GROUPES D'ORDRE IMPAIR

MICHAEL ATIYAH

Pour Alain Connes et l'Université de Fudan[1]

Résumé. Le théorème de Feit-Thompson qu'un groupe d'ordre impair est résoluble a toujours été un défi pour ceux qui croient que les beaux théorèmes devraient avoir de belles preuves.

1. Histoire et stratégie

La théorie des groupes et la théorie de Galois se sont développées ensemble il y a deux siècles lorsqu'on cherchait les conditions de résolubilité. C'est environ 150 ans plus tard que Feit et Thompson ont démontré leur théorème célèbre [1].

Théorème 1. *(Feit-Thompson) Tous les groupes d'ordre impair sont résolubles.*

Cela a été, à cette époque, le point de départ d'un effort collectif colossal par des théoriciens des groupes pour trouver tous les groupes simples finis. Pour un compte-rendu historique à ce sujet, voir [2].

Dans cette note, je présenterai une preuve du théorème 1 inspirée par les idées d'Emil Artin. En fin de compte, un groupe d'ordre impair est résoluble parce qu'un polynôme réel de degré impair a une racine réelle. Ce polynôme apparaîtra comme polynôme caractéristique d'une matrice sur un corps réel.

Je vais maintenant esquisser la stratégie de la preuve du théorème 1. Il s'agit de construire une grande famille de caractères complexes (homomorphes à $\mathbb{C}^*$) du groupe G (d'ordre impair N) et de montrer alors qu'ils ne peuvent pas être tous triviaux. Ceci, énoncé en section 4 comme théorème 2, amène facilement au théorème 1.

Ces caractères sont construits dans la section 5 à partir des déterminants des matrices représentatives qui proviennent de l'idée d'Artin de considérer l'action d'un groupe fini G sur tous ses sous-ensembles et alors d'utiliser les extensions d'algèbres de $\mathbb{Q}$. Les caractères complexes de G sont mieux compris à travers la ruse *unitaire* de Hermann Weyl, qui s'applique aux groupes de Lie compacts et en particulier aux

[1]En souvenir de la Conférence d'anniversaire pour les 70 ans d'Alain Connes et pour les Nominations comme Professeurs honoraires par l'Université Fudan de Shanghai, le 1er avril 2017. Date : 30 janvier 2018.

Traduction : Denise Vella-Chemla, septembre 2022.

groupes finis.

Nous utiliserons à la fois des nombres algébriques et des fonctions algébriques. Notons qu'une fonction algébrique définit une courbe algébrique qui en général est constituée de plusieurs courbes irréductibles. S'il n'y en a qu'une, les fonctions forment un corps. La théorie de Galois est traditionnellement définie seulement pour les corps. C'est une théorie beaucoup plus délicate que la théorie pour les algèbres. En particulier elle dépend grandement de l'arithmétique de l'entier N, le degré de la courbe. La preuve du théorème 1, par Feit et Thompson, fait intervenir ces considérations arithmétiques et la manière dont elles sont implémentées dans la structure du groupe G. Tout ceci est intimement relié à la théorie de Galois. Par contraste, notre approche, en se focalisant sur les algèbres et en ignorant les questions d'irréductibilité est plus grossière. C'est précisément parce qu'elle **ignore la théorie de Galois** qu'elle amène à une démonstration simple du théorème 1. Mais, par constraste avec la preuve de Feit-Thompson, elle n'amène aucune information à propos de la structure interne de G. Elle ne dit rien de la manière dont les sous-groupes de Sylow pour différents nombres premiers sont entremêlés. Notre preuve demande moins et donne moins. Mais elle donne une preuve courte et simple du théorème 1, répondant au défi énoncé dans le résumé, d'une **belle preuve d'un beau théorème**. Comme digression philosophique, laissez-moi donner une analogie. Si on vous demande, en tant que spectateur, si l'animal devant vous est un chameau ou un dromadaire, il y a deux manières de le savoir. La façon externe est de compter le nombre de bosses, facile. La façon interne est d'examiner l'ADN des deux animaux et de trouver la différence génétique. C'est trivialement beaucoup plus difficile, mais cela donne beaucoup plus d'information. Mais compter les bosses est suffisant pour répondre à la question. Feit et Thompson sont des généticiens, alors que je ne fais que compter les bosses.

En retournant maintenant à la stratégie de la preuve, on note que cela amène à notre première tranche de caractères et que cela permettra de détecter les groupes métabéliens.

2. Préliminaires algébriques

Un corps de nombres réels signifiera un corps de nombres algébriques k enchâssé dans les réels :

$$\mathbb{Q} \subset k \subset \mathbb{R}. \tag{2.1}$$

De façon similaire, un **corps de nombres complexes** signifiera un corps de nombres algébriques associé à un choix de plongement dans $\mathbb{C}$. Si on commence à partir d'une extension complexe de $\mathbb{Q}$, cela amènera à une complexification de (2.1). Le cas qui servira de cas de base à cet article est l'extension $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-3})$ dont les entiers sont appelés les entiers de Eisenstein E. C'est un domaine de factorisation unique et

les unités fondamentales sont (en excluant 1 et en faisant un choix de signes)

$$\rho = \frac{-1+\sqrt{-3}}{2} = \exp\frac{2\pi i}{3}, \quad \overline{\rho} = \frac{-1-\sqrt{-3}}{2} = \exp\frac{-2\pi i}{3}, \tag{2.2}$$

les solutions de l'équation

$$u^2 + u + 1 = 0. \tag{2.3}$$

Finalement, parlons des déterminants. Si V est un espace vectoriel de dimension N sur le corps des nombres réels k, le **déterminant** est un homomorphisme :

$$\det \ : \ \mathrm{Aut}(V) \to k^* \subset \mathbb{R}^* \tag{2.4}$$

De façon similaire, si V et l'automorphisme sont définis sur le corps des nombres complexes $k(\rho)$, det prend ses valeurs dans $k(\rho)^* \subset \mathbb{C}^*$.

Passons maintenant au recouvrement double de spins donné par le **changement de variable**

$$z = u^2 + u + 1. \tag{2.5}$$

Cela nous amène au corps de fonctions réelles $K := k(u)$ et à sa complexification $K(\rho) := k(\rho)(u)$, où u est une variable. De telles fonctions peuvent être évaluées aux points complexes (ou nombres) et donnent des nombres complexes dans le corps associé. Pour K, l'évaluation en ρ ou en $\sqrt{\rho} = -\rho^2$ fournit des valeurs dans $k(\rho)$.

Sur la surface de Riemann définie par (2.5), les fonctions peuvent être paires ou impaires selon l'involution

$$u \mapsto -u \tag{2.6}$$

et il y a (voir [10])

une structure de spin distinguée (2.7)

qui peut être paire ou impaire selon la valeur de

l'invariant de Arf d'une fonction quadratique. (2.8)

Comme module sur $k(z)$, K est de rang 2 et donc les endomorphismes de K peuvent être vus comme des matrices 2×2 sur $k(z)$: une algèbre non-commutative.

En termes de groupes d'éléments inversibles, on a que

$$\mathrm{End}(K)^* = k(u)^* \ltimes (\pm 1) \tag{2.9}$$

est un produit semi-direct avec l'involution $u \mapsto \overline{u}$ sur $k(u)^*$. Ainsi on voit $\mathrm{End}(K)^*$ comme un sous-groupe d'indice 2 dans les éléments unimodulaires de l'algèbre matricielle ; les deux choix correspondent à $\mathbb{C}^+$ et $\mathbb{C}^-$, les deux moitiés du plan complexe

moins la ligne réelle. Note : les géomètres peuvent reconnaître ici les deux classes des fibrés projectifs avec la fibre $P_1(\mathbb{C})$ déterminée par la parité de la première classe de Chern i.e. par la seconde classe de Stiefel-Whitney, dont l'évanouissement fournit le spin.

La distinction entre les fonctions paires et impaires, selon l'involution $u \mapsto -u$ s'étend aux vecteurs, aux matrices et aux valeurs propres.

3. Déterminants

Puisque K est une élévation de $k(z)$, toute matrice réelle $A \in GL(N, K)$ peut être vue comme une matrice dans $GL(2N, k(z))$, qui a comme valeurs propres les $2N$ variables conjuguées complexes :

$$(\lambda_1, \ldots, \lambda_N) \quad \text{et} \quad (\overline{\lambda_1}, \ldots, \overline{\lambda_N})$$

Les λ_l et $\overline{\lambda_l}$ se distinguent en choisissant

$$\lambda_l \in \mathbb{C}^+ \quad \text{et} \quad \overline{\lambda_l} \in \mathbb{C}^-.$$

Prendre le déterminant de A donne alors un homomorphisme

$$\det \ : \ GL(N, K) \to K^*.$$

Cela va maintenant être exprimé en plus grand détail en fonction des valeurs propres. Notons que $\zeta = \exp\frac{\pi i}{N}$ engendre le groupe cyclique d'ordre $2N$ qui se sépare en puissances paires et puissances impaires. Les puissances impaires ne sont jamais égales à $+1$ et donc, puisque N est impair, on a

$$\zeta^N = -1. \tag{3.1}$$

Les unités fondamentales de K_N, les matrices $N \times N$ inversibles sur K, ont des valeurs propres dans le demi-plan supérieur

$$\sqrt{\rho}\zeta^r \quad \text{où} \quad \zeta = \exp\frac{\pi i}{N} \quad \text{et} \quad 1 \leq r \leq N. \tag{3.2}$$

Ici ρ est l'élément primitif dans le corps $k(\rho)$ et ζ est une valeur complexe de la variable u. La figure 1 ci-dessous montre comment ces deux nombres sont reliés et comment la variable z dans (3.3) correspond au paramètre le long de la corde les joignant.

Étant donnée une base ordonnée pour un espace vectoriel, les automorphismes peuvent être exprimés comme des matrices et cela est naturel dans notre contexte puisque

notre groupe G fournira des bases. Notons que les déterminants sont inchangés par n'importe quelle permutation paire de la base.

Une matrice complexe A de taille $N \times N$, avec N impair, a N valeurs propres complexes. Si A est réel, i.e. $A = \overline{A}$, alors le polynôme caractéristique

$$\varphi(A, z) = \det(A - zI) \tag{3.3}$$

est réel et a un degré impair N. Par conséquent il doit avoir une racine réelle, donnant une valeur propre réelle λ_1 de A.

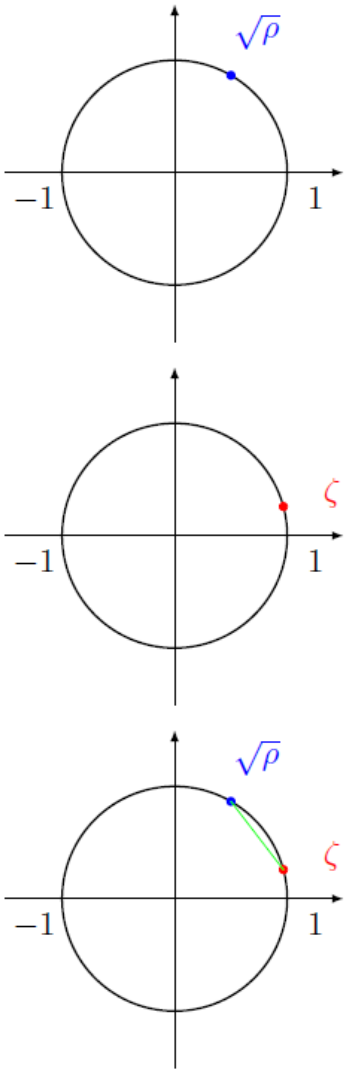

FIGURE 1. Relation entre les nombres $\sqrt{\rho}$ et ζ dans le plan complexe $\mathbb{C}$.

Le problème de trouver une racine réelle λ_1 est d'une profondeur inattendue. Alors que des algorithmes existent, ils ne sont pas robustes, de telle façon que de petites variations dans les données (les coefficients) peuvent amener à sautiller autour des

racines. Ceci est pertinent pour le théorème 1 si on veut trouver une chaîne résoluble d'extensions de corps. Ceci est une tâche difficile précisément à cause de l'*embarras du choix* mais, pour notre objectif, cela peut être ignoré.

Comme noté après (2.4), une matrice complexe A sur le corps complexe $k(\rho)$ a, quand elle est non singulière, un déterminant complexe det A qui donne un homomorphisme de groupes :

$$\det\ : GL(N, k(\rho)) \to k(\rho)^*. \tag{3.4}$$

La formule habituelle $|z^2| = z\overline{z}$ devient dans la version matricielle

$$\|A\|^2 = \det A\ \det\overline{A} \tag{3.5}$$

Le déterminant complexe det A est le produit de toutes les valeurs propres :

$$\det A = \prod_{l=1}^{N} \lambda_l. \tag{3.6}$$

où nous choisissons λ_l (comme opposé à son conjugué $\overline{\lambda_l}$) par la même convention que précédemment de telle façon que $\lambda_l \in \mathbb{C}^+$.

En supposant que A est unitaire et en remplaçant A par $A - zI$, avec z une variable, on obtient un homomorphisme

$$\det\ :\ GL(N, k(\rho)(z)) \to k(\rho)(z)^*. \tag{3.7}$$

On peut spécialiser la variable z à n'importe quelle valeur qui n'est pas une valeur propre de $A \in GL(N, k(\rho))$, puisqu'on a besoin d'un déterminant non nul. En fait, après le relèvement dans K, $z = u^2 + u + 1$ et on peut prendre $u = \sqrt{\rho}$ parce que les valeurs propres de la matrice $(A - \sqrt{\rho}I)$ sont, en utilisant (3.2):

$$\lambda - \sqrt{\rho}\zeta^r \ \text{ où } \ \lambda^N = 1. \tag{3.8}$$

et, parce que N est impair, aucun de ceux-ci n'est nul. Voir les figures 2 et 3. Le calcul de δ_3 vient de

$$\frac{1}{2} - \frac{1}{3} = \frac{1}{6} \tag{3.9}$$

qui mesure l'écart sur le cercle unité entre i et $\sqrt{\rho}$, en comparant les entiers de Gauss et les entiers de Eisenstein. Notons que les 3 points $-1, \sqrt{\rho}, i$, et la corde reliant i et $\sqrt{\rho}$ sont tous dans le disque unité fermé $|\lambda| \leq 1$, et correspondent aux 3 fractions apparaissant en (3.9). Le remplacement de 3 par 5, qui fait que les triangles réguliers deviennent des pentagones réguliers est illustré sur la figure 3. À nouveau, on a des pentagones pair et impair. Une équation comme (2.5) et ses généralisations donne des doubles recouvrements branchés sur les sommets d'un polygone pair avec un nombre

impair de côtés comme 3, 5. Les points des polygones impairs sont clairement distincts de ceux des polygones pairs. Quand on commence à itérer ces constructions, comme nous le ferons dans la section 5, on aura une séquence de points de branchement w_j indexée par j. En passant de j à $j+1$, on aura deux ensembles de points de branchement ; les "anciens" points étiquetés par j et les "nouveaux" étiquetés par $j+1$. On veut éviter qu'un quelconque nouveau point ne coïncide avec un quelconque ancien point et c'est ce à quoi l'on parvient par notre séparation en pairs et impairs. On a utilisé un autre symbole u à la place de w, puisqu'on veut que u soit pris successivement comme un w_j, permettant à notre argument d'être un argument inductif, avec les corps et les points de branchements étiquetés correctement. Notons que u_1 est la solution de l'équation (2.5). Cette explication est destinée à aider le lecteur à se repérer dans le formalisme de la section 5, qui sinon pourrait paraître déconcertant.

Par conséquent $A - \sqrt{\rho}I$ est non singulière et son déterminant donne le caractère impair

$$\varphi : GL(N, k(\rho)) \to K^*(\sqrt{\rho}). \tag{3.10}$$

Nous développerons à ce sujet dans la prochaine section. Notons que les nombres complexes (3.8) sont à l'intérieur mais non pas sur le cercle unité, de telle façon que le caractère (3.10) est *non unimodulaire*. Cela vient du fait que, dans les figures 2 et 3 (avec $N = 3$), $i - \sqrt{\rho}$ est la corde (ligne droite) joignant i à $\sqrt{\rho}$ et non l'arc de cercle d'angle $\pi/6$ apparaissant dans (3.9). Le point essentiel est que le cercle est convexe (voir la section 12 de [11] pour une discussion élargie de la convexité dans les groupes de Lie compacts).

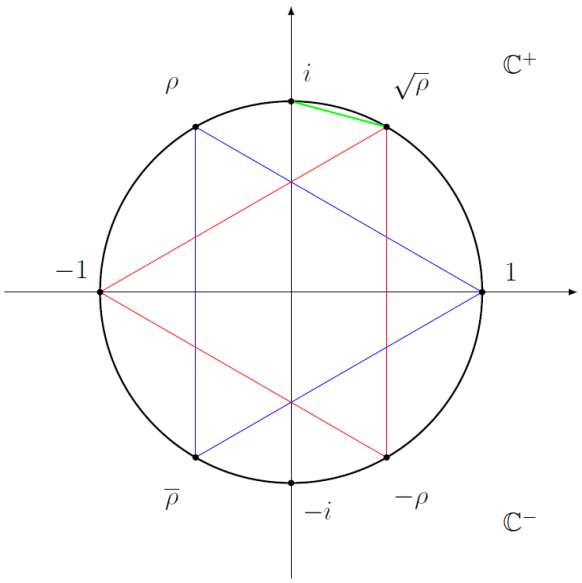

Figure 2. Pour $N = 3$, détail du cercle unité avec les unités pertinentes et la corde dont le point médian est à une distance de l'arc de $\delta_3 = 1 - \frac{\sqrt{3}}{2}$. Le triangle impair (bleu) correspond à ρ et le triangle pair (rouge) correspond à $\sqrt{\rho}$.

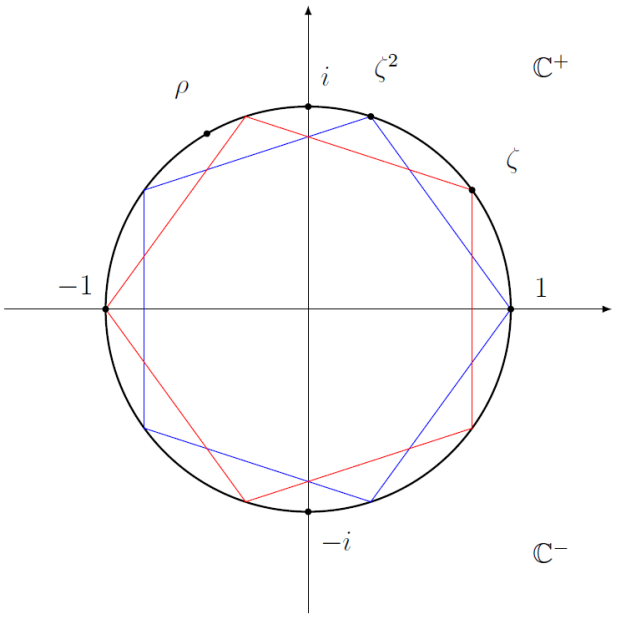

Figure 3. Pour $N = 5$, détail du cercle unité avec les unités pertinentes ; le diagramme donnera la distance δ_5. Plus généralement $\delta_N = 1 - \sin \frac{\pi}{N}$. Comme dans la figure précédente, le pentagone rouge est pair et le pentagone bleu est impair, pour $N = 5$.

Nous utiliserons deux symboles différents, n et N avec $n \leq N$ pour distinguer entre l'ordre n de ρ et l'ordre N de ζ^2.

Quand on considère un groupe fini G, comme nous le ferons dans la section ci-dessous, N sera l'ordre de G et n l'exposant de G, i.e. le plus petit n tel que $g^n = 1$ pour tout $g \in G$.

4. Groupes et ensembles

La section 2 était une révision des matrices et des déterminants et la section 3 était une révision des déterminants. Maintenant, nous commencerons à partir d'un groupe abstrait G d'ordre impair N et, suivant Artin, nous le verrons comme agissant sur l'ensemble S de ses éléments. Il agit via les permutations σ et, puisque N est impair, $\text{sign}(\sigma) = 1$ et G agit sur S via le sous-groupe alterné du groupe symétrique.

Un ensemble fini S avec un élément choisi s_1 (le point-base) est un **ensemble avec base**. S'il y a une involution (non-triviale) $s \mapsto s^{-1}$ fixant le point-base, on appellera S un **ensemble symétrique**. G agit sur S par une action à gauche $s \to \sigma s$ et une action à droite $s \to s\sigma^{-1}$. Les deux actions ensemble $s \to \sigma s \sigma^{-1}$ donnent l'**action de conjugaison** qui préserve la structure symétrique de S, où l'involution est l'inversion de groupe et où l'identité 1 est le point-base. Le centre $Z(G)$ est le noyau de l'action de G et les orbites sont les classes de conjugaison. Les classes de conjugaison sont

dites **réelles** si elles sont fixes par inversion et paires de **complexes conjuguées** sinon.

Si S est n'importe quel G-ensemble symétrique (i.e. un ensemble dont la G-action préserve la symétrie), on dénote par S^* l'ensemble S avec le point-base s_1 retiré. L'ensemble de tous les sous-ensembles de S est dénoté par 2^S avec cardinalité $|2^S| = 2^{|S|}$. Il y a un sous-ensemble distingué, notamment l'ensemble vide $\varnothing$. En l'enlevant de 2^S, il reste l'ensemble $(2^S)^*$ de *sous-ensembles non vides* de cardinalité $2^{|S|}-1$. Notons que si $|S| \neq 0$ alors $2^{|S|}-1 \neq 0$ et est **impair**. En fait, si $|S| \geq 3$ alors $2^{|S|}-1 \geq 7$.

En plus de $\varnothing$, il y a un autre sous-ensemble également distingué de S, notamment l'ensemble complet Ω. Il y a une dualité (en prenant les complémentaires) qui échange $\varnothing$ et Ω.

La théorie pourrait être poursuivie entièrement dans le paradigme des ensembles finis et des algèbres booléennes et c'était essentiellement l'idée d'Artin. En fait, pour relier cela à la théorie des corps, on se déplace maintenant vers l'algèbre linéaire en utilisant des matrices et des déterminants.

Si S est une base d'un espace vectoriel réel ou complexe V, alors 2^S est une base de l'algèbre extérieure $\wedge^\bullet(V)$ avec l'ensemble vide $\varnothing$ comme base de $\wedge^0(V)$ et l'ensemble plein Ω comme base de $\wedge^N(V)$ où $N = |S|$. Si V est un k-espace vectoriel alors, comme expliqué dans la section 2, on obtient le caractère impair φ de (3.10).

Garder trace de la parité d'un caractère de G devient assez délicat lorsqu'on procède à cette itération. La délicatesse de l'entreprise provient de l'invariant de Arf de (2.8). Mais il y a une alternative et un moyen plus facile de montrer la non trivialité d'un caractère complexe et cela consiste à montrer qu'il est *non unimodulaire*. C'est ce que nous allons maintenant faire effectivement en nous basant sur les remarques à la fin de la section 3, après la formule (3.9).

5. Le processus itératif

Ayant commencé par le processus d'Artin consistant à utiliser l'action de conjugaison de G sur ses sous-ensembles non vides, nous nous proposons maintenant d'itérer ce processus N fois. Comme expliqué à la fin de la section 3, le but de cette itération est de gérer les groupes de n'importe quel exposant impair $n \leq N$. L'index j augmente avec l'exposant n mais s'arrête finalement à la valeur N.

Notre processus interactif produira une séquence finie, indexée par j (avec $1 \leq j \leq N$)

(5.1) d'entiers impairs N_j, avec $N_1 = N = |G|, N_{j+1} = 2^{N_j} - 1$

(5.2) d'ensembles S_j avec $|S_j| = Nj,\ \ S_1 = G,\ \ S_{j+1} = (2^{S_j})^*$

(5.3) de corps réels k_j avec $k_1 = \mathbb{Q}$ et $k_{j+1} = N_j \times N_j$ matrices sur k_j

de telle façon que k_{j+1}^* contienne les matrices inversibles scalaires $N_j \times N_j$ sur k_j. On a aussi besoin d'itérer l'extraction des racines carrées définissant la séquence des variables w_j par

(5.4) $$w_j = w_{j+1}^2 + w_{j+1} + 1.$$

(5.5) les corps de fonctions K_j

(5.6) les liens par translation $K_j(w_j) = K_{j-1}(w_{j-1} - \sqrt{\rho_j - 1})$ pour $j > 1$

où ρ_{j+1} est une racine du polynôme du côté droit de (5.6),

(5.7) les modules $V_j = V(S_j)$ sur les corps dans (5.3) à (5.6)

(5.8) les éléments de volume $\Omega_j \in \wedge^{N_j}(V_j)$.

Les éléments inversibles de chaque algèbre agissent sur l'élément de volume par le déterminant

(5.9) $$\det\ :\ GL(N_j, K_j) \to K_j^*,$$

en donnant un caractère par la formule

(5.10) $$\psi_j(A_j) = \det(A_j - \sqrt{\rho_j} I).$$

où les ρ_j sont définis dans (5.6).

La translation $w_j \to w_j - \sqrt{\rho_j}$ induit une application affine

(5.11) $$\alpha_j\ :\ K_j \to K_{j-1}$$

qui est consistante avec les caractères ψ_j, de telle façon que l'on a le diagramme commutatif :

(5.12)
$$\begin{array}{ccc} GL(N_j, K_j) & \xrightarrow{\phi} & GL(N_{j-1}, K_{j-1}) \\ \downarrow{\scriptstyle \psi_j} & & \downarrow{\scriptstyle \psi_{j-1}} \\ K_j^* & \xrightarrow{\alpha_j} & K_{j-1}^* \end{array}$$

où l'application du haut est une conséquence du théorème de Cayley-Hamilton appliqué à notre contexte.

À la fin de la section 3, on explique la raison pour laquelle la formule inductive ci-dessus semble compliquée. Il y a un autre point que le lecteur pourrait trouver utile et qui concerne le diagramme commutatif (5.12) et la référence au théorème de Cayley-Hamilton. L'étape inductive de j à $j+1$ implique de remplacer un espace vectoriel par son algèbre extérieure, et une matrice A de taille $m \times m$ par les matrices $\binom{m}{r} \times \binom{m}{r}$, $A(r)$ agissant sur la $r^{\text{ième}}$ puissance extérieure. Pour tout scalaire z, la matrice translatée $A - zI$ (avec I la matrice identité) agit alors sur l'algèbre exérieure comme

$$\sum_r (-z)^{(m-r)} A(r) \tag{5.13}$$

Le déterminant de cette action est juste le polynôme caractéristique

$$\det(A - zI) \tag{5.14}$$

Le théorème de Cayley-Hamilton affirme que remplacer le scalaire z par la matrice A dans (5.13) donne zéro. Bien sûr la somme (5.13) ou le déterminant dans (5.14) sont maintenant les traces ou les déterminants de matrices beaucoup plus grandes. Dans (5.14) les matrices sont de tailles qui vont de $m \times m$ à $2^m \times 2^m$. En notation moderne, le théorème de Cayley-Hamilton semble évident parce que $A - AI = 0$. Mais l'algèbre moderne a été créée principalement par Hamilton et Cayley pour faire qu'un fait profond semble évident. Une façon sophistiquée d'interpréter le théorème de Cayley-Hamilton est de dire qu'un module projectif et sa résolution de Koszul, par l'algèbre extérieure, définissent des éléments équivalents de K-théorie sur l'anneau de base.

Cela explique le diagramme commutatif (5.12), en se rappelant que $r = 0$ indexe le module résolu. Notons que l'index j dans ces formules est naturellement décroissant, impliquant une descente décroissante (finie) commençant à partir de N. L'indexation de la variable u se termine par u_0 qui correspond à l'ensemble vide (c'est la fibre du point qui est en train d'être résolu). L'élévation vers w_1 correspond au module libre défini par V.

Ainsi, nous avons en effet construit une séquence de N caractères complexes et notre objectif est de montrer qu'ils ne peuvent pas tous être triviaux. En fait, nous montrerons que le caractère ψ_N de G est non unimodulaire et par conséquent est non trivial.

L'action de G sur l'espace vectoriel V_N sur le corps de fonctions complexes K_N peut ne pas être unitaire pour n'importe quelle métrique alors qu'il peut rester cependant unimodulaire, i.e. de déterminant 1. Nous montrerons que cela ne se produit pas. La raison est qu'au moins l'une des valeurs propres λ de la matrice adéquate a un module qui est *strictement inférieur à 1.* Cela est clair à partir de la géométrie des figures 2 et 3, montrant que la corde est à l'intérieur du cercle. La déviation à partir de 1 est

extrêmement petite, une estimation asymptotique grossière de la borne inférieure est

$$1 - |\lambda| \sim 2^{-N_j} \quad \text{pour de grandes valeur de } j. \tag{5.15}$$

Le déterminant est par conséquent juste inférieur à 1, et le caractère ψ_N est non trivial. C'est ce que nous avons entrepris de prouver.

Donc nous avons maintenant démontré le

Théorème 2. *Un groupe G d'ordre impair a un caractère complexe non trivial.*

Le théorème 1 est une conséquence facile du théorème 2 comme nous allons le montrer maintenant. Supposons que le théorème 1 est faux, alors il doit y avoir un groupe G d'ordre minimal impair N qui n'est pas résoluble. Appliquer le théorème 2 à G amène à une séquence exacte de groupes

$$1 \to H_1 \to G \to H_2 \to 1 \tag{5.16}$$

où $|H_1|$ et $|H_2|$ sont tous les deux inférieurs à N et par conséquent résolubles (par la supposition minimale : en fait, $H_2 \subset \mathbb{C}^*$ est nécessairement abélien). Mais alors (5.16) fournit une chaîne de sous-groupes de G, chacun étant normal dans son successeur, et avec un quotient abélien. C'est une définition de la résolubilité et cela fournit la contradiction souhaitée, établissant ainsi le théorème 1.

Ceci complète la démonstration formelle du théorème 1. Dans la dernière section ci-dessous, je ferai des commentaires sur la nature de la preuve et discuterai de ses implications.

6. Commentaires

Dans cet article, j'ai présenté une preuve courte du théorème de Feit-Thompson, en utilisant seulement des idées élémentaires d'algèbre linéaire et de théorie des nombres. La principale nouveauté a été l'utilisation d'un processus itératif basé sur des idées d'Artin et d'Hermann Weyl. Pour des raisons de simplicité, j'ai évité des idées plus sophistiquées et je suis resté dans la *lingua franca* commune à tous les mathématiciens et physiciens (excepté pour des remarques explicatives qui se sont éloignées vers l'algèbre moderne commutative). J'ai fait cela parce qu'il semblerait vraisemblable que les idées de cet article puissent s'appliquer à une classe plus étendue de problèmes, tirés de la géométrie, de la théorie des nombres et de la physique.

Pour prouver le théorème de Feit Thompson sans information arithmétique à propos de l'ordre N, on avait à utiliser le très grand nombre $M(N)$ et les bornes numériques

extrêmement petites (5.15). Ce programme peut être raffiné de façon évidente de différentes manières comme on l'indique brièvement ci-dessous :

5.1 Le nombre de fois où l'on doit élever à la puissance, en remplaçant N par 2^N, est l'exposant n du groupe G, qui peut être bien plus petit que son ordre. Cela amène à toute l'arène des problèmes de type Burnside reliés au travail de Zuk.

5.2 Les entiers qui ont beaucoup de facteurs premiers sont rares, et donc les méthodes probabilistes peuvent fournir des bornes bien meilleures.

Le fait que $|G|$ soit impair a été utilisé de différentes manières, mais la stratégie générale devrait encore marcher pour des groupes d'ordre pair, et faire la lumière sur la structure de tous les groupes finis. En particulier, cela devrait fournir une meilleure compréhension du programme complet décrit dans [2].

En théorie des nombres, le dernier théorème de Fermat, démontré de façon célèbre par Andrew Wiles, est un autre défi pour ceux qui cherchent des preuves simples. Les idées de cet article offrent un espoir pour cette tâche, comme on peut le déduire de mon exposé à l'Université de Fudan.

En physique, le processus d'itération que nous avons utilisé fait intervenir une mise à l'échelle et amène aux fractals et à la renormalisation. Les très petits nombres dans (5.15) sont importants pour la théorie mais pas dans les expériences, où on peut les ignorer.

La célèbre *mer* de particules et d'anti-particules de Dirac a des niveaux d'énergie modélisés ici par des puissances positives et négatives de 2, quand on exprime N dyadiquement. Est également relié à la mécanique quantique le fait que les points du cercle unité correspondant aux racines de l'unité, utilisés dans nos extensions de corps, définissent des polygones convexes d'une manière similaire à ce qui est fait dans [9].

J'espère illustrer cela dans des publications à venir avec des collègues plus jeunes. Mais plusieurs de mes articles précédents ont déjà utilisé les idées dans différents contextes. La non-existence d'une structure complexe sur la 6-sphère est traitée dans deux articles séparés [4] [6]. Une application en chimie faisant intervenir les éléments remarquables que sont l'hélium 4 et l'hélium 3 est décrite dans [3].

Il y a d'importants problèmes en topologie algébrique qui sont pertinents. Le premier d'entre eux est la solution maintenant ancienne du problème de l'invariant de Hopf par J.F. Adams et la courte preuve ultérieure dans mon article avec Adams [7]. Plus récemment, un théorème similaire mais plus profond à propos de l'invariant de

Kervaire a été (presque) complètement résolu par Hill, Hopkins et Ravenel [8]. Il est probable que les méthodes du présent article amèneront pareillement à une preuve plus courte.

L'article [8] est né à partir d'idées des théories des cordes et j'en anticipe des applications significatives dans cette direction. Ma tentative d'écriture d'un court article avec Greg Moore [5] s'adaptera, je l'espère, naturellement dans ce paradigme.

Le processus d'Artin a amené à des sous-groupes et son itération a amené à des micro-sous-groupes, beaucoup étudiés en physique, indiquant que notre modèle fournit un bon paradigme à toutes les échelles.

Finalement, je commenterai la finitude. La preuve du théorème 1 a utilisé, de façon essentielle, la finitude de l'ordre N du groupe. Il sera très intéressant de rechercher ce qui se passe quand on permet à N de croître à l'infini. En théorie des nombres, étudier ce qui se passe lorsque $N \to \infty$ a été le problème fondamental depuis les époques d'Euler et Riemann mais, comme cela est bien connu, on a besoin d'estimations plus précises maintenant.

En physique, garder N fini entraîne un cut-off de l'énergie et laisser $N \to \infty$ amène à des problèmes conceptuels difficiles et non résolus.

Il semble clair que des qualités logiques sérieuses sont nécessitées dans le processus de calcul des limites (à la fois en théorie des nombres et en physique). Cela nous ramène à la grande controverse d'il y a une centaine d'années entre Brouwer, Hilbert, Weyl et Gödel. En fin de compte, cette controverse dépend de notre compréhension des nombres réels.

Remerciements.

J'ai une dette envers tous ceux qui ont corrigé des erreurs ou fait des suggestions utiles, notamment envers Thomas Espitau. Mais je dois particulièrement remercier Graeme Segal, avec qui j'ai écrit précédemment de nombreux articles pertinents. Finalement, je remercie Andrew Ranicki d'Edimbourg pour son assistance technique, ainsi que Joseph Malkoun de Beyrouth et Carlos Zapata-Carratala d'Edimburgh.

Références

[1] Walter Feit, John G. Thompson, *Solvability of groups of odd order*. Pacific J. Math., vol. 13, n° 3 (1963).

[2] Ronald Solomon, *A brief history of the classification of the finite simple groups*. American Mathematical Society. Bulletin. New Series, 38 (3): 315-352 (2001).

[3] Michael F. Atiyah, *Geometric Models of Helium*. Modern Physics Letters A, vol 32, n° 1 (2017).

[4] Michael F. Atiyah, *The Non-Existent Complex 6-Sphere*. arXiv:1610.09366 (2016) https://arxiv.org/pdf/1610.09366.pdf.

[5] Michael F. Atiyah, Gregory W. Moore, *A Shifted View of Fundamental Physics*. Singer 85 J.Diff. Geometry vol 15 (2011).

[6] Michael F. Atiyah, *Understanding the 6-sphere*. The paper will be published in a Springer Book in the same special collection of Hilbert Books of 1917 about Foundations of Mathematics and Physics (2017).

[7] John F. Adams, Michael F. Atiyah, *K-Theory and the Hopf Invariant*. The Quarterly Journal of Mathematics, Volume 17, Issue 1, Pages 31-38 (1964).

[8] Michael A. Hill, Michael J. Hopkins, Douglas C. Ravenel, *On the non-existence of elements of Kervaire invariant one*. Annals of Mathematics, Pages 1-262, Volume 184, Issue 1 (2016).

[9] Michael F. Atiyah, Andrew N. Pressley, *Convexity and Loop Groups*. Progress in Mathematics 36 (1983), 33-64.

[10] Michael F. Atiyah, *Riemann surfaces and spin structures*. Ann. scient. Éc. Norm. Sup. 4 (1971), 47-62.

[11] Michael F. Atiyah, Raoul Bott, *Yang-Mills Equations over Riemann Surfaces*. Phil. Trans. R. Soc Lond, A 308, (1982), 523-615

Michael Atiyah
m.atiyah@ed.ac.uk
École de mathématiques
Université d'Edinburgh
Building James Clerk Maxwell
Buildings du RoiKing
Route Peter Guthrie Tait
Edimbourg EH9 3FD
Écosse, Royaume-Uni.