Histoire d'une classification : une guerre de 30 ans, un Monstre et des connexions inexpliquées

Théo JAMIN

Laboratoire angevin de recherche en mathématiques – Université d'Angers

February 14, 2022

Sommaire

Section 1

Définitions et intérêt des groupes simples.

Groupes simples

Sous-groupes normaux

Soit G un groupe et N un sous-groupe de G. On dit que N est un sous-groupe *normal* de G, et l'on note $N \lhd G$, s'il est stable par conjugaison, i.e.

$$N \lhd G \Leftrightarrow \forall n \in N,\ \forall g \in G,\ \iota_g(n) = gng^{-1} \in N$$

Groupes simples

Sous-groupes normaux

Soit G un groupe et N un sous-groupe de G. On dit que N est un sous-groupe *normal* de G, et l'on note $N \lhd G$, s'il est stable par conjugaison, i.e.

$$N \lhd G \Leftrightarrow \forall n \in N, \forall g \in G, \iota_g(n) = gng^{-1} \in N$$

Groupes simples

Un groupe G est dit simple si les seuls sous-groupes normaux de G sont $\{e\}$ et lui même.

Intérêt des groupes simples

"Les groupes simples sont aux groupes ce que les nombres premiers sont aux entiers".

Intérêt des groupes simples

"Les groupes simples sont aux groupes ce que les nombres premiers sont aux entiers".

Si G n'est pas un simple, alors l'existence d'un groupe normal N permet de construire le quotient G/N et l'étude de G peut se ramener à l'étude de N et celle de G/N. En itérant ce procédé, on peut "décomposer" l'étude d'un groupe à ses sous-groupes normaux qui sont des groupes simples.

Plus formellement

Suites de composition

Soit G un groupe. On appelle suite de composition de G une suite $(H_0, \cdots, H_n)$ telle que

$$e = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$$

et telle que H_{i+1}/H_i soit simple (ou de façon équivalente, H_i est un sous-groupe normal maximal de H_{i+1}).

Plus formellement

Théorème de Jordan-Hölder

Soit G un groupe et soient

$$e = I_0 \lhd I_1 \lhd \cdots \lhd I_n = G$$

$$e = J_0 \lhd J_1 \lhd \cdots \lhd J_m = G$$

deux suites de compositions de G. Alors $m = n$ et

$$\{I_1/I_0, \cdots, I_n/I_{n-1}\} = \{J_1/J_0, \cdots, J_m/J_{m-1}\}$$

à permutation et isomorphismes près.

Plus formellement

Théorème de Jordan-Hölder

Soit G un groupe et soient

$$e = I_0 \lhd I_1 \lhd \cdots \lhd I_n = G$$

$$e = J_0 \lhd J_1 \lhd \cdots \lhd J_m = G$$

deux suites de compositions de G. Alors $m = n$ et

$$\{I_1/I_0, \cdots, I_n/I_{n-1}\} = \{J_1/J_0, \cdots, J_m/J_{m-1}\}$$

à permutation et isomorphismes près.

On appellera $\mathrm{JH}(G)$ l'ensemble des groupes quotients successifs d'une suite de composition de G, à permutation et à isomorphismes près.

Là où s'arrête la comparaison

On aurait envie de reconstruire, comme pour les nombres premiers, un groupe à partir d'une suite de composition. Mais ce n'est pas toujours possible :

Là où s'arrête la comparaison

On aurait envie de reconstruire, comme pour les nombres premiers, un groupe à partir d'une suite de composition. Mais ce n'est pas toujours possible :

C_6 et D_6

Considérons d'une part le groupe cyclique C_6. On a alors deux suites de compositions

$$1 \lhd C_2 \lhd C_6 \qquad\qquad 1 \lhd C_3 \lhd C_6$$

dont on récupère $\mathrm{JH}(G) = \{C_2, C_3\}$ comme ensemble des quotients successifs.

Là où s'arrête la comparaison

On aurait envie de reconstruire, comme pour les nombres premiers, un groupe à partir d'une suite de composition. Mais ce n'est pas toujours possible :

C_6 et D_6

Considérons d'une part le groupe cyclique C_6. On a alors deux suites de compositions

$$1 \lhd C_2 \lhd C_6 \qquad\qquad 1 \lhd C_3 \lhd C_6$$

dont on récupère $\mathrm{JH}(G) = \{C_2, C_3\}$ comme ensemble des quotients successifs.
D'autre part, on peut vérifier que $\mathrm{JH}(D_6) = \mathrm{JH}(C_6)$.

Là où s'arrête la comparaison (pour aller plus loin)

Extension de groupe

Soient N et Q deux groupes. Une extension de Q par N est une suite exacte

$$1 \to N \xrightarrow{\iota} G \to Q \to 1$$

telle que $\iota(N)$ soit un sous-groupe normal de G et $Q \simeq G/\iota(N)$.

Là où s'arrête la comparaison (pour aller plus loin)

Extension de groupe

Soient N et Q deux groupes. Une extension de Q par N est une suite exacte

$$1 \to N \xrightarrow{\iota} G \to Q \to 1$$

telle que $\iota(N)$ soit un sous-groupe normal de G et $Q \simeq G/\iota(N)$.

Soient I et J deux groupes simples.
Trouver un groupe G dont $\mathrm{JH}(G) = \{I, J\}$, revient à trouver une extension de J par I.

Là où s'arrête la comparaison (pour aller plus loin)

Isomorphisme d'extension

Soient N et Q deux groupes. On dit que deux extensions

$$1 \to N \xrightarrow{\iota} G \to Q \to 1 \qquad\qquad 1 \to N \xrightarrow{\iota'} G' \to Q \to 1$$

sont isomorphes s'il existe $T : G \to G'$ tel que

$$\begin{tikzcd}
 & & G \arrow[dd, "T"] \arrow[dr] & & \\
1 \arrow[r] & N \arrow[ur] \arrow[dr] & & Q \arrow[r] & 1 \\
 & & G' \arrow[ur] & &
\end{tikzcd}$$

commute.

Là où s'arrête la comparaison (pour aller plus loin)

Soient I et J deux groupes simples. Lorsque l'on cherche G tel que $\mathrm{JH}(G) = \{I, J\}$, on le cherche à isomorphisme près.

Là où s'arrête la comparaison (pour aller plus loin)

Soient I et J deux groupes simples. Lorsque l'on cherche G tel que $\mathrm{JH}(G) = \{I, J\}$, on le cherche à isomorphisme près.
Pour ceux qui ont dans leur boîte à outil la cohomologie des groupes, on a le théorème suivant :

Théorème

Soient N et Q deux groupes.
Les classes d'équivalence d'extensions de Q par N sont en bijection avec $H^2(Q, N)$.

Là où s'arrête la comparaison (pour aller plus loin)

Soient I et J deux groupes simples. Lorsque l'on cherche G tel que $\mathrm{JH}(G) = \{I, J\}$, on le cherche à isomorphisme près.
Pour ceux qui ont dans leur boîte à outil la cohomologie des groupes, on a le théorème suivant :

Théorème

Soient N et Q deux groupes.
Les classes d'équivalence d'extensions de Q par N sont en bijection avec $H^2(Q, N)$.

En général, $H^2(Q, N)$ n'est pas nul et il existe donc plusieurs extensions.

Résumé de l'intérêt

Soient Q et N des groupes finis simples et G un groupe fini.

Résumé de l'intérêt

Soient Q et N des groupes finis simples et G un groupe fini.

+ A partir de G, on a une "décomposition" en groupes simples, unique à permutation et isomorphismes près, via $\mathrm{JH}(G)$.

Résumé de l'intérêt

Soient Q et N des groupes finis simples et G un groupe fini.

+ A partir de G, on a une "décomposition" en groupes simples, unique à permutation et isomorphismes près, via $\mathrm{JH}(G)$.
– Étant donné une décomposition, il est possible de trouver $G' \not\simeq G$ tel que $\mathrm{JH}(G) = \mathrm{JH}(G')$.

Résumé de l'intérêt

Soient Q et N des groupes finis simples et G un groupe fini.

+ A partir de G, on a une "décomposition" en groupes simples, unique à permutation et isomorphismes près, via $\mathrm{JH}(G)$.
– Étant donné une décomposition, il est possible de trouver $G' \not\simeq G$ tel que $\mathrm{JH}(G) = \mathrm{JH}(G')$.
+ Via l'étude de la cohomologie, on peut retrouver toutes les extensions et par conséquent tout les G' tels que $\mathrm{JH}(G) = \mathrm{FH}(G')$.

Résumé de l'intérêt

Soient Q et N des groupes finis simples et G un groupe fini.

+ A partir de G, on a une "décomposition" en groupes simples, unique à permutation et isomorphismes près, via $\mathrm{JH}(G)$.
– Étant donné une décomposition, il est possible de trouver $G' \not\simeq G$ tel que $\mathrm{JH}(G) = \mathrm{JH}(G')$.
+ Via l'étude de la cohomologie, on peut retrouver toutes les extensions et par conséquent tout les G' tels que $\mathrm{JH}(G) = \mathrm{FH}(G')$.

On en arrive aux questions :

- Donner une classification des groupes finis simples.
- Donner toutes les extensions de Q par N.

Section 2

Quelques définitions le théorème de classification.

Préliminaires à la classification - Groupes A_n

Rappel : une permutation $\sigma \in S_n$ se décompose en produit de transpositions et la signature de σ est $\epsilon(\sigma) = (-1)^N$, où N est le nombre de transpositions dans cette décomposition.

Préliminaires à la classification - Groupes A_n

Rappel : une permutation $\sigma \in S_n$ se décompose en produit de transpositions et la signature de σ est $\epsilon(\sigma) = (-1)^N$, où N est le nombre de transpositions dans cette décomposition.

Groupes alternés

Le groupe *alterné* A_n est le sous-groupe de S_n obtenu par les permutations dont la signature est 1.

Préliminaires à la classification - Groupes A_n

Rappel : une permutation $\sigma \in S_n$ se décompose en produit de transpositions et la signature de σ est $\epsilon(\sigma) = (-1)^N$, où N est le nombre de transpositions dans cette décomposition.

Groupes alternés

Le groupe *alterné* A_n est le sous-groupe de S_n obtenu par les permutations dont la signature est 1.

Proposition

Le groupe A_n est simple pour $n \geqslant 5$.

Préliminaires à la classification - Groupes de type Lie

C'est la classe la plus large intervenant dans la classification.

Groupes de type Lie

Un groupe fini G est dit *de type Lie* s'il est définit comme l'ensemble des $\mathbb{F}_p$-points d'un groupe algébrique réductif et connexe G fixés par un endomorphisme de Steinberg, ou comme sous-groupe normal d'un tel groupe ou encore comme quotient d'un tel groupe par un sous-groupe central.

Préliminaires à la classification - Groupes de type Lie

C'est la classe la plus large intervenant dans la classification.

Groupes de type Lie

Un groupe fini G est dit *de type Lie* s'il est définit comme l'ensemble des $\mathbb{F}_p$-points d'un groupe algébrique réductif et connexe G fixés par un endomorphisme de Steinberg, ou comme sous-groupe normal d'un tel groupe ou encore comme quotient d'un tel groupe par un sous-groupe central.

Pas si simple...

Préliminaires à la classification - Groupes de type Lie

Avantage de cette définition :

Théorème de Chevalley

Les groupes réductifs (sur un quelconque corps algébriquement clos) sont classifiés, à isomorphismes près, par leur *système de racines*.

Préliminaires à la classification - Groupes de type Lie

Avantage de cette définition :

Théorème de Chevalley

Les groupes réductifs (sur un quelconque corps algébriquement clos) sont classifiés, à isomorphismes près, par leur *système de racines*.

En pratique :
Il n'existe une multitude de caractérisation de ces groupes, comme l'existence d'une (B, N)-structure, les points rationnels d'un groupe de Lie etc.

Préliminaires à la classification - Groupes de type Lie

On peut construire un groupe de type Lie en prenant un groupe de Lie sur $\mathbb{F}_p$.

Préliminaires à la classification - Groupes de type Lie

On peut construire un groupe de type Lie en prenant un groupe de Lie sur $\mathbb{F}_p$.

Exemples

- $\mathrm{GL}(n, p)$ le groupe des matrices de taille n de déterminant non nul sur $\mathbb{F}_p$.

Préliminaires à la classification - Groupes de type Lie

On peut construire un groupe de type Lie en prenant un groupe de Lie sur $\mathbb{F}_p$.

Exemples

- $\mathrm{GL}(n, p)$ le groupe des matrices de taille n de déterminant non nul sur $\mathbb{F}_p$.
- $\mathrm{SL}(n, p)$ le groupe des matrices de taille n de déterminant 1 sur $\mathbb{F}_p$.

Préliminaires à la classification - Groupes de type Lie

On peut construire un groupe de type Lie en prenant un groupe de Lie sur $\mathbb{F}_p$.

Exemples

- $\mathrm{GL}(n,p)$ le groupe des matrices de taille n de déterminant non nul sur $\mathbb{F}_p$.
- $\mathrm{SL}(n,p)$ le groupe des matrices de taille n de déterminant 1 sur $\mathbb{F}_p$.

La classification

Classification des groupes finis simples

Un groupe fini simple appartient à l'une (au moins) des familles suivantes :

La classification

Classification des groupes finis simples

Un groupe fini simple appartient à l'une (au moins) des familles suivantes :

- Les groupes cycliques C_p, avec p premier,

La classification

Classification des groupes finis simples

Un groupe fini simple appartient à l'une (au moins) des familles suivantes :

- Les groupes cycliques C_p, avec p premier,
- Les groupes alternés A_n, avec $n \geqslant 5$,

La classification

Classification des groupes finis simples

Un groupe fini simple appartient à l'une (au moins) des familles suivantes :

- Les groupes cycliques C_p, avec p premier,
- Les groupes alternés A_n, avec $n \geqslant 5$,
- Les groupes finis de type Lie,

La classification

Classification des groupes finis simples

Un groupe fini simple appartient à l'une (au moins) des familles suivantes :

- Les groupes cycliques C_p, avec p premier,
- Les groupes alternés A_n, avec $n \geqslant 5$,
- Les groupes finis de type Lie,
- Les 26 groupes sporadiques.

La classification

Classification des groupes finis simples

Un groupe fini simple appartient à l'une (au moins) des familles suivantes :

- Les groupes cycliques C_p, avec p premier,
- Les groupes alternés A_n, avec $n \geqslant 5$,
- Les groupes finis de type Lie,
- Les 26 groupes sporadiques.

Pourquoi 26 ? Et bien, il faut lire la preuve...

Section 3

La guerre de 30 ans

Théorème précurseur

En 1963, W. Feit et J. Thompson démontrent ce qu'avait conjecturé W. Burnside 50 ans plus tôt à savoir le *théorème de l'ordre impaire* :

Théorème de Feit-Thompson

Si G est un groupe fini, simple et d'ordre impair alors il est cyclique.

Théorème précurseur

En 1963, W. Feit et J. Thompson démontrent ce qu'avait conjecturé W. Burnside 50 ans plus tôt à savoir le *théorème de l'ordre impaire* :

Théorème de Feit-Thompson

Si G est un groupe fini, simple et d'ordre impair alors il est cyclique.

Même si ce théorème ne résout pas le problème de classification des groupes finis simples, les techniques utilisées dans la preuve joueront un rôle essentiel dans la suite de l'histoire.

Une nouvelle technique : Centralisateur d'involution

Soit G un groupe fini et simple.

Définitions

- Un élément t est appelé *involution* si $t^2 = e$,
- on appelle *centralisateur* de $g \in G$ le groupe $C_G(g)$ formé des éléments qui commute à g.

Une nouvelle technique : Centralisateur d'involution

Soit G un groupe fini et simple.

Définitions

- Un élément t est appelé *involution* si $t^2 = e$,
- on appelle *centralisateur* de $g \in G$ le groupe $C_G(g)$ formé des éléments qui commute à g.

Théorème de Brauer-Fowler

Soit t une involution d'un groupe G fini et simple. Alors,

$$|C_G(t)| = n \implies |G| \leqslant (2n^2)!$$

Une nouvelle technique : Centralisateur d'involution

Soit G un groupe fini et simple.

Définitions

- Un élément t est appelé *involution* si $t^2 = e$,
- on appelle *centralisateur* de $g \in G$ le groupe $C_G(g)$ formé des éléments qui commute à g.

Théorème de Brauer-Fowler

Soit t une involution d'un groupe G fini et simple. Alors,

$$|C_G(t)| = n \implies |G| \leqslant (2n^2)!$$

En particulier, si on fixe un groupe C, il n'existe qu'un nombre fini de groupes finis et simples qui ont C comme centralisateur d'involution.

Histoire de la preuve

Un corollaire immédiat du théorème de l'ordre impaire est qu'un groupe simple non cyclique contient toujours une involution.

Histoire de la preuve

Un corollaire immédiat du théorème de l'ordre impaire est qu'un groupe simple non cyclique contient toujours une involution.

En 1972, Gorenstein propose un programme pour décomposer la preuve en 16 étapes. L'idée de la preuve est sommairement la suivante :

Histoire de la preuve

Un corollaire immédiat du théorème de l'ordre impaire est qu'un groupe simple non cyclique contient toujours une involution.

En 1972, Gorenstein propose un programme pour décomposer la preuve en 16 étapes. L'idée de la preuve est sommairement la suivante :

- Étape 1 : Déterminer toutes les structures possibles des centralisateurs d'involution dans un groupe simple.

Histoire de la preuve

Un corollaire immédiat du théorème de l'ordre impaire est qu'un groupe simple non cyclique contient toujours une involution.

En 1972, Gorenstein propose un programme pour décomposer la preuve en 16 étapes. L'idée de la preuve est sommairement la suivante :

- Étape 1 : Déterminer toutes les structures possibles des centralisateurs d'involution dans un groupe simple.
- Étape 2 : Pour chaque structure possible, déterminer tous les groupes simples admettant de tels centralisateurs d'involution.

Histoire de la preuve

Un corollaire immédiat du théorème de l'ordre impaire est qu'un groupe simple non cyclique contient toujours une involution.

En 1972, Gorenstein propose un programme pour décomposer la preuve en 16 étapes. L'idée de la preuve est sommairement la suivante :

- Étape 1 : Déterminer toutes les structures possibles des centralisateurs d'involution dans un groupe simple.
- Étape 2 : Pour chaque structure possible, déterminer tous les groupes simples admettant de tels centralisateurs d'involution.

Histoire de la preuve

A l'annonce du programme, aucun mathématicien ne pensais que la classification ne sera faite dans le siècle suivant.

Histoire de la preuve

A l'annonce du programme, aucun mathématicien ne pensais que la classification ne sera faite dans le siècle suivant.
L'espoir naitra lorsque Michael Aschbacher acheva la B-conjecture, le problème du groupe fin, ou encore le "Strongly p-embedded 2-local problem"...

Histoire de la preuve

A l'annonce du programme, aucun mathématicien ne pensais que la classification ne sera faite dans le siècle suivant. L'espoir naitra lorsque Michael Aschbacher acheva la B-conjecture, le problème du groupe fin, ou encore le "Strongly p-embedded 2-local problem"...

En 1983, Gorenstein annonce la fin de la classification avec une première "publication" de la preuve longue de 15000 pages.

Histoire de la preuve

A l'annonce du programme, aucun mathématicien ne pensais que la classification ne sera faite dans le siècle suivant. L'espoir naitra lorsque Michael Aschbacher acheva la B-conjecture, le problème du groupe fin, ou encore le "Strongly p-embedded 2-local problem"...

En 1983, Gorenstein annonce la fin de la classification avec une première "publication" de la preuve longue de 15000 pages.

Annonce prématurée puisqu'il faudra attendre 2004 pour Aschbacher et Smith pour réparer une erreur sur les groupes quasi-fins.

Histoire de la preuve

A l'annonce du programme, aucun mathématicien ne pensais que la classification ne sera faite dans le siècle suivant. L'espoir naitra lorsque Michael Aschbacher acheva la B-conjecture, le problème du groupe fin, ou encore le "Strongly p-embedded 2-local problem"...

En 1983, Gorenstein annonce la fin de la classification avec une première "publication" de la preuve longue de 15000 pages.

Annonce prématurée puisqu'il faudra attendre 2004 pour Aschbacher et Smith pour réparer une erreur sur les groupes quasi-fins.

Et finalement, en 2008 un autre (et dernier ?) gap sera comblé par deux autres mathématiciens.

Auteurs

En 2019, une preuve de seconde génération à été publiée en 8 volumes, beaucoup moins longue que la première (environ 1200 pages).

Auteurs

En 2019, une preuve de seconde génération à été publiée en 8 volumes, beaucoup moins longue que la première (environ 1200 pages).

Parmis les auteurs de la preuve, on peux citer :

Jordan, Sylow, Hölder, Cole, Frobenius, Burnside, Dickson, Brauer, Zassenhaus, Chevalley, Thompson, Feit, Gorenstein, Janko, Conway, Fischer, Aschbacher, Griess...

Section 4

Groupes sporadiques.

Les groupes de Mathieu

Avant 1900, E. Mathieu s'intéresse aux groupes k-transitifs :

Les groupes de Mathieu

Avant 1900, E. Mathieu s'intéresse aux groupes k-transitifs :

k-transitivité

Un groupe G est dit k-transitif si pour toute paire de k-uplet $(a_1, \cdots, a_k)$, $(b_1, \cdots, b_k)$ d'éléments distincts deux à deux, il existe un élément $g \in G$ tel $g.a_i = b_i$.

Les groupes de Mathieu

Avant 1900, E. Mathieu s'intéresse aux groupes k-transitifs :

k-transitivité

Un groupe G est dit k-transitif si pour toute paire de k-uplet $(a_1, \cdots, a_k)$, $(b_1, \cdots, b_k)$ d'éléments distincts deux à deux, il existe un élément $g \in G$ tel $g.a_i = b_i$.

Il s'intéressa alors à des sous-groupes k-transitif de groupes de permutations et trouva cinq groupes $M_n \subset S_n$, pour $n = 11, 12, 22, 23$ ou 24 et sont donc les 5 premiers groupes sporadiques decouverts.

p-Sylow sous-groupes

Définition

Soit G un groupe fini. Un sous groupe H de G est un p-sous-groupe de Sylow si son ordre est la plus grande puissance de p divisant l'ordre de G.

p-Sylow sous-groupes

Définition

Soit G un groupe fini. Un sous groupe H de G est un p-sous-groupe de Sylow si son ordre est la plus grande puissance de p divisant l'ordre de G.

Intérêts :

- Théorème de Sylow : Pout tout premier p de multiplicité n dans la décomposition de l'ordre de G, il existe un p-sous-groupe de Sylow.
- Théorème de Burnside : si G est un groupe simple contenant un p-sous groupe de Sylow cyclique alors $|G| = p$.
- etc.

Groupe de Janko

Il existe bon nombre de propositions qui rigidifie la structure d'un groupe étant donné un centralisateur d'involution. En particulier, à partir des travaux de ses prédécesseurs sur les groupes de Ree, Janko, voulait montrer le résultat suivant

Groupe de Janko

Il existe bon nombre de propositions qui rigidifie la structure d'un groupe étant donné un centralisateur d'involution. En particulier, à partir des travaux de ses prédécesseurs sur les groupes de Ree, Janko, voulait montrer le résultat suivant

~~Théorème~~

Soit G un groupe fini tel que

- Les sous-groupes 2-Sylow de G sont abélien,
- G n'a pas de sous-groupe d'indice 2,
- G contient une involution t tel que $C_G(t)$ soit isomorphe à $C_2 \times PSL(2, q)$, avec $q > 3$ une puissance d'un nombre premier.

Alors G est simple, $q = 3^{2n+1}$, $n \geqslant 1$.

Groupe de Janko

Il existe bon nombre de propositions qui rigidifie la structure d'un groupe étant donné un centralisateur d'involution. En particulier, à partir des travaux de ses prédécesseurs sur les groupes de Ree, Janko, voulait montrer le résultat suivant

~~Théorème~~

Soit G un groupe fini tel que

- Les sous-groupes 2-Sylow de G sont abélien,
- G n'a pas de sous-groupe d'indice 2,
- G contient une involution t tel que $C_G(t)$ soit isomorphe à $C_2 \times PSL(2, q)$, avec $q > 3$ une puissance d'un nombre premier.

Alors G est simple, $q = 3^{2n+1}$, $n \geqslant 1$.

Il réussit à le démontrer en supposant $q > 5$.

Groupe de Janko

Mais, il ne parvint pas à le montrer pour $q = 5$.

Groupe de Janko

Mais, il ne parvint pas à le montrer pour $q = 5$.Il chercha des exemples de groupes vérifiant ce ~~théorème~~ pour $q = 5$ et prouver l'existence de

J1

Si G est un groupe simple avec un centralisateur d'involution isomorphe à $C_2 \times A_5$ et G contient un 2-Sylow sous-groupe abélien d'ordre 8 alors G est d'ordre 175560. De plus s'il existe il est unique, à isomorphisme près.

Groupe de Janko

Mais, il ne parvint pas à le montrer pour $q = 5$.Il chercha des exemples de groupes vérifiant ce ~~théorème~~ pour $q = 5$ et prouver l'existence de

J1

Si G est un groupe simple avec un centralisateur d'involution isomorphe à $C_2 \times A_5$ et G contient un 2-Sylow sous-groupe abélien d'ordre 8 alors G est d'ordre 175560. De plus s'il existe il est unique, à isomorphisme près.

Sur des constructions similaires, il aboutit à l'existence d'autres groupes, sans pouvoir en trouver la preuve expérimentale. D'autres mathématiciens finiront, plus tard, par exhiber des générateurs de ces groupes nommés J_2, J_3 et J_4.

Représentations

Quelques mois après ce travail il réussit à exhiber une représentation fidèle de $J1$.

Représentations

Quelques mois après ce travail il réussit à exhiber une représentation fidèle de $J1$.

Représentation

Soit V un $\mathbb{C}$-espace vectoriel et G un groupe. Une *représentation* de G est la donnée d'un morphisme de G dans $GL(V)$.

Représentations

Quelques mois après ce travail il réussit à exhiber une représentation fidèle de $J1$.

Représentation

Soit V un $\mathbb{C}$-espace vectoriel et G un groupe. Une *représentation* de G est la donnée d'un morphisme de G dans $GL(V)$.
On dit qu'une représentation ρ est irréductible s'il n'existe pas de sous-espace $W \subset V$ tel que $\rho|_W$ soit une représentation de G.

Représentations

Quelques mois après ce travail il réussit à exhiber une représentation fidèle de $J1$.

Représentation

Soit V un $\mathbb{C}$-espace vectoriel et G un groupe. Une *représentation* de G est la donnée d'un morphisme de G dans $GL(V)$.

On dit qu'une représentation ρ est irréductible s'il n'existe pas de sous-espace $W \subset V$ tel que $\rho|_W$ soit une représentation de G.

Une représentation est fidèle si son noyau est réduit à $\{e\}$.

Proposition

Les représentations irréductibles de G sont en bijection avec les classes de conjugaison de G.

Conway et le réseau de Leech

En travaillant sur la transmission de messages codés, J. Leech construit le réseau Λ_{24} (groupe libre abélien, de rang fini, dans $\mathbb{R}^{24}$), qui porte son nom

Conway et le réseau de Leech

En travaillant sur la transmission de messages codés, J. Leech construit le réseau Λ_{24} (groupe libre abélien, de rang fini, dans $\mathbb{R}^{24}$), qui porte son nom

Réseau de Leech

Il existe un unique réseau, noté Λ_{24} vérifiant :

- Λ_{24} est engendré par les colonnes d'une matrice de determinant 1,
- Le carré de la longueur de tout vecteur de Λ_{24} est un entier pair,
- La longueur de tout vecteur (non nul) de Λ_{24} est au moins 2.

Conway et le réseau de Leech

En travaillant sur la transmission de messages codés, J. Leech construit le réseau Λ_{24} (groupe libre abélien, de rang fini, dans $\mathbb{R}^{24}$), qui porte son nom

Réseau de Leech

Il existe un unique réseau, noté Λ_{24} vérifiant :

- Λ_{24} est engendré par les colonnes d'une matrice de determinant 1,
- Le carré de la longueur de tout vecteur de Λ_{24} est un entier pair,
- La longueur de tout vecteur (non nul) de Λ_{24} est au moins 2.

Un an plus tard, J. Conway s'intéressa au groupe d'automorphismes de ce réseau et trouva les groupes Co_1, Co_2 et Co_3 qui sont simples et sporadiques.

Section 5

La capture du Monstre.

Conjecture de Griess

Indépendamment, Griess et Fischer conjecturent l'existence d'un groupe sporadique plus gros que ceux trouvés jusque là. Un groupe d'ordre :

$$2^{46}.3^{20}.5^{9}.7^{6}.11^{2}.13^{3}.17.19.23.29.31.41.47.59.71 \simeq 8.10^{54}.$$

Conjecture de Griess

Indépendamment, Griess et Fischer conjecturent l'existence d'un groupe sporadique plus gros que ceux trouvés jusque là. Un groupe d'ordre :

$$2^{46}.3^{20}.5^{9}.7^{6}.11^{2}.13^{3}.17.19.23.29.31.41.47.59.71 \simeq 8.10^{54}.$$

Et réussirent à construire ce groupe comme groupe d'automorphisme d'une algèbre de dimension 196884 et un dernier résultat de Norton a permis de prouver l'unicité de ce groupe et avec ça, conclure la classification.

Conjecture de Griess

Indépendamment, Griess et Fischer conjecturent l'existence d'un groupe sporadique plus gros que ceux trouvés jusque là.
Un groupe d'ordre :

$$2^{46}.3^{20}.5^{9}.7^{6}.11^{2}.13^{3}.17.19.23.29.31.41.47.59.71 \simeq 8.10^{54}.$$

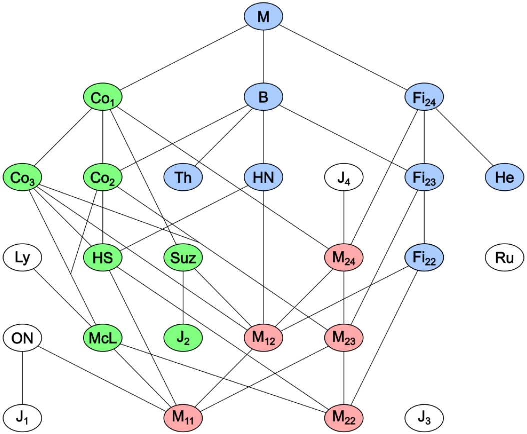
Et réussirent à construire ce groupe comme groupe d'automorphisme d'une algèbre de dimension 196884 et un dernier résultat de Norton a permis de prouver l'unicité de ce groupe et avec ça, conclure la classification.
Ils appellent ce groupe, le groupe Monstre M.

Le groupe Monstre : le père de la Happy Familly

Presque tous les groupes sporadiques dérivent du groupe Monstre comme sous-groupe ou sous-groupe de quotient.

Le groupe Monstre : le père de la Happy Familly

Presque tous les groupes sporadiques dérivent du groupe Monstre comme sous-groupe ou sous-groupe de quotient. Voici la diagramme des connexions entre eux :



Section 6

Des connexions étranges.

1 - Groupes fondamentaux de surfaces hyperboliques

J-P. Serre, Thompson et Ogg étuidèrent les surfaces hyperboliques et en particulier leur groupes fondamentaux (qui peuvent être vu dans $Isom^+(\mathbb{H}^2) \simeq PSL_2(\mathbb{R})$ et relevés à $SL_2(\mathbb{R})$). Une classe de ce genre de groupes est les groupes de congruences, par exemple :

1 - Groupes fondamentaux de surfaces hyperboliques

J-P. Serre, Thompson et Ogg étuidèrent les surfaces hyperboliques et en particulier leur groupes fondamentaux (qui peuvent être vu dans $Isom^{+}(\mathbb{H}^2) \simeq PSL_2(\mathbb{R})$ et relevés à $SL_2(\mathbb{R})$). Une classe de ce genre de groupes est les groupes de congruences, par exemple :

Groupes de Hecke

Le n-ième groupe de congruence de Hecke est définit par

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, c \equiv 0[n] \right\} \subset SL_2(\mathbb{Z})$$

1 - Groupes fondamentaux de surfaces hyperboliques

Surface de genre 0 et groupe de Hecke

Soit S une surface hyperbolique dont le groupe fondamental est isomorphe au normalisateur d'un groupe de Hecke. Alors, S est de genre 0 si, et seulement si, n est un nombre premier intervenant dans la décomposition de l'ordre du groupe Monstre.

1 - Groupes fondamentaux de surfaces hyperboliques

Surface de genre 0 et groupe de Hecke

Soit S une surface hyperbolique dont le groupe fondamental est isomorphe au normalisateur d'un groupe de Hecke. Alors, S est de genre 0 si, et seulement si, n est un nombre premier intervenant dans la décomposition de l'ordre du groupe Monstre.

La connexion avec le groupe Monstre n'est pas du tout faite dans la preuve.

1 - Groupes fondamentaux de surfaces hyperboliques

Surface de genre 0 et groupe de Hecke

Soit S une surface hyperbolique dont le groupe fondamental est isomorphe au normalisateur d'un groupe de Hecke. Alors, S est de genre 0 si, et seulement si, n est un nombre premier intervenant dans la décomposition de l'ordre du groupe Monstre.

La connexion avec le groupe Monstre n'est pas du tout faite dans la preuve.
D'ailleurs, pour ceux qui aiment le whisky, Andrew Ogg offre une bouteille de Jack Daniel's à quiconque lui donnant ce lien.

2 - Transformée de Fourier de fonction J - Monstruous Moonshine

Soit $\tau \in \mathbb{C}$, $\operatorname{Im}(\tau) > 0$, i.e. $\tau \in \mathbb{H}$. On peut construire un réseau $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ dans $\mathbb{C}$ et considérer le quotient $\mathbb{C}/\Lambda$. Ce quotient est un tore complexe noté T_τ.

2 - Transformée de Fourier de fonction J - Monstruous Moonshine

Soit $\tau \in \mathbb{C}$, $\mathrm{Im}(\tau) > 0$, i.e. $\tau \in \mathbb{H}$. On peut construire un réseau $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ dans $\mathbb{C}$ et considérer le quotient $\mathbb{C}/\Lambda$. Ce quotient est un tore complexe noté T_τ.On sait qu'il existe une fonction $j : \mathbb{H} \to \mathbb{C}$ qui détermine si deux tores sont biholomorphes : $j(\tau) = j(\tau')$ si, et seulement si, $T_\tau \simeq T_{\tau'}$.

2 - Transformée de Fourier de fonction J - Monstruous Moonshine

Soit $\tau \in \mathbb{C}$, $\mathrm{Im}(\tau) > 0$, i.e. $\tau \in \mathbb{H}$. On peut construire un réseau $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ dans $\mathbb{C}$ et considérer le quotient $\mathbb{C}/\Lambda$. Ce quotient est un tore complexe noté T_τ.On sait qu'il existe une fonction $j : \mathbb{H} \to \mathbb{C}$ qui détermine si deux tores sont biholomorphes : $j(\tau) = j(\tau')$ si, et seulement si, $T_\tau \simeq T_{\tau'}$. Conway calcula le développement de Fourier de cette fonction j

$$j(\tau) = \frac{1}{q} + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

où $q = e^{2i\pi\tau}$

2 - Transformée de Fourier de fonction J - Monstruous Moonshine

Conway et Norton ont conjecturé que les coefficients peuvent être exprimés en termes de combinaisons linéaires des dimensions des représentations irréductibles du groupe monstre M :

$$\begin{aligned}
1 &= r_1 \\
196884 &= r_1 + r_2 \\
21493760 &= r_1 + r_2 + r_3 \\
864299970 &= 2r_1 + 2r_2 + r_3 + r_4 \\
&\cdots
\end{aligned}$$

2 - Transformée de Fourier de fonction J - Monstruous Moonshine

Conway et Norton ont conjecturé que les coefficients peuvent être exprimés en termes de combinaisons linéaires des dimensions des représentations irréductibles du groupe monstre M :

$$\begin{aligned} 1 &= r_1 \\ 196884 &= r_1 + r_2 \\ 21493760 &= r_1 + r_2 + r_3 \\ 864299970 &= 2r_1 + 2r_2 + r_3 + r_4 \\ &\dots \end{aligned}$$

Ce sera Richard Ewen Borcherds qui le démontra en 1992 et reçu la médaille Fields en partie pour ce travail.

Merci de votre attention !