GROUPES FINIS *

La chasse est fermée

Issue des travaux de A. Cauchy, E. Galois et C. Jordan, la théorie des groupes finis s'est fortement développée à la fin du 19ème siècle et au début du 20ème siècle sous l'impulsion de W. Burnside, G. Frobenius, I. Schur et leurs élèves, pour connaître ensuite une période de stagnation relative. Mais, à la suite des travaux de R. Brauer, P. Hall et H. Zassenhaus, pour ne citer qu'eux, cette théorie a connu depuis les années 50 un développement extraordinaire. Plusieurs problèmes jugés en 1900 comme inaccessibles viennent de trouver une solution; tout récemment, en 1980, l'un des plus importants d'entre eux, à savoir la détermination de tous les groupes finis simples, vient d'être résolu. Le but des lignes qui suivent est de retracer brièvement l'historique de cette découverte et de donner quelques références.

1. Groupes à dévisser et à étendre.

Tous les groupes dont il sera question sont finis. La loi de composition d'un groupe sera notée multiplicativement et si G est un groupe ou un ensemble fini, $|G|$ désigne son cardinal. Rappelons d'abord quelques définitions: si G est un groupe, un sous-groupe $H \subseteq G$ est dit distingué dans G si, pour tout $g \in G$ on a $g^{-1}Hg = H$, ce qui signifie que $g^{-1}hg \in H$ quel que soit $h \in H$. Un groupe G est dit simple si les seuls sous-groupes distingués de G sont les sous-groupes triviaux de G, c'est-à-dire G lui-même et $1 = \{1\}$, 1 désignant l'élément neutre de G. Naturellement, si G est commutatif (on dit aussi abélien), tout sous-groupe est distingué.

Voici quelques exemples: 1) désignons par S_3 le groupe des permutations de $\{1, 2, 3\}$; on a $|S_3| = 6$ et S_3 peut être décrit par l'écriture en cycles de la manière suivante:
$S_3 = \{id, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. Par exemple $(1\ 3\ 2)$ est la permutation $1 \mapsto 3$, $3 \mapsto 2$, $2 \mapsto 1$ tandis que $(1\ 2)$ est la per-

* Voici l'article annoncé dans l'Ouvert n°24

mutation $1 \mapsto 2$, $2 \mapsto 1$, $3 \to 3$. Il est alors facile de voir que $\{ id, (1\ 2\ 3), (1\ 3\ 2)\}$ est un sous-groupe distingué de S_3, tandis $\{ id, (1\ 2)\}$, $\{id, (1\ 3)\}$ et $\{id, (2\ 3)\}$ sont des sous-groupes qui ne sont pas distingués dans S_3.

2) Soit $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ le groupe des quaternions avec $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$; il est facile de vérifier que Q est un groupe non commutatif dont tous les sous-groupes sont distingués . Q est à ce titre un groupe assez exceptionnel.

3) Dans S_4 le groupe D_4 défini par $D_4 = \{id, (1\ 3), (2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\}$ n'est pas distingué; D_4 est le groupe dièdral d'ordre 8 et on peut se le représenter comme le groupe des isométries planes qui invarient globalement un carré.

Puisque l'ordre d'un sous-groupe divise l'ordre d'un groupe (théorème de Lagrange), les groupes cycliques d'ordre premier sont évidemment simples. Il est très facile de voir que ce sont les seuls groupes simples commutatifs; on obtient ainsi une première série infinie de groupes finis simples. Dans S_n, groupe des permutations de $\{1, 2, \ldots, n\}$, le sous-groupe a_n formé des permutations paires est un sous-groupe distingué.
Disons tout de suite que a_n est simple non abélien dès que $n \geqslant 5$. Ce résultat pas tout à fait évident étant connu de Galois et c'est parce que a_n est simple, pour $n \geqslant 5$, que l'équation générale de degré n ne peut être résolue au moyen des seules opérations d'addition, de soustraction, de multiplication, de division et d'extraction de racines m ièmes effectuées sur ces coefficients. Avec les $a_n (n \geqslant 5)$, on obtient donc une deuxième série infinie de groupes simples.

Donnons maintenant l'idée du dévissage d'un groupe: si G est un groupe, ou bien G est simple ou bien il ne l'est pas: dans le premier cas il n'y a rien à dire. Si G n'est pas simple, G possède un

sous-groupe strict G_1 distingué, différent de $\mathbb{1}$ qu'on peut en outre supposer maximal pour ces propriétés. Dire qu'un sous-groupe H d'un groupe G est distingué, ce que l'on note $H \trianglelefteq G$, revient à dire que la loi $(gH)(g_1H) = (gg_1)H$ munit l'ensemble G/H des classes à gauche de G modulo H d'une structure de groupe telle que l'application $g \mapsto gH$ soit un homomorphisme surjectif de G sur G/H dont le noyau est précisément H. Pour exprimer que H est distingué dans G et différent de G, on écrit $H \triangleleft G$ ou $G \triangleright H$. Revenons alors à notre groupe G et son sous-groupe distingué G_1; dire que G_1 est maximal revient à dire que le quotient $G/G_1 = H_1$ est simple.

On est donc dans la situation $G = G_o \triangleright G_1$ avec $G_o/G_1 = H_1$ simple et on a une suite exacte $\mathbb{1} \to G_1 \to G_o \to H_1 \to \mathbb{1}$. Si maintenant G_1 est simple, c'est terminé, sinon il existe G_2 distingué maximal dans G_1 et on a $G_1 \triangleright G_2$ avec $G_1/G_2 = H_2$ simple. Puis on recommence; comme G est fini le processus s'arrête au bout d'un certain nombre de pas. Il est donc clair qu'il existe une suite de sous-groupes emboîtés :

$G = G_o \triangleright G_1 \triangleright G_2 \triangleright \ \ldots \triangleright G_{n-1} \triangleright G_n = \mathbb{1}$ avec $H_i = G_{i-1}/G_i$ simple pour $1 \leqslant i \leqslant n$. Une telle suite s'appelle une suite de Jordan-Hölder du groupe G. Il y a alors un théorème (dit de Jordan-Hölder) qui affirme que si on a une autre suite de Jordan-Hölder de G, soit :

$G = G'_o \triangleright G'_1 \triangleright G'_2 \triangleright \ \ldots \triangleright G'_m = \mathbb{1}$, alors $m = n$ et il existe une permutation σ de $\{1, 2, \ldots, n\}$ telle que $H_i = G_{i-1}/G_i$ soit isomorphe à $H'_{\sigma(i)} = G'_{\sigma(i)-1}/G'_{\sigma(i)}$. Il n'y a pas en général unicité de la suite de Jordan-Hölder, mais l'ensemble des quotients simples successifs $\{G_{i-1}/G_i \mid 1 \leqslant i \leqslant n\}$ est lui essentiellement unique. Remarquons dès à présent que le théorème de Jordan-Hölder n'est pas un théorème profond de la théorie des groupes finis. Par exemple, il y a 5 groupes non isomorphes à 8 éléments; ce sont, C_k désignant le groupe cyclique d'ordre k, C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, Q et D_4; chacun d'entre eux possède une suite de Jordan- Hölder du type $G = G_o \triangleright G_1 \triangleright G_2 \triangleright G_3 = \mathbb{1}$ avec $G_{i-1}/G_i \simeq C_2$ quel que soit i, $1 \leqslant i \leqslant 3$.

Donnons néanmoins une application pratique immédiate de ce théorème: soient G et G' deux groupes finis de même ordre,

$G = G_o \triangleright G_1 \triangleright \ \ldots \triangleright G_n = \mathbb{1}$ une suite de Jordan-Hölder de G et

$G' = G'_o \triangleright G'_1 \triangleright \ \ldots \triangleright G'_m = \mathbb{1}$ une suite, non nécessairement maximale de

sous-groupes de G'.

Si pour un j, $1 \leq j \leq m$, G'_{j-1} / G'_j est un groupe simple qui n'est pas isomorphe à aucun des G_{i-1} / G_i $(1 \leq i \leq n)$, alors on peut affirmer que G et G' ne sont pas isomorphes. Cela résulte du fait qu'on peut toujours plonger une suite de sous-groupes emboîtés, comme pour G', dans une suite maximale, c'est-à-dire de Jordan-Hölder.

La théorie de l'extension de O. Schreier, jointe au théorème de Jordan-Hölder, permet du moins en théorie, de construire tous les groupes G ayant un cardinal donné m dès que l'on connaît tous les groupes simples. En 1926, O. Schreier a résolu le problème suivant: étant donnés deux groupes N et H, trouver tous les groupes G tel que N soit un sous-groupe distingué de G vérifiant $G/N \simeq H$. Un tel groupe G s'appelle une extension de N par le facteur H. Par exemple, si m = 6, on trouve deux extensions de C_3 par C_2 à savoir $C_3 \times C_2 \simeq C_6$ et S_3 et on trouve une extension de C_2 par C_3 à savoir $C_3 \times C_3 \simeq C_6$. Il y a donc exactement, à isomorphie près, deux groupes à 6 éléments. Supposons que l'on connaisse la famille S de tous les groupes finis simples, soit m fixé et G un groupe tel que $|G| = m$. Il n'y a clairement qu'un nombre fini de possibilités, compte tenu du fait qu'à cardinal donné, on a évidemment qu'un nombre fini de groupes simples ayant ce cardinal, pour un dévissage de G du style $G = G_o \rhd G_1 \rhd G_2 \rhd \dots \rhd G_{r-1} \rhd G_r = 1\!\!1$ où $G_{i-1}/G_i = S_i$ est un groupe simple puisé dans la famille S (qu'on est censé connaître) pour $1 \leq i \leq r$.

On a alors $S_r = G_{r-1} \lhd G_{r-2}$ et $G_{r-2} / G_{r-1} \simeq S_{r-1}$: la théorie de l'extension de Schreier nous donne alors tous les G_{r-2} possibles.

Puis on recommence:

$G_{r-2} \lhd G_{r-3}$ et $G_{r-3} / G_{r-2} \simeq S_{r-2}$ et on détermine tous les G_{r-3} possibles etc...

Ceci peut être fait pour tous les r-uples $(S_1, S_2, \dots S_r)$ où $S_i \in S$, la condition étant que $|S_1| \times |S_2| \times \dots \times |S_r| = m$. Il est donc clair que la connaissance de tous les groupes finis simples permet théoriquement de déterminer tous les groupes finis: à ce titre les groupes simples apparaissent comme les briques élémentaires à partir desquelles on construit tous les groupes. Remarquons tout de même que la théorie de

l'extension ne nous donne que la table de G et on ne connait pas à ce jour de procédure simple générale qui permette de décider si, deux tables étant données, elles correspondent à des groupes isomorphes ou non. Ce qui précède est donc bien théorique et les groupes ne se découvrent pas en général par ce procédé. Pour se convaincre de cela, prenez par exemple la table de $\mathcal{A}_5$ (groupe des permutations paires de $\{1, 2, 3, 4, 5\}$) dressée de façon un peu sauvage et demandez à quelqu'un qui connait suffisamment les groupes s'il reconnait là la table de $\mathcal{A}_5$... Il n'en reste pas moins que la détermination de tous les groupes finis simples est un problème central de la théorie des groupes finis.

2. Des origines à 1955

Jusqu'à présent, on a rencontré deux familles de groupes simples, les cycliques C_p (p premier) et les groupes alternés $\mathcal{A}_n$ ($n \geqslant 5$). Donnons maintenant un troisième exemple de famille infinie qui sera en quelque sorte prototypique des groupes simples qui proviennent des groupes linéaires classiques.

Soit K un corps fini; d'après un théorème de Wedderburn un tel corps est nécessairement commutatif et il est facile de voir que $|K| = p^r$ où p est un entier premier et r un entier $\geqslant 1$. En outre, si $q = p^r$ est un nombre de cette forme, il existe un et un seul corps fini noté $\mathbb{F}_q$ à q éléments: c'est le corps de rupture du polynôme $X^q - X$ de $\mathbb{F}_p[X]$. Soit alors GL(n, q), le groupe de matrices carrées inversibles $n \times n$ à coefficients dans $\mathbb{F}_q$. L'application "déterminant" est un homomorphisme surjectif de GL (n, q) sur $\mathbb{F}^*_q$ dont le noyau est SL(n, q) lequel est donc un sous-groupe distingué de GL(n, q). Le centre Z de GL(n, q) est formé des matrices $\alpha.1_n$ où $\alpha \in \mathbb{F}^*_q$.

Le groupe quotient GL(n, q)/Z se note PGL (n, q) et on désigne par PSL(n, q) l'image de SL(n, q) dans PGL(n, q). On a alors le résultat suivant qui remonte à Jordan et Dickson: sauf si n = 2 et q = 2 ou 3, le groupe PSL (n, q) est simple non abélien d'ordre

$$\frac{1}{d} q^{\frac{n(n-1)}{2}} (q^2-1)(q^3-1)\ldots(q^n-1) \text{ où } d = \text{pgcd}(n, q-1).$$

Il est facile de voir que $PSL(2, 2) \simeq \mathfrak{S}_3$, que $PSL(2, 3) \simeq \mathfrak{A}_4$ et S_3 et $\mathfrak{A}_4$ ne sont pas simples. Remarquons en outre que si $(n, q) \neq (2, 2)$ ou $(2, 3)$, $PSL(n, q)$ est le seul facteur de Jordan-Hölder de $GL(n, q)$ qui soit simple et non cyclique.
Les autres groupes linéaires classiques s'obtiennent comme groupes d'automorphismes de certaines formes bilinéaires ou hermitiennes non dégénérées définies sur le $\mathbb{F}_q$ - espace vectoriel $V = \mathbb{F}_q^n$ $(n \geqslant 2)$. Il y a alors une procédure uniforme pour, partant d'un groupe linéaire classique, obtenir un groupe simple et ceci à un nombre fini d'exceptions près: si G est un groupe linéaire classique, soit G' le groupe dérivé, c'est-à-dire le sous-groupe de G engendré par les commutateurs $[x, y] = x^{-1}y^{-1}xy$ $(x, y \in G)$. Alors si Z' désigne le centre de G', sauf dans un nombre fini de cas, le quotient G'/Z' est un groupe simple non abélien.
Par exemple $GL(n, q)' = SL(n, q)$ et Z' = centre de $SL(n, q)$ $= Z \cap SL(n, q)$ où Z = centre de $GL(n, q)$.
Certaines démonstrations de simplicité sont laborieuses et difficiles, particulièrement dans le cas orthogonal élucidé par Dieudonné. On obtient ainsi six nouvelles familles infinies de groupes simples: la famille $PSL(n, q)$; la famille symplectique (correspondant à une forme bilinéaire antisymétrique) notée $PS_p(2n, q)$ $(n \geqslant 2)$; la famille unitaire (forme hermitienne) notée $PSU(n, q)$ $(n \geqslant 3)$; les trois familles orthogonales (forme bilinéaire symétrique), notées $P\Omega(2n + 1, q)$ $(n \geqslant 3)$, $P\Omega(2n, q, +)$ $(n \geqslant 4)$ et $P\Omega(2n, q, -)$ $(n \geqslant 4)$.
Pour les ordres, on pourra consulter la table 1 placée à la fin.

Entre 1901 et 1908, L. Dickson découvrit deux autres familles infinies de groupes simples notés $G_2(q)$ et $E_6(q)$: elles sont reliées aux algèbres de Lie simples complexes G_2 et E_6. Si on ajoute aux dix familles infinies énumérées jusqu'à présent les cinq groupes simples isolés découverts en 1861 par E. Mathieu et baptisés groupes sporadiques par W. Burnside, on obtient tous les groupes simples finis

connus au début de 1955. A cette époque, les groupes de Mathieu étaient considérés comme des curiosités naturelles sans réelle importance pour le problème général de la classification des groupes finis simples, mais dans les dernières années, leurs rôles ont considérablement grandi. En 1955, la situation allait être bouleversée par la parution de deux articles, l'un de C. Chevalley, l'autre de R. Brauer et K. Fowler.

3. La période des groupes de Chevalley et leurs variantes: 1955-1966

Chevalley donne une méthode générale pour construire, à partir des algèbres de Lie simples complexes, entièrement classés par W.Killing et E. Cartan au siècle dernier, des familles infinies de groupes simples infinis (appelés depuis groupes de Chevalley ou groupes du type de Lie). Indiquons très sommairement la méthode de Chevalley:

Soit G un groupe de Lie complexe connexe et soit g son algèbre de Lie, si $x \in g$, ad(x) est l'endomorphisme de g défini par $y \longmapsto ad(x)(y) = [x,y]$, $[\ ,\ ]$ étant le crochet usuel des champs de vecteurs sur G. L'application $t \longmapsto \exp(t\,ad(x)) = \sum_{m=0}^{\infty} \frac{t^m}{m!} (ad(x))^m$ de $\mathbb{C}$ dans $Aut(g) \subseteq GL(g)$ est un homomorphisme du groupe additif $\mathbb{C}$ sur un sous-groupe à un paramètre de Aut(g) : ces sous-groupes engendrent un sous- groupe de Aut(g) appelé groupe adjoint et d'ailleurs isomorphe à G/Z où Z est le centre de G.

Si G est un groupe de Lie presque simple (c'est-à-dire si G ne contient aucun sous-groupe distingué fermé non trivial de dimension > 0), Chevalley a montré qu'il existe une base de g dont certains éléments x_r ont la propriété que les sous-groupes à un paramètre X_r: $t \longmapsto \exp(t\,ad(x_r))$ qui leur correspondent engendrent déjà à eux seuls le groupe adjoint et sont tels qu'en outre : 1) la matrice $(ad(x_r))^m$ est nulle pour m assez grand de sorte que $X_r(t) = \sum_{m=0}^{\infty} \frac{t^m}{m!} (ad(x_r))^m$ est une somme finie et que donc $X_r(t)$ est une matrice dont les coefficients sont en fait des polynômes en t et 2) en outre, ces polynômes sont à coefficients entiers.

On peut alors, dans ces polynômes, remplacer t par les éléments d'un corps commutatif quelconque K et on obtient ainsi un groupe $X_r(K)$, sous-groupe à un paramètre de GL(n,K) si n=dim G = dim$_{\mathbb{C}}$g.
On montre alors qu'à quatre exceptions près ($A_1(2)$, $A_1(3)$, $B_2(2)$, $G_2(2)$), le groupe $G_k \leqslant GL(n,K)$ engendré par les $X_r(K)$ est simple (et même dans les cas non simples le groupe G_K a un centre trivial). Prenant alors pour K un corps fini $\mathbb{F}_q$ on obtient ainsi des séries de groupes finis simples.
Rapidement R.Ree montra que la méthode de Chevalley fournissait les familles infinies classiques du § 2, sauf pour les PSU(n,q) et certains groupes orthogonaux; il s'aperçut ainsi que la méthode donnait également les familles $G_2(\mathfrak{g})$ et $E_6(\mathfrak{g})$ de Dickson, Chevalley lui-même avait montré que les familles infinies correspondant aux algèbres de Lie simples exceptionnelles F_4, E_7 et E_8 étaient nouvelles; on obtient donc ainsi trois nouvelles familles infinies de groupes simples notées $F_4(\mathfrak{g})$, $E_7(\mathfrak{g})$ et $E_8(\mathfrak{g})$ qui étaient inconnues avant 1955. Des rafinements apportés à la méthode de Chevalley permirent alors à R.Steinberg, J.Tits et D. Hertzig non seulement de faire rentrer les familles PSU(n,q) et PΩ(2n,q,-) dans le cadre de Chevalley, mais encore de trouver deux nouvelles séries notées ${}^3D_4(\mathfrak{g})$ et ${}^2E_6(\mathfrak{g})$. Ces rafinements sont basés sur des symétries de diagrammes de Dynkin de certaines algèbres de Lie simples complexes (en l'occurence A_l ($l \geq 2$), D_l ($l \geq 4$) et E_6). Toutes ces procédures furent unifiées par Tits.
En 1960, M. Suzuki trouve, en étudiant les groupes dits de Zassenhaus, une nouvelle famille infinie de groupes simples de permutations, mais dès 1961, R.Ree s'aperçut qu'on pouvait obtenir les groupes de Suzuki avec une nouvelle variante de la méthode de Chevalley et en même temps il construisait, toujours avec une adaptation de cette méthode, deux nouvelles familles infinies de groupes simples: ces trois nouvelles familles infinies (celle de Suzuki et les deux de Ree) sont notées ${}^2B_2(q)$, ${}^2G_2(\mathfrak{g})$ et ${}^2F_4(\mathfrak{g})$.

En 1961, la technique de recherche de groupes finis simples, basée sur la théorie des groupes et algèbres de Lie, avait donc permit d'agrandir l'ensemble des familles de groupes finis simples de 8 nouvelles familles portant ainsi leur nombre à 18, lequel est resté inchangé jusqu'à ce jour. Bien des spécialistes des groupes finis crurent alors que la classification des groupes simples finis était achevée.
L'autre résultat des années 55, du à R. Brauer et K. Fowler est le suivant:

Soit G un groupe fini simple et soit t une involution de G (c'est-à-dire un élément d'ordre 2). Alors, si $S = C_G(t) = \{x \in G \mid xt = tx\}$ est le centralisateur de t dans G, on a $|G| < (|S|^2)!$. Il résulte immédiatement de cela qu'il n'y a qu'un nombre fini de groupes simples admettant pour centralisateur d'une involution un groupe donné. Les théoriciens des groupes s'attaquèrent alors au problème suivant : étant donné un groupe S contenant une involution dans son centre, trouver tous les groupes simples G tel que $S \simeq C_G(t)$ pour une certaine involution t de G. Notons que le théorème de Brauer-Fowler, malgré son importance, n'est pas très difcile. Il n'en va pas de même du résultat suivant, établi en 1963 par W. Feit et J.Thompson: tout groupe fini simple non abélien est d'ordre pair. C'est la plus longue démonstration actuellement connue en mathématiques (environ 300 pages d'une revue). Un ancien résultat de Cauchy dit que si un nombre premier p divise l'ordre d'un groupe fini G, alors G contient un élément d'ordre p. Le théorème de Feit et Thompson assure alors que tout groupe fini simple non abélien contient une involution. Le problème de la détermination des groupes simples ayant pour centralisateur d'une involution un groupe donné s'en trouvait ainsi grandi et allait faire désormais l'objet de recherches actives de la part des théoriciens des groupes.

4. La période des groupes sporadiques: 1966-1980

Soit G un groupe fini, p un nombre premier divisant l'ordre de G et écrivons $|G| = p^a m$ où p ne divise pas m. Un sous-groupe P de G d'ordre p^a s'appelle un p-sous-groupe de Sylow de G; un célèbre théorème du à Sylow affirme alors que si p divise G 1) G possède au moins un p-sous-groupe de Sylow 2) tous les p-sous-groupes de Sylow de G sont conjugués et 3) leur nombre est congru à 1 modulo p et divise $|G|$.

Un non moins célèbre théorème du à Burnside affirme que l'ordre d'un groupe simple non abélien est divisible par au moins 3 nombres premiers distincts (c'est le mieux qu'on peut espérer, au moins naïvement car $\mathcal{A}_5$ est simple et $|\mathcal{A}_5| = 2^2.3.5$).

En 1966, coup de théâtre: environ un siècle après les découvertes de Mathieu, Z.Janko, en classifiant les groupes simples dont les 2 sous-groupes de Sylow sont abéliens, trouve un nouveau groupe simple qui ne rentre dans aucune des 18 familles connues. Le groupe G est caractérisé par les faits suivants: (a) G ne possède pas de sous-groupe d'indice 2.
(b) les 2 sous-groupes de Sylow de G sont abéliens

(en fait ils sont isomorphes à $C_2 x C_2 x C_2$)

© G possède une involution dont le centralisateur est isomorphe à $C_2 x \mathcal{A}_5$. Janko prouve d'abord qu'un tel groupe est nécessairement simple; ensuite il montre son existence en le présentant comme sous-groupe de GL $(7, \mathbb{F}_{11})$: c'est le sous-groupe engendré par les matrices.

$$A = \begin{bmatrix} 0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0 \end{bmatrix} \qquad B = \begin{bmatrix} -3&2&-1&-1&-3&-1&-3 \\ -2&1&1&3&1&3&3 \\ -1&-1&-3&-1&-3&-3&2 \\ -1&-3&-1&-3&-3&2&-1 \\ -3&-1&-3&-3&2&-1&-1 \\ 1&3&3&-2&1&1&3 \\ 3&3&2&1&1&3&1 \end{bmatrix}$$

A et B sont des matrices à coefficients dans le corps fini $\mathbb{F}_{11} = \mathbb{Z}/11\mathbb{Z}$, d'ordres 7 et 5 respectivement. Ce groupe, le premier sporadique découvert par Janko, est généralement désigné par J ou Ja ou encore J1. Son ordre est $|J1| = 2^3.3.5.7.11.19 = 175.560$.

Désormais la chasse aux groupes sporadiques est commencée et elle va être fructueuse puisque entre 1967 et 1980, 20 autres groupes sporadiques, outre les 5 groupes de Mathieu et le groupe de Janko J1, vont être découverts. Les méthodes utilisées sont variées et complexes et souvent l'existence est prouvée par un ou plusieurs autres théoriciens des groupes que celui ou ceux qui proposèrent la possibilité du groupe avec sa caractérisation. On renvoie le lecteur à la table 2 située à la fin.

Signalons quand même un résultat important obtenu par J.Thompson en 1968: disons qu'un groupe simple non abélien est minimal s'il ne contient strictement aucun autre groupe simple non abélien. Puisqu'un groupe d'ordre < 60 n'est pas simple non abélien, $\mathcal{A}_5$ est clairement simple minimal et c'est le seul groupe alterné simple minimal. Thompson a déterminé tous les groupes simples minimaux; de façon précise, soit G un groupe simple non abélien, alors G contient l'un des groupes suivants : PSL (3,3), PSL(2,p) (p premier > 3 et $p^2+1 \equiv 0 \bmod 5$), PSL $(2,2^p)$, PSL $(2,3^p)$ (p premier impair) ou ${}^2B_2(2^p) = Sz(2^p)$ (p premier impair).

Pour terminer ce paragraphe, on peut faire la remarque suivante: les 26 groupes sporadiques ne sont pas 26 entités isolées. Il y a entre eux des

liens et on peut les grouper selon la ou les techniques qui ont permis de les "détecter" puis d'établir leur existence. Disons en gros que les 5 groupes de Mathieu peuvent être obtenus comme extensions de groupes multitransitifs; il en va de même pour les groupes de Higman-Sims et de McLaughlin, (les groupes de Mathieu peuvent aussi s'obtenir comme groupes d'automorphismes de système de Steiner appropriés). Les groupes de Higman-Sims, de McLaughlin, de Suzuki, de Hall-Janko ainsi que les 3 groupes de Fischer peuvent se caractériser comme groupes d'automorphismes de graphes convenables, tandis que les 3 groupes de Conway sont issus de l'étude du réseau de Leech dans $\mathbb{R}^{24}$. C'est en cherchant à caractériser les centralisateurs d'involutions (cf § 3) qu'on a découvert les groupes de Janko, de Hall-Janko, de Higman Janko-McKay, de Held-Higman-McKay, de Lyons-Sims ainsi que le J4 (le dernier sporadique découvert).

Les groupes de Harada-Norton, de Thompson-Smith, de O'Nan et de Rudvalis sont issus de problèmes de classification; enfin le Bébé Monstre B et le Monstre M furent découverts lorsque B.Fischer s'attaqua au problème de la classification des groupes engendrés par une classe de conjugaison d'involutions dont le produit de deux quelconques d'entre elles est d'ordre ≤ 4.

5. L'achèvement

Fin 1979, les experts estimaient qu'il n'existait que 26 groupes sporadiques, mais ils n'en connaissaient effectivement que 24: il leur en manquait donc deux, à savoir le "monstre" M = F1 et le groupe J4. Le groupe J4 est un groupe d'ordre $2^{21}.3^3.5.7.11^3.23.29.31.37.43$ dont l'existence avait été conjecturée dès 1973 par Zvonimir Janko (Université de Heidelberg). Pour ce qui est du groupe F1, c'est un groupe d'ordre

$$2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71$$

Ce nombre est de l'ordre 10^{54}: à titre de comparaison, disons qu'on estime que le nombre total de protons et de neutrons de la Terre est de l'ordre de 4×10^{51}. L'existence du groupe F1 avait été prédite en 1972 par Bernd Fischer (Université de Bielefeld) et Robert Griess (Université du Michigan); c'est John Conway (Université de Cambridge) qui l'a baptisé le "monstre" vu son cardinal. En janvier 1980, R. Griess annonçait qu'il avait construit le monstre à la main, c'est-à-dire sans ordinateur: la construction utilise un groupe de symétries dans un espace de dimension 196.833. Ceci est d'autant plus surprenant que le monstre "contient" d'une certaine façon (voir plus loin)

nombre de sporadiques dont les existences ne peuvent être établies qu'à l'aide de l'ordinateur. D'autre part, le 20 février 1980, D. Benson, J. Conway, S. Norton, R.Parker et J.Thackray (Université de Cambridge) annoncèrent l'existence, prouvée par des techniques d'ordinateurs, du groupe J4.

Disons qu'un groupe H intervient dans un groupe G si G possède deux sous-groupes K et L tels que L soit distingué dans K et tels que K/L soit isomorphes à H. Clairement si H intervient dans G, $|H|$ divise $|G|$. Puisque 37 divise $|J4|$ et ne divise pas $|F1|$, J4 n'intervient pas dans F1; néanmoins 20 des 26 groupes sporadiques interviennent dans le monstre F1. (R.Griess parle de "he and his happy family").

Tout récemment (octobre 1980), on vient d'apprendre que des théoriciens des groupes (on pense généralement à M. Ashbacher (Université de Californie), J. Conway et D.Gorenstein (Université Rutgens)) auraient démontré qu'il n'existe pas d'autre groupe sporadique que les 26 connus.

Moralité: on connait tous les groupes simples finis. Jusqu'à présent, aucun article (à la connaissance du rédacteur) n'a encore été publié au sujet de l'existence de J4 et F1 ou du fait qu'il y a exactement 26 groupes sporadiques.

6. Quelques conséquences

La classification de tous les groupes finis simples va permettre d'apporter une réponse à plusieurs vieilles conjectures ou problèmes. Signalons entre autres :

a) la conjecture de Schreier: si G est un groupe simple ExtG = Aut G/Int G est un groupe résoluble. La réponse sera oui.

b) la conjecture de Frobenius : soit G un groupe fini et soit m un diviseur de $|G|$: si dans G, l'équation $x^m = 1$ possède exactement m solutions, celles-ci forment un sous-groupe (alors nécessairement distingué) de G.

Réponse : oui.

c) il n'existe pas de groupes 6 -transitifs autres que S_n($n \geq 6$) et $a_n (n \geq 8)$.

La réponse sera oui.

d) un groupe simple est engendré par deux éléments.

e) la détermination de tous les groupes 2-transitifs, voire primitifs.

Pour terminer, signalons un fait surprenant: si G est un groupe, une représentation linéaire (ordinaire) de G est un homomorphisme $R: G \longmapsto GL(V)$ où V est un $\mathbb{C}$ - espace vectoriel de dimension finie. R est irréductible s'il n'existe pas de sous-espace $0 < W < V$ stable par toutes les opérations $R(g)$ (pour $g \in G$) et le caractère d'une représentation n'est rien d'autre que l'application $g \longmapsto \chi(g)$ = Trace de $R(g)$ de G dans $\mathbb{C}$. Il est assez facile de montrer que le nombre de représentations irréductibles d'un groupe G (non isomorphes entre elles) est égal au nombre de classes de conjugaison de G et manifestement un caractère est constant sur une classe de conjugaison. On peut donc parler de la table (carrée) des caractères irréductibles d'un groupe G. Il se trouve que les coefficients de la table des caractères irréductibles du monstre F 1 (c'est une table 194x194) sont intimement reliés aux premiers coefficients de la série de la fonction modulaire elliptique ($q=e^{2\pi iz}$)

$$j(z) = q^{-1} + 744 + 196884\ q + 21493760\ q^2 + \ldots$$

Cette numérologie pour le moins étrange a été découverte et étudiée par J.McKay, J.G.Thompson, J.H. Conway, S.P.Norton.

Table I : Les 18 familles infinies de groupes finis simples.

Découvert par	Notation de Lie	Ordre	
C_p		p (p premier)	
$\mathfrak{A}_n$ ($n \geq 5$)		$\frac{1}{2} n!$	
$PSL(n,q)$ ($n \geq 2$)	$A_{n-1}(q)$	$(1/d)\, q^{n(n-1)/2} (q^n-1)(q^{n-1}-1)\dots(q^2-1)$	$d = (n, q-1)$
$PSp(2n,q)$ ($n \geq 2$)	$C_n(q)$	$(1/d)\, q^{n^2} (q^{2n}-1)(q^{2(n-1)}-1)\dots(q^2-1)$	$d = (2, q-1)$
$PSU(n,q)$ ($n \geq 3$)	${}^2A_{n-1}(q)$	$(1/d)\, q^{n(n-1)/2} (q^n-(-1)^n)(q^{n-1}-(-1)^{n-1})\dots(q^2-1)$	$d = (n, q-1)$
$P\Omega(2n+1,q)$ ($n \geq 3$)	$B_n(q)$	$(1/d)\, q^{n^2} (q^{2n}-1)(q^{2(n-1)}-1)\dots(q^2-1)$	$d = (2, q-1)$
$P\Omega(2n,q,+)$ ($n \geq 4$)	$D_n(q)$	$(1/d)\, q^{n(n-1)} (q^n-1) \prod_{i=1}^{n-1} (q^{2i}-1)$	$d = (4, q^n-1)$
$P\Omega(2n,q,-)$ ($n \geq 4$)	${}^2D_n(q)$	$(1/d)\, q^{n(n-1)} (q^n+1) \prod_{i=1}^{n-1} (q^{2i}-1)$	$d = (4, q^n+1)$
Dickson (1901)	$G_2(q)$	$q^6(q^6-1)(q^2-1)$	
Dickson (1905)	$E_6(q)$	$(1/d)\, q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)$	$d = (3, q-1)$
↑ ce qui était connu en 1955 ↑		↓ ce qui a été découvert entre 1955 et 1961 ↓	
Chevalley (1955)	$F_4(q)$	$q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$	
Chevalley (1955)	$E_7(q)$	$(1/d)\, q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1)$	$d = (2, q-1)$
Chevalley (1955)	$E_8(q)$	$q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1)$	
Steinberg (1959)	${}^3D_4(q)$	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$	
Steinberg (1959)	${}^2E_6(q)$	$(1/d)\, q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5+1)(q^2-1)$	$d = (3, q+1)$
Suzuki $Sz(q)$ (1960)	${}^2B_2(q)$ $q = 2^{2n+1}$	$q^2(q^2+1)(q-1)$	
Ree $R_1(q)$ (1961)	${}^2G_2(q)$ $q = 3^{2n+1}$	$q^3(q^3+1)(q-1)$	
Ree $R_2(q)$ (1961)	${}^2F_4(q)$ $q = 2^{2n+1}$	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$	

Exceptions : $PSL(2,2)$, $PSL(2,3)$, $PSU(3,2)$ et ${}^2B_2(2)$ sont des groupes résolubles ; $PSp(4,2)$, $G_2(2)$ et ${}^2F_4(2)$ ont un groupe dérivé d'indice 2 qui est simple ; ${}^2G_2(3)$ a un groupe dérivé d'indice 3 qui est simple.

Isomorphismes : $B_1(q) \simeq C_1(q) \simeq A_1(q) \simeq {}^2A_1(q)$; $B_2(q) \simeq C_2(q)$; $D_2(q) \simeq A_1(q) \times A_1(q)$; ${}^2D_2(q) \simeq A_1(q^2)$; $D_3(q) \simeq A_3(q)$; ${}^2D_3(q) \simeq {}^2A_3(q)$ Si $q=2$ $B_n(q) \simeq C_n(q)$ ($n \geq 3$) ; $\mathfrak{A}_5 \simeq PSL(2,4) \simeq PSL(2,5)$; $\mathfrak{A}_6 \simeq PSL(2,9) \simeq PSp(4,2)'$; $\mathfrak{A}_8 \simeq PSL(4,2)$; $PSL(2,7) \simeq PS(3,2)$ $PSp(4,3) \simeq PSU(4,2)$; $PSU(3,3) \simeq G_2(2)'$; $PSL(2,8) \simeq {}^2G_2(3)'$.

Table II : Les 26 groupes simples sporadiques

Détecté par	Confirmé par	Symboles	Ordre
Mathieu (1861)	Mathieu (1861)	M_{11}	$2^4.3^2.5.11 = 7.920$
Mathieu (1861)	Mathieu (1861)	M_{12}	$2^6.3^3.5.11 = 95.040$
Mathieu (1873)	Mathieu (1873)	M_{22}	$2^7.3^2.5.7.11 = 443.520$
Mathieu (1873)	Mathieu (1873)	M_{23}	$2^7.3^2.5.7.11.23 = 10.200.960$
Mathieu (1873)	Mathieu (1873)	M_{24}	$2^{10}.3^3.5.7.11.23 = 244.823.040$
Janko (1965)	Janko (1965)	J ou J1 ou Ja	$2^3.3.5.7.11.19 = 175.560$
D. Higman, Sims (1967)	D. Higman, Sims (1967)	HS ou HiS	$2^9.3^2.5^3.7.11 = 44.352.000$
Hall, Janko (1967)	Hall, Wales (1967)	J2 ou HaJ ou HaJW	$2^7.3^3.5^2.7 = 604.800$
McLaughlin (1968)	McLaughlin (1968)	McL	$2^7.3^6.5^3.7.11 = 898.128.000$
Suzuki (1968)	Suzuki (1968)	Sz	$2^{13}.3^7.5^2.7.11.13 = 448.345.497.600$
Janko (1967)	G. Higman, McKay (1968)	J3 ou H-J-McK	$2^7.3^5.5.17.19 = 50.232.960$
Conway (1968)	Conway (1968)	$\cdot 1$ ou Co_1	$2^{21}.3^9.5^4.7^2.11.13.23 = 4.157.771.806.543.360.000$
Conway (1968)	Conway (1968)	$\cdot 2$ ou Co_2	$2^{18}.3^6.5^3.7.11.23 = 42.305.421.312.000$
Conway (1968)	Conway (1968)	$\cdot 3$ ou Co_3	$2^{10}.3^7.5^3.7.11.23 = 495.766.656.000$
Held (1968)	G. Higman, McKay (1968)	He ou H-H-McK	$2^{10}.3^3.5^2.7^3.17 = 4.030.387.200$
Fischer (1969)	Fischer (1969)	Fi_{22} ou M(22)	$2^{17}.3^9.5^2.7.11.13 = 64.561.751.654.400$
Fischer (1969)	Fischer (1969)	Fi_{23} ou M(23)	$2^{18}.3^{13}.5^2.7.11.13.17.23 = 4.089.470.473.293.004.800$
Fischer (1969)	Fischer (1969)	Fi_{24} ou M(24)	$2^{21}.3^{16}.5^2.7^3.11.13.17.23.29 = 1.225.205.709.190.661.721.292.800$
Lyons (1970)	Sims (1970)	Ly ou Ly-S	$2^8.3^7.5^6.7.11.31.37.67 = 51.765.179.004.000.000$
Rudvalis (1972)	Conway, Wales (1972)	Rv ou R-C-W	$2^{14}.3^3.5^3.7.13.29 = 145.926.144.000$
O'Nan (1972)	Sims (1973)	O'N ou O'N-S	$2^9.3^4.5.7^3.11.19.31 = 460.815.505.920$
Thompson (1973)	Smith (1974)	T	$2^{15}.3^{10}.5^3.7^2.13.19.31 = 90.745.943.887.872.000$
Harada, Norton (1974)	Conway, Smith (1974)	H-N ou Ha-C-N-S	$2^{14}.3^6.5^6.7.11.19 = 273.030.912.000.000$
Fischer (1973)	Leon, Sims (1976)	B ou F ou F-L-S	$2^{41}.3^{13}.5^6.7^2.11.13.17.19.23.31.47 \approx 4{,}15 \times 10^{34}$
Fischer, Griess (1972)	Griess (1980)	M ou F1	$2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71 \approx 8{,}08 \times 10^{53}$
Janko (1973)	Norton, Parker, Benson, Conway, Thackray (1980)	J4	$2^{21}.3^3.5.7.11^3.23.29.31.37.43 = 86.775.571.046.077.562.880$

$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$ interviennent dans M_{24}

$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$, J2, Sz, H-S, McL, Co_3, Co_2 et Co_1 interviennent dans Co_1

$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$, J2, Sz, H-S, McL, Co_3, Co_2, Co_1, He, Fi_{22}, Fi_{23} et Fi_{24} interviennent dans Fi_{24}

$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$, J2, Sz, H-S, McL, Co_3, Co_2, Co_1, He, Fi_{22}, Fi_{23}, Fi_{24}, H-N, T, B et M interviennent dans le monstre M.

L'ordre adopté correspond à la chronologie de la confirmation.