frac{6\pi}{11}, \qquad x_4=2\cos\frac{8\pi}{11}, \qquad x_5=2\cos\frac{10\pi}{11}.$$

Considérées comme nombres réels, elles n'ont pas plus de symétrie que celles de l'exemple 3. Lorsque l'on s'intéresse seulement aux relations rationnelles entre elles, elles en ont même moins : on a, en effet,

$$x_1^2-2=x_2, \qquad x_2^2-2=x_4, \qquad x_4^2-2=x_3, \qquad x_3^2-2=x_5, \qquad x_5^2-2=x_1.$$

Les symétries de cet ensemble d'équations sont celles de la figure suivante :

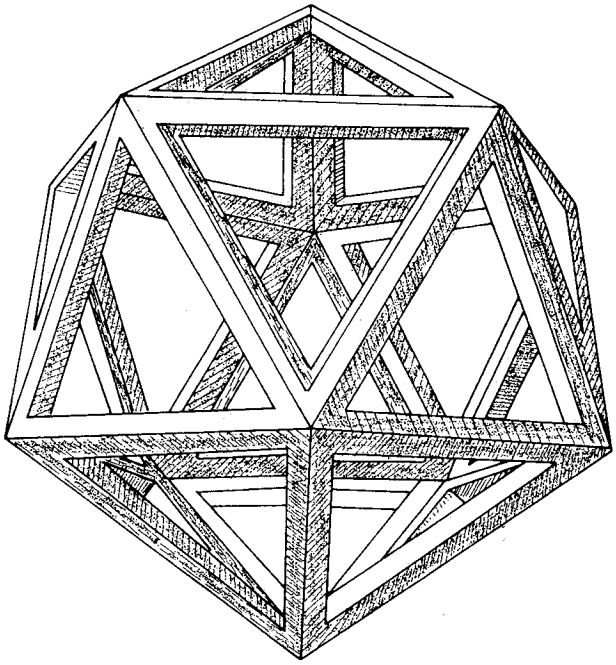


Elles forment un *groupe cyclique* d'ordre 5. De cette constatation, la théorie de Galois permet de déduire que l'équation donnée peut se résoudre à l'aide d'extractions de racines carrées et cinquièmes.

d'un icosaèdre en tronquant de la même façon chacun de ses sommets, et vice versa; ces deux solides ont donc manisfestement les « mêmes » symétries.

Lorsqu'on analyse ce concept (dans l'esprit de Félix Klein) on est conduit à attribuer à deux objets les « mêmes » symétries lorsque leurs groupes d'automorphismes sont *isomorphes*, ce qui signifie qu'on peut établir une correspondance biunivoque entre les automorphismes de l'un et les automorphismes de l'autre de telle sorte que la composition des automorphismes se corresponde (exemples 1 et 2; 3 et 5; 6). La loi de composition constitue la « table de multiplication » du groupe; deux groupes isomorphes ont donc « la même » table de multiplication.

Exemple 5



(Planche attribuée à Léonard de Vinci.) Le groupe des rotations de l'icosaèdre sur lui-même, c'est-à-dire des automorphismes de cette figure *du point de vue de la géométrie euclidienne orientée* est un groupe d'ordre 60, « le même » que (c'est-à-dire, isomorphe à) celui de l'exemple 3 : il est possible de deux façons d'inscrire dans l'icosaèdre cinq tétraèdres et d'attacher à chacun d'eux l'un des x_i de l'exemple 3 de telle façon que les automorphismes se correspondent. Si l'on fait abstraction de l'orientation, ce qui revient à admettre comme automorphismes les réflexions dans un miroir (ou la symétrie par rapport au centre), le groupe d'automorphismes devient un groupe d'ordre 120, *différent de celui de l'exemple* 3.

Il convient de souligner que cette notion de « mêmes » symétries est sensiblement plus abstraite que celle du langage courant : ainsi, une symétrie centrale et une symétrie par réflexion (symétrie bilatérale) donnent lieu toutes deux à la table de multiplication

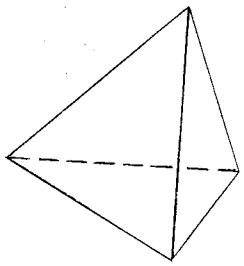
	+	−
+	+	−
−	−	+

[+ = l'identité, − = symétrie d'ordre 2] et ne se distinguent donc pas du point de vue que l'on vient de décrire.

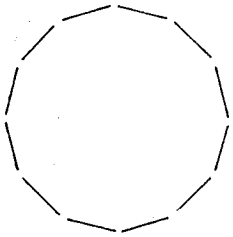
Disons que les symétries de deux objets sont de *même type* si elles sont les « mêmes » au sens précédent. Il y a équivalence entre la notion ainsi décrite de *type de symétrie* et

Exemple 6

Le tétraèdre régulier :



et le dodécagone régulier :



ont chacun douze ou vingt-quatre automorphismes selon qu'on tient compte de l'orientation ou non. Mais les groupes d'automorphismes en question *ne sont pas isomorphes* (par exemple : le tétraèdre orienté n'a que trois symétries d'ordre 2 et l'hexagone en a six).

la notion mathématique de *groupe* (on dit aussi parfois, pour raisons historiques, groupe « abstrait »). On voit donc qu'un groupe est caractérisé par sa *table de multiplication.* Ceci ne veut pas dire que toute table de multiplication est celle d'un groupe : il faut pour cela qu'elle puisse être réalisée comme la table de multiplication du groupe des automorphismes d'un objet, ce qui se traduit par des axiomes que l'on trouve dans les premières pages de tout manuel d'algèbre (associativité, existence d'un élément neutre et d'un inverse bilatère).

Symétries et groupes composés; groupes simples

Il peut arriver que le groupe des symétries d'un objet se « décompose » en deux groupes plus petits. Commençons par donner un exemple simple de ce phénomène.

Considérons le système formé de deux boules blanches, deux boules noires et deux boules rouges. Si l'on s'intéresse seulement aux différences de couleurs mais non aux couleurs elles-mêmes, ce système possède quarante-huit automorphismes : chacun d'eux « induit » l'une des six permutations possibles des trois couleurs, et chacune de ces

permutations est induite par huit automorphismes du système; en particulier, si l'on individualise à présent les couleurs (occasionnant ainsi une « brisure de symétrie »), le groupe d'automorphismes du système se réduit aux huit permutations qui préservent les couleurs, c'est-à-dire, qui « induisent l'identité » sur l'ensemble des trois couleurs. Ainsi, le groupe de départ, d'ordre quarante-huit (on appelle *ordre* d'un groupe le nombre de ses éléments) apparaît en quelque sorte comme « composé » d'un groupe d'ordre six (groupe des permutations des trois couleurs) et d'un groupe d'ordre huit.

De façon générale, soit G le groupe des automorphismes d'un ensemble structuré E. Supposons que l'on puisse déduire de E un nouvel ensemble structuré E′ et que G induise le groupe des automorphismes G′ de celui-ci (dans l'exemple précédent, E′ était l'ensemble des trois couleurs et G′ le groupe de ses six permutations). Soit G″ le sous-groupe des éléments de G qui induisent l'identité de E′. Ainsi, G décrit les symétries de E tel qu'il est donné initialement, G″ les symétries de ce même ensemble dont on a enrichi la structure en individualisant chaque point de E′, et G′ les symétries de E′. On dit alors que G″ est un *sous-groupe distingué* de G et que G′ est le groupe *quotient* de G par G″, où encore que G est *extension* de G′ par G″. Ces notions, sans doute les plus importantes de la théorie des groupes, sont, elles aussi, dues à Galois (qui utilisait évidemment une autre terminologie). Comme précédemment, nous omettrons les définitions formelles, qui ne pourraient qu'être recopiées de traités élémentaires.

On dit qu'un groupe est *simple* s'il ne peut pas être « décomposé » au sens qui vient d'être décrit, c'est-à-dire s'il ne possède aucun sous-groupe distingué (autre que lui-même et le sous-groupe réduit à l'identité : la conscience du mathématicien lui impose hélas la lourdeur de telles précisions). C'est là, à vrai dire, un emploi du mot « simple » assez détourné de son sens commun : les groupes simples sont, à certains égards, les plus difficiles à appréhender puisque leur étude ne peut pas être ramenée à celle de groupes plus petits qu'eux. Le terme « indivisible » ([1]) donnerait une idée plus juste de la notion; d'ailleurs, on peut établir un parallèle entre les groupes simples et les nombres premiers (eux aussi indivisibles).

Le problème de l'énumération des types de symétrie; classification des groupes finis simples

Peut-on énumérer ou décrire tous les types de symétrie — donc tous les groupes abstraits — existants?

Avant d'aborder cette question, il est nécessaire de souligner ici que, bien que cela n'ait jamais été postulé explicitement, on a surtout pensé, dans les considérations qui précèdent, aux *symétries finies*, c'est-à-dire aux groupes dont l'ordre est fini. C'est là une restriction considérable. Déjà dans la vie courante, les symétries infinies abondent : symétries cylindriques, symétries sphériques, symétries de translations (de certains ornements, de réseaux cristallins), etc. En mathématique, les groupes infinis sont la matière de domaines importants et vastes (groupes topologiques, groupes de Lie, groupes algébriques, groupes arithmétiques, groupes libres, etc.). Mais il faut se limiter : revenons-en donc, désormais, aux seuls *groupes finis*.

Exemple 7

Nombre S des « types de symétrie » (= classes d'isomorphismes de groupes) d'ordre n :

n	1	2	3	4	5	6	7	8	9	10	11	12	...	31	32	33	...
S	1	1	1	2	1	2	1	5	2	2	1	5	...	1	51	1	...

Même moyennant cette restriction, le problème de la description ou de l'énumération de tous les groupes finis existants ne paraît pas abordable (ni même raisonnable), du moins avec les concepts actuels. Cependant, l'extrême complexité de cette question réside surtout dans la trop grande variété des « compositions » possibles de groupes simples. Ainsi, on peut montrer que, par la « composition » successive de cinq groupes d'ordre 2, on peut construire cinquante-et-un groupes d'ordre 32 différents (c'est-à-dire, non isomorphes), tandis qu'il existe un seul groupe d'ordre 31 (car 31 est premier) et un seul groupe d'ordre 33 (exemple 7). On peut éviter délibérément cette complication et se proposer seulement de déterminer tous les groupes (finis) *simples*, c'est-à-dire, *tous les types de symétrie non « décomposables »*. Il y a encore vingt ans, ce problème aurait, lui aussi, paru inabordable; il vient cependant d'être résolu.

L'histoire de cette découverte est intéressante et le résultat surprenant. E. Galois avait, dès 1820, mis en évidence l'existence d'une infinité de groupes simples. D'autres séries infinies de tels groupes furent ensuite découvertes par C. Jordan (vers 1870), puis par L. E. J. Dickson (aux environs de 1900).

Après un nouveau hiatus de plus d'un demi-siècle, un pas décisif a été accompli en 1955 par C. Chevalley, non seulement par la mise à jour d'autres séries infinies, encore inconnues, mais surtout par le développement d'une théorie unificatrice, s'appliquant à la plupart des groupes simples connus à l'époque. (Comme l'a souligné J. Leray dans la discussion qui a suivi l'exposé oral, les progrès réalisés en 1955 par C. Chevalley reflétaient ceux accomplis entre-temps, notamment grâce à l'œuvre fondamentale d'Elie Cartan, en théorie des groupes de Lie; il est d'ailleurs significatif qu'aussi bien les groupes découverts par Jordan et par Dickson que ceux de Chevalley ont été aperçus grâce à leur analogie avec des groupes *infinis* — des groupes de Lie — connus avant eux.)

Après que quelques autres séries infinies (dues à R. Steinberg, M. Suzuki, R. Ree et l'auteur), s'inscrivant bien dans la voie tracée par Chevalley, soient venues s'ajouter aux précédentes, on pouvait, vers 1960, brosser un tableau assez cohérent et « compréhensible » des groupes finis simples connus, ceux-ci se répartissant pour la plupart en quelques familles infinies que l'on pouvait rattacher de façon naturelle et pour ainsi dire algorithmique aux groupes de Lie simples, eux-mêmes entièrement classifiés dès la fin du siècle dernier par W. Killing et E. Cartan. A ce bel ordre échappaient, il est vrai, cinq groupes isolés, découverts entre 1861 et 1873 par E. Mathieu, mais il s'agissait là de vieilles connaissances, un peu excentriques, et plus d'un était prêt à conjecturer que tous les groupes finis simples étaient désormais connus. C'est en 1966 que Z. Janko causa une première surprise en « produisant » un nouveau groupe simple, d'ordre 175 560.

Deux ans après, Janko récidivait, avec deux autres groupes, et D. Higman et C. Sims en exhibaient un quatrième.

Puis ce fut le tour de J. McLaughlin (1969), D. Held (1969), M. Suzuki (1969), J. Conway (trois d'un coup, en 1969), B. Fischer (trois également, en 1970),... L'épidémie cessa abruptement, après une dernière trouvaille de Janko (un groupe d'ordre $\sim 8{,}7 \cdot 10^{19}$) en 1975. On sait à présent, cela a été prouvé depuis (à un détail près : voir la note ([3])), qu'outre les groupes appartenant aux séries infinies « du type de Lie » ([2]), groupes susceptibles d'une description unifiée, cohérente, il existe en tout et pour tout vingt-six groupes exceptionnels, on les appelle *sporadiques*, à savoir les cinq groupes de Mathieu et dix-neuf autres, ceux-là même découverts entre 1966 et 1975, pour l'existence desquels on n'a pas encore d'« explication » vraiment satisfaisante.

Le statut du théorème de classification qui vient d'être énoncé est peu commun. Il est, fait unique en mathématique, le résultat d'un travail collectif de plusieurs dizaines de chercheurs, répartis dans le monde entier (surtout aux États-Unis et en Allemagne, mais aussi en Angleterre, au Japon, en France,...). Les articles qui contribuent au résultat final, et dont certains n'existent encore qu'à l'état d'ébauches, occupent quelques milliers de pages dont personne, sans doute, ne domine l'ensemble, même si quelques experts ont assurément une idée précise de ses principales articulations. Parmi eux, il faut citer celui qui s'est improvisé l'orchestrateur des recherches : D. Gorenstein. Il n'est pas douteux que l'édifice comporte encore quelques failles : c'est toujours inévitable dans une œuvre de cette ampleur, et ce l'est plus encore dans le cas présent étant donné la précipitation qui a marqué la mise au point de certaines parties de l'ensemble et le fait que quelques-uns des protagonistes brillent plus par leur intuition, parfois géniale, que par une extrême rigueur dans leur expression. Cependant, les spécialistes ne conservent guère de doute sur l'exactitude du théorème, leur confiance étant justifiée précisément par l'intuition remarquable (le terme anglais « insight » serait mieux approprié) des principaux artisans du résultat et par les nombreux recoupements qui semblent exclure la possibilité d'une faute majeure.

Autre particularité remarquable : près de la moitié des groupes sporadiques ont été « découverts », ce qui veut dire que leurs principales propriétés ont pu être décrites, plusieurs mois, voire des années, avant que leur existence ait été prouvée (souvent à l'aide d'ordinateurs). Cela fait davantage penser à certaines branches de la physique, à la théorie de particules élémentaires par exemple, qu'à la façon habituelle dont progressent les mathématiques. En tous cas, les philosophes pourront y trouver matière à réflexion sur la nature de ces « objets mathématiques », dont l'existence est devinée longtemps avant d'être prouvée (souvent par quelqu'un d'autre que le premier « découvreur »).

Le « Monstre » de Griess-Fischer

Terminons cet exposé par quelques mots concernant le plus remarquable des groupes sporadiques, l'un des derniers-nés et aussi le plus gros de tous. Appelons-le M.

C'est un groupe d'ordre $N \sim 8 \cdot 10^{53}$ (pour la valeur exacte de N, *cf.* l'exemple 8) « découvert » indépendemment, un même week-end de novembre 1973, par B. Fischer à Bielefeld et par R. Griess à Ann Arbor. Son existence a été prouvée par le même Griess en 1981 ([3]).

Exemple 8

Le « Monstre » de Griess-Fischer

Groupe M d'ordre

N = 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

= groupe des automorphismes d'un graphe d'ordre

5 791 748 068 511 982 636 944 259 375

= groupe des automorphismes d'une algèbre de dimension

196 883.

Comment peut-on montrer l'existence d'un tel « Monstre » ? (C'est le nom qu'il a reçu, assez injustement d'ailleurs étant donné les merveilleuses propriétés de symétrie qu'il recèle.) La tâche dépasse les capacités de tout ordinateur présent et,sans doute, à venir; il y a donc ici matière à s'exercer pour l'esprit humain. Écrire la table de multiplication du groupe (une table à N lignes et N colonnes, dont chaque élément est un nombre à cinquante-quatre chiffres !) est évidemment hors de question. Il est naturel, et cela nous ramène au sujet de l'exposé, de chercher à décrire M comme le groupe des symétries d'un objet approprié. Le type d'objet auquel les spécialistes songent d'emblée est un *graphe*, ensemble de points (les « sommets » du graphe) dont certaines paires sont reliées par un trait (arête du graphe) (*cf.* l'exemple 1). Hélas, un graphe ayant le Monstre pour groupe d'automorphismes devrait avoir au moins 5.10^{27} sommets (exemple 8), ce qui le rend malaisé à dessiner ! Griess procède autrement : il « engendre » M par certains de ses éléments de la même façon, par exemple, que le groupe des soixante rotations d'un icosaèdre peut être engendré par deux de ses éléments, convenablement choisis (on peut prendre comme éléments générateurs une symétrie axiale d d'ordre 2 et une symétrie axiale c d'ordre 5; toute rotation est alors le résultat de la succession de c et de d pris avec répétition et dans un ordre convenable). Dans le cas du Monstre, et de sa construction par R. Griess, il ne s'agit plus de deux rotations ordinaires, mais de rotations en beaucoup plus grand nombre, d'un espace euclidien E à 196 883 dimensions. La preuve d'existence fait intervenir de façon auxiliaire une certaine loi de multiplication dans E (une « loi d'algèbre ») invariante par M et il est alors naturel de se demander quel est le groupe de *tous* les automorphismes de cette loi. L'auteur a pu montrer que ce groupe n'est autre que le Monstre M lui-même, qui apparaît, de la sorte, comme le groupe de toutes les symétries d'un objet, d'ailleurs assez facile à décrire [8].

La théorie des groupes après le théorème de classification

Loin de mettre un terme aux recherches sur les groupes finis, l'achèvement de la classification des groupes simples a donné à ces recherches une vigueur nouvelle, ne serait-ce qu'en libérant des énergies qui étaient orientées dans ces derniers temps vers un but quelque peu négatif (puisqu'il s'agissait, au fond, de montrer la non-existence de groupes finis simples n'appartenant pas à une liste établie dès 1976).

Bien que la conclusion en soit désormais connue, on ne peut certes pas dire que le théorème de classification a atteint son état final. Il a été fait allusion, plus haut, à la preuve qui nous en est donnée : preuve touffue, sans unité, assurément pleine de redondances et de détours, occupant des milliers de pages parfois peu lisibles. De nombreux travaux en cours visent à la « décantation » de cette démonstration et à la recherche d'autres voies d'accès, que l'on espère plus courtes et plus conceptuelles, permettant d'atteindre le résultat; on leur a donné le nom de « Révisionnisme » (et, comme pour tous les révisionnismes, plusieurs écoles de pensées s'affrontent, très pacifiquement d'ailleurs !). Dans un ordre d'idées voisin, les groupes sporadiques offrent des perspectives de recherches riches et fascinantes. Ces groupes nous apparaissent encore comme des « accidents » isolés et plusieurs d'entre eux restent totalement mystérieux (notamment les trois ou quatre dont la preuve d'existence requiert encore, à ce jour, un ordinateur). Les « comprendre » c'est-à-dire les incorporer à un système cohérent qui rende leur existence naturelle, proche de l'évidence, est un défi à l'ingéniosité du mathématicien et une tâche passionnante, dont l'accomplissement requerra probablement des idées extérieures à la théorie des groupes finis (*cf.* [7]).

La solution du problème de classification a changé l'aspect de bien des domaines de la théorie des groupes finis. De nombreuses questions posées et restées en suspens depuis des années, voire des décennies, peuvent à présent être traitées par simple inspection de tous les cas possibles (*cf.* [3]). Cependant, cette façon de procéder est souvent jugée peu élégante (on ne tue pas une mouche avec un canon !) et, lorsqu'il s'agit de résultats importants, la « preuve par la classification » doit plutôt être prise comme un simple encouragement (de poids, il est vrai) à la recherche de voies plus directes.

Les groupes « abstraits » ont ici été assimilés aux « types de symétrie ». La connaissance de ces types — et notamment de tous les groupes simples — n'est qu'un pas dans l'étude des objets ayant ces symétries. C'est là un vaste sujet de recherches recoupant les domaines les plus divers des mathématiques, et notamment de la géométrie, à laquelle la classification a donné un nouveau souffle.

Mais le fait que le présent exposé, consacré à la notion de symétrie, a été axé sur la classification des groupes finis simples, ne doit pas faire croire que celle-ci constitue l'essence unique de la théorie des groupes finis. D'autres domaines de cette dernière sont d'une importance au moins égale. Ainsi, l'étude des représentations linéaires, peu influencée par la classification, est depuis de nombreuses années un des domaines les plus actifs de la théorie. Ici aussi, de nombreux problèmes restent posés malgré les progrès spectaculaires réalisés dans ces dernières années, par P. Deligne et G. Lusztig notamment.

Enfin, il convient de redire que la théorie des groupes finis n'est qu'une petite partie de la théorie des groupes et que diverses espèces de groupes infinis (groupes de Lie, groupes algébriques, groupes arithmétiques et autres groupes « discrets », ...) jouent un rôle toujours croissant dans les mathématiques et les autres sciences.

NOTES

([1]) « Indécomposable » conviendrait mieux encore, mais est réservé par les mathématiciens à un concept plus général : tout groupe simple est indécomposable mais la réciproque n'est pas vraie.

([2]) Pour la commodité de l'exposé, on range ici les groupes alternés et les groupes cycliques d'ordre premier dans les groupes du type de Lie.

([3]) A ma connaissance, il n'est pas entièrement prouvé – bien que personne n'en doute – que le nombre N de l'exemple 8 est l'ordre d'un seul groupe simple. C'est le seul point qui reste en suspens dans la classification des groupes finis simples.

RÉFÉRENCES

[1] *Écrits et mémoires mathématiques d'Evariste Galois*, R. BOURGNE, J.-P. AZRA éd., Gauthier-Villars, Paris, 1962.
[Naissance de la théorie des Groupes.]

[2] H. WEYL, *Symmetry*, Princeton University Press, 1952.
[Un classique.]

[3] W. FEIT, Some consequences of the classification of finite simple groups, *in* The Santa Cruz Conference on finite groups, *Proc. Symp. Pure Math.*, **37**, 1980, p. 175-181.
[Sur les implications, parfois surprenantes, du théorème de classification.]

[4] The geometric vein, in *The Coxeter Festschrift*, C. DAVIS, B. GRÜNBAUM, F. A. SHERK éd., Springer-Verlag, New York, Heidelberg, Berlin, 1981.
[Un recueil d'articles, riche en images et en références, comprenant une liste des œuvres de H. S. M. Coxeter, qui incarne plus que tout autre la symétrie géométrique sous ses diverses formes.]

[5] D. GORENSTEIN, *Finite simple groups*, Plenum Press, New York and London, 1982.
[Les grandes lignes du théorème de classification exposées par le maître d'œuvre.]

[6] F. BUEKENHOUT, Les groupes sporadiques, *La Recherche*, **131**, 1982, p. 348-355.
[Une introduction à la géométrie des groupes sporadiques, accessible aux non-spécialistes.]

[7] J. H. CONWAY, S. P. NORTON, Monstrous moonshine, *Bull. London Math. Soc.*, **11**, 1979, p. 508-539. I. FRENKEL, J. LEPOWSKY, A. MEURMAN, A natural representation of the Fischer-Griess Monster with the modular function j as character, *Proc. Nat. Acad. Sci. U.S.A.*, **81**, 1984, p. 3256-3260.
[Où l'on voit que la théorie des groupes finis n'est pas un système fermé !]

[8] J. TITS, Le Monstre (d'après R. GRIESS, B. FISCHER *et al.*); *Séminaire Bourbaki*, exposé n° 620, novembre 1983; *Astérisque*, **121-122**, 1985, p. 105-122.