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.

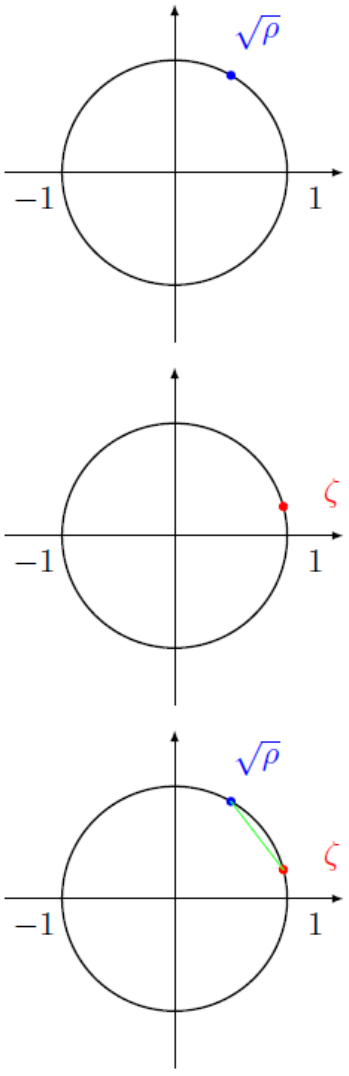


FIGURE 1. Relation entre les nombres $\sqrt{\rho}$ et ζ dans le plan complexe $\mathbb{C}$.

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).

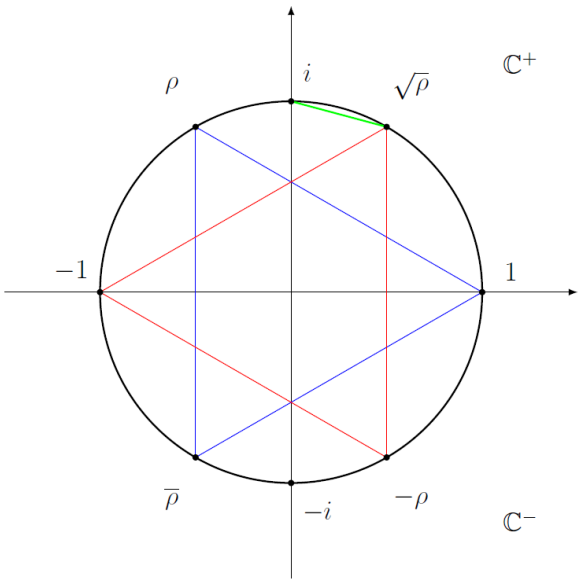


Figure 2. Pour $N = 3$, détail du cercle unité avec les unités pertinentes et la corde dont le point médian est à une distance de l'arc de $\delta_3 = 1 - \frac{\sqrt{3}}{2}$. Le triangle impair (bleu) correspond à ρ et le triangle pair (rouge) correspond à $\sqrt{\rho}$.

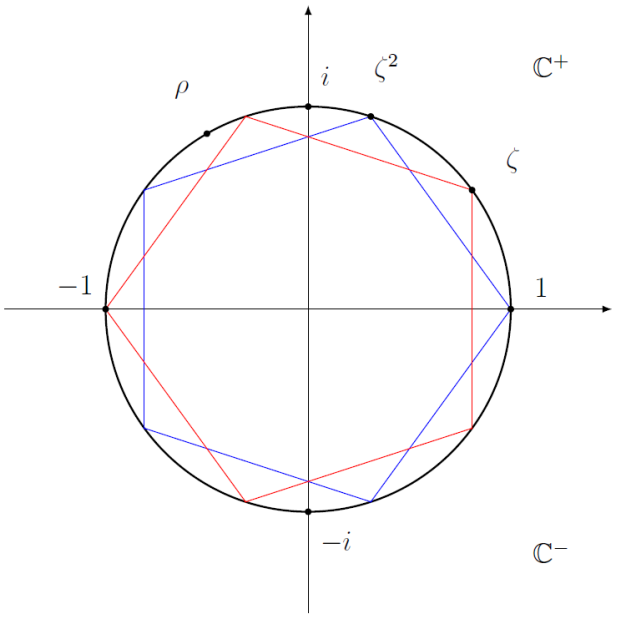


Figure 3. Pour $N = 5$, détail du cercle unité avec les unités pertinentes ; le diagramme donnera la distance δ_5. Plus généralement $\delta_N = 1 - \sin \frac{\pi}{N}$. Comme dans la figure précédente, le pentagone rouge est pair et le pentagone bleu est impair, pour $N = 5$.

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.

Donner le même nom à deux choses différentes
Jean-Pierre Bourguignon
2018

Présentation du conférencier par Gérard Berry

Nous allons avoir le plaisir d'entendre Jean-Pierre Bourguignon. Jean-Pierre Bourguignon est mathématicien, en géométrie différentielle, en équations aux dérivées partielles (EDP), en lien avec la physique, la relativité générale, etc. Il a eu une longue carrière aussi, et l'occasion de s'occuper de la recherche à travers la direction de la Société Mathématique de France, de l'IHES, et il est maintenant Directeur du Conseil Européen de la Recherche, du fameux ERC, qui donne des bourses de chercheurs très sélectives, très sérieusement examinées, et ce sont des choses qui changent la vie d'un chercheur et de ses collaborateurs, la France se comportant d'ailleurs très bien vis-à-vis de ça. À l'époque, il faut le rappeler, d'une période de vaches maigres pour la recherche, on peut le dire haut et fort. Merci pour ce travail fondamental, Jean-Pierre, ce sont des choses qui font beaucoup de bien à la recherche et donc voilà, son exposé a un titre assez simple, mais j'attends... C'est un peu mystérieux, c'est "*Donner le même nom à deux choses différentes*". Ce n'est pas la chose qui est mystérieuse, c'est ce qu'on va entendre, pour moi.

Exposé de Jean-Pierre Bourguignon

Bonjour, merci en tout cas aux organisateurs de me donner l'occasion de parler devant vous dans ce colloque assez extraordinaire. Donc moi, mon sujet, c'est effectivement celui qui est là, qui est en fait une citation d'Henri Poincaré, voilà. Donc effectivement, il s'agit de cette citation de Henri Poincaré dans *Science et méthode*, qui dit :

> "*Je ne sais si je n'ai pas déjà dit quelque part (*Donc ça veut dire que c'est une chose qu'il avait en tête depuis longtemps.*) que la mathématique est l'art de donner le même nom à des choses différentes. Il convient que ces choses différentes par la matière soient semblables par la forme, et qu'elles puissent pour ainsi dire se couler dans le même moule.*"

Donc voilà. En fait il continue dans ce texte, donc dans *Science et méthode* qui peut toujours être lu avec tout à fait intérêt, vous savez, il y a eu cette trilogie qui était une trilogie de textes à la fois scientifiques mais aussi philosophiques, destinés un grand public, qui s'appellent *Science et hypothèse, Science et méthode, La valeur de la science*, au début du XIX^{e} siècle, et qui vient d'être d'ailleurs rééditée par Dunod, qui est très intéressante et qui permet de voir qu'un scientifique du niveau de Poincaré n'hésitait pas à passer du temps à écrire des textes de vulgarisation de haut niveau, sans concession mais quand même remarquablement clairs.

Donc il continue dans ce texte, juste après cette citation :

> "*Quand le langage a été bien choisi, on est tout étonné de voir que toutes les démonstrations, faites pour un objet connu, s'appliquent immédiatement à beaucoup d'objets nouveaux ; on n'a rien à changer, pas même les mots, puisque les noms sont devenus les mêmes.*"

Transcription des sous-titres (obtenus par downsub) d'une conférence donnée dans le cadre du Colloque de rentrée 2018 du Collège de France visionnable ici https://www.college-de-france.fr/site/colloque-2018/symposium-2018-10-19-10h10.htm, Denise Vella-Chemla, 16.4.2022

Voilà, donc ça, c'est cette citation en fait. Il continue encore :

> "*Un mot bien choisi suffit le plus souvent pour faire disparaître les exceptions que comportaient les règles énoncées dans l'ancien langage. C'est pour cela qu'on a imaginé les quantités négatives, les quantités imaginaires, les points à l'infini et que sais-je encore. Les exceptions, ne l'oublions pas, sont pernicieuses, parce qu'elles cachent les lois.*"

Donc c'est une très bonne, disons, introduction à ce thème qui est de savoir comment le langage aide à la pensée, au développement de la science, mais aussi comment... par quels efforts, comment on arrive à trouver ces identifications. Donc si vous voulez, mon propos, donc, ça va être de parler de ce sujet, bien entendu, puisque j'ai choisi de le mettre en titre. Mais à partir d'un certain nombre de textes tout à fait significatifs dans l'histoire des mathématiques. Donc d'abord, ces textes de Poincaré, enfin je m'en n'inspirerai de diverses façons ; un texte qui pour moi est très important et souvent mal connu, qui vient juste d'être traduit en français par M. Lobo, qui est un texte d'Hermann Weyl, qui s'appelle *Philosophie des mathématiques et des sciences de la nature*, dont il existe deux éditions, une première édition en allemand puis l'édition complétée dans les années 20, et ensuite une édition complétée après la guerre en 1949, qui est cette fois traduite en anglais avec des notices historiques de Hermann Weyl, dans lesquelles souvent il fait remarquer qu'il avait quand même vu juste quelques années auparavant, ce qui est un commentaire intéressant. Et puis aussi d'autres textes très importants pour les géomètres, en tout cas pour le géomètre différentiel que je suis, de Riemann et un texte extrêmement important et méconnu de Lagrange, que je vais donc essayer de commenter. Donc voilà, et après, j'arriverai à des conclusions. Donc voilà un peu ce que je veux faire et en fait, je voudrais prendre trois exemples de situations justement, où les problèmes de terminologie, de concepts à identifier ont vraiment... sont apparus... ont mis du temps à apparaître, et dans quel contexte ils sont vraiment apparus.

Donc le premier exemple que je voudrais prendre a trait au nombre et à la géométrie. Donc la notion de nombre est une notion qui évidemment existe dans énormément de civilisations, d'abord la notion de nombre entier, il s'agit de compter. Déjà un peu plus sophistiquée, la notion de fractions, donc de nombre rationnels, diviser deux nombres entiers, diviser un nombre entier par un autre à condition qu'il ne soit pas nul, voilà. Et alors, comme vous savez, pour les Grecs, c'est une chose qui a déjà été évoquée hier, une des choses qui est apparue comme problématique et qui du coup a amené un peu un schisme dans les mathématiques, c'est que pour les pythagoriciens, les seuls nombres acceptables étaient les nombres rationnels. Or dès que vous faites de la géométrie, que vous connaissez le théorème de Pythagore, en fait, vous regardez la longueur de la diagonale du carré et vous tombez sur le nombre racine de deux, c'était connu des Grecs et ce n'est pas très difficile, c'est un exercice intéressant, même pour un élève du collège, de démontrer que racine de deux ne peut pas être un nombre rationnel.

Donc du coup, apparaissent dans la géométrie des scandales, des nombres qui ne peuvent pas être acceptés comme nombres, qui sont des nombres irrationnels. D'où l'idée qu'il doit y avoir deux mondes : il y a le monde des figures, la géométrie, et le monde des nombres, parce qu'on se limite aux nombres rationnels. Donc ça, ça a été quand même une chose qui a pesé dans l'histoire des mathématiques pendant très très longtemps, et donc comme je vais y revenir dans une minute, a donc amené à ce schisme. Et alors parmi les règles, cette fois si on se limite pour quelques minutes aux nombres rationnels d'une certaine façon, il y avait quand même le fait qui est apparu assez

rapidement la règle bien connue que quand je multiplie un nombre positif par un nombre positif, j'obtiens un nombre positif, donc plus par plus donnent plus, ainsi que moins par moins donnent plus, et du coup ça veut dire que quand je fais le carré d'un nombre, il n'y a pas moyen que le résultat soit un nombre négatif. Mais pourtant il apparaissait utile, en particulier c'est Cardan qui, le premier, a mis ça en évidence, voilà, donc dans ce texte, dans lequel, alors, c'est intéressant, parce que Cardan n'est pas celui qui a découvert la formule explicite pour résoudre l'équation du troisième degré, c'est Tartaglia avant lui, et peut-être même Ferrari avant lui. Mais en tout cas, Cardan est le premier, il avait à écrire une solution générale des équations du troisième degré, à se rendre compte que ce serait vraiment utile si on avait des nombres dont le carré était négatif. Donc c'est le premier à avoir introduit donc les nombres qu'on appelle imaginaires, puisque visiblement ce ne sont pas des vrais nombres, c'est autre chose. Et donc ces nombres imaginaires sont apparus dans les mathématiques à ce moment-là, mais un peu comme une commodité d'écriture, c'est-à-dire on n'était pas encore dans quelque chose qui avait vraiment un sens. Et d'une certaine façon pour qu'on aille au stade d'après, il était indispensable de faire une révolution encore plus grande, qui était donc de faire abolir ce schisme que j'ai évoqué, qui était donc ce schisme de... Alors peut-être un commentaire sur les nombres imaginaires qui est quand même intéressant : il y a un commentaire qui est fait disons très tôt, à propos des nombres imaginaires, comme quoi c'est vraiment quelque chose qui a un parfum de scandale et que du coup on n'est pas sûr qu'on a le droit de les appeler des nombres ; donc c'est pour ça qu'on a mis le codicille *imaginaires*. En tout cas, la chose vraiment importante, c'est donc qu'il y ait l'affirmation par Descartes, comme je vais le montrer dans une minute, non dans le *Discours de la méthode* mais plutôt dans un ajout du *Discours de la méthode* qui s'appelle la *Géométrie* que justement Descartes dit qu'eh bien, non, en fait, ce schisme n'a pas raison d'être et on doit accepter que toute figure géométrique peut être décrite par des nombres. Et alors voilà comment il commence sa *Géométrie* et dans laquelle vous voyez que c'est juste en passant, donc ce n'est même pas une affirmation philosophique, c'est que vraiment si on veut résoudre, avoir des outils de résolution et aussi enrichir la géométrie, il est indispensable d'accepter qu'on représente tout par des nombres. Et donc le principal enrichissement auquel il pense, c'est l'enrichissement qui consiste à regarder dans le plan des courbes bien plus compliquées que les coniques, qui évidemment avaient droit de cité depuis les Grecs de façon massive, étaient un des lieux de géométrie les plus élaborés, avec des théorèmes extrêmement profonds. Donc Descartes a dit "Mais après tout, si je prends une équation algébrique, et que je prends des coordonnées, et que je regarde les courbes de 3^{e} degré, 4^{e} degré, 5^{e} degré, voilà des objets géométriques que je peux manipuler puisque je peux calculer sur eux aussi bien qu'avec les coniques qui sont des objets du second degré, et il n'y a pas de raison de se limiter." Donc c'est dans ce contexte un petit peu limité que Descartes affirme ça.

Mais en tout cas, ça, c'est une affirmation extrêmement importante, et donc dans le cas de Descartes donc c'est une... Alors une chose très intéressante, à ce propos, même si c'est quand vous lisez le texte et le texte continue plus loin mais vous voyez bien que dès l'introduction, quand il parle de ça, il en parle en passant, sans en faire une prise de position philosophique, Hermann Weyl, dans son texte *Sur la philosophie des mathématiques et des sciences de la nature* dit la chose suivante :

> "*L'introduction des nombres comme coordonnées, en faisant référence au processus particulier de la division du continu à une dimension est un acte de violence dont la seule justification est le fait qu'elle permet d'utiliser la souplesse calculatoire que ce continu offre avec ses quatre opérations.*"

Vous voyez que parce qu'il s'agissait de faire cesser un schisme, ce n'est pas du tout quelque chose d'anecdotique, ça change complètement les choses. Et aujourd'hui, évidemment, alors que tout le monde, y compris les enfants, quand ils font des jeux sur leur téléphone ou sur leur tablette, utilisent des coordonnées, donc l'affirmation de ces coordonnées est devenue une banalité totale alors qu'historiquement, elle n'était pas une banalité totale. Cela ne veut pas du tout dire que les Grecs s'interdisaient dans le temps d'utiliser des nombres pour faire des calculs géométriques, mais en tout cas l'affirmation qu'il y a complète correspondance entre ces deux mondes.

Donc je reviens aux nombres imaginaires parce que maintenant, vous allez voir, je vais pouvoir me servir de cette affirmation, pour peut-être voir les nombres imaginaires un peu différemment. Le premier, semble-t-il, qui a entrevu l'idée de peut être relier les nombres imaginaires à des constructions géométriques dans le plan, en fait, c'est Johaniss Wallis, dans ce *De Algebra Tractatus*. Mais en fait, là, c'est aussi en passant, en faisant remarquer qu'après tout, on pourrait peut-être voir les nombres imaginaires, les représenter comme des objets dans le plan, mais il n'en fait pas de théorie. Et c'est très étrange qu'il ait fallu attendre très longtemps, c'est-à-dire le début du XIX^{e} siècle, enfin même le XIX^{e} siècle et Jean-Robert Argand qui a vraiment cette fois parlé d'un plan complexe, c'est-à-dire de dire qu'après tout, si on rapporte les coordonnées du plan avec les nombres réels, qui sont l'axe habituel des x et si on met sur l'axe des y donc, qu'on a tendance à représenter verticalement, le nombre imaginaire i, alors brusquement tout un tas de choses qu'on fait sur les nombres imaginaires deviennent extrêmement simples, à condition que l'on fasse donc ce qu'on appelle maintenant le plan complexe, c'est-à-dire qu'on définisse, dans ce plan, tout ce qu'on fait d'habitude avec les nombres, c'est-à-dire des additions, ça, on sait faire, on ajoute les deux coordonnées, Descartes le faisait, mais aussi une multiplication, donc c'est ça la nouveauté. Et pourquoi cette multiplication devient très naturelle et pourquoi elle représente naturellement les nombres imaginaires, eh bien si on pense que la multiplication par i qui consiste à passer de 1 à i, ça consiste à faire à une rotation de 90 degrés, si je fais deux fois cette opération, je multiplie i par lui même, je trouve 90^{o} plus 90^{o}, 180 degrés, donc je trouve la multiplication par -1 et donc j'ai représenté la vertu fondamentale des nombres imaginaires, qui est que le carré de i c'est -1. Et donc ça, évidemment, ça donne une représentation extrêmement simple et surtout, on dispose d'un nouvel objet mathématique, qui est le corps des nombres complexes parce qu'après ça, on peut démontrer qu'avec ce plan, avec ces nouvelles opérations, les additions, les multiplications, on peut faire comme on fait d'habitude, à part le nombre 0, tout nombre a un inverse, on sait calculer l'inverse très simplement, donc c'est un corps, au sens des mathématiciens, aussi intéressant que le corps des nombres réels, pour lequel on est habitué à faire des additions, des multiplications, des soustractions des divisions, à condition de ne pas diviser par 0. Donc voilà.

Donc ça, ça a été, ce passage d'un objet purement algébrique à un objet qui devient géométrique, mais pour lequel l'opération algébrique devient limpide, d'une certaine façon, ce n'est plus du tout une bizarrerie et du coup, on dispose à ce moment-là d'un objet extrêmement intéressant. Mais pour montrer qu'il y a quand même des choses étonnantes, on peut se dire après tout, j'ai fait ça, je suis parti des nombres ordinaires, que j'ai représentés sur la droite réelle, donc ce continu à une dimension, donc, on a fait cette extension à deux dimensions et pourquoi on ne recommencerait pas ? Et faire donc des nombres hyper-complexes, c'est-à-dire faire sur les nombres complexes ce qu'on a fait sur les nombres réels, donc, introduire de nouvelles coordonnées. Donc ça, ça a été fait, donc, au milieu du XIX^{e} siècle, par William Rowan Hamilton, en introduisant ce qu'on appelle

les quaternions. Donc qu'est ce que c'est que les quaternions, donc c'est effectivement, cette fois, on va être à quatre dimensions, puisqu'on a pris des nombres complexes et on a fait un produit par les nombres complexes. Donc cette fois, on a toujours les nombres réels qui sont un axe, avec 1 comme unité, mais maintenant on a trois dimensions imaginaires, le i qu'on avait avant, ce i, qui était dans les nombres complexes, et puis un j et un k, ce sont les notations qu'on prend d'habitude pour la partie complexe de cette extension. Et alors, évidemment, on demande que j au carré soit -1 comme i au carré, on demande que k au carré, ça soit -1 et c'est un tout petit calcul élémentaire, je ne vais pas le faire, mais je l'ai sur mon écran, là, qui consiste à dire que si vous faites ça, le fait que vous imposiez que le produit de i par j soit k, automatiquement, entraîne que la partie imaginaire de ces nombres ne sont plus commutatifs, vous savez, quand on multiplie deux nombres xy et yx pour les nombres ordinaires, c'est la même chose. Autrement dit, on peut échanger l'ordre. Eh bien, là dans les quaternions, le fait d'avoir fait cette extension en passant aux nombres hyper-complexes, on perd la commutativité.

Et donc ça, c'est intéressant, et du coup ça m'amène un commentaire, pour dire que la création mathématique de ces objets, donc la création par Hamilton des quaternions, on se dit mais après tout, on n'a qu'à continuer. Et puisqu'on a fait les quaternions, on va faire des octaves, c'est Cayley qui a fait ça. Donc on est passé cette fois à huit dimensions et là, le prix qu'on paie, il est assez élevé parce qu'en fait, on perd bien plus, ce n'est pas seulement que ça va pas être commutatif, mais en fait on perd même ce qu'on appelle l'associativité, c'est-à-dire le fait que le produit d'un nombre par la somme de 2 nombres, on peut distribuer les choses et malheureusement ça, on ne peut plus le faire et donc il y a vraiment des choses, algébriquement, il y a des choses qui font ça. Donc on est passé des nombres réels aux nombres complexes puis aux nombres hyper-complexes avec les quaternions. On peut aller jusqu'aux octaves de Cayley et je savais, peut-être que vous ne le savez pas, mais un des experts des octaves de Cayley dans le monde, c'est Jacques Tits qui était professeur dans cette maison, et la chose extraordinaire qui montre que les mathématiques peuvent dire des choses profondes sur des objets qu'on a l'impression de construire facilement de façon algébrique, c'est si vous voulez aller au-delà des octaves de Cayley, vous passez à la dimension 16, vous ne pouvez plus, à cause de la structure topologique de la sphère dans l'espace à 16 dimensions, donc une sphère à 15 dimensions, qui vous empêche de construire un objet algébrique qui serait aussi intéressant que les octaves de Cayley. Donc ça veut dire qu'avec cette construction qui semblait algébriquement toute simple on est passé de 1 à 2, puis de 2 à 4, puis de 4 à 8, en fait, la nature des objets que vous regardez est suffisamment cachée, et complexe, pour que ce que vous voudriez faire par, comment dire, spontanéité algébrique, vous est interdit par une topologie beaucoup plus profonde. C'était un commentaire en passant mais pour montrer que, là-encore au niveau du langage, ce qu'on peut croire comme des opérations banales, en fait, sous-jacente, il y a une réalité d'une subtilité beaucoup plus grande et pour lesquelles les outils mathématiques à mobiliser sont complètement d'un autre ordre. C'est en fait de la topologie algébrique, inventée par Henri Poincaré. Voilà. Donc ça c'était mon premier sujet, qui était de parler du passage de l'introduction des nombres imaginaires, mais aussi de la nécessité d'accepter les systèmes de coordonnées, donc de repérer les objets, de faire une synthèse entre la géométrie et l'arithmétique, mais en fait l'utilisation des nombres, et de montrer comment ces choses-là amènent à des objets mathématiques extrêmement intéressants, extrêmement profonds.

La deuxième notion que je voudrais discuter qui est en fait, pour les géomètres évidemment, fon-

damentale, qui est la notion d'espace. Donc pour tout le monde, quand on parle de l'espace, c'est l'espace qui nous entoure, c'est un espace à trois dimensions, on a l'impression qu'on a le contrôle sensible et historiquement, c'est une chose qui est... évidemment les travaux d'Euclide ont été fondamentaux, on peut mesurer des distances dans l'espace ordinaire, et c'est ça qui fait sa valeur, qui fait sa richesse, qui fait sa solidité. Et pendant longtemps, beaucoup de gens ont considéré que l'espace, l'espace euclidien, et même l'espace euclidien à trois dimensions était en fait le seul espace concevable. C'est intéressant, dans le livre d'Emmanuel Kant donc, la *Critique de la raison pure*, un des impératifs absolu, c'est justement l'espace euclidien. Alors en fait si vous lisez un peu plus Emmanuel Kant, un peu avant la *Critique de la raison pure*, il discute à un moment, après tout, pourquoi l'espace a trois dimensions, et pourquoi est-ce qu'il ne pourrait pas en avoir plus. Mais finalement, quand il vient à *Critique de la raison pure*, qu'il veut définir les impératifs absolus, la seule chose qui compte, c'est l'espace euclidien à trois dimensions. Donc déjà, l'idée de concevoir un espace à plus de trois dimensions était problématique, mais surtout un espace qui soit structuré par la notion de longueur, telle qu'on la connaît chez Euclide, avec tous les théorèmes qu'on connaît. Donc d'une certaine façon, quand on a commencé... alors, une des choses qui était un ver dans le fruit pour les mathématiciens, c'était le fameux postulat des parallèles. Ce postulat des parallèles qui arrive dans la description d'Euclide à un certain niveau, en général, on le présente comme le cinquième postulat, en fait, c'est un peu plus compliqué quand on compte, parce qu'il y a des postulats qui ont des codicilles. En tout cas, appelons-le le cinquième postulat, qui est un postulat extrêmement simple et naturel, qui consiste à dire que si je prends une droite, dans un plan, si je prends un point extérieur à la droite, alors il existe une et une seule droite passant par ce point parallèle à cette droite. Si vous regardez vraiment la façon dont Euclide l'a énoncé, il ne l'a pas énoncé comme je viens de l'énoncer ; il l'a énoncé en disant qu'il existe une droite qui, si je la prolonge indéfiniment, ne rencontrera pas l'autre droite. Donc vous voyez que là, c'est déjà une chose un tout petit peu plus subtile, en ce sens que ça fait appel à l'infini, puisqu'il faut prolonger la droite indéfiniment. Évidemment ce que vous ne pouvez pas faire matériellement. Donc c'est déjà forcément une abstraction. En tout cas, ce postulat était problématique, pourquoi ? Il était présenté comme postulat chez Euclide mais la question se posait "est-ce qu'il n'y a pas moyen de déduire ce postulat comme un théorème déduit des postulats précédents ? Et il y a eu énormément de tentatives pour faire ça, toutes fausses. Toutes les fois, il y avait une erreur dans la démonstration. Et du coup, un certain nombre de gens se sont mis vraiment à discuter ce postulat très sérieusement, et vers la fin du XVIII^{e} siècle il a commencé à y avoir avec Legendre et quelques autres des tentatives qui commençaient à être vraiment intéressantes sur ce postulat. En fait le premier qui probablement a compris qu'on pouvait construire des géométries sans ce postulat, c'est en fait Gauss. Mais vous savez, la devise de Gauss, c 'était "*Pauca sed matura*". ("*Peu de choses mais des choses mûres*".) donc il n'a pas publié à ce propos. Mais finalement, le scandale de l'existence de géométries non euclidiennes est arrivé avec Nikolaï Lobatchevski, qui était à ce moment-là recteur de l'université de Kazan. C'est très intéressant parce que pour Lobatchevski, quand il a parlé de publier son article sur les géométries non euclidiennes, qu'est-ce qu'il a pris comme mot "*géométrie imaginaire*". C'est tout à fait intéressant ; après, il a un autre article qui s'appelle la théorie des parallèles, c'est même un livre, justement où il développe que l'on peut faire une géométrie non euclidienne ; il prend le soin en discutant dans cet article qu'évidemment quand on fait des mesures dans l'espace qui nous entoure, on a l'impression qu'on est quand-même bien dans un espace euclidien, que ça, c'est une sorte de création un peu abstraite. Et ça ça a été vu quand même pendant longtemps comme un scandale, il y a même eu encore, sans vouloir insul-

ter mes ancêtres mathématiciens français, jusque vers 1870, parce que la théorie de la géométrie non euclidienne s'est beaucoup développée en Allemagne, aussi en Italie, et il y a quand même eu une note aux Comptes-Rendus, par un mathématicien français, professeur à l'école Polytechnique, disant que tout ça, c'était de l'intoxication par de la mathématique allemande. Donc vous voyez que le nationalisme peut se nicher dans des choses assez dramatiques. Donc en tout cas, il n'y a pas de doute qu'on peut construire des géométrie non euclidiennes. Donc déjà la notion d' espace euclidien comme seul géométrie pensable était battue en brèche. Donc voilà.

Donc ces géométries... Alors la chose extraordinaire, c'est qu'en fait, beaucoup de gens manipulaient des géométries non euclidiennes depuis très longtemps, en particulier les astronomes. Quand des astronomes regardaient la voûte céleste, ils ont développé même une trigonométrie pour la voûte céleste, pour calculer les positions des étoiles. En fait, ils développaient une géométrie qui est la géométrie sur la sphère. Si sur la sphère on appelle droites des grands cercles, en fait, on a une géométrie parfaitement conforme à la géométrie d'Euclide sauf le postulat des parallèles, puisqu'évidemment sur la sphère, je ne peux jamais tracer des parallèles par un point puisque tous les grands cercles se coupent. Donc voilà, le postulat des parallèles est violé, mais tous les autres postulats sont corrects, dans la géométrie non euclidienne sphérique. Et alors l'invention de Lobatchevski, c'est une géométrie hyperbolique comme on l'appelle, qui au contraire est dans le point de vue du postulat des parallèles exactement le contraire. C'est que par un point extérieur à une droite, alors à ce moment-là, une représentation possible, c'est de représenter l'espace comme l'intérieur d'un disque, et à ce moment-là de prendre comme droites les cercles qui sont orthogonaux au bord du disque. Et évidemment, si vous prenez un point extérieur au cercle, vous vous rendez compte qu'il y a une infinité de parallèles qui passent par ce point donc évidemment, vous violez le cinquième postulat d'Euclide. Donc ça c'est aussi une géométrie non euclidienne, extrêmement intéressante, particulièrement pertinente pour les informaticiens, puisque du point de vue des réseaux, c'est plutôt ce type de géométrie qui est pertinente. Ce que je voudrais dire, c'est qu'un pas très important dans la généralisation de la notion d'espace est venu chez Riemann. En plus dans un moment tout à fait particulier, puisque c'était en fait sa soutenance de thèse, et vous connaissez le système allemand qui a existé jusqu'à il y a très peu de temps, qui était qu'évidemment le candidat présentait ses résultats, mais il devait aussi présenter une leçon sur un des trois sujets proposés par la Faculté. Dans le jury de Riemann, il y avait Gauss qui a proposé un sujet sur justement les hypothèses sur lesquelles la géométrie est fondée. Et dans ce texte, donc, conçu en très peu de temps, Riemann à ce moment-là réfléchissait beaucoup à la théorie de l'éther de la physique, c'est-à-dire le substrat sur lequel toute la physique devait être fondée, donc il réfléchissait aussi à quelle géométrie est la géométrie de l'éther, en fait, il introduit une géométrie beaucoup plus générale et qui pousse l'idée de Descartes beaucoup plus loin, en disant mais en fait, on peut définir des géométries, à partir du moment où on se donne des coordonnées et on donne une façon de mesurer les longueurs, en chaque point mais qui varie en fonction du point. Et ce qui caractérise la géométrie euclidienne, c'est tout simplement que je peux trouver un système de coordonnées dans lequel je peux rendre ces coefficients, de cette façon de mesurer les longueurs, de cette métrique, constants. Et une façon de le mesurer, c'est par un invariant introduit par Riemann qui s'appelle la courbure, et donc un espace qui n'a pas de courbure est un espace euclidien, et tous les autres espaces ont de la courbure. Et les espaces non euclidiens, la sphère ou l'espace hyperbolique, sont très simples du point de vue de Riemann puisque ce sont des espaces dont la courbure est constante. Après ça, il y a plein d'autres objets, bien plus compliqués avec des

bossss, etc. et donc ça c'est une généralisation considérable de la notion d' espace. Et c'est très intéressant parce que dans le texte de Riemann, dans ce texte, là, dont vous voyez l'introduction, qui a été publié après sa mort, donc ça, c'est donc tout à fait significatif, Riemann a eu une vie très courte, il a en plus souffert dans la dernière partie de sa vie d'une tuberculose très marquée qui faisait qu'il était extrêmement affaibli, mais sa production était extraordinaire et donc je cite ce passage de Riemann enfin, la traduction française de ce passage, vraiment, entre parenthèses, si quelqu'un peut-être, c'est une chose qu'il faut que je fasse dans ma retraite, la traduction existante en français du texte de Riemann est particulièrement faible. Je veux dire, elle contient y compris des contresens, ce qui est quand même gênant. Elle remonte au début du XX^{e} siècle. En tout cas, voilà une traduction dont je pense qu'elle ne contient pas de contresens, en tout cas, j'espère.

> *Au contraire les occasions qui peuvent faire naître les concepts dont les modes de détermination forment une variété continue, (*donc c'est l'idée de ces espaces paramétrés par des nombres*) sont si rares dans la vie ordinaire que les positions des objets concrets et les couleurs sont à peu près les seuls concepts simples dont les modes de détermination forment une variété à plusieurs dimensions.*

Donc variétés à plusieurs dimensions, ça veut dire simplement qui peuvent être repérées par des collections de nombres. Alors pourquoi est-ce qu'il fait référence aux positions des objets concrets, eh bien tout simplement quand on remonte à Euler, il y a une chose dont vous avez peut-être entendu parler qui s'appelle les angles d'Euler, qui permettent de repérer la position d'un solide par rapport à un solide de référence, c'est très important, donc, ça veut dire qu'on peut repérer la position d'un solide par rapport à un autre par des nombres. Donc ça rentre dans la catégorie de Riemann et évidemment, c'est tout à fait important et chose très intéressante, c'est que Riemann parle de l'espace des couleurs. Et effectivement, on savait déjà à ce moment-là que du point de vue physiologique, la perception de la couleur était faite avec 3 détections donc il y avait trois couleurs fondamentales qui permettaient de recomposer, en tout cas pour l'œil, les couleurs. Alors faire attention parce que c'est effectivement 3 quantités mais ces quantités sont en fait des quantités qui sont plutôt des coordonnées dans un espace projectif, je sais que Karine Chemla va parler de l'espace projectif cet après-midi donc ça veut dire qu'elles sont déterminées à un coefficient près. Donc en fait, le vrai espace des couleurs, la chromaticité, c'est vraiment à deux dimensions, même si on dit souvent trois paramètres pour les repérer. Et après ça, comme vous savez, aujourd'hui, manipuler des couleurs est un objet fondamental du point de vue industriel, à cause des écrans, à cause de l'impression, donc c'est devenu un sujet extrêmement intéressant, mais c'est quand-même intéressant de voir que dans son texte aussi fondamental que ça, Riemann parle de l'espace des couleurs. Alors c'est intéressant aussi de voir qu'Hermann Weyl fait la même chose : il discute dans son livre sur la philosophie des mathématiques de l'espace des couleurs avec une certaine intensité.

Alors ce que je voudrais dire, c'est qu'en fait, Riemann a raté quand même quelque chose qui est qu'il y a vraiment quelqu'un qui a créé un espace vraiment nouveau, vraiment abstrait, qui est en fait Joseph-Louis de Lagrange. Donc ce texte qui remonte à 1808 est un texte extrêmement intéressant parce qu'à ma connaissance, c'est la première fois qu'un espace abstrait a été utilisé en mathématiques. Alors que faisait Lagrange ? Ça c'est une remarque que je voudrais faire, parce que je vous ai dit déjà pour Cardan quand il a introduit les imaginaires, c'était vraiment parce qu'il était embêté, il avait quelque chose à écrire et il n'avait pas les outils donc il a introduit les

nombres imaginaires et vous voyez que pour Joseph-Louis Lagrange, même s'il a vraiment compris quelque chose de très profond à propos de ce qu'il faisait, il le fait d'une certaine façon en passant : c'est-à-dire il a un problème en tête très précis, qui est le problème de la variation des éléments des planètes, c'est-à-dire on s'intéresse au mouvement des planètes autour du soleil et on essaye de le prévoir de la façon aussi précise qu'on peut. Alors on sait qu'il y a un mouvement très très simple : s'il y avait une seule planète autour du soleil, alors Kepler, Newton nous ont donné tous les outils pour trouver le mouvement des planètes. Le problème, c'est qu'il n'y a pas qu'une planète, il y en a plusieurs, donc les autres planètes viennent perturber le mouvement des planètes. Et donc cette perturbation évidemment rend les calculs beaucoup plus compliqués. Donc il y a eu toute une théorie des perturbations qui a été développée qui fait des choses remarquables mais malgré tout, par exemple une des choses qu'on n'arrive pas à prévoir, c'est est-ce qu'on peut anticiper qu'une planète va être éjectée du système solaire ou pas ? Donc ça, c'était un des sujets qui intéressait Lagrange et donc là, il développe une technique radicalement nouvelle pour le faire, et donc tout de suite dans son texte, il fait remarquer, voilà :

> "*On entend en astronomie par éléments un certain nombre de choses qui permettent de repérer les planètes*"

et simplement, il dit que :

> "*ces cinq quantités jointes* (à l'époque, donc l'époque, c'est la position d'une planète sur son orbite, donc c'est le moment de l'année, si vous voulez)*, étant connues pour une planète, on peut trouver en tout temps son lieu dans le ciel par le moyen de ces deux lois découvertes par Kepler que les aires décrites...*"

Alors après, il dit justement qu'après, il y a les perturbations qui viennent changer les choses. Et alors, il dit mais oui, en fait, utiliser ces coordonnées, dans cet espace, ce n'est pas ça qui va vous permettre de résoudre le problème. Et donc dans ce mémoire, il développe ce qu'il appelle, enfin, ce qu'il n'appelle pas, mais en tout cas ce qu'on peut appeler l'espace des mouvements elliptiques. Et la chose extraordinaire, c'est qu'il se rend compte, et en tout cas il l'introduit de façon très explicite, que cet espace des moments elliptiques est un espace à six dimensions qui ne sont pas seulement des objets disons concrets, mais aussi des objets abstraits. En fait, il démontre qu'étudier le mouvement dans l'espace à six dimensions, c'est infiniment plus facile que dans l'espace concret auquel on pense. Et pourquoi ? Parce que cet espace à six dimensions a de façon naturelle une géométrie radicalement nouvelle, qu'on appelle aujourd'hui une géométrie symplectique, qu'il décrit de façon remarquable dans son texte, et dans laquelle on peut écrire des équations d'une simplicité extraordinaire qui permettent de traiter, avec une seule fonction, qui est la fonction de perturbation, tout le mouvement de tout le système. Et donc ça veut dire qu'on transpose le mouvement habituel qui est le mouvement avec les trois positions dans l'espace plus les trois vitesses qui sont les six paramètres qui sont là, dans un autre espace à six dimensions qui est l'espace des mouvements elliptiques dans lequel la traduction des équations du mouvement devient extrêmement simple, à condition qu'on ait compris qu'il y a sous-jacente, pas une notion de distance, mais une notion qu'on appelle aujourd'hui de forme symplectique, qui est un objet anti-symétrique, alors que les objets de distance sont des objets symétriques. Et ce texte de façon extraordinaire est resté quand même largement incompris, inconnu, pendant longtemps : les gens utilisaient les résultats mais n'avaient pas compris qu'il y avait là un acte fondateur d'un nouveau secteur de la géométrie.

C'est intéressant dans des échanges de lettres entre Lagrange et Laplace, Laplace ne comprend absolument pas ce que fait Lagrange, avec tout le respect que j'ai pour Laplace bien entendu, qui a fait des choses extraordinaires, et donc il y a un espèce de dialogue de sourds. Lagrange avait absolument compris ce qu'il faisait, il fait remarquer d'ailleurs que, même si l'attraction de la gravitation, qui est la cause du mouvement, n'était pas donnée par les lois de Kepler, en fait, on a quand même un espace des mouvements, alors plus elliptique, évidemment puisque elliptique c'était parce que... Alors pourquoi cet espace est abstrait, tout simplement c'est à cause de la chose suivante : c'est que s'il n'y avait qu'une planète et le soleil, ce serait vraiment un mouvement elliptique. Mais il y a les perturbations des autres. Donc l'idée, c'est de se dire je vais tracer une trajectoire dans l'espace des mouvements elliptiques en me disant qu'à chaque moment la trajectoire réelle, en fait, elle a un contact maximum avec le fait de donc... on s'intéresse à la façon dont l'ellipse, qui devrait être le mouvement pur, est perturbée, par la présence des autres planètes.

Donc c'est ça cette idée superbe qui en fait a donné lieu à une nouvelle géométrie qui aujourd'hui est spectaculaire. Donc je vais terminer sur ce chapitre et j'arrive au dernier chapitre qui va me permettre de conclure, qui était de donner un exemple explicite d'un isomorphisme puisque c'est la chose qui est fondamentale chez les mathématiciens, qui est dans un livre que vient de publier Laurent Lafforgue qui est un livre de cours pour des professeurs du secondaire, peut-être un peu coriace, mais en tout cas remarquablement écrit, particulièrement pédagogique, sur justement deux mondes qui sont isomorphes au sens des mathématiciens, donc qui parlent de la même chose, qui sont d'un côté l'espace des plans affines, construits sur un corps quelconque, et d'un autre côté l'espace des corps au sens des mathématiciens, c'est-à-dire un espace, enfin un objet algébrique, dans lequel on a une addition, une multiplication, et toutes les opérations habituelles qu'on connaît, avec les propriétés qu'on connaît. Et en particulier, comment ces notions correspondent l'une avec l'autre, et donc la correspondance que je voulais vous faire voir, c'est donc ça.

Ça, c'est la propriété de Desargues, qui est une propriété fondamentale de la géométrie élémentaire. Donc qu'est-ce que vous vous donnez ? Donc regardez la situation du bas qui est peut-être plus simple. Je prends deux droites qui se coupent en un point P. Maintenant, je prends deux couples de parallèles, donc les parallèles Δ_3, Δ'_3 et puis Δ_1, Δ'_1. Eh bien le théorème de Desargues dit que les points d'intersection de ces parallèles avec les droites D_1, D_2, D_3 me permettent de créer justement, en pointillés, deux droites, et la propriété de Desargues est que ces droites sont parallèles. Donc ça, c'est à la base de la théorie des espaces affines, donc ça, c'est la première propriété, et la deuxième propriété est la propriété de Pappus : si je fais une construction qui est un petit peu analogue, mais pas tout à fait la même, je prends toujours mes deux droites de base D et D' qui se coupent en un point P, je prends maintenant deux droites parallèles Δ_1 et Δ_2, deux autres droites parallèles Δ'_1 et Δ'_2 ; eh bien vous voyez que je peux trouver de nouveau des droites en pointillés qui sont liées, là, au point d'intersection de ces familles de droites, eh bien, la propriété de Pappus, c'est d'affirmer que ces droites sont parallèles. Eh bien, la chose extraordinaire, c'est que si je me donne un plan affine à deux dimensions, qui vérifie la propriété de Desargues, alors si je m'intéresse dedans à toutes les transformations qui préservent les propriétés affines, je fabrique quelque chose qui est un corps et que le fait que ce corps soit commutatif, c'est-à-dire que les produits de deux éléments commutent, est directement lié à la propriété de Pappus. Donc le dictionnaire complet, c'est qu'étant donné un plan affine, je peux construire un corps ; connaissant un corps, je peux construire un plan affine, tout simplement en prenant les paires de nombres pris dans le corps, et

automatiquement ça vérifiera la propriété de Desargues, et si le corps est commutatif, ça vérifiera la priorité de Pappus. Donc voilà un exemple de deux mondes a priori différents, un totalement algébrique qui est la théorie des corps, un autre complètement géométrique qui est la théorie des plans affines, pour lesquels il y a un dictionnaire complet. Et donc ma conclusion, c'est donc de dire à quel point

> "*cette notion d'isomorphisme, (*là, je suis en train de citer Hermann Weyl*) est d'une importance capitale pour la théorie de la connaissance. On peut dire des domaines isomorphes qu'ils possèdent la même structure, (*et en fait les mathématiques, c'est la science des structures*). Pour toute proposition pertinente vraie au sujet du premier modèle, il y a une proposition correspondante et formulée de façon identique au sujet du second. C'est ainsi par exemple que l'espace est appliqué de manière isomorphe par l'utilisation des coordonnées de Descartes, domaine opératoire de l'algèbre linéaire. Et puis, l'exemple que je viens de donner pour la théorie des corps."*

Et donc, la chose après pour la théorie de la connaissance, qui est donc tout à fait importante à citer, donc je cite de nouveau Hermann Weil, cette fois dans un ajout de la version de 1949 :

> *"Une science ne peut établir son domaine de recherche que jusqu'à une application isomorphe ; elle reste totalement indifférente à l'essence de ses objets. l'idée d'isomorphisme marque à l'évidence la limite insurpassable du savoir."*

Merci.

Extrait du livre de Jean-Claude Carrega sur les points constructibles à la règle accompagnée, ici à la règle accompagnée du bissecteur

Chapitre IX : La règle accompagnée

Nous présentons dans ce chapitre les types de constructions les plus classiques utilisant conjointement la règle et un autre instrument ou procédé de construction. Les éléments que nous adjoindrons à la règle sont les suivants :

- L'équerre traceuse de parallèles
- L'équerre
- Un cercle donné dans le plan
- Le bissecteur
- Le transporteur de distance.

[...Sections 1 à 4...]

5. Règle et bissecteur. Pliages

5.1. Points constructibles à la règle et au bissecteur

Supposons que l'on dispose en plus de la règle, d'un instrument permettant de construire la bissectrice de n'importe quel angle donné. Un tel instrument est appelé *bissecteur*. Nous ne nous attarderons pas sur la réalisation technique d'un tel instrument car l'utilisation d'une règle et d'un bissecteur est en fait équivalente à l'utilisation des *pliages* effectués sur une feuille de papier :

- *pliage de première espèce*, effectué pour représenter par un pli la droite qui joint deux points donnés de la feuille.
- *pliage de seconde espèce*, par lequel on fait coïncider les deux côtés d'un angle. Le pli obtenu représente alors la bissectrice de l'angle.

Remarquons que si A est un point d'une droite D, la bissectrice de l'angle plat de sommet A porté par D est en fait la perpendiculaire en A à la droite D. Celle-ci peut donc être obtenue par le bissecteur ou les pliages.

Donnons nous deux points O et I d'un plan euclidien P et cherchons l'ensemble des points du plan P que l'on peut construire à partir de O et I à l'aide de la règle et du bissecteur.

Nous allons tout d'abord construire un repère du plan P. On trace la droite OI, puis les perpendiculaires en O et I à la droite OI. La bissectrice d'un angle droit de sommet I permet d'obtenir

---

Référence : *Théorie des corps, la règle et le compas*, Hermann, collection formation des enseignants, nouvelle édition, 1989, p. 140 et p. 156 à 163.
Avant la table des matières du livre nous est fournie la biographie très résumée de Jean-Claude Carrega : né en 1944 à Montélimar, il est agrégé de mathématiques ; il est maître de conférences à l'Université Claude-Bernard, Lyon I où il effectue, en outre, des recherches au Laboratoire de logique mathématique.
Transcription en LaTeX : Denise Vella-Chemla, novembre2025.

un point J de la perpendiculaire en O à la droite OI tel que $OI = OJ$. On obtient de même un point K tel que $OIKJ$ soit un carré. (O, I, J) est un repère orthonormé du plan P. Les côtés du carré $OIKJ$ nous fournissent deux couples de droites parallèles. Nous savons alors, d'après la construction C2 donnée en VIII.3, construire à la règle la parallèle à une droite donnée passant par un point donné. Nous savons que cette construction nécessite parfois l'emploi de points arbitraires (catalyseurs) qui ne sont ni des points de base ni des points déjà obtenus. Nous acceptons dans cette étude ce procédé de construction que nous limiterons à la construction de la parallèle à une droite donnée passant par un point donné.

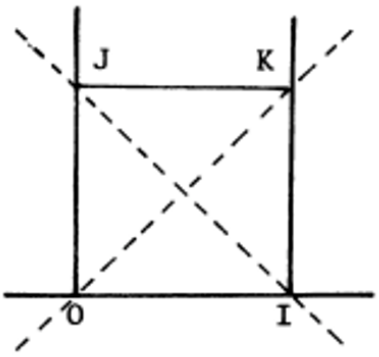


FIG. 98

Il est facile de deviner ce que nous appelons *point constructible et droite constructible à partir des points de base O et I à la règle et au bissecteur*. Donnons simplement la définition abrégée suivante :

- Un point constructible est un point d'intersection de deux droites constructibles.
- Une droite constructible est une droite d'un des trois types suivants :
  1) droite passant par deux points qui sont des points constructibles ou des points de base,
  2) droite passant par un point de base ou constructible et parallèle à une droite constructible,
  3) bissectrice d'un angle formé par deux droites constructibles.

Dans cette définition les droites du type 2) sont introduites pour tenir compte de l'utilisation de la construction C2.

THÉORÈME 1. *L'ensemble des coordonnées dans (O, I, J) des points du plan P constructibles à la règle et au bissecteur à partir des points de base O et I est un corps. Ce corps est le plus petit sous-corps de $\mathbb{R}$ qui soit pythagoricien.*

Précisons tout de suite qu'un *sous-corps* L de $\mathbb{R}$ est dit *pythagoricien* si quels que soient u et v dans L, $\sqrt{u^2 + v^2}$ est dans L. Notons l'ensemble des coordonnées dans (O, I, J) des points du plan P constructibles à la règle et au bissecteur à partir des points de base O et I.

- *$\mathscr{C}_b$ est un corps.* Puisque nous disposons de la construction C2, nous pouvons tracer à la règle la parallèle à une droite donnée passant par un point donné.

Nous pouvons alors reproduire les constructions qui ont permis de démontrer en IX.1 que $\mathscr{C}'_R$ est un corps. On obtient alors que :

- $\mathscr{C}_b$ est l'ensemble des abscisses des points constructibles de la droite OI.
- $\mathscr{C}_b$ est un corps (sous-corps de $\mathbb{R}$).
  - *$\mathscr{C}_b$ est pythagoricien.* Soient u et v dans $\mathscr{C}_b$. Nous allons démontrer que $\sqrt{u^2+v^2} \in \mathscr{C}_b$. On peut supposer $v \neq 0$. On a alors $\dfrac{u}{v} \in \mathscr{C}_b$ et $\dfrac{u}{v}$ est alors l'abscisse d'un point constructible de la droite OI. En traçant une parallèle à la droite OJ passant par ce point, on construit un point M de la droite JK d'abscisse $\dfrac{u}{v}$. La bissectrice de l'angle $\widehat{IOM}$ coupe la droite IK en N. On note $\alpha = \widehat{ION}$, on a alors : $\overline{IN} = \operatorname{tg}\alpha, \overline{JM} = \operatorname{cotan} 2\alpha = \dfrac{u}{v}$. Mais $2\alpha = \dfrac{1-\tan^2\alpha}{2\tan\alpha}$, d'où :

$$\tan^2\alpha + 2\frac{u}{v}\tan\alpha - 1 = 0$$

et

$$\begin{aligned}\tan\alpha &= -\frac{u}{v} \pm \sqrt{\frac{u^2}{v^2}+1} \\ &= -\frac{u}{v} \pm \frac{1}{|v|}\sqrt{u^2+v^2}.\end{aligned}$$

tan α est point constructible N d'où $-\dfrac{u}{v} \pm \dfrac{1}{|v|}\sqrt{u^2+v^2} \in \mathscr{C}_b$ et comme $\mathscr{C}_b$ est un corps contenant u et ν, on a aussi $\sqrt{u^2+v^2} \in \mathscr{C}_b$.

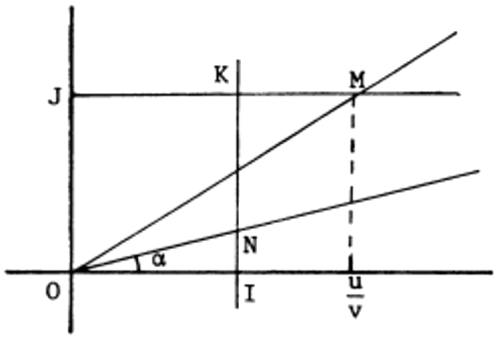


FIG. 99

- *$\mathscr{C}_b$ est le plus petit sous-corps pythagoricien de $\mathbb{R}$.*

  Soit L un sous-corps pythagoricien de $\mathbb{R}$. Nous allons démontrer que $\mathscr{C}_b \subset L$.

  Pour cela, il suffit de démontrer que toute droite constructible a une équation à coefficients dans L ; ce qui se fait par récurrence :

- La droite OI a bien sûr une équation $(y = 0)$ à coefficients dans L.
- Soit D une droite constructible, supposons par hypothèse de récurrence que les droites construites antérieurement à D ont des équations à coefficients dans L.

Les points construits antérieurement à D ont alors des coordonnées dans L et il en résulte que si D est du type 1 ou 2, elle a une équation à coefficients dans L.

Si D est du type 3, elle est bissectrice d'un angle formé par deux droites D_1 et D_2 qui ont des équations à coefficients dans L et dont le point d'intersection A a ses coordonnées dans L.

- Si $D_1 = D_2$, D est la perpendiculaire en A à D_1, qui a une équation à coefficients dans L.
- Si $D_1 \neq D_2$, notons $\overrightarrow{u_1}$ et $\overrightarrow{u_2}$ des vecteurs directeurs des demi-droites portés par D_1 et D_2 et qui sont les côtés de l'angle dont D est bissectrice. Puisque D_1 et D_2 ont des équations à coefficients dans L, on peut choisir $\overrightarrow{u_1}$ et $\overrightarrow{u_2}$ avec des composantes dans L :

$$\overrightarrow{u_1}\Big|\begin{matrix}\alpha_1\\ \alpha_2\end{matrix} \qquad\qquad \overrightarrow{u_2}\Big|\begin{matrix}\alpha_2\\ \beta_2\end{matrix}$$

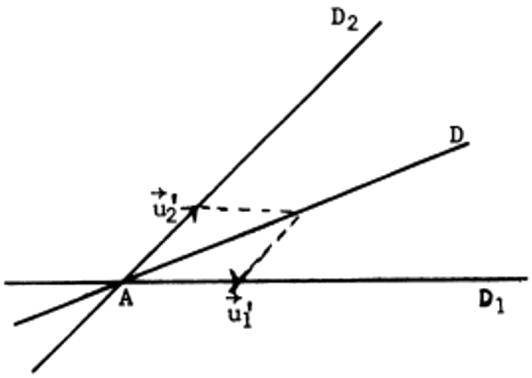


FIG. 100

Les vecteurs unitaires correspondant sont alors

$$\overrightarrow{u_1}' = \frac{\overrightarrow{u_1}}{\sqrt{\alpha_1^2 + \beta_1^2}} \qquad \text{et} \qquad \frac{\overrightarrow{u_2}}{\sqrt{\alpha_2^2 + \beta_2^2}}$$

Comme L est pythagoricien, ces vecteurs ont des composantes dans L ; il en est de même du vecteur $\overrightarrow{u_1}' + \overrightarrow{u_2}'$ qui est vecteur directeur de la bissectrice D. Il en résulte que D, qui passe d'une part par le point A à coordonnées dans L, a une équation à coefficients dans L.

Remarques. 1) Le théorème se généralise au cas de constructions avec plus de deux points de base. Si on désigne par $\alpha_1, \ldots, \alpha_n$ les coordonnées dans (O, I, J) des autres points de base, on obtient

que $\mathscr{C}$ est le plus petit sous-corps pythagoricien de $\mathbb{R}$ contenant $\alpha_1, \ldots, \alpha_n$.

2) On a bien sûr $\mathbb{Q} \subset \mathscr{C}_b$. On peut mettre en évidence d'autres éléments de $\mathscr{C}_b$, par exemple, $\sqrt{2}$ car $\sqrt{2} = \sqrt{1^2 + 1^2}$ et par récurrence sur n, $\sqrt{n} = \sqrt{1^2 + (\sqrt{n-1})^2}$.

3) Il est intéressant de comparer le corps $\mathscr{C}_b$ au corps des nombres constructibles à la règle et au compas introduit au chapitre II. C'est ce que nous faisons dans l'étude suivante.

5.2. Comparaison Règle-compas et Règle-bissecteur

Il est clair que $\mathscr{C}_b \subset \mathscr{C}$. Cela se voit géométriquement car la règle et le compas permettent de construire la bissectrice d'un angle ; cela se retrouve algébriquement car le corps $\mathscr{C}$, qui est stable par racine carrée, est a fortiori pythagoricien.

Le problème qui se pose alors est de savoir si les corps $\mathscr{C}_b$ et $\mathscr{C}$ coïncident ou bien si l'inclusion $\mathscr{C}_b \subset \mathscr{C}$ est stricte.

On pense que l'inclusion est stricte car a priori, $\mathscr{C}_b$ n'est stable que pour certaines racines carrées, celles qui portent sur une somme de carrés.

En fait comme D. Hilbert l'a démontré l'inclusion est bien stricte. Cela résultera immédiatement d'une propriété du corps $\mathscr{C}_b$ que nous allons maintenant établir.

PROPOSITION 1. *Si $\alpha \in \mathscr{C}_b$ et si $P(X) \in \mathbb{Q}[X]$ est le polynôme minimal de α sur $\mathbb{Q}$, toutes les racines de $P(X)$ sont dans $\mathscr{C}_b$.*

Soit β une autre racine de $P(X)$. On a a priori $\beta \in \mathbb{C}$, on va démontrer que $\beta \in \mathscr{C}_b$.

D'après X.2.2. théorème 3, il existe un isomorphisme de corps σ de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}(\beta)$ tel que $\sigma(\alpha) = \beta$.

D'après X.2.3. théorème 2, l'isomorphisme σ, que l'on peut considérer comme un isomorphisme de $\mathbb{Q}(\alpha)$ dans $\mathscr{C}_b$[1] se prolonge en un isomorphisme $\overline{\sigma}$ de $\mathscr{C}_b$ dans $\mathbb{C}$. Considérons alors l'ensemble $\overline{\sigma}^{-1}(\mathscr{C}_b) = \{x \in \mathscr{C}_b \ / \ \overline{\sigma}(x) \in \mathscr{C}_b\}$. On a $\overline{\sigma}^{-1}(\mathscr{C}_b) \subset \mathscr{C}_b$; il est facile de démontrer que $\overline{\sigma}^{-1}(\mathscr{C}_b)$ est un corps, c'est même un corps pythagoricien. En effet, si u et v sont dans $\overline{\sigma}^{-1}(\mathscr{C}_b)$, posons $w = \sqrt{u^2 + v^2}$, on a

$$\overline{\sigma}(w^2) = \overline{\sigma}(w)^2 = \overline{\sigma}(u)^2 + \overline{\sigma}(v)^2 \qquad \text{et} \qquad \overline{\sigma}(w) = \pm\sqrt{\overline{\sigma}(u)^2 + \overline{\sigma}(v)^2}.$$

Comme $\overline{\sigma}(u)$ et $\overline{\sigma}(v)$ sont dans $\mathscr{C}_b$ qui est pythagoricien, on a $\overline{\sigma}(w) \in \mathscr{C}_b$ et ainsi $w \in \overline{\sigma}^{-1}(\mathscr{C}_b)$.

Comme $\overline{\sigma}^{-1}(\mathscr{C}_b) \subset \mathscr{C}_b$ et que $\mathscr{C}_b$ est le plus petit sous-corps pythagoricien de $\mathbb{R}$, on a $\overline{\sigma}^{-1}(\mathscr{C}_b) = \mathscr{C}_b$.

Il en résulte que $\beta = \sigma(\alpha) = \overline{\sigma}(\alpha) \in \mathscr{C}_b$.

1. mal lisible.

THÉORÈME 1. *Les corps $\mathscr{C}$ et $\mathscr{C}_b$ sont distincts.*

La proposition précédente nous permet facilement de mettre en évidence des éléments de $\mathscr{C}$ qui ne sont pas dans $\mathscr{C}_b$.

Par exemple si $\alpha = \sqrt[4]{2}$, on sait que $\alpha \in \mathscr{C}$. Il est facile de voir que le polynôme minimal de α sur $\mathbb{Q}$ est $X^4 - 2$ (voir les critères d'irréductibilité en X.1.3.).

Les racines dans $\mathbb{C}$ de ce polynôme sont $\pm\sqrt[4]{2}$ et $\pm i\sqrt[4]{2}$, ces racines, qui ne sont pas toutes réelles, ne peuvent pas être toutes dans $\mathscr{C}_b$; la proposition précédente permet alors de dire que $\alpha = \sqrt[4]{2} \notin \mathscr{C}_b$.

Il est bien sûr facile de donner d'autres exemples : $\sqrt[4]{3}, \sqrt{\sqrt{2} - 1}$, etc.

REMARQUES SUR LA SIGNATURE D'UNE PERMUTATION

par P. Cartier (Strasbourg)

Introduction

La théorie des permutations est considérée par la plupart des débutants comme un sujet difficile. On y rencontre en effet des raisonnements d'un type assez différent de ceux auxquels ils ont été habitués dans leurs études antérieures. Il semble pourtant inévitable de l'enseigner dans un cours de première année d'Université, à cause des applications à la théorie des déterminants et à celle des polynômes symétriques.

Cette note est consacrée à un examen des diverses méthodes par lesquelles on peut introduire la signature d'une permutation. Nous avons nous-même expérimenté la plupart de ces méthodes, et discuté à plusieurs reprises de ces questions avec nos collègues J. L. Koszul et P. Gabriel. La comparaison des avantages et inconvénients des diverses méthodes s'appuie donc sur une expérience pédagogique réelle. Du point de vue mathématique, la seule nouveauté est la définition de la signature d'une permutation présentée au n° 4.

1. Permutations paires et impaires.

Rappelons les faits connus. Notons n un entier strictement positif et X l'ensemble des entiers $1, 2, ..., n$. Une permutation (de rang n) est une bijection s de X sur X, c'est-à-dire une application de X dans X telle que tout élément de X soit le transformé d'un élément et d'un seul. Si s et t sont deux permutations, leur produit st est l'application qui à i fait correspondre $s(t(i))$. La permutation identique ε associe chaque élément de X à lui-même. Enfin, si s est une permutation, la permutation inverse s^{-1} est telle que l'on ait $s^{-1}(i) = j$ si et seulement si $s(j) = i$. Avec cette définition du produit, de l'unité et de l'inverse, les permutations forment un groupe S_n.

Nous supposons connue la définition de la transposition s_{ij} ; échangeant i et j, et le fait que toute permutation est produit de transpositions ; en fait, nous utiliserons plusieurs fois le fait que toute permutation est produit d'une suite finie de transpositions de la forme $\pi_1, \ldots, \pi_{n-1}$ avec $\pi_i = s_{i,i+1}$.

Appelons permutation *paire* toute permutation qui est produit d'un nombre pair de transpositions, et notons S_n^+ leur ensemble ; définissons de manière analogue l'ensemble S_n^-, des permutations impaires. Ces définitions entraînent immédiatement les propriétés suivantes :

a) On a $S_n = S_n^+ \cup S_n^-$; autrement dit, toute permutation est paire ou impaire.

b) Il existe des permutations paires, par exemple ε, et des permutations impaires, par exemple les transpositions.

c) "Règle des signes" : le produit de deux permutations de même parité est pair, le produit de deux permutations de parité distincte est impair. De plus, toute permutation a même parité que son inverse.

L'enseignement mathématique, t. XVI, fasc. 2, 1970, p. 7-19.

A priori, rien n'exclut qu'une permutation puisse être à la fois paire et impaire. Examinons les deux possibilités :

A) Il n'existe aucune permutation à la fois paire et impaire. Alors les ensembles non vides S_n^+ et S_n^- forment une *partition* de S_n. On peut définir la *signature* d'une permutation s comme le nombre $sgn\ s$ égal à 1 si s est paire et à -1 si s est impaire. La règle des signes se traduit alors en formule:

(1) $$sgn\ st = (sgn\ s) \cdot (sgn\ t),$$

et par définition, on a

(2) $$sgn\ s_{ij} = -1.$$

B) Il existe une permutation qui est à la fois paire et impaire. Si a est une telle permutation, la règle des signes montre que a^{-1} est impaire, donc que $\varepsilon = aa^{-1}$ est impaire. Une nouvelle application de la règle des signes montre que pour toute permutation s paire (impaire), alors $s = \varepsilon s$ est impaire (paire). Autrement dit, toute permutation est paire et impaire, et l'on a $S_n^+ = S_n^- = S_n$.

De manière plus succincte, on peut dire ceci : le groupe S_n est engendré par les transpositions, qui sont des éléments d'ordre 2 ; l'ensemble S_n^+ des permutations paires est le sous-groupe de S_n engendré par les produits de deux transpositions, et S_n^- est de la forme $S_n^+ t$; on a donc $S_n = S_n^+ \cup S_n^+ t$, et par suite, ou bien S_n^+ est d'indice 2 dans S_n, et S_n^- est la classe modulo S_n^+ qui ne contient pas ε, ou bien S_n^+ est d'indice 1 dans S_n, auquel cas on a $S_n = S_n^+ = S_n^-$.

2. Relations entre transpositions.

Un résultat fondamental de la théorie des permutations est que le cas B) ne peut se présenter. Nous allons d'abord esquisser une démonstration directe, mais laborieuse. Nous avons déjà rappelé que le groupe S_n est engendré par $\pi_1, \ldots, \pi_{n-1}$; de plus, on établit facilement les relations suivantes entre ces transpositions

(3_a)	$\pi_i^2 = \varepsilon$	pour $1 \leq i \leq n-1$
(3_b)	$(\pi_i \pi_{i+1})^3 = \varepsilon$	pour $1 \leq i \leq n-2$
(3_c)	$(\pi_i \pi_j)^2 = \varepsilon$	lorsque $\lvert i-j \rvert \geq 2$.

Compte tenu de $\pi_i^2 = \varepsilon$, on peut écrire (3_b) et (3_c) sous la forme suivante qui est plus avantageuse

$(3'_b)$	$\pi_i \pi_{i+1} \pi_i = \pi_{i+1} \pi_i \pi_{i+1}$	pour $1 \leq i \leq n-2$
$(3'_c)$	$\pi_i \pi_j = \pi_j \pi_i$	lorsque $\lvert i-j \rvert \geq 2$.

L'existence de ces relations permet la transformation des produits de transpositions π_i. Dans un produit de telles transpositions, on peut, sans en changer la valeur, effectuer les opérations suivantes:

a) supprimer deux termes égaux qui se suivent, ou au contraire insérer deux nouveaux termes consécutifs égaux ;

b) remplacer un produit partiel du type $\pi_i \pi_{i+1} \pi_i$ par $\pi_{i+1} \pi_i \pi_{i+1}$ sans toucher aux autres termes (les trois termes modifiés doivent être consécutifs) ;

c) déplacer un terme π_i vers la gauche ou la droite, pourvu qu'il n'ait pas à sauter par-dessus π_{i-1} ou π_{i+1}.

Un théorème classique, dû à Moore (1897), affirme que les relations (3'$_a$), (3'$_b$) et (3'$_c$) suffisent à engendrer toutes les relations entre $\pi_1, ..., \pi_{n-1}$ dans S_n (cf. Burnside, [3], note C). Cela signifie que si les produits de deux suites de π_i représentent la même permutation, on passe de l'un à l'autre par une suite de transformations des types a), b) et c).

Illustrons ceci par un exemple. Nous considérons les deux produits

$$A = \pi_2\pi_1\pi_3\pi_6\pi_2\pi_3\pi_1\pi_6\pi_3\pi_4\pi_3\pi_6\pi_5\pi_4\pi_7$$
$$B = \pi_6\pi_7\pi_3\pi_2\pi_3\pi_4\pi_5\pi_1\pi_2\pi_3\pi_4$$

dans le groupe S_8. L'évaluation de ces produits est faite dans les deux tableaux suivants et obéit aux règles usuelles : le produit est effectué de la droite vers la gauche, une opération π_i fait passer d'une ligne à la suivante en échangeant les nombres i et $i+1$ (mais non pas les termes de rang i et $i+1$).

Calcul de A

	1	2	3	4	5	6	7	8
π_7	1	2	3	4	5	6	8	7
π_4	1	2	3	5	4	6	8	7
π_5	1	2	3	6	4	5	8	7
π_6	1	2	3	7	4	5	8	6
π_3	1	2	4	7	3	5	8	6
π_4	1	2	5	7	3	4	8	6
π_3	1	2	5	7	4	3	8	6
π_6	1	2	5	6	4	3	8	7
π_1	2	1	5	6	4	3	8	7
π_3	2	1	5	6	3	4	8	7
π_2	3	1	5	6	2	4	8	7
π_6	3	1	5	7	2	4	8	6
π_3	4	1	5	7	2	3	8	6
π_1	4	2	5	7	1	3	8	6
π_2	4	3	5	7	1	2	8	6

Calcul de B

	1	2	3	4	5	6	7	8
π_4	1	2	3	5	4	6	7	8
π_3	1	2	4	5	3	6	7	8
π_2	1	3	4	5	2	6	7	8
π_1	2	3	4	5	1	6	7	8
π_5	2	3	4	6	1	5	7	8
π_4	2	3	5	6	1	4	7	8
π_3	2	4	5	6	1	3	7	8
π_2	3	4	5	6	1	2	7	8
π_3	4	3	5	6	1	2	7	8
π_7	4	3	5	6	1	2	8	7
π_6	4	3	5	7	1	2	8	6

On voit donc que A et B sont tous deux égaux à la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 5 & 7 & 1 & 2 & 8 & 6 \end{pmatrix}$. Nous indiquons maintenant par un tableau une suite de transformations faisant passer de A à B ; nous avons omis d'inscrire les π dans les produits, en ne gardant que les indices.

		Règle
$A =$	2 1 3 6 2 3 1 $\overline{6\ 3}$ 1 3 4 3 6 5 4 7	
		c
	2 1 3 6 2 3 $\overline{1\ 3}$ 6 1 3 4 3 6 5 4 7	
		c
	2 1 3 6 2 $\overline{3\ 3}$ 1 6 1 3 4 3 6 5 4 7	
		a

$$
\begin{array}{ll}
2\,1\,3\,6\,2\,1\,6\,4\,\overline{3\,6}\,5\,4\,7 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
2\,1\,3\,6\,2\,1\,6\,\overline{4\,6}\,3\,5\,4\,7 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
2\,1\,3\,6\,2\,1\,\overline{6\,6}\,4\,3\,5\,4\,7 & \text{Migration de 6 vers la gauche} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad a & \\
2\,1\,\overline{3\,6}\,2\,1\,4\,3\,5\,4\,7 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
2\,\overline{1\,6}\,3\,2\,1\,4\,3\,5\,4\,7 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
\overline{2\,6}\,1\,3\,2\,1\,4\,3\,5\,4\,7 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,2\,1\,3\,2\,1\,4\,3\,5\,\overline{4\,7} & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,2\,1\,3\,2\,1\,4\,3\,\overline{5\,7}\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,2\,1\,3\,2\,1\,4\,\overline{3\,7}\,5\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,2\,1\,3\,2\,1\,\overline{4\,7}\,3\,5\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,2\,1\,3\,2\,\overline{1\,7}\,4\,3\,5\,4 & \text{Migration de 7 vers la gauche} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,2\,1\,3\,\overline{2\,7}\,1\,4\,3\,5\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,2\,1\,\overline{3\,7}\,2\,1\,4\,3\,5\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,2\,\overline{1\,7}\,3\,2\,1\,4\,3\,5\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,\overline{2\,7}\,1\,3\,2\,1\,4\,3\,5\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,7\,2\,\overline{1\,3}\,2\,1\,4\,3\,5\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,7\,2\,3\,\overline{1\,2\,1}\,4\,3\,5\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,7\,\overline{2\,3\,2}\,1\,2\,4\,3\,5\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,7\,3\,2\,3\,1\,\overline{2\,4}\,3\,5\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,7\,3\,2\,3\,\overline{1\,4}\,2\,3\,5\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,7\,3\,2\,3\,4\,1\,2\,\overline{3\,5}\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,7\,3\,2\,3\,4\,1\,\overline{2\,5}\,3\,4 & \text{Migration de 5 vers la gauche} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
6\,7\,3\,2\,3\,4\,\overline{1\,5}\,2\,3\,4 & \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad c & \\
B = \quad 6\,7\,3\,2\,3\,4\,5\,1\,2\,3\,4 &
\end{array}
$$

Montrons comment le théorème de Moore entraîne le résultat cherché sur la parité. Tout d'abord, la relation $s_{ij}\pi_i s_{i+1}\pi_i$ (pour $i \leq j-2$) entraîne par récurrence la formule

(4) $$s_{ij} = \pi_i\pi_{i+1}\dots\pi_{j-2}\pi_{j-1}\pi_{j-2}\dots\pi_{i+1}\pi_i \qquad \text{(pour } i < j\text{)}.$$

Par suite, toute transposition est produit d'un nombre impair de générateurs, et l'on peut définir

les permutations paires (impaires) comme les produits d'un nombre pair (impair) de générateurs π_i. Or, une transformation de type a) appliquée à un produit de π_i augmente ou diminue de deux le nombre des facteurs, alors que ce nombre de facteurs est inchangé par les transformations de type b) ou c). Une application des transformations de type a), b) ou c) ne peut donc modifier la parité du nombre des facteurs ; le théorème de Moore montre alors qu'un produit d'un nombre pair de π_i ne peut être égal à un produit d'un nombre impair de tels facteurs, donc qu'une permutation ne peut être à la fois paire et impaire.

3. Nombre d'inversions d'une permutation.

La démonstration du théorème de Moore est un peu délicate pour avoir sa place dans un cours élémentaire. L'intérêt de ce théorème est ailleurs ; il n'est en effet que le prototype de résultats s'appliquant à une vaste classe de groupes, les groupes de Coxeter, dont on rencontre de nombreuses applications géométriques. On peut consulter à ce sujet les monographies de Coxeter et Moser [5] et de Bourbaki [2].

Les méthodes que nous allons maintenant examiner ont toutes un point commun. Par un procédé ou un autre, on associe à toute permutation s un nombre $\alpha(s)$ égal à 1 ou -1 de telle sorte que l'on ait la relation

$$\alpha(st) = \alpha(s)\alpha(t) \tag{5}$$

pour deux permutations s et t. Il suffit alors de prouver que $\alpha(s)$ est égal à -1 pour une transposition s, ou même simplement de prouver la formule $\alpha(\pi_i) = -1$ pour $1 \leq i < n$; on en déduit en effet que $\alpha(s)$ est égal à 1 pour les permutations paires et à -1 pour les permutations impaires. On a ainsi distingué entre les deux espèces de permutations et indiqué un procédé de construction de la signature.

Un premier groupe de méthodes tourne autour de l'idée d'*inversion* d'une permutation. Rappelons quelques définitions: si $x_1, ..., x_n$, est une suite de n nombres réels distincts, une inversion de la suite est un couple extrait de la suite en question qui se trouve dérangé de l'ordre usuel ; autrement dit, c'est un couple $x_i x_j$ avec $i < j$ et $x_i > x_j$. Ainsi, dans la suite 6 3 1 2 4 5, les inversions sont les couples

$$6\,3\ ,\ 6\,1\ ,\ 6\,2\ ,\ 6\,4\ ,\ 6\,5\ ,\ 3\,1\ ,\ 3\,2.$$

Si s est une permutation, on note $N(s)$ le nombre d'inversions de la suite $s(1), ..., s(n)$; dans ce n°, on pose $\alpha(s) = (-1)^{N(s)}$.

A) La méthode la plus classique consiste à comparer $N(s)$ et $N(t)$ pour $t = s\pi_i$. La suite $t(1), ..., t(n)$ ne diffère de la suite $s(1), ..., s(n)$ que par l'échange des termes de rang i et $i+1$. Les couples que l'on peut extraire de la suite $t(1), ..., t(n)$ sont donc les mêmes que ceux que l'on peut extraire de la suite $s(1), ..., s(n)$, à l'exception de $s(i), s(i+1)$ qui est remplacé par $s(i+1), s(i)$. En passant de s à t, le nombre d'inversions est augmenté ou diminué d'une unité selon que l'on a $s(i) < s(i+1)$ ou $s(i) > s(i+1)$. En tout cas, on a $\alpha(s\pi_i) = -\alpha(s)$. Comme le nombre d'inversions de la permutation identique ε est nul, on en déduit par récurrence sur k la formule $\alpha(s) = (-1)^k$ si s est produit de k générateurs π_i. Par suite, $\alpha(s)$ vaut 1 pour les permutations paires et -1 pour les permutations

impaires[1].

B) On peut aussi considérer des fonctions de n variables $f(x_1, ..., x_n)$; la nature de ces variables est indifférente, il peut s'agir de nombres entiers, réels ou complexes, et l'on peut aussi considérer des polynômes formels à n indéterminées. Une permutation s de rang n transforme f en une nouvelle fonction sf par la règle

(6) $$(sf)(x_1, ..., x_n) = f(x_{s(1)}, ..., x_{s(n)}).$$

La suite du raisonnement repose sur la formule

(7) $$(st)f = s(tf)$$

où s et t sont deux permutations de rang n et f une fonction de n variables.

On introduit ensuite une fonction particulière D définie par

(8) $$D(x_1, ..., x_n) = \prod_{k<l}(x_k - x_l)$$

Pour passer de D à $\pi_i D$, il faut échanger x_i et x_{i+1} donc, remplacer $x_i - x_{i+1}$ par $x_{i+1} - x_i$, échanger les facteurs de la forme $x_k - x_i$ et $x_k - x_{i+1}$ pour $1 \leq k < i$, et échanger les facteurs de la forme $x_i - x_l$ et $x_{i+1} - x_l$ pour $i + 1 < l$; au total, on a $\pi_i D = -D$. Si s est le produit de k générateurs π_i, la formule (7) montre alors que l'on a $sD = (-1)^k D$; autrement dit, on a $sD = D$ si s est paire et $sD = -D$ si s est impaire. Comme la fonction D n'est pas identiquement nulle, une même permutation ne peut être à la fois paire et impaire.

Le raisonnement précédent a été présenté sans faire jouer de rôle explicite aux inversions. En fait, par un argument du même type, mais un peu plus délicat, on montre que dans le passage de D à sD, il y a permutation des facteurs et $N(s)$ changements de signe, d'où $sD = (-1)^{N(s)} D$.

C) Dans la méthode précédente, tant les variables $x_1, ..., x_n$ que les fonctions f jouent un rôle assez fictif. On peut en présenter une variante plus "économique" de la manière suivante. À chaque permutation s de rang n, on associe l'entier $\Pi(s) = \prod_{i<j}(s(j) - s(i))$. On remarque ensuite que, la permutation s étant fixée, toute partie à deux éléments de l'ensemble $X = \{1, 2, ..., n\}$ se représente de manière unique sous la forme $\{s(i), s(j)\}$ avec $i < j$; de plus, $|k - l|$ ne dépend évidemment que de la *partie* $\{k, l\}$. Par suite $\Pi(s) = \prod_{i<j} |s(i) - s(j)|$ est égal à $\prod_{\{k,l\}} |k - l| = \prod_{k<l}(l - k) = D$. De plus, dans le produit définissant $\Pi(s)$, les facteurs négatifs correspondent exactement aux inversions de la suite $s(1), ..., s(n)$. On en conclut

(9) $$\Pi(s) = \alpha(s) \cdot D.$$

On considère ensuite deux permutations s et t. Dans le produit

$$\frac{\Pi(st)}{\Pi(t)} = \prod_{i<j} \frac{s(t(j)) - s(t(i))}{t(j) - t(i)},$$

[1] Une variante consiste à comparer $N(s)$ et $N(ss_{ij})$ pour une transposition s_{ij} quelconque. Le principe est analogue, mais l'énumération des inversions de ss_{ij} est un peu plus compliquée.

chaque facteur est invariant par l'échange de i et j, et ne dépend donc que de la partie $\{t(i), t(j)\}$. On a donc

$$\frac{\Pi(st)}{\Pi(t)} = \prod_{\{k,l\}} \frac{s(l) - s(k)}{l - k} = \prod_{k<l} \frac{s(l) - s(k)}{l - k} = \frac{\Pi(s)}{D} = \alpha(s),$$

c'est-à-dire

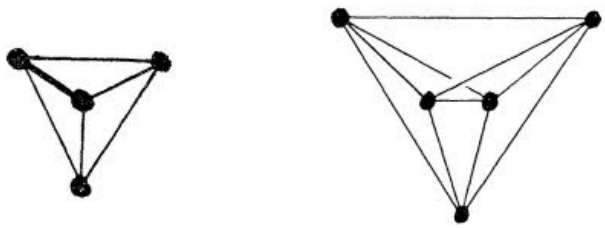
(10) $$\Pi(st) = \alpha(s)\Pi(t).$$

De (9) et (10), on déduit $\alpha(st) \cdot D = \Pi(st) = \alpha(s) \cdot \Pi(t) = \alpha(s)\alpha(t) \cdot D$, d'où $\alpha(st) = \alpha(s)\alpha(t)$ puisque D est non nul. On prouve ensuite que le nombre d'inversions de π_i est égal à 1, d'où $\alpha(\pi_i) = -1$. Comme on l'a déjà remarqué, cela suffit à montrer qu'une permutation ne peut être à la fois paire et impaire.

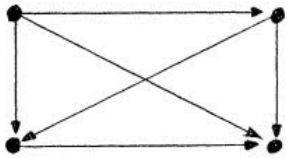
4. Permutations et graphes.

Comme J. L. Koszul me l'a fait plusieurs fois remarquer, l'inconvénient de la définition de la signature au moyen du nombre d'inversions est de dépendre étroitement de la relation d'ordre entre entiers ; de même, les transpositions π_i de deux entiers consécutifs jouent un rôle privilégié dans les démonstrations précédentes. Or, on a souvent besoin d'utiliser les permutations d'un ensemble fini X non numéroté à l'avance. Pour pouvoir définir le nombre d'inversions d'une permutation s de X, il faut choisir une énumération de X, ou ce qui revient au même une relation d'ordre total sur X. Le nombre d'inversions $N(s)$ dépend de ce choix, mais comme on le constate *a posteriori*, la parité de $N(s)$ a un caractère intrinsèque.

Pour répondre à cette objection, on peut présenter l'élaboration suivante de la méthode des inversions ; l'idée en est qu'il suffit d'orienter les parties à deux éléments pour définir les inversions. Nous adoptons un mode d'exposition fondé sur la notion de *graphe*. Soit donc X un ensemble fini à n éléments, que nous représentons par des points d'un plan appelés *sommets*. Deux sommets distincts sont joints par un arc, comme dans les deux figures suivantes, qui correspondent aux cas $n = 4$ et $n = 5$.



La figure ainsi obtenue s'appelle d'ordinaire le *graphe complet à n sommets*. Orienter un tel graphe consiste à choisir sur chaque arc un sens de parcours, représenté par une flèche dans l'exemple suivant :



Les arcs du graphe correspondent aux *parties* à deux éléments de X et orienter le graphe consiste à choisir dans chaque partie à deux éléments un premier et un deuxième élément. Il revient au même de dire qu'une *orientation* est un ensemble o de couples ordonnés (i, j) formés d'éléments distincts de X, tel que l'on ait, soit $(i, j) \in o$, soit $(j, i) \in o$ pour deux éléments distincts i et j de X. Une permutation s de X transforme l'orientation o en une nouvelle orientation so qui se compose des couples $(s(i), s(j))$ avec (i, j) dans o. De manière intuitive, s définit un réarrangement des sommets du graphe qui entraîne un réarrangement des arcs, et l'on transporte avec chaque arc son orientation.

Soient o et o' deux orientations ; soit m le nombre des arcs qui ont des orientations distinctes par rapport à o et o', c'est-à-dire le nombre des couples qui appartiennent à o', mais non à o ; on pose $d(o, o') = (-1)^m$. Le formulaire suivant s'établit par des raisonnements élémentaires[2]

(11) $$d(o, o) = 1$$

(12) $$d(o, o') = d(o', 0)$$

(13) $$d(o, o')d(o', o'') = d(o, o'')$$

(14) $$d(so, so') = d(o, o').$$

On peut alors prouver que $d(o, so)$ est indépendant de l'orientation o choisie ; en effet, si o et o' sont deux orientations, on a

$$\begin{aligned} d(o', so') &= d(o', o)d(o, so)d(so, so') && \text{d'après (13)} \\ &= d(o, o')d(o, so)d(o, o') && \text{d'après (12) et (14)} \\ &= d(o, so) && \text{car } d(o, o')^2 = 1. \end{aligned}$$

À toute permutation s de X, on fait correspondre alors le nombre $\alpha(s)$ qui est égal à $d(o, so)$ pour toute orientation o. Si s et t sont deux permutations, on a

$$\alpha(st) = d(o, st\, o) = d(o, to)d(to, s(to)) = \alpha(t)\alpha(s).$$

Pour calculer $\alpha(S_{ab})$, nous choisissons une orientation o convenable ; on oriente l'arc ab de a vers b, chaque arc ax de a vers x, chaque arc bx de b vers x et les autres arcs de manière arbitraire. Le seul effet de la transposition s_{ab} est de changer l'orientation de l'arc ab, d'où $\alpha(s_{ab}) = -1$.

On peut donc définir la signature de s comme le nombre $\alpha(s)$. Supposons en particulier que X soit l'ensemble des entiers $1, 2, ..., n$ et prenons pour o l'ensemble des couples (i, j) avec $i < j$; alors so se compose des couples de la forme $(s(i), s(j))$ avec $i < j$; les éléments de so qui n'appartiennent pas à o sont donc les couples $(s(i), s(j))$ avec $i < j$ et $s(i) > s(j)$ et leur nombre est égal à $N(s)$. On retrouve donc la définition de la signature comme égale à $(-1)^{N(s)}$.

5. Autres méthodes.

On peut aussi utiliser les *cycles* d'une permutation pour définir sa signature ([6], chap. 8). Soit $c(s)$ le nombre de cycles de la permutation s de rang n ; les définitions usuelles de la signature

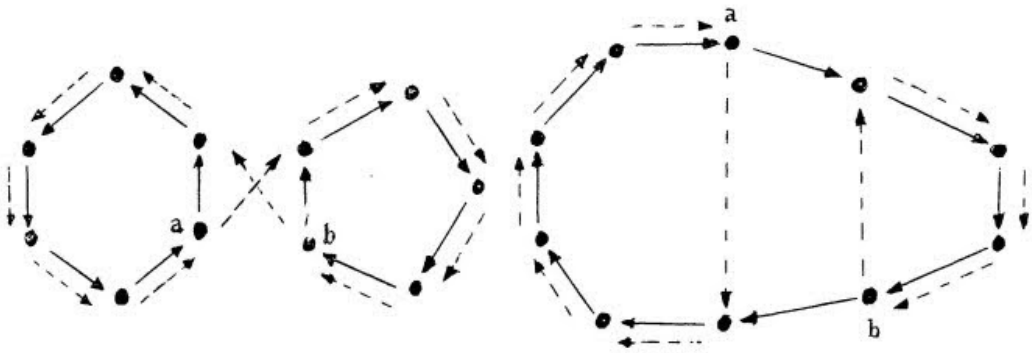
[2] On pourra consulter la note [4] pour des considérations plus générales.

permettent de prouver qu'elle est égale à $z(s) = (-1)^{n+c(s)}$. Si l'on veut *définir* la signature de s par le nombre $z(s)$, il faut établir *a priori* la relation

(15) $$c(ss_{ab}) = c(s) \pm 1.$$

En effet, cette relation entraîne $z(ss_{ab}) = -z(s)$; mais on a $c(\varepsilon) = n$, d'où $z(\varepsilon) = 1$ et il est alors immédiat que $z(s)$ est égal à 1 ou à -1 selon que s est paire ou impaire.

Pour établir la formule (15), il faut distinguer deux cas. Si a et b appartiennent à deux cycles distincts de s, ces deux cycles se regroupent en un seul cycle de ss_{ab}. Si au contraire, a et b appartiennent au même cycle de s, ce cycle se scinde en deux cycles de ss_{ab}. En tout état de cause, les cycles de s qui ne contiennent ni a ni b sont des cycles pour ss_{ab}. Les deux figures suivantes nous dispenseront de faire un raisonnement plus explicite[3].



Une dernière manière de procéder consiste à éviter le problème. Dans un cours élémentaire, la principale utilité de la signature d'une permutation est de permettre la définition du déterminant d'une matrice. Or, on peut définir directement les déterminants par récurrence sur leur ordre, en procédant par exemple par développement selon les éléments de la première colonne. Il n'est pas trop difficile de développer toute la théorie des déterminants à partir de cette définition, sans utiliser une seule fois les permutations. Une fois ceci fait, on définit la signature d'une permutation comme le déterminant de la matrice de permutation correspondante. La règle de multiplication pour les déterminants redonne alors la règle de multiplication des signatures pour les permutations. Cette méthode nous a été signalée par P. Gabriel, qui l'a utilisée plusieurs fois dans ses cours.

6. Considérations pédagogiques.

Les méthodes fondées sur le nombre d'inversions (ou la variante proposée au n° 4) reposent sur la distinction entre un *ensemble* à deux éléments et un *couple* ; cette distinction est capitale, mais assez délicate à saisir pour des débutants. Ces méthodes utilisent aussi la notion de réarrangement des termes d'un produit sous une forme assez subtile. Elles comportent enfin un aspect combinatoire important dans l'énumération des inversions. On connaît bien les difficultés d'exposition des

[3]On peut aussi montrer que la signature d'une permutation s est égale à $(-1)^{c'(s)}$ où $c'(s)$ est le nombre des cycles de longueur paire de s. Si l'on prend ceci comme définition de la signature, il faut montrer que $c'(ss_{ab})$ a une parité différente de celle de $c'(s)$. Les raisonnements sont analogues, mais il faut y ajouter quelques considérations de parité qui les rendent moins immédiatement évidents.

théories combinatoires ; si l'on peut se faire une idée assez nette des mécanismes en jeu sur un exemple bien explicité, il est difficile de formuler des raisonnements généraux et en particulier de s'assurer du caractère exhaustif de l'énumération des cas. Il y faut une imagination assez particulière qui ne se développe qu'à l'usage. Ces raisons expliquent la peine qu'éprouvent les débutants à suivre de tels raisonnements.

On peut aussi juger les méthodes précédentes sur leur économie de moyens. De ce point de vue, la méthode C) du n° 3 introduit le minimum de notions étrangères, mais sa sobriété la rend assez difficile à suivre. Bourbaki l'expose de manière concise dans [1], page 99 ; il emploie la notation trop suggestive $\pi(V_n)$ pour $\Pi(\pi)$, ce qui a induit en erreur certains de ceux qui l'ont recopié [7, page 153]. Parmi les notions étrangères que nous avons introduites, celle de permutation des variables dans une fonction se retrouvera inévitablement dans l'étude des polynômes symétriques ; celle de graphe me semble devoir être présentée le plus tôt possible aux étudiants, mais l'expérience m'a montré que la démonstration du n° 4 nécessitait beaucoup d'explications pour être comprise. Enfin, la notion de cycle d'une permutation me semble avoir sa place, même dans un cours introductif.

Toutes ces raisons nous font préférer la méthode de permutation des variables (cf. n° 3, B)) et celle des cycles à toutes les autres.

Bibliographie

[1] Bourbaki N., *Algèbre*, Chapitre I, 2e édition. Hermann, Paris, 1964.

[2] ----------, *Groupes et Algèbres de Lie*, Chapitres 4 à 6. Hermann, Paris, 1968.

[3] Burnside W., *Theory of groups of finite order*. Dover, New York, 1955.

[4] Cartier P., Sur une généralisation du transfert en théorie des groupes. Ce même volume, pp. 49-57.

[5] Coxeter H. et Moser W., Generators and relations for discrete groups. *Erg. der Math.*, Bd 14, Springer-Verlag (2e édition, 1965).

[6] Papy G., Groupes. Dunod, Paris 1964.

[7] Queysanne M., Algèbre. Armand Colin, Paris 1964.

Institut de recherche mathématique avancée
Rue René Descartes, 67
Strasbourg

(Reçu le 1er novembre 1969)

Sur les équations du 3ème et du 4ème degré : de Galois et Lagrange au miracle de Morley

Alain Connes et Jacques Dixmier

Résumé. Le Théorème de Morley en géométrie plane, associe à un triangle 18 triangles équilatères, construits à partir des intersections des trissectrices des angles. Nous généralisons ce théorème en un résultat sur les équations algébriques du troisième et du quatrième degré sur un corps K. Nous associons à un choix cohérent, parmi les 18 possibles, de racines cubiques des birapports des racines, une configuration *équiharmonique* de quatre éléments de la clôture algébrique de K.

L'espoir de trouver du nouveau sur les équations du troisième et du quatrième degré évoque irrésistiblement des chercheurs d'or des siècles passés égarés aujourd'hui à la quête de précieuses pépites dans les rues de San Francisco. Anachronisme sans doute, tant l'article de Lagrange de 1770 [4] semble mettre un point d'orgue à ce sujet.

Notre présentation, qui peut être considérée comme une initiation à la théorie de Galois dans ces cas simples, consiste à donner explicitement les transformations des racines qui proviennent, pour le degré trois de l'action transitive du sous-groupe distingué $A_3 \subset S_3$ et pour le degré quatre du sous-groupe distingué d'ordre 4, $M_4 \subset A_4 \subset S_4$. Cela révèle un lien étroit entre les formules obtenues et les invariants des formes binaires.

Tout cela prépare notre résultat principal qui est une généralisation, dans le cadre des équations du 3ème et du 4ème degré, du Théorème de Morley sur les 18 triangles équilatères associés à un triangle. Cette généralisation (Théorème S) associe à un choix cohérent, parmi les 18 possibles, de racines cubiques des birapports des racines, une configuration *équiharmonique*. Il est obtenu en utilisant la preuve algébrique [2] du théorème de Morley.

1. Introduction

Dans tout cet article k désigne un corps commutatif de caractéristique nulle, $\overline{k}$ une clôture algébrique de k et K, $k \subset K \subset \overline{k}$ une extension finie de k. Étant donnés trois éléments distincts $a, b, c \in K$ il existe une transformation affine $g \in A(K)$ unique telle que $g(b) = 1,\ g(c) = 0$. Elle transforme

Enseignement mathématique (2) 70, 2024, p. 283-306.
Reçu le 29 juin 2023.
Alain Connes, Collège de France, 3 rue d'Ulm, 75231 Paris, France ;
e-mail : alain@connes.org.
Jacques Dixmier, 11 bis rue du Val de Grâce, 75005 Paris, France.

(a,b,c) en $(\omega,1,0)$ où $\omega = \dfrac{a-c}{b-c}$. Aux six permutations de (a,b,c) correspondent les éléments de l'orbite de ω,

$$\left\{\omega, 1-\omega, \frac{1}{\omega}, \frac{\omega-1}{\omega}, \frac{1}{1-\omega}, \frac{\omega}{\omega-1}\right\}$$

sous l'action du groupe symétrique S_3 sur l'espace projectif $\mathbb{P}^1(K)$. Les orbites de S_3 dans $\mathbb{P}^1(K)$ sont de cardinal 6, sauf les orbites

$$\left\{-1, \frac{1}{2}, 2\right\}, \quad \{0,1,\infty\}, \quad \{-j,-j^2\},$$

où $1+j+j^2=0$. Si la fonction $V(a,b,c) = \dfrac{a-c}{b-c}$ prend six valeurs différentes quand on permute (a,b,c), il existe une transformation affine g, uniquement déterminée par le sous-ensemble $\{a,b,c\} \subset K$, et telle que l'on ait

$$g(a)+g(b)+g(c)=0, \quad \frac{1}{3}(g(a)^{-1}+g(b)^{-1}+g(c)^{-1}) = 1 \tag{1}$$

Nous commencerons par donner, dans la Section 2, Théorème A, les fractions rationnelles $R_j(\omega)$ qui expriment $g(a), g(b), g(c)$ en fonction de ω, et que l'on obtient en appliquant la méthode de Lagrange (que nous rappelons brièvement au début de la section). Nous montrons dans cette Section 2 comment marche la théorie de Galois pour l'équation du troisième degré quand on utilise la fonction $V(a,b,c)$ pour briser la symétrie entre les racines et que l'on suit sa méthode. C'est l'adjonction d'une racine carrée du discriminant Δ qui réduit le groupe de Galois au groupe alterné A_3 et nous donnons explicitement l'action de celui-ci sur les racines α, β, γ de l'équation $X^3+pX+q=0$ par la formule

$$\beta, \gamma = -\frac{\alpha}{2} \pm \frac{-4p^2+9q\alpha-6p\alpha^2}{2\sqrt{\Delta}} \tag{2}$$

Pour l'équation du quatrième degré nous avons obtenu un analogue de la formule (2) qui permet de passer d'une racine à une autre. Le groupe symétrique S_4 a ceci de particulier que le sous-groupe alterné $A_4 \subset S_4$ n'est pas un groupe simple. Il contient un sous-groupe distingué M_4 d'ordre 4, familièrement appelé le "groupe du matelas". C'est l'action transitive de ce sous-groupe sur les racines $(\alpha,\beta,\gamma,\delta)$ de l'équation

$$P(X) = X^4+pX^2+qX+r=0$$

que nous calculons. Le Corollaire B du Théorème A donne la solution. Ce corollaire montre que si les six birapports de quatre éléments $(\alpha,\beta,\gamma,\delta)$ d'un corps K sont distincts, il existe une unique transformation projective h de $\mathbb{P}^1(K)$ telle que $h(\alpha)=\infty$ et que $(h(\beta),h(\gamma),h(\delta))$ vérifient les conditions (1). Il donne de plus les fractions rationnelles $R_i(\omega)$ pour $(h(\beta),h(\gamma),h(\delta))$ en fonction du birapport ω de $(\alpha,\beta,\gamma,\delta)$. Or on vérifie que, α étant fixé, et en posant $\rho = P'(\alpha) = 4\alpha^3+2\alpha p+q$, $\sigma = \frac{1}{2}P''(\alpha) = 6\alpha^2+p$, la transformation projective

$$x \mapsto \frac{1}{x-\alpha} + \frac{\sigma}{3\rho}$$

a les propriétés requises pour h à une homothétie près. En comparant les formules obtenues pour $(h(\beta), h(\gamma), h(\delta))$ on obtient les transformations suivantes de α vers les trois autres racines

$$T_j(\alpha) := \alpha - P'(\alpha)\left(\frac{p}{3} + 12\frac{J}{I}R_j(\omega) + 2\alpha^2\right)^{-1} \tag{3}$$

où I et J sont des fonctions polynomiales explicites de p, q, r dont nous donnons l'interprétation géométrique connue en termes des invariants des formes binaires de degré quatre (voir Section 3.1). En fait, nous montrons comment arriver directement aux formules (3) donnant l'action de M_4 en utilisant un Lemme E classique qui donne les résolvantes $\alpha\beta + \gamma\delta, \alpha\gamma + \beta\delta, \alpha\delta + \beta\gamma$ en fonction du birapport ω.

Nous traitons en détail dans la Section 3.3 le cas particulier harmonique : quand les birapports des racines forment l'orbite $\{-1, \frac{1}{2}, 2\}$. Nous donnons les formules pour l'action du groupe de Galois de l'extension galoisienne $K = k(\alpha, \beta, \gamma, \delta)$ dans les trois cas possibles et montrons (Théorème I) que si K est de degré 2 sur le corps $k(\sqrt{\Delta})$, le groupe de Galois de K sur k est $\mathbb{Z}/4$.

Dans la Section 4.1, nous donnons l'interprétation géométrique, dans le cas du corps des complexes, d'une résolvante qui apparaît dans l'article [4] de Lagrange de 1770. Cette interprétation est en termes de l'intersection de quatre cercles circonscrits à des triangles dont deux sommets sont des racines et le troisième une intersection de diagonales du quadrilatère dont les sommets sont les racines.

Enfin nous terminons cet article par une généralisation du théorème découvert par Frank Morley en 1898, qui affirme que les intersections des trissectrices des angles d'un triangle forment un triangle équilatéral. Notre généralisation (Théorème S) s'énonce dans le cadre ci-dessus des équations algébriques de degré 3 et 4. On suppose que K possède une racine cubique $j \in K, j \neq 1$, de l'unité, et un automorphisme σ de K sur k tel que $\sigma(j) = j^2, \sigma^2 = \mathrm{Id}$. Nous introduisons (Définition R) la notion de "racine cubique des birapports" de quatre éléments $(\alpha, \beta, \gamma, \delta)$ de K. Cette extraction de racine cubique admet en général 18 solutions. Elles correspondent aux 18 triangles de Morley. Nous construisons une configuration équiharmonique avec les points fixes de produits de deux transformations projectives fixant deux racines et de valeur propre (plus précisément rapport de valeurs propres) donnée par les rapports $u/\sigma(u)$ des racines cubiques u des birapports.

2. L'équation du troisième degré

Le point de départ des travaux d'Abel et de Galois sur la théorie des équations est un lemme, implicite chez Lagrange, et que Galois énonce sous la forme suivante [1] :

(1) Etant donnée une équation quelconque, qui n'a pas de racines égales, dont les racines sont $a, b, c, ...$, on peut toujours former une fonction V des racines, telle qu'aucune des valeurs que l'on obtient en permutant dans cette fonction les racines de toutes manières ne soient égales.

(2) La fonction V étant choisie comme il est indiqué dans l'article précédent, elle jouira de cette propriété que toutes les racines de l'équation proposée s'exprimeront rationnellement en fonction de V.

L'équation en V, i.e., $Q(V) = 0$, où le polynôme Q,

$$Q(X) = \prod_{\sigma}(X - V(\sigma(a), \sigma(b), ..., \sigma(z)))$$

s'exprime en fonction des coefficients de l'équation proposée, a la propriété particulière suivante : si x est l'une quelconque de ses racines, toute autre racine s'écrit $R(x)$ où R est une fonction rationnelle à coefficients dans le corps k des coefficients de l'équation. En particulier, il suffit d'adjoindre formellement une racine de cette équation, en travaillant avec l'algèbre des polynômes modulo les multiples de Q, pour adjoindre en fait toutes les racines. En général, Q n'est pas irréductible et Galois note que, de même, les racines de l'équation $Q_1(V) = 0$ obtenue à partir d'un facteur irréductible de l'équation en V, sont fonctions rationnelles de l'une quelconque d'entre elles et que (en travaillant modulo Q_1) ces fonctions forment un groupe pour la composition. Ce qui est loin d'être évident à ce stade est que ce groupe est en fait indépendant des choix effectués, en particulier celui de la fonction auxiliaire $V(a, b, ...)$ et ne dépend donc que de l'équation proposée. Cette indépendance est un point crucial de la théorie de Galois.

Pour l'équation du troisième degré, Lagrange utilise la résolvante

$$V(a, b, c) = a + jb + j^2c$$

où j est racine cubique de l'unité et montre que l'équation de degré 6 ayant pour racines les 6 valeurs de V obtenues en permutant dans cette fonction les racines de toutes manières, ne fait intervenir que X^3 et X^6 et donc se ramène au degré 2. Comme on le sait, il est indispensable d'utiliser les nombres complexes pour résoudre par radicaux une équation de degré 3 dont les trois racines sont réelles, et ce cas là est en effet à l'origine de l'utilisation des nombres complexes.

Soit

$$\Omega := \frac{4}{27}\frac{(1 - \omega + \omega^2)^3}{\omega^2(1-\omega)^2} \tag{4}$$

Alors Ω est un invariant de l'orbite de l'action de S_3

$$\left\{\omega, 1 - \omega, \frac{1}{\omega}, \frac{\omega - 1}{\omega}, \frac{1}{1 - \omega}, \frac{\omega}{\omega - 1}\right\} \tag{5}$$

Etant donnée une équation du $3^{\text{ème}}$ degré, irréductible à coefficients dans k, dont les racines ne forment pas les sommets d'un triangle équilatère, on peut, par une transformation affine à coefficients dans k, mettre l'équation sous la forme

$$X^3 - 3sX + s = 0 \tag{6}$$

On a en effet $p \neq 0$ une fois l'équation mise sous la forme $x^3 + px + q = 0$ et il suffit de multiplier les racines par $-\frac{1}{3}\frac{p}{q} \neq 0$ pour que le barycentre de leurs inverses soit égal à 1, i.e., que l'équation soit de la forme indiquée.

Quels que soient les éléments $\alpha, \beta, \gamma, \delta \in K \cup \{\infty\}$ nous noterons leur birapport

$$\langle \alpha, \beta, \gamma, \delta \rangle := \frac{\alpha - \gamma}{\beta - \gamma} / \frac{\alpha - \delta}{\beta - \delta}.$$

Nous montrons, pour l'équation sous la forme (6), qu'il existe une fonction rationnelle explicite $V(a, b, c)$ (7), des racines qui donne une forme universelle simple de l'équation $Q(V) = 0$ des fonctions rationnelles $R_j(V)$ et des transformations rationnelles de l'équation $Q(V) = 0$ en les reliant directement à l'action ci-dessus de S_3 sur l'espace projectif. On a le

Théorème A. *Considérons l'équation (6).*

(i) L'équation $Q(V) = 0$ associée à la fonction rationnelle des trois racines de (6)

$$V(a, b, c) = \frac{a - c}{b - c} = \langle a, b, c, \infty \rangle \tag{7}$$

est la suivante, où $\Omega = \dfrac{4s}{4s - 1}$

$$Q(V) = (1 - V + V^2)^3 - \frac{27}{4} \Omega V^2 (1 - V)^2 \tag{8}$$

(ii) *Les trois racines de l'équation (6) sont les fonctions rationnelles suivantes de* V*,*

$$R_1(V) = -\frac{V^2 - V + 1}{(V - 2)(V + 1)}$$

$$R_2(V) = \frac{V^2 - V + 1}{2(V - \frac{1}{2})(V + 1)} \qquad R_3(V) = \frac{V^2 - V + 1}{2(V - 2)(V - \frac{1}{2})}$$

(iii) *Les transformations rationnelles des racines de (8) de la forme*

$$V \mapsto V(R_i(V), R_j(V), R_k(V)), \tag{9}$$

où (i, j, k) *est une permutation de* $(1, 2, 3)$*, sont données par l'action (5) du groupe symétrique* S_3 *dans l'espace projectif d'une clôture*[1] *algébrique de* k*.*

Les six valeurs de V obtenues en permutant (a, b, c) en $(p(a), p(b), p(c))$ sont les six valeurs des birapports $\langle p(a), p(b), p(c), \infty \rangle$ et forment une orbite de l'action de S_3 sur $\mathbb{P}^1(K)$ dont l'invariant est donné par Ω. On vérifie ensuite que la somme des $R_j(V)$ est égale à 0 et que la somme des $1/R_j(V)$ est égale à 3 alors que le produit vaut

$$\prod R_j(V) = -\frac{(V^2 - V + 1)^3}{(1 - 2V)^2 (V - 2)^2 (V + 1)^2}$$

ce qui donne

$$\frac{4s}{4s - 1} = \frac{4(V^2 - V + 1)^3}{27(V - 1)^2 V^2} = \Omega$$

[1] Note DCV : extension ?

On vérifie également que pour $V = \dfrac{a-c}{b-c}$, on a $R_1(V) = a$ en utilisant les relations $a+b+c = 0$ et $1/a+1/b+1/c = 3$. Les transformations (9) sont celles du birapport $\langle a, b, c, \infty\rangle$ quand on permute (a, b, c), i.e., plus précisément

$$\begin{pmatrix} \{1,2,3\} & \omega \\ \{1,3,2\} & 1-\omega \\ \{2,1,3\} & \dfrac{1}{\omega} \\ \{2,3,1\} & \dfrac{\omega-1}{\omega} \\ \{3,1,2\} & \dfrac{1}{1-\omega} \\ \{3,2,1\} & \dfrac{\omega}{\omega-1} \end{pmatrix}$$

Comme la fonction $V(a, b, c)$ est invariante par le groupe affine, on note que c'est aussi le cas pour les fonctions $R_j(V(a, b, c))$ qui ont donc comme propriété de normaliser le triplet (a, b, c) de telle sorte que sa somme soit nulle et que le barycentre des inverses soit égal à 1. Cette normalisation du triplet (a, b, c) est effectuée par une unique transformation affine et de plus celle-ci est à coefficients dans le corps des fonctions symétriques de (a, b, c).

Corollaire B. *Soient $\alpha, \beta, \gamma, \delta \in K$ quatre éléments dont les birapports prennent six valeurs distinctes. Il existe une unique transformation projective $g \in \mathrm{PGL}_2(K)$ telle que $g(\delta) = \infty$ et que*

$$g(\alpha) + g(\beta) + g(\gamma) = 0, \quad \frac{1}{3}(g(\alpha)^{-1} + g(\beta)^{-1} + g(\gamma)^{-1}) = 1 \tag{10}$$

De plus si ω désigne l'un des birapports de $\alpha, \beta, \gamma, \delta$, alors $\{g(\alpha), g(\beta), g(\gamma)\} \subset K$ est égal au sous-ensemble $\{R_j(\omega) | 1 \leq j \leq 3\} \subset K$.

L'existence résulte du Théorème A. Pour montrer l'unicité, on se ramène au cas $\delta = \infty$ et l'on voit que l'identité est la seule transformation affine qui préserve les conditions (10). La deuxième partie résulte du Théorème A.

Nous montrons dans la Section 3 comment utiliser ce corollaire pour passer d'une racine à l'autre pour l'équation générale du quatrième degré.

Pour obtenir le groupe de Galois de l'équation (6), il faut décomposer le polynôme $Q(V)$ de (8) en facteurs irréductibles. On obtient facilement en utilisant l'action du sous-groupe $A_3 \subset S_3$ la factorisation

$$\begin{aligned} Q(X) &= (X^3 - tX^2 + (t-3)X + 1)(X^3 + (t-3)X^2 - tX + 1) \\ &= Q_1(X)Q_2(X) \end{aligned}$$

à condition que $t = \frac{3}{2}(1 \pm \sqrt{3}\sqrt{\Omega - 1})$. L'adjonction de t correspond à celle d'une racine carrée du discriminant $\Delta = 27s^2(4s-1)$ de (6).

Par construction le groupe A_3 agit sur les racines de l'équation $Q_1(X) = 0$ par la transformation d'ordre 3, $\omega \mapsto \dfrac{1}{1-\omega}$; les racines donnent les trois branches $(\alpha(t), \beta(t), \gamma(t))$ de la fonction inverse de la fonction suivante

$$\Omega_1 := \frac{1 - 3 + \omega^3}{\omega(\omega - 1)} \tag{11}$$

Remarque C. Si le corps de base est contenu dans $\mathbb{R}$, les trois branches sont, pour $t \in \mathbb{R}$, réelles et définies sans ambiguité par les conditions $\alpha(t) > 1 > \beta(t) > 0 > \gamma(t)$. Alors α, β, γ donnent des isomorphismes analytiques croissants

$$\alpha : \mathbb{R} \to (1, \infty), \quad \beta : \mathbb{R} \to (0, 1), \quad \gamma : \mathbb{R} \to (-\infty, 0).$$

On a

$$\beta(t) = 1 - \frac{1}{\alpha(t)}, \quad \gamma(t) = \frac{1}{1 - \alpha(t)}, \quad \beta(t) + \beta(3 - t) = 1, \quad \gamma(3 - t) + \alpha(t) = 1,$$

de plus $\alpha(t) = t - 1 + o(1)$ quand $t \to +\infty$, et $\gamma(t) = t - 1 + o(1)$ quand $t \to -\infty$.

On vérifie que, comme le groupe de Galois agit de manière rationnelle sur les racines de l'équation $Q_1(X) = 0$, le discriminant Δ de Q_1 est un carré. On a $\Delta = (t^2 - 3t + 9)^2$. Plus généralement la Proposition D donne la matrice de l'action du groupe de Galois dans la base $(1, X, X^2)$ en fonction de la racine carrée du discriminant, ce qui montre en particulier que si l'action du groupe de Galois est rationnelle, le discriminant est un carré. Plus précisément, soient $p, q \in k$ et $P(X) := X^3 + pX + q \in k[X]$. Soient α, β, γ, les racines de $P(X) = 0$ et Δ le discriminant de P :

$$\Delta = -4p^3 - 27q^2.$$

On suppose une fois pour toutes $\Delta \neq 0$, les racines sont donc distinctes.

Proposition D. *Avec les notations ci-dessus, on a les égalités*

$$\beta, \gamma = -\frac{\alpha}{2} \pm \frac{-4p^2 + 9q\alpha - 6p\alpha^2}{2\sqrt{\Delta}}. \tag{12}$$

La matrice de l'automorphisme de Galois d'ordre 3 de $k(\sqrt{\Delta})[x]/P$ est donnée par

$$\begin{pmatrix} 1 & 0 & 0 \\ \dfrac{2p^2}{\sqrt{\Delta}} & -\dfrac{9q}{2\sqrt{\Delta}} - \dfrac{1}{2} & \dfrac{3p}{\sqrt{\Delta}} \\ \dfrac{3pq}{\sqrt{\Delta}} - p & \dfrac{p^2}{\sqrt{\Delta}} & \dfrac{9q}{2\sqrt{\Delta}} - \dfrac{1}{2} \end{pmatrix}$$

On arrive facilement à ce résultat de la façon suivante : on a

$$\sqrt{\Delta} = (\alpha-\beta)(\alpha-\gamma)(\beta-\gamma) = (\beta-\gamma)(\alpha^2-\alpha(\beta+\gamma)+\beta\gamma) \tag{13}$$

et en utilisant $\alpha+\beta+\gamma=0$ et $\alpha(\beta+\gamma)+\beta\gamma=p$, (13) donne

$$\sqrt{\Delta} = (\beta-\gamma)(3\alpha^2+p)$$

d'où

$$\alpha+2\beta = \frac{\sqrt{\Delta}}{3\alpha^2+p}, \tag{14}$$

qui donne β en fonction rationnelle de $\alpha, p, q, \sqrt{\Delta}$ et se réécrit sous la forme (12) en utilisant $P(\alpha)=0$ pour inverser $(3\alpha^2+p)$ (i.e., $(3x^2+p)$ dans $k(\sqrt{\Delta})[x]/P$) ce qui donne

$$\frac{1}{3\alpha^2+p} = -\frac{1}{\Delta}(6p\alpha^2-9q\alpha+4p^2), \tag{15}$$

(12) résulte alors de (14) et (15).

La matrice de l'automorphisme d'ordre 3 de $k(\sqrt{\Delta})[x]/P$ s'en déduit.

3. L'équation du quatrième degré

Il s'agit ci-dessous d'expliciter, comme dans la Proposition D dans le cas du 3ème degré, l'action du groupe M_4 sur les racines d'une équation du quatrième degré, après adjonction du birapport des racines, laquelle réduit le groupe de Galois au groupe M_4. Cette réduction a lieu sauf quand les birapports des racines forment l'orbite $\{-1, \frac{1}{2}, 2\}$ (cas harmonique) ou $\{-j, -j^2\}$ (cas équiharmonique) et nous traitons séparément ces deux cas.

3.1. Rappels, formes binaires de degré 4. Cette section contient des rappels concernant les formes binaires, voir [3]. Considérons les formes binaires de degré 4 à coefficients dans k :

$$\phi(X,Y) = aX^4+4bX^3Y+6cX^2Y^2+4dXY^3+eY^4.$$

Elles constituent un k-espace vectoriel W de dimension 5. Le groupe $G=GL(2,k)$ opère naturellement sur $kX\oplus kY$ et donc dans W. L'annulation de ϕ définit un faisceau de 4 droites à condition de passer à la clôture algébrique $\overline{k}$ de k.

Considérons maintenant a, b, c, d, e comme des indéterminées. Dans $k[a,b,c,d,e]$ le groupe G agit naturellement. La sous-algèbre des invariants sous $SL(2,k)$ est engendrée par les polynômes I et J suivants, qui sont algébriquement indépendants

$$I = ae-4bd+3c^2, \quad J = \mathrm{Det}\begin{pmatrix} a & b & c \\ b & c & d \\ c & d & e \end{pmatrix}$$

Considérons les G-orbites dans $W\backslash\{0\}$. Il y a 3 orbites exceptionnelles C_4, C_5, C_6 qui sont des cônes de dimensions 3, 3, 2. Ignorons-les désormais et supposons provisoirement $k = \overline{k}$. Les autres orbites sont des cônes de dimension quatre. Si on leur adjoint l'origine, ils sont fermés sauf un seul, C_3 (dont le bord est $C_4 \cup C_5 \cup C_6$). Il y a trois cônes remarquables :

- C_1 correspondant aux faisceaux harmoniques de quatre droites ;
- C_2 correspondant aux faisceaux équiharmoniques de quatre droites ;
- C_3 (déjà introduit) correspondant aux faisceaux qui ont une droite double.

La valeur de J^2/I^3 repère bijectivement les orbites de dimension quatre. Cette valeur est 0 sur C_1, ∞ sur C_2, $\frac{1}{27}$ sur C_3.

Le discriminant de ϕ est le discriminant, multiplié par a^6 du polynôme $\frac{1}{a}P(X)$ où

$$P(X) := aX^4 + 4bX^3 + 6cX^2 + 4dX + e. \tag{16}$$

Il vaut $\Delta = 2^8(I^3 - 27J^2)$.

Soient $\alpha, \beta, \gamma, \delta \in \overline{k}$ les inverses des pentes des quatre droites du faisceau. Ainsi $\alpha, \beta, \gamma, \delta$ sont aussi les racines du polynôme $P(X)$ de (16), avec une racine égale à ∞ si $a = 0$ (dans ce cas la droite $Y = 0$ fait partie du faisceau).

Les invariants I et J s'expriment en fonction de $\alpha, \beta, \gamma, \delta$: en posant

$$u = (\alpha - \beta)(\gamma - \delta), \quad v = (\alpha - \gamma)(\delta - \beta), \quad w = (\alpha - \delta)(\beta - \gamma),$$

on a alors ([3]),

$$I = \frac{a^2}{24}(u^2 + v^2 + w^2), \qquad J = \frac{a^3}{432}(u - v)(v - w)(w - u)$$

Posons $K = k(\alpha, \beta, \gamma, \delta) \subset \overline{k}$. Pour a, b, c, d, e génériques, K est une extension galoisienne de k de degré 24 de groupe de Galois S_4. Soit $K_1, k \subset K_1 \subset K$ le sous-corps des éléments de K invariants par A_4. On a $K_1 = k(\sqrt{\Delta})$. Définissons K_2 où $k \subset K_1 \subset K_2 \subset K$, comme le sous-corps des éléments de K invariants par M_4. C'est une extension galoisienne de degré 3 de K_1 et K est une extension galoisienne de K_2 de degré 4 et de groupe de Galois M_4.

Soient $\omega_j, 1 \leq j \leq 6$ les birapports de $\{\alpha, \beta, \gamma, \delta\}$ ils forment une orbite de l'action de S_3 sur $\mathbb{P}^1$ et soit Ω défini en (4), on a alors

$$\Omega = \frac{I^3}{I^3 - 27J^2} = 2^8\frac{I^3}{\Delta}.$$

On a donc $K_1 = k(\sqrt{\Delta}) = k(\sqrt{3(\Omega - 1)}) = k(\Omega_1)$ avec Ω_1 défini en (11).

Lemme E. *Soient $\omega = \langle \alpha, \beta, \gamma, \delta \rangle, R_j(V)$ les trois fonctions du Théorème A. On a*

$$\begin{aligned} \alpha\delta + \beta\gamma &= \frac{2c}{a} + 12\frac{J}{aI}R_1(\omega), \\ \alpha\gamma + \beta\delta &= \frac{2c}{a} + 12\frac{J}{aI}R_2(\omega), \\ \alpha\beta + \gamma\delta &= \frac{2c}{a} + 12\frac{J}{aI}R_3(\omega). \end{aligned} \tag{17}$$

Il s'agit d'un simple calcul en remplaçant dans I et J les termes a, b, c, d, e comme fonctions symétriques de $\{\alpha, \beta, \gamma, \delta\}$.

3.2. Action du groupe M_4 sur les racines. Soient $p, q, r \in k$

$$P(X) := X^4 + pX^2 + qX + r \in k[X].$$

On va étudier l'équation

$$P(X) = 0. \tag{18}$$

Soient $\alpha, \beta, \gamma, \delta$ les racines de (18), et Δ le discriminant de P. On a

$$\Delta = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3.$$

On suppose une fois pour toutes $\Delta \neq 0$, les racines sont donc distinctes.

L'invariant I de la forme homogénéisée de P est

$$I = r + 3\left(\frac{p}{6}\right)^2 = \frac{1}{12}(p^2 + 12r).$$

Donc la condition $p^2 + 12r = 0$ signifie que $\{\alpha, \beta, \gamma, \delta\}$ est équiharmonique. Ce cas sera traité dans la Section 3.4. Pour l'instant, on suppose

$$p^2 + 12r \neq 0.$$

L'invariant J de la forme homogénéisée de P est

$$\begin{pmatrix} 1 & 0 & p/6 \\ 0 & p/6 & q/4 \\ p/6 & q/4 & r \end{pmatrix} = 2^{-4}3^{-3}(-2p^3 + 72pr - 27q^2).$$

La condition $-2p^3 + 72pr - 27q^2 = 0$ signifie que $\{\alpha, \beta, \gamma, \delta\}$ est harmonique. Ce cas sera traité dans la section 3.3. Pour l'instant, on suppose $-2p^3 + 72pr - 27q^2 \neq 0$.

On suppose $\alpha, \beta, \gamma, \delta$ génériques, $K = k(\alpha, \beta, \gamma, \delta)$ est une extension galoisienne de k de degré 24, de groupe de Galois S_4. Donc $k(\alpha)$ est loin d'être égal à K (même si l'on adjoint $\sqrt{\Delta}$).

Soient

$$\left\{\omega, 1-\omega, \frac{1}{\omega}, \frac{\omega-1}{\omega}, \frac{1}{1-\omega}, \frac{\omega}{\omega-1}\right\}$$

les birapports de $\alpha, \beta, \gamma, \delta$. Le corps $K_2 = k(\omega)$ est une extension galoisienne de k formée des éléments de K invariants sous M_4. Le corps K_2 est de degré 6 sur k et K de degré 4 sur K_2. Donc $K_2(\alpha) = K, K = k(\omega, \alpha)$. Le but est d'exprimer explicitement β, γ, δ en fonction rationnelle de p, q, r, ω, α.

Proposition F. *L'action du groupe M_4 sur les racines $\alpha, \beta, \gamma, \delta$ est donnée par*

$$T_j(x) := x - P'(x)\left(\frac{p}{3} + 12\frac{J}{I}R_j(\omega) + 2x^2\right)^{-1}.$$

Montrons que la transformation T_1 vérifie

$$T_1(\alpha) = \delta, \quad T_1(\delta) = \alpha, \quad T_1(\beta) = \gamma, \quad T_1(\gamma) = \beta.$$

On a d'après (17)

$$\alpha\delta + \beta\gamma = \frac{p}{3} + 12\frac{J}{I}R_1(\omega).$$

Vue la symétrie de cette égalité, il suffit de montrer, que $T_1(\alpha) = \delta$, i.e., que

$$\delta = \alpha - P'(\alpha)/(\alpha\delta + \beta\gamma + 2\alpha^2).$$

Cela résulte de $P'(\alpha) = (\alpha-\beta)(\alpha-\gamma)(\alpha-\delta)$ et $\alpha+\beta+\gamma+\delta = 0$, d'où

$$(\alpha-\delta)(\alpha\delta + \beta\gamma + 2\alpha^2) = P'(\alpha)$$

3.3. Le cas harmonique. Dans cette section, on va analyser en grands détails le cas où $\{\alpha, \beta, \gamma, \delta\}$ est harmonique, i.e., $J = 0$. Alors $\Delta = 2^8 I^3$; la condition générale $\Delta \neq 0$ implique $I \neq 0$, et $K_1 = k(\sqrt{\Delta}) = k(\sqrt{I})$.

On note G_1 le groupe de Galois de K sur K_1, G le groupe de Galois de K sur k. On suppose bien entendu que P est irréductible sur k.

3.3.1. On reprend d'abord rapidement le cas général, sans hypothèse sur J. D'après la formule de Taylor, $\beta-\alpha, \gamma-\alpha, \delta-\alpha, \alpha-\alpha = 0$ sont solutions de

$$X^4 + 4\alpha X^3 + \sigma X^2 + \rho X + P(\alpha) = 0$$

où $\rho = P'(\alpha), \sigma = \frac{1}{2}P''(\alpha)$. Donc $1/(\beta-\alpha), 1/(\gamma-\alpha), 1/(\delta-\alpha)$ sont solutions de

$$X^3 + \frac{\sigma}{\rho}X^2 + \frac{4\alpha}{\rho}X + \frac{1}{\rho} = 0.$$

On pose

$$\beta' = \frac{\sigma}{3\rho} + \frac{1}{\beta - \alpha}, \quad \gamma' = \frac{\sigma}{3\rho} + \frac{1}{\gamma - \alpha}, \quad \delta' = \frac{\sigma}{3\rho} + \frac{1}{\delta - \alpha}.$$

Alors, d'une part, les birapports de $\{\alpha, \beta, \gamma, \delta\}$ sont égaux aux birapports de $\{\infty, \beta', \gamma', \delta'\}$ et d'autre part β', γ', δ' sont les solutions de

$$\left(X - \frac{\sigma}{3\rho}\right)^3 + \frac{\sigma}{\rho}\left(X - \frac{\sigma}{3\rho}\right)^2 + \frac{4\alpha}{\rho}\left(X - \frac{\sigma}{3\rho}\right) + \frac{1}{\rho} = 0.$$

Après quelques calculs, cette équation s'écrit

$$X^3 - \frac{4I}{\rho^2}X - \frac{16J}{\rho^3} = 0.$$

On en déduit

$$\beta' + \gamma' + \delta' = 0 \tag{19}$$

$$\beta'\gamma' + \beta'\delta' + \gamma'\delta' = -\frac{4I}{\rho^2}, \tag{20}$$

$$\beta'\gamma'\delta' = \frac{16J}{\rho^3}. \tag{21}$$

3.3.2. Dans toute la fin de cette Section 3.3, on suppose à nouveau $J = 0$. D'après (19), (20), (21), on a, à une permutation près de β', γ', δ'

$$\beta' = 0, \quad \gamma' = \frac{2\sqrt{I}}{\rho}, \quad \delta' = -\frac{2\sqrt{I}}{\rho}, \tag{22}$$

d'où

$$\frac{1}{\beta - \alpha} = -\frac{\sigma}{3\rho}, \quad \frac{1}{\gamma - \alpha} = -\frac{\sigma - 6\sqrt{I}}{3\rho}, \quad \frac{1}{\delta - \alpha} = -\frac{\sigma + 6\sqrt{I}}{3\rho}. \tag{23}$$

On en déduit d'abord

$$\sigma \neq 0, \quad \sigma \neq 6\sqrt{I}, \quad \sigma \neq -6\sqrt{I},$$

puis les formules suivantes qui permettent de passer de α aux trois autres racines

$$\beta = \alpha - \frac{3\rho}{\sigma}, \quad \gamma = \alpha - \frac{3\rho}{\sigma - 6\sqrt{I}}, \quad \delta = \alpha - \frac{3\rho}{\sigma + 6\sqrt{I}}, \tag{24}$$

3.3.3. On rappelle que G_1 est le groupe de Galois de K sur $K_1 = k(\sqrt{\Delta}) = k(\sqrt{I})$ et G celui de K sur k.

Lemme G. *On suppose que* $\{\alpha, \beta, \gamma, \delta\}$ *est harmonique.*

(i) On a $K = K_1(\alpha) = K_1(\beta) = K_1(\gamma) = K_1(\delta)$;

(ii) L'extension K de K_1 est galoisienne de degré 2 ou 4.

(iii) Si l'extension K de K_1 est de degré 4, son groupe de Galois G_1 est M_4 et il agit simplement transitivement sur $\{\alpha, \beta, \gamma, \delta\}$.

Démonstration. (i) D'après (24) on a $\beta, \gamma, \delta \in K_1(\alpha)$. Donc $K = K_1(\alpha)$, ce qui entraîne (i), car les raisonnements ci-dessus, qui font jouer un rôle spécial à α, s'appliquent à β, γ, δ.

(ii) Le (i) montre que l'extension K de K_1, qui est galoisienne par construction, est engendrée par α. Son degré $d \leq 4$ est divisible par 2 car $k(\alpha) \subset K$ donc 4 divise $2d$.

(iii) Comme K_1 contient $\sqrt{\Delta}$, K est engendré par α, le groupe G_1 est contenu dans le groupe alterné A_4. Or celui-ci contient un seul sous-groupe d'ordre 4, à savoir M_4. Comme l'extension K de K_1 est galoisienne, G_1 agit transitivement sur $\{\alpha, \beta, \gamma, \delta\}$ et comme G_1 est d'ordre 4, cette action est simplement transitive. □

3.3.4. Notons $S \subset S_4$ le sous-groupe formé en adjoignant à $M_4 \subset S_4$ une transposition s, $s^2 = 1$. Ce sous-groupe est unique à conjugaison près et est un sous-groupe de Sylow associé au nombre premier $p = 2$.

Proposition H. *On suppose que* $(\alpha, \beta, \gamma, \delta)$ *est harmonique.*

(i) Si le discriminant Δ n'est pas un carré dans k et si l'extension K de K_1 est de degré 4, le groupe de Galois G de K sur k est d'ordre 8, conjugué à S.

(ii) Si les conditions de (i) ne sont pas vérifiées, l'extension K de k est de degré 4, égale à $k(\alpha)$.

Démonstration. (i) L'extension K_1 est de degré 2 sur k et K de degré 4 sur K_1 donc l'extension galoisienne K de k est de degré 8. Le sous-groupe S est, à conjugaison près, le seul sous-groupe d'ordre 8 dans S_4 (par le théorème de Sylow).

(ii) Si les conditions de (i) ne sont pas vérifiées, on a soit $K_1 = k$ et le Lemme G montre que $K = k(\alpha)$, soit l'extension K de K_1 est de degré 2 et donc de degré 4 sur k de sorte que $K = k(\alpha)$. □

3.3.5. Exemples. Soit $P(x) = x^4 - \frac{15x^2}{2} + 5x + \frac{5}{16}$. On vérifie que l'on a $J = 0$, de plus l'extension associée est galoisienne de groupe de Galois $\mathbb{Z}/4\mathbb{Z}$. On a

$$P(x) = \left(x^2 + \sqrt{5}x - \frac{1}{4}(2\sqrt{5} + 5)\right)\left(x^2 - \sqrt{5}x - \frac{1}{4}(5 - 2\sqrt{5})\right).$$

Le corps K est l'extension quadratique de $K_1 = \mathbb{Q}(\sqrt{5})$ obtenue en adjoignant une racine carrée de $z = 10 + 2\sqrt{5}$. L'extension de l'automorphisme de $\mathbb{Q}(\sqrt{5})$ au corps K admet pour carré l'automorphisme de Galois de K sur $\mathbb{Q}(\sqrt{5})$ qui change z en $-z$, ce qui montre que $G = \mathbb{Z}/4\mathbb{Z}$.

Le polynôme $P(x) = x^4 + 6x^2 + 1$ donne un exemple où $J = 0, \Delta = 2^{14}$ est un carré, et le groupe G est égal à M_4 (Lemme G (iii)).

3.3.6. Si $p = 0$, la condition $J = 0$ donne $q = 0$ et $P(X) = X^4 + r$. On a $I = r$.

Si k contient $i = \sqrt{-1}$, l'extension galoisienne K est égale à $k[X]/P(X)$, son groupe de Galois est le groupe $G = \mathbb{Z}/4$ engendré par $X \mapsto iX$. Le sous-corps $K_1 = k(\sqrt{I})$ est le sous-corps de $k[X]/P(X)$ formé des polynômes pairs. Le corps K est de dimension 2 sur K_1.

Si le polynôme X^2+1 est irréductible sur k, l'extension galoisienne K est égale à $k(i)[X]/P(X)$, elle est de degré 8 sur k. Le groupe de Galois G de K sur k s'identifie au groupe diédral $D = \mathbb{Z}/4 \rtimes \mathbb{Z}/2$, où l'action de $\mathbb{Z}/4$ sur $k(i)[X]/P(X)$ est donnée par $X \mapsto i^k X$ et celle du générateur de $\mathbb{Z}/2$ par la conjugaison $i \mapsto -i$ sur $k(i)$. Ce groupe D est isomorphe à $S = M_4 \rtimes \mathbb{Z}/2$. Le sous-corps $K_1 = k(\sqrt{I})$ est engendré par l'élément $iX^2 \in k(i)[X]/P(X)$. Le sous-groupe $G_1 \subset G$ qui fixe iX^2 est engendré par l'élément d'ordre 2 de $\mathbb{Z}/4 \subset D$ et $1 \in \mathbb{Z}/2 \subset D$, il est isomorphe à M_4.

3.3.7. Supposons $p \neq 0$. On utilise l'égalité $J = 0$ pour exprimer r en fonction de p, q, i.e.,

$$r = \frac{2p^3 + 27q^2}{72p}$$

On peut calculer la matrice Σ, dans la base $1, X, X^2, X^3$ de l'automorphisme ϕ de $k[X]/P(X)$ qui provient de la transformation $\alpha \mapsto \beta$ de (24). On obtient en utilisant $I = \frac{p^2}{9} + \frac{3q^2}{8p} \neq 0$,

$$\Sigma = \frac{1}{8p^3 + 27q^2} \times \begin{pmatrix} 8p^3 + 27q^2 & 0 & 0 & 0 \\ -18p^2q & -3(16p^3 + 9q^2) & 36pq & -48p^2 \\ -8p^4 - 54pq^2 & -60p^2q & 27q^2 - 8p^3 & -72pq \\ 9p^3q - \frac{81q^3}{2} & \frac{140p^4}{3} & -42p^2q & 48p^3 - 27q^2 \end{pmatrix} \tag{25}$$

et l'on vérifie directement que $\Sigma^2 = 1$ et que le déterminant de Σ vaut 1. On obtient de même la matrice Σ' associée à la transformation $\alpha \mapsto \gamma$. On a, comme $I = \frac{p^2}{9} + \frac{3q^2}{8p} \neq 0$.

$$(8p^3 + 27q^2)\Sigma' = \begin{pmatrix} 8p^3 + 27q^2 & 0 & 0 & 0 \\ \frac{9}{2}pq(2p - \sqrt{I}) & p^2(20p - 7\sqrt{I}) & -18pq & 6p(4p - \sqrt{I}) \\ p^3(\sqrt{I} - 4p) & -3pq(\sqrt{I} - 10p) & 2p^2\sqrt{I} - 27q^2 & 36pq \\ -\frac{3}{4}q(-6p^2\sqrt{I} + 22p^3 + 27q^2) & \sqrt{I}\left(\frac{35p^3}{6} - \frac{9q^2}{4}\right) - \frac{70p^4}{3} & \frac{3}{2}pq(\sqrt{I} + 14p) & p^2(5\sqrt{I} - 28p) \end{pmatrix} \tag{26}$$

et l'on vérifie que $\Sigma'^2 = 1$ et que $\Sigma\Sigma' = \Sigma'\Sigma$.

Si $\sqrt{I} \in k$ (i.e., $\sqrt{\Delta} \in k$) la formule (26) définit un automorphisme ϕ' de $k[X]/P(X)$ et ϕ, ϕ' donnent l'action de M_4 sur cette extension galoisienne de k.

Quand l'extension galoisienne K de k est de degré 8, on est dans le cas (i) de la Proposition H, l'extension K est obtenue en adjoignant $\sqrt{I}$ au corps $k[X]/P(X)$ et nous l'identifions avec $k(\sqrt{I})[X]/P(X)$. Elle admet une involution unique θ qui est l'identité sur $k[X]/P(X)$ et telle que $\theta(\sqrt{I}) = -\sqrt{I}$. De plus comme $I \in k$, l'automorphisme ϕ de $k[X]/P(X)$ se prolonge à K en fixant $\sqrt{I}$. La matrice Σ' est une matrice à coefficients dans $k(\sqrt{I})$ et définit un automorphisme ϕ' de K fixant $\sqrt{I}$. On obtient ainsi la description du groupe de Galois comme produit semi-direct S de M_4 qui agit par ϕ, ϕ' et de l'involution θ qui transforme ϕ' en son inverse.

Supposons maintenant que K est de dimension 4 sur $k\sqrt{I} \notin k$. On identifie K avec $k[X]/P(X)$. L'équation $X^2 = I$ admet ses racines $\pm\xi(X) \in k[X]/P(X)$ dans le corps K et celles-ci engendrent le corps $K_1 \subset K$. L'automorphisme ϕ de K donné par la matrice Σ permute les racines $\alpha, \beta, \gamma, \delta \in k[X]/P(X)$ et comme $\phi(\alpha) = \beta$ et la permutation est paire car le déterminant de Σ vaut 1, on a $\phi(\gamma) = \delta$. La matrice Σ' n'a plus de sens en tant que transformation de K, mais il reste vrai que les quatre racines de $P(X) = 0$ qui forment une base de K sur k vérifient (23), d'où

$$\frac{1}{\gamma - \alpha} - \frac{1}{\delta - \alpha} = \frac{4\sqrt{I}}{\rho}$$

d'où, en utilisant $\rho = (\alpha - \beta)(\alpha - \gamma)(\alpha - \delta)$, on déduit

$$4\sqrt{I} = -(\alpha - \beta)(\alpha - \delta) + (\alpha - \beta)(\alpha - \gamma) = (\alpha - \beta)(\delta - \gamma)$$

et il en résulte, comme la permutation des racines associée à ϕ est

$$(\alpha, \beta, \gamma, \delta) \mapsto (\beta, \alpha, \delta, \gamma)$$

que $\phi(\sqrt{I}) = \sqrt{I}$. Ainsi le sous-corps $K_1 = k(\sqrt{I})$ est le corps fixe de ϕ. Comme K est une extension galoisienne de k, l'automorphisme $\psi : \sqrt{I} \mapsto -\sqrt{I}$ de K_1 se prolonge en un automorphisme $\widetilde{\psi}$ de K. Montrons que la permutation correspondante des racines est soit $\eta : (\alpha, \beta, \gamma, \delta) \mapsto (\gamma, \delta, \beta, \alpha)$ soit η' : $(\alpha, \beta, \gamma, \delta) \mapsto (\delta, \gamma, \alpha, \beta)$. La condition d'harmonicité réduit le groupe des permutations possibles à 8 permutations parmi lesquelles seules 4 sont impaires, et donc transforment $\sqrt{I}$ en $-\sqrt{I}$. Les permutations η, η' transforment le birapport des racines en son inverse, ce qui est compatible avec la condition d'harmonicité. Elles transforment $(\alpha - \beta)(\delta - \gamma)$ en son opposé, et donc $\sqrt{I}$ en $-\sqrt{I}$. Mais ces deux propriétés sont également vérifiées par les deux permutations

$$(\alpha, \beta, \gamma, \delta) \mapsto (\beta, \alpha, \gamma, \delta) \quad \text{et} \quad (\alpha, \beta, \gamma, \delta) \mapsto (\alpha, \beta, \delta, \gamma)$$

La raison pour laquelle celles-ci sont exclues est la transitivité du groupe de Galois sur les racines. En effet le groupe de permutations obtenues en incluant ϕ préserverait la partition des racines en $\{\alpha, \beta\} \cup \{\gamma, \delta\}$ ce qui est exclu car le polynôme $P(X)$ est irréductible sur k. On a alors, toujours sous les hypothèses $J = 0, p \neq 0$ le théorème suivant :

Théorème I. *Si l'extension K de $k(\sqrt{\Delta})$ est de degré 2, on a $K \sim k[X]/P(X)$ et le groupe de Galois de l'extension K de k est le groupe $\mathbb{Z}/4$. Le sous-corps $k(\sqrt{\Delta})$ est le corps des points fixes de l'automorphisme involutif ϕ donné par la matrice Σ de (25).*

La Proposition H montre que $K \sim k[X]/P(X)$. Comme $\beta' = 0$ et $\gamma' + \delta' = 0$ par (22), on a $\langle \alpha, \beta, \gamma, \delta \rangle = -1$. Le raisonnement ci-dessus montre que la permutation $\widetilde{\psi}$ des racines est soit

$$(\alpha, \beta, \gamma, \delta) \mapsto (\gamma, \delta, \beta, \alpha) \quad \text{soit} \quad (\alpha, \beta, \gamma, \delta) \mapsto (\delta, \gamma, \alpha, \beta).$$

Dans les deux cas, le carré de ψ est égal à ϕ et le groupe de Galois est $\mathbb{Z}/4$.

3.4. Le cas équiharmonique. Pour simplifier, on suppose que k contient les trois racines de l'équation $X^3 = 1$. On note $j \in k, j \neq 1$, une racine cubique de l'unité, on a $j - j^2 = i\sqrt{3}$. Soit $P(X)$ équiharmonique. On a $I = 0$ donc $J \neq 0, 2^{-8}\Delta = -27J^2 = (3i\sqrt{3}J)^2$ donc $\sqrt{\Delta} \in k, K_1 = k(\sqrt{\Delta}) = k$. Les équations de la Section 3.3.1 montrent que $\beta', \gamma', \delta' \neq 0$ et, après permutation éventuelle de γ', δ' que $\gamma' = j\beta', \delta' = j^2\beta'$ et $\beta'^3 = 16J/\rho^3$. Soit $\sqrt[3]{2J} \in \overline{k}$ la racine cubique de $2J$ égale à $\frac{1}{2}\rho\beta'$. On a $\sqrt[3]{2J} \in K$. Posons $K_1' = k(\sqrt[3]{2J})$. C'est une extension galoisienne de k de groupe de Galois $\mathbb{Z}/3$ ou $\{e\}$. On a, après une permutation éventuelle de $\{\beta', \gamma', \delta'\}$,

$$\beta' = 2\frac{\sqrt[3]{2J}}{\rho}, \qquad \gamma' = 2j\frac{\sqrt[3]{2J}}{\rho}, \qquad \delta' = 2j^2\frac{\sqrt[3]{2J}}{\rho}$$

$$(\beta - \alpha)^{-1} = \beta' - \frac{\sigma}{3\rho} = \frac{1}{3\rho}(6\sqrt[3]{2J} - \sigma),$$

$$\beta = \alpha + \frac{3\rho}{6\sqrt[3]{2J} - \sigma}, \qquad \gamma = \alpha + \frac{3\rho}{6j\sqrt[3]{2J} - \sigma}, \qquad \delta = \alpha + \frac{3\rho}{6j^2\sqrt[3]{2J} - \sigma}.$$

On a donc $K = K_1'(\alpha)$ et le degré de l'extension K de K_1' est ≤ 4.

Proposition J. *On suppose $j \in k$. Soit $P(X)$ équiharmonique. Alors $\sqrt{\Delta} \in k$ et deux cas sont possibles :*

(1) *$K_1' = k$. Le groupe de Galois de K sur k est M_4 ;*

(2) *$K_1' \neq k$. Alors K_1' est extension galoisienne de k de groupe Z_3. K est extension galoisienne de K_1' de groupe M_4 et extension galoisienne de k de groupe A_4.*

Si $K_1' = k$, le degré de K sur k est 4, le groupe de Galois de K sur k est le seul sous-groupe de A_4 d'ordre 4. Si $K_1' \neq k$, K_1' est extension galoisienne de k de $K_1' = k$ de groupe $\mathbb{Z}_3$, comme le degré de K sur k est divisible par 4 car $k(\alpha) \subset K$, l'extension galoisienne K de K_1' est necessairement de degré 4 et son groupe de Galois est M_4. Le groupe de Galois de K sur k est le groupe A_4.

Il est facile de donner des exemples de ce deuxième cas. Un exemple du premier cas est donné par le polynome $P(x) = x^4 - 3x^2 + 3x - \frac{3}{4}$ sur $k = \mathbb{Q}(j)$. On vérifie que dans ce cas $I = 0$ et $2J = -\frac{1}{8}$. Son groupe de Galois sur $\mathbb{Q}(j)$ est M_4 et son groupe de Galois sur $\mathbb{Q}$ est un sous-groupe de Sylow d'ordre 8.

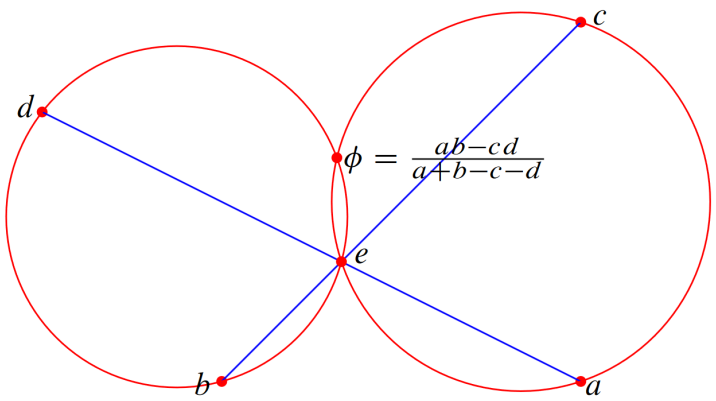


FIGURE 1 : Les deux cercles (a, c, e) et (b, d, e) se recoupent en ϕ.

4. L'ange de la géométrie et le diable de l'algèbre

4.1. Lagrange. On trouve à la fin de l'article de Lagrange [4] sur l'équation du quatrième degré, dans sa discussion de l'article de Bézout de 1762, la fonction rationnelle suivante des quatre racines (a, b, c, d) qui ne prend que trois valeurs différentes quand on permute les racines :

$$\varphi(a, b, c, d) = \frac{ab - cd}{a + b - c - d}. \tag{27}$$

Cette expression est rationnellement équivalente à la fonction classique

$$\psi(a, b, c, d) = ab + cd$$

et l'on vérifie par un calcul direct, en notant s_j les fonctions symétriques des racines, les égalités

$$\varphi = \frac{s_1\psi - 2s_3}{4\psi + s_1^2 - 4s_2}, \quad \psi = \frac{(s_1^2 - 4s_2)\varphi + 2s_3}{s_1 - 4\varphi}.$$

L'expression (27) est covariante pour l'action du groupe affine, i.e., on a pour $g(z) = \lambda z + \mu, \lambda \neq 0$,

$$\varphi(g(a), g(b), g(c), g(d)) = g(\varphi(a, b, c, d)).$$

Cette covariance indique que le point $\varphi(a, b, c, d)$ doit s'interpréter géométriquement dans le plan complexe. Nous donnons une interprétation géométrique de $\varphi(a, b, c, d)$.

Proposition K. *Soient $a, b, c, d \in \mathbb{C}$. Le point $\varphi(a, b, c, d) \in \mathbb{C}$ est le point d'intersection des quatre cercles circonscrits aux triangles $(a, c, e), (b, d, e), (a, d, f), (b, c, f)$ où e est l'intersection des diagonales (ad) et (bc) et f l'intersection des diagonales (ac) et (bd).*

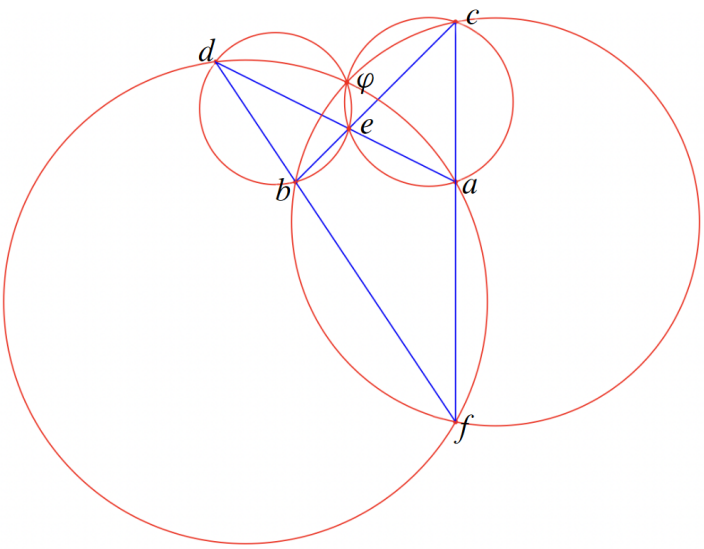


FIGURE 2 : Le point φ est l'intersection des cercles $(a,c,e),(b,d,e),(a,d,f),(b,c,f)$.

Il suffit de démontrer que le point φ est le deuxième point d'intersection des cercles circonscrits aux triangles $(a,c,e),(b,d,e)$. Voir Figures 1 et 2. On utilise la covariance pour le groupe affine qui permet de supposer que $e=0$. Une inversion de centre e (plus précisemment l'application $z\mapsto 1/z$ du plan complexe), réduit alors l'égalité à un calcul simple.

4.2. Morley.

4.2.1. Dans cette section, nous montrons comment généraliser le théorème de Morley (Figure 3) dans le cadre des équations du $3^{\text{ème}}$ et du $4^{\text{ème}}$ degré. Le point de départ est la démonstration [2] du théorème de Morley utilisant les nombres complexes. La résolvante donnée par le birapport $\langle a,b,c,\infty\rangle$ du Théorème A joue un rôle crucial dans notre généralisation. L'idée de [2] consiste à décrire les sommets du triangle de Morley comme points fixes du produit de deux rotations autour des sommets A,B,C d'un triangle et d'observer que le produit des cubes de ces rotations est l'identité. On utilise alors un lemme algébrique général sur le groupe $H(K)$ des transformations d'un corps K de la forme

$$x\mapsto g(x)=\alpha x+\beta,$$

où $\alpha,\beta\in K,\alpha\neq 0$ est le morphisme $\chi : H(K)\to K^\times$ qui associe à $g\in H(K)$ l'élément $\chi(g)=\alpha\in K^\times$. Si $\chi(g)\neq 1$, on note $\mathrm{fix}(g)$ l'unique point fixe de g, i.e., $x\in K$ tel que $g(x)=x$. Le lemme est le suivant,

Lemme L. ([2]). Soient $f,g,h\in H(K)$ tels que $f^3g^3h^3=1$ et que $j:=\chi(fgh)\neq 1$. On suppose que f^3,g^3 et h^3 ne sont pas des translations. Alors fg, gh et hf ne sont pas des translations et

$$\mathrm{fix}(fg)+j\,\mathrm{fix}(gh)+j^2\,\mathrm{fix}(hf)=0$$

Comme $f^3g^3h^3=1$, on a $j^3=1$ et j est donc une racine cubique primitive de 1 dans K.

Remarque M. Soient $a, b, c \in K$; les conditions suivantes sont équivalentes :

(1) Il existe $j \neq 1, j^3 = 1$ tel que $a + jb + j^2c = 0$;

(2) Il existe $j \neq 1, j^3 = 1$ tel que $\langle a, b, c, \infty \rangle = -j$;

(3) La configuration a, b, c, ∞ est équiharmonique.

Quand $K = \mathbb{C}$ les conditions précédentes signifient que le triangle (a, b, c) est équilatère.

Soient $z \in \mathbb{P}^1(K), H_z \subset \mathrm{PGL}_2(K)$ le sous-groupe des éléments qui fixent z. L'application $\chi_z : H_z \to K^\times$ définie par

$$\chi_z(f) = \chi(hfh^{-1})$$

indépendamment du choix de $h \in \mathrm{PGL}_2(K)$ tel que $h(z) = \infty$ est un morphisme de groupe canonique $\chi_z : H_z \to K^\times$. On note $\ker(\chi_z)$ le noyau de χ_z. Soit $f \in H_z$ tel que $\chi_z(f) \neq 1$, on note $\mathrm{fix}_{\neq z}(f) \in \mathbb{P}^1(K)$ l'autre point fixe de f.

Corollaire N. *Soient $z \in \mathbb{P}^1(K),\ f, g, h \in H_z$ tels que $f^3g^3h^3 = \mathrm{Id}$ et que $j := \chi_z(fgh) \neq 1$. On suppose que f^3, g^3 et h^3 ne sont pas dans $\ker(\chi_z)$. Alors fg, gh et hf ne sont pas dans $\ker(\chi_z)$ et la configuration $(z, \mathrm{fix}_{\neq z}(fg), \mathrm{fix}_{\neq z}(gh), \mathrm{fix}_{\neq z}(hf))$ est équiharmonique.*

On se ramène par conjugaison par un élément de $\mathrm{PGL}_2(K)$ au cas où $z = \infty$ et on applique le Lemme L et la Remarque M.

4.2.2. Soient K un corps contenant une racine cubique de l'unité, $j \neq 1$, et $\sigma \in \mathrm{Aut}(K)$ un automorphisme de K, tel que $\sigma^2 = \mathrm{Id}$ et que $\sigma(j) = j^2$. Soit $H = H(K)$ le groupe affine de K, on note $h(\alpha, \beta) \in H(K)$ l'élément tel que

$$h(\alpha, \beta)(x) = \alpha x + \beta,$$

pour tout $x \in K$. Soit $\widetilde{H} = H \rtimes_\sigma \mathbb{Z}/2$ le produit semi-direct de H par l'automorphisme σ. Ses éléments sont de la forme $h(\alpha, \beta)$ ou $h(\alpha, \beta)\sigma$ avec $\sigma^2 = 1, \sigma h(\alpha, \beta) = h(\sigma(\alpha), \sigma(\beta))\sigma$. Le corps K est un espace vectoriel dimension 2 sur le sous-corps K^σ des points fixes de σ.

Lemme O. *Soient K et J comme ci-dessus.*

(i) *Soient $a, b \in K, a \neq b$. L'égalité*

$$s(a, b) = h\left(\frac{a - b}{\sigma(a) - \sigma(b)}, \frac{a\sigma(b) - b\sigma(a)}{\sigma(b) - \sigma(a)}\right)\sigma$$

définit une involution, $s(a, b)^2 = 1$ dont les point fixes forment la droite passant par a et b dans le plan $K \sim (K^\sigma)^2$.

(ii) *Soient $a, b, c \in K$ trois éléments distincts non-alignés sur $K^\sigma, \omega = \langle a, b, c, \infty \rangle$.*

Le produit $s(a, c)s(b, c)$ est l'unique élément $g \in H$ qui fixe le point c et tel que

$$\chi(g) = \omega/\sigma(\omega).$$

(iii) *Soit $g \in H$ comme dans (ii). On a $g = h(\chi(g), x)$ où $x = c - c\omega/\sigma(\omega)$.*

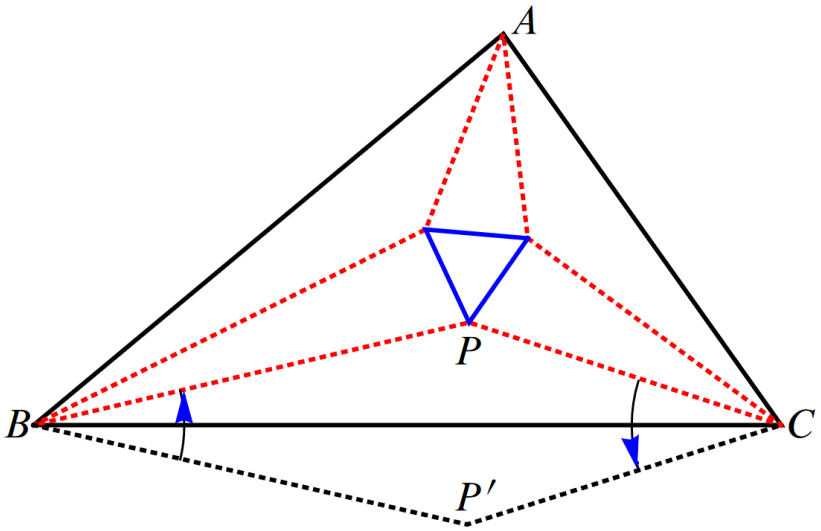


FIGURE 3 : Le point P, intersection des trisectrices issues de B et C, est le point fixe du produit $R_B R_C$ de rotations de centre B et C. On a $R_A^3 R_B^3 R_C^3 = 1$.

Démonstration. (i) L'unique élément g de H tel que $g(a) = 0$ et $g(b) = 1$ est

$$h\left(\frac{1}{b-a}, -\frac{a}{b-a}\right).$$

On a

$$s(a,b) = g^{-1}\sigma g.$$

On est donc ramené au cas où $a = 0, b = 1$ et dans ce cas, l'involution σ a bien pour points fixes la droite du plan $K \sim (K^\sigma)^2$ passant par $a = 0, b = 1$.

(ii) Par construction $s(a,c)$ et $s(b,c)$ fixent c. Le calcul du produit montre que l'élément $s(a,c)s(b,c)$ de H est de la forme indiquée. Comme a, b, c sont non-alignés, on a $\omega \neq \sigma(\omega)$ et l'unicité de x tel que $h(\omega/\sigma(\omega), x) = s(a,c)s(b,c)$ en résulte.

(iii) Comme $g(c) = c$ et $\chi(g) = \omega/\sigma(\omega)$, on a $x = c - c\omega/\sigma(\omega)$. □

Notons,

$$\theta(a,b;c) := h(\omega/\sigma(\omega), c - c\omega/\sigma(\omega)), \quad \omega := \langle a, b, c, \infty \rangle. \tag{28}$$

Lemme P. *Soient $a, b, c \in K$ trois éléments distincts non-alignés sur K^σ. On a*

$$\theta(a,b;c)\theta(c,a;b)\theta(b,c;a) = \mathrm{Id} \tag{29}$$

Cela résulte des simplifications suivantes

$$(s(a,c)s(b,c))(s(b,c)s(a,b))(s(a,b)s(a,c)) = s(a,c)s(a,c) = \mathrm{Id}.$$

Si $\omega = \langle a, b, c, \infty\rangle$, le produit des trois birapports impliqués dans (4.6) est

$$\omega \cdot \frac{1}{1-\omega} \cdot \frac{\omega - 1}{\omega} = -1$$

et donc le produit des rapports avec les transformés par σ vaut bien 1.

Pour $x, y \in \mathbb{P}^1(K), x \neq y$ et $u \in K^\times$, on note $\rho(u; x, y)$ l'unique élément g de $H_y(K)$ tel que $g(x) = x$ et que $\chi_y(g) = u$.

Corollaire Q. *Soient $\alpha, \beta, \gamma, \delta \in K$ quatre éléments distincts, $\omega = \langle \beta, \gamma, \delta, \alpha\rangle \notin K^\sigma$. On note*

$$\omega' = \frac{1}{1-\omega}, \quad \omega'' = \frac{\omega - 1}{\omega}.$$

On a alors

$$\rho(\omega/\sigma(\omega); \delta, \alpha)\rho(\omega'/\sigma(\omega'); \gamma, \alpha)\rho(\omega''/\sigma(\omega''); \beta, \alpha) = \mathrm{Id}. \tag{30}$$

Supposons d'abord $\alpha = \infty$; on a alors, en utilisant (28), avec $a = \beta, b = \gamma, c = \delta$ les égalités

$$\rho(\omega/\sigma(\omega); \delta, pha) = \theta(a,b;c),$$

$$\rho(\omega'/\sigma(\omega'); \gamma, \alpha) = \theta(c,a;b), \qquad \rho(\omega''/\sigma(\omega''); \beta, \alpha) = \theta(b,c;a),$$

ainsi que $\omega = \langle a, b, c, \infty\rangle$ et (30) se déduit du Lemme P. Supposons $\alpha \neq \infty$. On a pour tout $h \in \mathrm{PGL}_2(K), x, y \in \mathbb{P}^1(K), x \neq y.$ et $u \in K^\times$ l'égalité

$$\rho(u; h(x), h(y)) = h\rho(u; x, y)h^{-1}.$$

Soit $h \in \mathrm{PGL}_2(K)$ la transformation projective $h(z) := (z - \alpha)^{-1}$. Soient

$$a = h(\beta), \quad b = h(\gamma), \quad c = h(\delta).$$

On a

$$\omega = \langle \beta, \gamma, \delta, \alpha\rangle = \langle a, b, c, \infty\rangle$$

et les trois termes du produit (30) sont les conjugués par h des trois termes de (29) et on obtient (30) grâce au Lemme P.

4.2.3. Racines cubiques des birapports. Soit

$$\varpi = \left\{\omega, 1-\omega, \frac{1}{\omega}, \frac{\omega-1}{\omega}, \frac{1}{1-\omega}, \frac{\omega}{\omega-1}\right\}$$

une orbite pour l'action du groupe symétrique S_3 sur le plan projectif $\mathbb{P}^1(K)$.

Définition R. Une racine cubique $\sqrt[3]{\varpi}$ de ϖ est le choix $u \mapsto \sqrt[3]{\omega}$ d'une racine cubique pour chacun des éléments de ϖ tel que

- si $u, v \in \varpi$ vérifient $uv = 1$ alors $\sqrt[3]{u}\sqrt[3]{v} = 1$;
- si $u, v, w \in \varpi$ vérifient $uvw = -1$ alors $\sqrt[3]{u}\sqrt[3]{v}\sqrt[3]{w} \neq -1$.

On vérifie que, dans le cas général, ϖ admet 18 racines cubiques, qui sont des applications de ϖ dans $\overline{k}$.

4.2.4. Généralisation du théorème de Morley. On utilise les notations k, K, j, σ ci-dessus. On prolonge σ en un automorphisme (pas nécessairement involutif) de la clôture algébrique $\overline{k} \supset K$ de k. Soit u in $\overline{k}, u \notin \{0, 1\}$. Soient $\alpha, \beta \in \mathbb{P}^1(K), \alpha \neq \beta$. Il existe un unique élément de $\mathrm{PGL}_2(k)$ qui fixe α et β et tel que u soit l'élément correspondant du groupe multiplicatif $G_m(\overline{k})$ (par conjugaison par une transformation projective transformant α en 0 et β en ∞). On note, comme ci-dessus, cet élément $\rho(u; \alpha, \beta)$. On a $\rho(u; \beta, \alpha) = \rho(u^{-1}; \alpha, \beta)$. Compte tenu de la Remarque M, le théorème suivant est une généralisation du théorème de Morley.

Théorème S. *Soient $\alpha, \beta, \gamma, \delta \in K$ quatre éléments distincts dont les birapports prennent six valeurs distinctes hors de K^σ. Soit $\sqrt[3]{\varpi}$ une racine cubique de ces birapports. Posons*

$$u = \langle \beta, \gamma, \delta, \alpha\rangle^{1/3}, \quad v = \langle \delta, \beta, \gamma, \alpha\rangle^{1/3}, \quad w = \langle \gamma, \delta, \beta, \alpha\rangle^{1/3}$$

(les valeurs des racines cubiques étant spécifiées par $\sqrt[3]{\varpi}$). Soient

$$\phi = \rho(u/\sigma(u); \delta, \alpha), \quad \psi = \rho(v/\sigma(v); \gamma, \alpha), \quad \chi = \rho(w/\sigma(\omega); \beta, \alpha).$$

Alors la configuration $(\alpha, \mathrm{fix}_{\neq\alpha}(\phi\psi), \mathrm{fix}_{\neq\alpha}(\psi\chi), \mathrm{fix}_{\neq\alpha}(\chi\phi))$ est équiharmonique.

En effet, le Corollaire Q montre que l'on a $\phi^3\psi^3\chi^3 = \mathrm{Id}$. On applique alors le Corollaire N en utilisant la deuxième condition de la Définition R pour assurer que les hypothèses sont vérifiées. Il en résulte que la configuration

$$(\alpha, \mathrm{fix}_{\neq\alpha}(\phi\psi), \ \mathrm{fix}_{\neq\alpha}(\psi\chi), \ \mathrm{fix}_{\neq\alpha}(\chi\phi))$$

est équiharmonique.

Remerciements. Nous remercions le rapporteur pour ses judicieuses observations.

Références

[1] R. Bourgne, J.-P. Azra (eds.), *Écrits et mémoires mathématiques d'Évariste Galois*, Gauthier-Villars, Paris, 1962. Zbl 0192.01502 MR 0150016.

[2] A. Connes, *A new proof of Morley's theorem. In Les relations entre les mathématiques et la physique théorique*, pp. 43-46, Institut des Hautes Études Scientifiques, Bures-sur-Yvette, 1998. Zbl 1006.51010 MR 1667897.

[3] E. Elliott, *An introduction to the algebra of quantics.* Seconde edition, Clarendon Press, Oxford, 1913. Zbl 44.0155.05.

[4] J.-L. Lagrange, *Réflexions sur la résolution algébrique des équations.* Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin, années 1770 et 1771. In Oeuvres complètes. Volume 3, pp. 205-421, Gauthier-Villars, Paris, 1867.

Une nouvelle preuve du théorème de Morley
Alain Connes

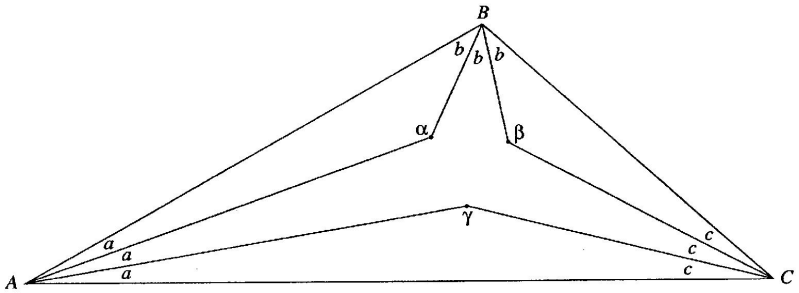
Cela fait maintenant 22 ans que l'IHÉS m'a offert l'hospitalité. J'ai appris ici la plupart des mathématiques que je connais, principalement grâce à des conversations impromptues au déjeuner avec des visiteurs ou des membres permanents.

Quand je suis arrivé, j'étais obnubilé par mon propre travail et j'ai éprouvé un sentiment d'humilité en réalisant à quel point je comprenais peu ce dont il était alors question dans les discussions habituelles. Dennis Sullivan prit soin de moi, et me donna un cours rapide en géométrie qui a influencé ma manière de penser pour le reste de ma vie.

C'est aussi à Bures, grâce aux physiciens, que j'ai compris la véracité d'une phrase de J. Hadamard sur la profondeur des concepts mathématiques venant de la physique :

"Non cette nouveauté à la vie courte qui trop souvent ne peut influencer que le mathématicien rivé à ses propres préoccupations, mais cette nouveauté infiniment féconde qui jaillit de la nature des choses."

Pour donner un peu l'esprit de l'atmosphère de compétition conviviale caractéristique de l'IHÉS, j'ai choisi l'exemple spécifique d'une conversation que nous avons eue lors d'un déjeuner au printemps dernier et qui m'a amené à un nouveau résultat amusant.



Vers 1899, F. Morley prouva un théorème remarquable sur la géométrie élémentaire des triangles Euclidiens :

"Etant donné un triangle A, B, C, les intersections 2 à 2, α, β, γ des trissectrices sont les sommets d'un triangle équilatéral" (*cf.* Fig. 1).

L'un de nous mentionna ce résultat pendant le déjeuner et l'attribua (par erreur) à Napoléon. Bonaparte avait effectivement étudié les mathématiques dans son jeune âge et, en plus d'apprendre l'anglais, il enseignait les mathématiques au fils de Las Cases pendant son exil de Sainte Hélène à Longwood.

C'était la première fois que j'entendais parler du résultat de Morley et quand je suis rentré chez moi, suivant l'un des conseils de Littlewood, j'ai commencé à chercher une preuve, non pas dans les livres mais dans ma tête. Ma seule motivation en plus de la curiosité était le challenge évident "c'est l'un des rares exploits de Bonaparte auquel je devrais pouvoir m'attaquer". Après quelques tentatives infructueuses, j'ai vite réalisé que les intersections de trissectrices consécutives sont les points fixes de produits

1. Ce texte provient de l'ouvrage fêtant les 40 ans de l'IHÉS intitulé Les relations entre les mathématiques et la physique théorique, IHÉS, 1998, p. 43-46. On peut également le lire ici : http://www.numdam.org/article/PMIHES_1998__S88_43_0.pdf.

2. Collège de France, Paris, et IHÉS, 91440 Bures-sur-Yvette, France.

de 2 rotations g_i autour des sommets du triangle (rotations d'angles égaux à deux tiers des angles correspondant du triangle). Il était alors naturel de chercher la symétrie g du triangle équilatéral comme un élément du groupe Γ engendré par les trois rotations g_i. Maintenant, il était facile de construire un exemple (en géométrie sphérique) qui montre que le théorème de Morley ne peut s'appliquer en géométrie non-euclidienne, de telle façon que la preuve devait utiliser des propriétés euclidiennes particulières du groupe des isométries.

Du coup, je passais quelque temps à essayer de trouver une formule de g en fonction des g_i, en utilisant la construction simple (toute isométrie d'angle $2\pi/n, n \geq 2$ est automatiquement d'ordre n), de plein d'éléments d'ordre 3 dans le groupe Γ, comme $g_1g_2g_3$. Après beaucoup d'efforts, je réalisais que c'était en vain (*cf.* Rem. 2 ci-dessous) et que le groupe qui intervient est le groupe affine de la droite, plutôt que le groupe d'isométrie du plan.

Le but de cette courte note est de donner une preuve conceptuelle du théorème de Morley comme propriété théorique du groupe de l'action du groupe affine sur la droite. Il sera valide pour tout corps (commutatif) k (de caractéristique arbitraire, même si en caractéristique 3, l'hypothèse du théorème ne peut être remplie). Ainsi soit k un tel corps et G le groupe affine sur k, en d'autres termes, le groupe des matrices 2×2 $g = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ où $a \in k, a \neq 0, b \in k$. Pour $g \in G$, posons

$$\delta(g) = a \in k^*. \tag{1}$$

Par construction, δ est un morphisme de G dans le groupe multiplicatif k^* des éléments non nuls de k, et le sous-groupe $T = \text{Ker } \delta$ est le groupe des translations, i.e. le groupe additif de k. Chaque $g \in G$ dans G définit une transformation,

$$g(x) = ax + b \qquad \forall x \in k, \tag{2}$$

et si $a \neq 1$, elle admet un et un seul point fixe,

$$fix(g) = \frac{b}{1-a}. \tag{3}$$

Prouvons le simple fait suivant :

Théorème. Soient $g_1, g_2, g_3 \in G$ tels que g_1g_2, g_2g_3, g_3g_1 et $g_1g_2g_3$ ne sont pas des translations et posons $j = \delta(g_1g_2g_3)$. Les conditions suivantes sont équivalentes,

a) $g_1^3g_2^3g_3^3 = 1$.

b) $j^3 = 1$ et $\alpha + j\beta + j^2\gamma = 0$ où $\alpha = fix(g_1g_2), \beta = fix(g_2g_3), \gamma = fix(g_3g_1)$.

Preuve. Posons $g_i = \begin{bmatrix} a_i & b_i \\ 0 & 1 \end{bmatrix}$. L'égalité $g_1^3g_2^3g_3^3 = 1$ est équivalente à $\delta(g_1^3g_2^3g_3^3) = 1$, et $b = 0$, où b est la partie translationnelle de $g_1^3g_2^3g_3^3$. La première condition est exactement $j^3 = 1$. Notons que $j \neq 1$ par hypothèse. Alors on a

$$b = \left(a_1^2 + a_1 + 1\right) b_1 + a_1^3 \left(a_2^2 + a_2 + 1\right) b_2 + (a_1a_2)^3 \left(a_3^2 + a_3 + 1\right) b_3. \tag{4}$$

Un calcul évident, en utilisant le fait que $a_1a_2a_3 = j$ donne,

$$b = -ja_1^2a_2(a_1 - j)(a_2 - j)(a_3 - j)(\alpha + j\beta + j^2\gamma), \tag{5}$$

où, α, β, γ sont les points fixes

$$\alpha = \frac{a_1b_2 + b_1}{1 - a_1a_2}, \beta = \frac{a_2b_3 + b_2}{1 - a_2a_3}, \gamma = \frac{a_3b_1 + b_3}{1 - a_3a_1}. \tag{6}$$

Maintenant, $a_k - j \neq 0$ puisque par hypothèse, les produits deux à deux des g_j *ne sont pas* des translations. Ainsi, et quelque soit la caractéristique de k, nous obtenons que a) $\Leftrightarrow$ b).

Corollaire. Théorème de Morley.

Démonstration. Prenons $k = \mathbb{C}$ et définissons g_1 comme la rotation de centre A et d'angle $2a$, où $3a$ est l'angle BAC et de manière similaire pour g_2 et g_3. On a $g_1^3 g_2^3 g_3^3 = 1$ puisque chaque g_i^3 peut être exprimé comme le produit des symétries le long des côtés consécutifs. De plus, pour une raison similaire $\alpha = fix(g_1 g_2), \beta = fix(g_2 g_3), \gamma = fix(g_3 g_1)$ sont les intersections des trissectrices. Ainsi, de a) $\Rightarrow$ b), on obtient $\alpha + j\beta + j^2\gamma = 0$ qui est une caractérisation classique des triangles équilatéraux.

Remarque 1. Sans altérer les cubes g_1^3, g_2^3, g_3^3, on peut multiplier chaque g_i par une racine cubique de 1, on obtient de cette manière les 18 triangles équilatéraux non-dégénérés des variantes du théorème de Morley.

Remarque 2. Nous montrerons maintenant qu'en général, la rotation g qui permute cycliquement les points α, β, γ n'appartient pas au sous-groupe Γ de G engendré par g_1, g_2, g_3. Sous l'hypothèse du théorème, on peut supposer que le corps k contient une racine cubique de l'unité non triviale, $j \neq 1$, et que de ce fait, sa caractéristique n'est pas égale à 3. La rotation qui permute cycliquement les points α, β, γ est ainsi l'élément de G donné par,

$$g = \begin{bmatrix} j & b \\ 0 & 1 \end{bmatrix}, 3b = (1-j)(\alpha + \beta + \gamma). \tag{7}$$

Maintenant, pour tout élément $g = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ du groupe Γ engendré par g_1, g_2, g_3, on a les polynômes de Laurent P_i en les variables a_j tels que,

$$b = b_1 P_1 + b_2 P_2 + b_3 P_3. \tag{8}$$

Ainsi, en exprimant, avec les notations ci-dessus b_i en termes de α, β, γ,

$$\begin{array}{llll} b_1 = (1+j)^{-1}\big(a_3^{-1} & (a_3 - j)\alpha - & (a_1 - j)\beta + a_1 & (a_2 - j)\gamma\big) \\ b_2 = (1+j)^{-1}\big(a_2 & (a_3 - j)\alpha + a_1^{-1} & (a_1 - j)\beta - & (a_2 - j)\gamma\big) \\ b_1 = (1+j)^{-1}\big(- & (a_3 - j)\alpha + a_3 & (a_1 - j)\beta + a_2^{-1} & (a_2 - j)\gamma\big) \end{array} \tag{9}$$

nous obtenons les polynômes de Laurent Q_i tel que,

$$b = (a_3 - j)\alpha Q_1 + (a_1 - j)\beta Q_2 + (a_2 - j)\gamma Q_3. \tag{10}$$

On peut alors supposer qu'on a trouvé des polynômes de Laurent Q_i tel que pour tout $a_1, a_2, a_3 \in k^*$, avec $a_1 a_2 a_3 = j$, et tout $\alpha, \beta, \gamma \in k$ avec $\alpha + j\beta + j^2\gamma = 0$, l'identité suivante est vérifiée,

$$(1-j)(\alpha + \beta + \gamma) = 3((a_3 - j)\alpha Q_1 + (a_1 - j)\beta Q_2 + (a_2 - j)\gamma Q_3). \tag{11}$$

Nous choisissons alors $a_1 = j, a_2 = j, a_3 = j^2, \alpha = 0, \beta = -j, \gamma = 1$ et obtenons une contradiction. En passant au corps des fonctions sur k, cela suffit à démontrer que, en général, $g \notin \Gamma$.

Programme Python pour démonstration du théorème de Morley par Alain Connes

(Denise Vella-Chemla, 28.8.2020)

On voudrait fournir ici des résultats surprenants qui nous ont été inspirés par un travail tout l'été autour de la preuve par Alain Connes du théorème de Morley ([1]).

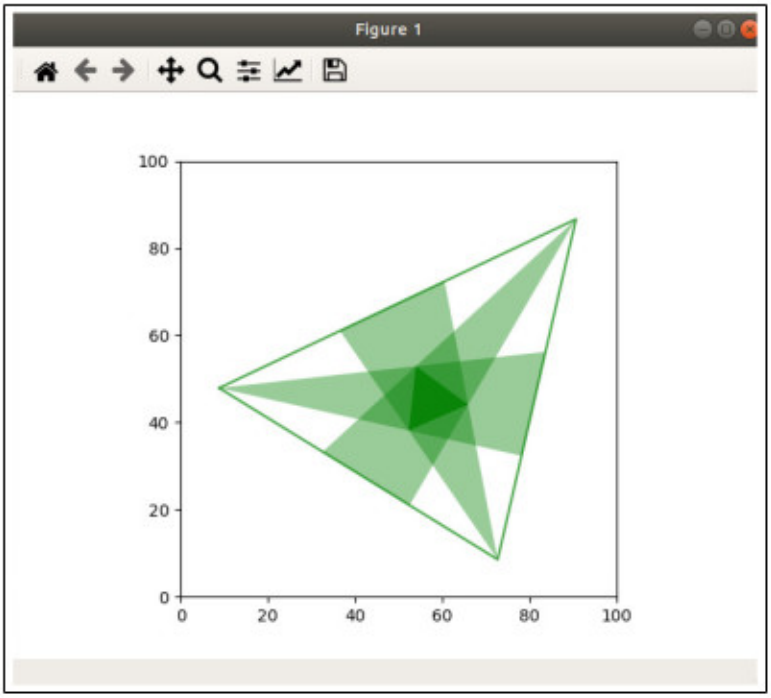
En effet, on souhaitait programmer la preuve pour essayer de vérifier que le théorème n'est pas applicable pour les triangles sphériques (voir notamment la conférence [2]).

Programme de vérification et visualisation du Théorème de Morley dans le plan

```
from math import *
from matplotlib import *
from matplotlib.pyplot import *

def vecteur(point1, point2):
  return [y - x for x, y in zip(point1, point2)]

def add(vecteur1, vecteur2):
  return [x + y for x, y in zip(vecteur1, vecteur2)]

def norme(vecteur):
  return sqrt(prodscal(vecteur, vecteur))

def prodscal(vecteur1, vecteur2):
  return sum([x*y for x, y in zip(vecteur1, vecteur2)])

def determ(vecteur1, vecteur2):
 return vecteur1[0]*vecteur2[1]-vecteur1[1]*vecteur2[0]

def angle(vecteur1, vecteur2):
  cosinus=prodscal(vecteur1, vecteur2)/(norme(vecteur1)*norme(vecteur2))
  sinus=determ(vecteur1, vecteur2)/(norme(vecteur1)*norme(vecteur2))
  return atan2(sinus,cosinus)

def rotation(u, theta):
  return [u[0]*cos(theta)-u[1]*sin(theta),u[0]*sin(theta)+u[1]*cos(theta)]

def intersecte(x, y, z, t):
  a1 = (y[1]-x[1])/(y[0]-x[0])
  b1 = x[1]-a1*x[0]
  a2 = (t[1]-z[1])/(t[0]-z[0])
  b2 = z[1]-a2*z[0]
  return [(b2-b1)/(a1-a2),((b2-b1)/(a1-a2))*a1+b1]

a=[8.83, 47.89]
b=[72.74, 8.55]
c=[90.72, 86.63]
ab = vecteur(a,b) ; ac = vecteur(a,c)
ba = vecteur(b,a) ; bc = vecteur(b,c)
ca = vecteur(c,a) ; cb = vecteur(c,b)
anglea=angle(ab,ac)  ; angleb=angle(bc,ba)  ; anglec=angle(ca,cb)
aprime = add(a, rotation(ab,anglea/3.0))  ; aseconde = add(a, rotation(ab,anglea*2.0/3.0))
bprime = add(b, rotation(bc,angleb/3.0)) ; bseconde = add(b, rotation(bc,angleb*2.0/3.0))
cprime = add(c, rotation(ca,anglec/3.0)) ; cseconde = add(c, rotation(ca,anglec*2.0/3.0))
p=intersecte(a,aseconde,b,c) ; q=intersecte(a,aprime,b,c)
r=intersecte(c,cseconde,a,b) ; s=intersecte(c,cprime,a,b)
t=intersecte(b,bseconde,c,a) ; u=intersecte(b,bprime,c,a)
n=intersecte(a,aseconde,c,cprime)
o=intersecte(c,cseconde,b,bprime)
x=intersecte(b,bseconde,a,aprime)
print('Normes des cotes %3.15f '% norme(vecteur(n,o)))
print('Normes des cotes %3.15f '% norme(vecteur(o,x)))
print('Normes des cotes %3.15f '% norme(vecteur(x,n)))

fig = matplotlib.pyplot.figure()
ax = fig.add_subplot(111)
matplotlib.pyplot.plot([a[0],b[0],c[0],a[0]],[a[1],b[1],c[1],a[1]], 'g', alpha=0.7)
matplotlib.pyplot.fill([a[0],p[0],q[0]],[a[1],p[1],q[1]], 'g', 2, alpha=0.4)
matplotlib.pyplot.fill([c[0],r[0],s[0]],[c[1],r[1],s[1]], 'g', 2, alpha=0.4)
matplotlib.pyplot.fill([b[0],t[0],u[0]],[b[1],t[1],u[1]], 'g', 2, alpha=0.4)
matplotlib.pyplot.fill([n[0],o[0],x[0]],[n[1],o[1],x[1]], 'g', 2, alpha=0.8)
matplotlib.pyplot.xlim(0,100)
matplotlib.pyplot.ylim(0,100)
ax.set\_aspect('equal')
matplotlib.pyplot.show()
```

Le programme ci-dessus produit la visualisation ci-après, et imprime comme longueur des normes des côtés du triangle de Morley (le triangle équilatéral de sommets les intersections des trissectrices adjacentes du triangle quelconque "externe") la valeur 14.863746806168091 pour deux côtés et la valeur 14.863746806168082 pour

le troisième côté : la différence entre les valeurs est négligeable, les côtés sont de longueur égale, le théorème le prouve, même si l'ordinateur ne le constate qu'à un ε près (d'ailleurs, l'ordinateur détecte toujours l'égalité de flottants (les réels en langage informatique) à un ε près).



On avait également programmé des rotations dans le cercle unité en langage Asymptote, puis en langage python, pour visualiser les décomposants de Goldbach sur le cercle par les programmes suivants :

Bibliographie

[1] Alain Connes, "A new proof of Morley's theorem", *Publications Mathématiques de l'IHÉS*, **S88** : 43-46, 1998.

[2] Transcription d'une vidéo d'Alain Connes au Collège de France, visionnable ici :https://www.college-de-france.fr/site/colloque-2018/symposium-2018-10-18-10h00.htm, http://denisevellachemla.eu/transc-AC-langage.pdf.

[3] Denise Vella-Chemla, Snurpf, exemple, 2019.http://denisevellachemla.eu/snurpf-exemple.pdf, démonstration de la caractérisation :http://denisevellachemla.eu/demo-caracterisation-DG.pdf.

Petite note pour mémoire d'août 2020

Denise Vella-Chemla

Cette petite note est destinée à garder trace d'une expérience de programmation de la preuve par Alain Connes du théorème de Morley par un fichier texte plutôt que par le contenu d'un blog, vite enfoui par sédimentation dans les limbes de la toile.

Selon le célèbre titre de l'opus de Donald E. Knuth (*The Art Of Computer Programming*), la programmation des ordinateurs est un art. Certains informaticiens sont des artistes en effet.

La démonstration par Alain Connes du théorème de Morley est une démonstration géométrique utilisant les affixes complexes des sommets d'un triangle. On trouvera sa traduction dans l'item 47) de la liste Transcriptions AC.

Inspiré par un tableau visible à cette adresse Johnson-Smithsonian, le tableau de Crockett Johnson de 1969 intitulé CJ69, représentant le théorème de Morley, un artiste de la programmation[1] a écrit un programme esthétique en asymptote, programme dont le résultat est cette belle image jctM.jpg.

Le programme en asymptote est consultable ici : Morley-asymptote.pdf.

On peut coller[2] le code fourni juste ci-dessus à cette adresse pour l'exécuter :Asymptote en ligne.

Ici une version dynamique en geogebra : on peut modifier les positions des sommets du triangle et on peut également modifier la position du point M, laissé invariant par le produit des cubes des symétries par rapport aux côtés du triangle initial :

Théorème de Morley - démonstration d'Alain Connes en geogebra.

[1] Jacques Chemla

[2] Faire un Copier (Ctrl+C), Coller (Ctrl+V) du code dans la fenêtre de code à gauche et cliquer sur le bouton Execute, le résultat du programme apparaît dans la fenêtre de droite.

Symétries

Alain Connes

Résumé : Le concept de symétrie va bien au-delà des simples symétries géométriques. De l'organisation harmonieuse des phases finales des coupes de football à la résolution des équations, en passant par le jeu de l'icosaèdre et le théorème de Morley, vous découvrirez les multiples facettes de ce concept.

Cet article se propose d'initier le lecteur, par quelques exemples illustratifs, à la notion de symétrie en mathématiques.

Pour mettre en évidence l'ubiquité de ce concept, au sens du mathématicien, nous commencerons par évoquer le lien entre la symétrie qui gouverne l'organisation de la phase finale des coupes de football et... la technique de résolution des équations du quatrième degré.

Le passage aux équations de degré supérieur sera l'occasion d'évoquer le jeu de l'icosaèdre et les "icosions", définis par le mathématicien irlandais William Hamilton au XIXe siècle.

Nous terminerons par une réflexion sur un théorème de géométrie, démontré par Frank Morley vers 1899, où la symétrie d'un triangle équilatère surgit comme par miracle d'un triangle arbitraire en prenant l'inter-section des "trissectrices" consécutives (les deux droites qui partagent un angle en trois parties égales). J'en ai donné, en 1998, une formulation et une démonstration algébriques que nous verrons ici.

Les phases finales des coupes de football

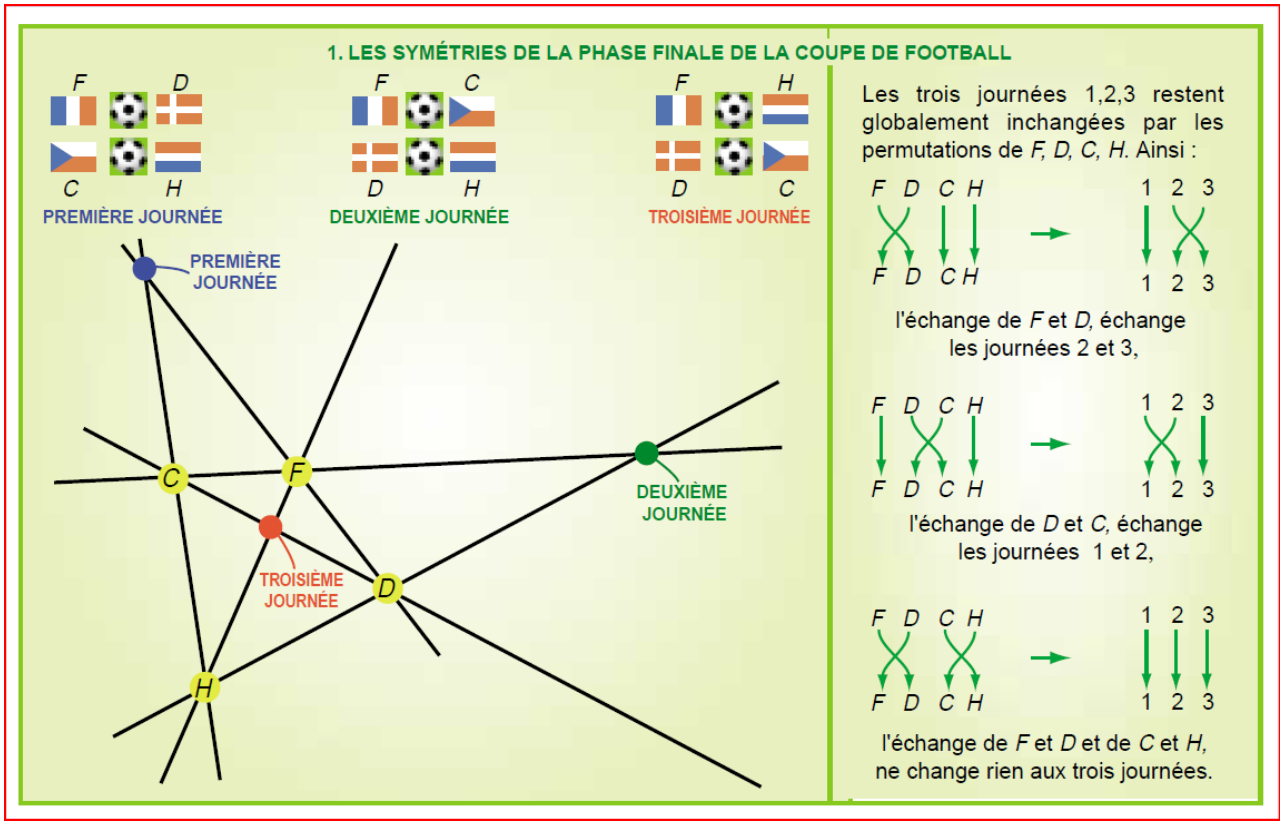
Commençons par l'organisation des coupes de football, par exemple de la dernière coupe d'Europe. Durant la phase finale, les équipes se retrouvent par poules de quatre au sein desquelles elles doivent se départager. La France, par exemple, se trouvait dans un groupe de quatre équipes, Danemark, France, Pays-Bas et République Tchèque (abrégées en D, F, H et C). Pour départager ces quatre équipes de manière équitable, il faut que chacune d'elles rencontre chacune des trois autres, de sorte que trois journées sont nécessaires. Quand deux équipes se rencontrent, D et F par exemple, les deux autres, H et C, s'affrontent le même jour et il suffit donc de trois journées pour obtenir toutes les configurations de rencontres possibles.

Dans l'exemple de la coupe d'Europe, les matchs des trois journées étaient, pour la première journée, les rencontres FD et CH, pour la deuxième journée, FC et DH, pour la dernière FH et DC. On perçoit intuitivement qu'une telle organisation est harmonieuse car aucune des quatre équipes n'est privilégiée. Ainsi l'on vérifie que si l'on permute arbitrairement certaines équipes, par exemple si l'on échange D et H, il en résulte une simple permutation des première et troisième journées.

Nous pouvons visualiser la symétrie qui est à l'œuvre en plaçant les lettres D, F, C, H représentant les équipes en quatre points du plan. À un match entre deux équipes correspond la droite joignant ces deux points et chacune des trois journées correspond naturellement au point d'intersection de

Référence : article du magazine Pour la Science de février 2001, n° 292, p. 36-43.
Transcription en LaTeX : Denise Vella-Chemla, août 2025.

deux droites, représentant les deux confrontations de la journée. Ainsi aux rencontres FD et CH, on associe l'intersection des droites FD et CH et ainsi de suite pour les deux autres couples, de sorte que la deuxième journée est à l'intersection des droites FC et DH et la troisième à l'intersection des droites FH et DC.



La figure ainsi construite, formée de quatre points et six droites, se nomme un quadrilatère complet. Elle est parfaitement symétrique (au sens abstrait, même si des symétries géométriques au sens commun - symétries par rapport à un point ou une droite - n'y apparaissent pas), puisque chacun des quatre points F, D, C et H joue exactement le même rôle que les autres, et qu'il en va de même des trois points de rencontre symbolisant les journées.

Après avoir visualisé ce quadrilatère complet, nous pouvons aussi formuler algébriquement la symétrie en question. Ainsi, la fonction qui aux quatre nombres a, b, c et d associe $\alpha = ab + cd$ ne prend que trois déterminations différentes quand on permute a, b, c et d : les deux autres déterminations étant $\beta = ac + bd$ et $\gamma = ad + bc$.

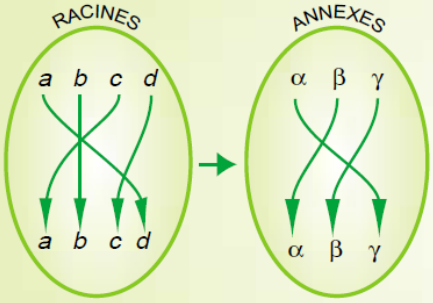
La résolution par radicaux des équations du 4° degré

Ce fait surprenant est à la base de la méthode générale permettant de résoudre "par radicaux" les équations du quatrième degré. Cette résolution consiste à exprimer les zéros a, b, c et d du polynôme $x^4 + nx^3 + px^2 + qx + r = (x-a)(x-b)(x-c)(x-d)$, c'est-à-dire les valeurs de x qui annulent le polynôme, en fonction des coefficients n, p, q, r et de l'extraction de racines.

Pour comprendre cette affirmation, il faut revenir un peu en arrière dans l'Histoire et examiner les résolutions des équations de degré inférieur à quatre.

2. SYMÉTRIES ET RÉSOLUTION PAR RADICAUX DES ÉQUATIONS DE DEGRÉ 3 et 4

La résolution par radicaux des équations polynomiales nécessite l'élaboration de fonctions annexes des racines, présentant des propriétés de symétries quand on permute les racines de ces équations.



L'ensemble de ces fonctions annexes est globalement inchangé par permutations des racines de l'équation. Dans les équations de degrés 3 et 4 ces fonctions annexes permettent de ramener la résolution de l'équation initiale à une équation "réduite" de degré inférieur.

1) Équation du troisième degré :

$x^3 + 3px + 2q = (x-a)(x-b)(x-c) = 0$.

Équation réduite : $x^2 + 2qx - p^3 = (x-\alpha)(x-\beta)$.

Trois racines : *a, b, c.*	Deux fonctions annexes : $\alpha = [(a + bj + cj^2)/3]^3$ $\beta = [(a + bj^2 + cj)/3]^3$ avec $j = (-1+i\sqrt{3})/2$, $j^2 = (-1-i\sqrt{3})/2$, *i* étant une racine carrée de –1, d'où $j^3 = 1$ et $j^2 + j + 1 = 0$.	Symétrie La symétrie réalisée par n'importe quelle permutation entre *a, b et c,* laisse globalement invariant l'ensemble des fonctions annexes {α,β}.	Solutions *Soient* $u = \sqrt[3]{\alpha}$ et $v = \sqrt[3]{\beta}$ tels que $uv = -p$. On a alors : $a = u + v$ $b = j^2u + jv$ $c = ju + j^2v$.

2) Équation du quatrième degré :

$x^4 + px^2 + qx + r = (x-a)(x-b)(x-c)(x-d) = 0$

Équation réduite :

$x^3 - px^2 - 4rx + (4pr - q^2) = (x-\alpha)(x-\beta)(x-\gamma) = 0$

Quatres racines : *a, b, c, d*	Trois fonctions annexes: $\alpha = ab + cd$ $\beta = ac + bd$ $\gamma = ad + bc$	Symétrie La symétrie réalisée par n'importe quelle permutation entre *a, b, c* et *d* laisse globalement invariant l'ensemble des trois fonctions annexes {α, β, γ}.	Solutions *1) Connaissant α=ab+cd et r=(ab)(cd), on en déduit les produits ab et cd. 2) Si ab≠cd, le système (a+b)+(c+d)= 0 et cd(a+b) + ab(c+d) = – q, donne a+b et c+d. 3) Connaissant ab et a+b on en déduit a et b. De même pour c et d.*

Si la technique de résolution des équations du second degré remonte à la plus haute antiquité (Babyloniens, Egyptiens...), elle n'a pu être étendue au troisième degré que bien plus tard, et ne sera publiée par Girolamo (Jérôme) Cardano qu'en 1545 dans les chapitres 11 à 23 de son livre *Ars magna sive de regulis algebraicis*. Bien que cela n'ait été reconnu qu'au XVIIIe siècle, la clef de la résolution par radicaux de l'équation du troisième degré, $x^3 + nx^2 + px + q = 0$, de racines a, b, c, est l'existence d'une fonction polynomiale $f(a, b, c)$ de a, b, c, qui ne prend que deux déterminations différentes sous l'action des six permutations de a, b, c.

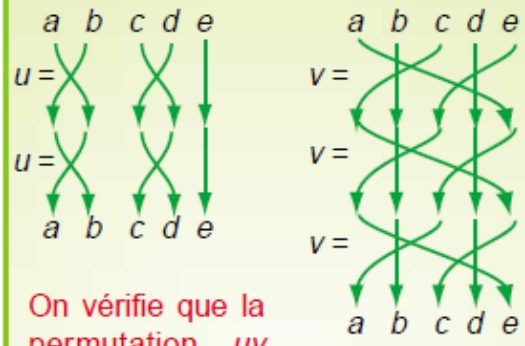
La méthode de Cardano revient à poser $\alpha = [(1/3)(a + bj + cj^2)]^3$, le nombre j étant la première racine cubique de l'unité, soit $\dfrac{-1 + i\sqrt{3}}{2}$, où i est une racine carrée de -1. La permutation circulaire transformant, à la fois a en b, b en c et c en a, laisse manifestement la fonction α inchangée et la seule autre détermination de la fonction α sous l'action des six permutations de a, b, c, est obtenue en transposant b et c par exemple, soit $\beta = [(1/3)(a + cj + bj^2)]^3$.

Comme l'ensemble de ces deux nombres α et β est invariant par toutes les permutations de a, b, c, le polynôme du second degré dont α et β sont racines est facile à calculer en fonction des coefficients de l'équation initiale $x^3 + nx^2 + px + q = 0$: c'est $x^2 + 2qx - p^3 = (x + q + s)(x + q - s)$, où s est l'une des racines carrées de $p^3 + q^2$ et où, pour simplifier les formules, l'on a réécrit l'équation

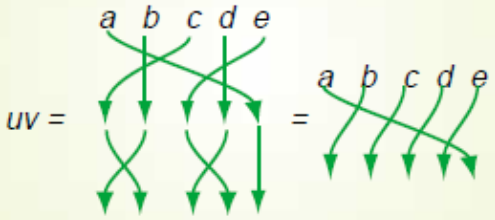
initiale sous la forme équivalente $x^3 + 3px + 2q = 0$ débarrassée du terme du deuxième degré en effectuant une translation convenable des racines et où l'on a introduit les coefficients 2 et 3.

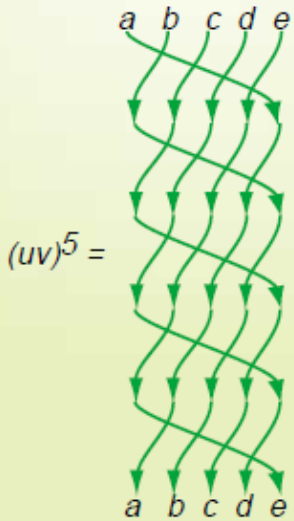
3. ORDRE D'UNE PERMUTATION

L'ordre d'une permutation est le plus petit entier n tel que si l'on applique n fois la permutation on obtient la permutation identique.
Ainsi la permutation u est d'ordre 2 et la permutation v est d'ordre 3 :



On vérifie que la permutation uv est d'ordre 5.





Un calcul simple montre alors que chacune des racines a, b et c, de l'équation initiale s'exprime

comme somme de l'une des trois racines cubiques de α et de l'une des trois racines cubiques de β ces deux choix étant liés par le fait que leur produit doit être impérativement égal à $-p$ (il n'y a donc que trois couples de choix de ces racines à prendre en compte, ce qui est rassurant, à la place des neuf possibilités que l'on aurait pu envisager a priori).

C'est à l'occasion de ces formules que l'utilisation des nombres complexes s'est imposée. En effet, même dans le cas où les trois racines sont réelles, il se peut que $p^3 + q^2$ soit négatif et que α et β soient alors nécessairement des nombres complexes.

Si la résolution des équations du troisième degré que nous venons d'exposer a été très longue à être mise au point (sans doute pour au moins l'un de ses cas particuliers par Scipione del Ferro entre 1500 et 1515), celle du quatrième degré a été plus preste à la suivre puisqu'elle figure également dans l'*Ars magna* (chapitre 39) où Cardano l'attribue à son secrétaire Ludovico Ferrari qui l'aurait trouvée entre 1540 et 1545 (René Descartes en publiera une autre en 1637). Et c'est cette résolution qui nous ramène à la première symétrie que nous avons rencontrée, celle de l'organisation des finales, du quadrilatère complet, et de la fonction $ab + cd$. Ici encore, l'on peut partir d'un polynôme débarrassé du coefficient de x^3, annulé par la même technique que précédemment, soit $x^4 + px^2 + qx + r = (x - a)(x - b)(x - c)(x - d)$. L'ensemble des trois nombres $\alpha = ab+cd, \beta = ac+bd, \gamma = ad+bc$ est invariant par chacune des 24 permutations agissant sur a, b, c et d. Ce sont donc les racines d'une équation du troisième degré dont les coefficients s'expriment facilement en fonction de p, q et r. Le calcul montre que le polynôme $(x-\alpha)(x-\beta)(x-\gamma)$ est égal à $x^3 - px^2 - 4rx + (4pr - q^2)$. II peut donc être décomposé comme on l'a vu plus haut pour en déduire α, β, et γ ; en fait, il suffit même de calculer l'une seulement de ces racines, disons α, pour en déduire a, b, c et d (nous connaissons alors en effet la somme α et le produit r des deux nombres ab et cd, donc ces deux nombres eux-mêmes par une équation du second degré, et il ne reste plus qu'à exploiter les éga-lités $(a + b) + (c + d) = 0$ et $ab(c + d) + cd(a + b) = -q$ pour en déduire $a + b$ et $c + d$, donc enfin a, b, c et d).

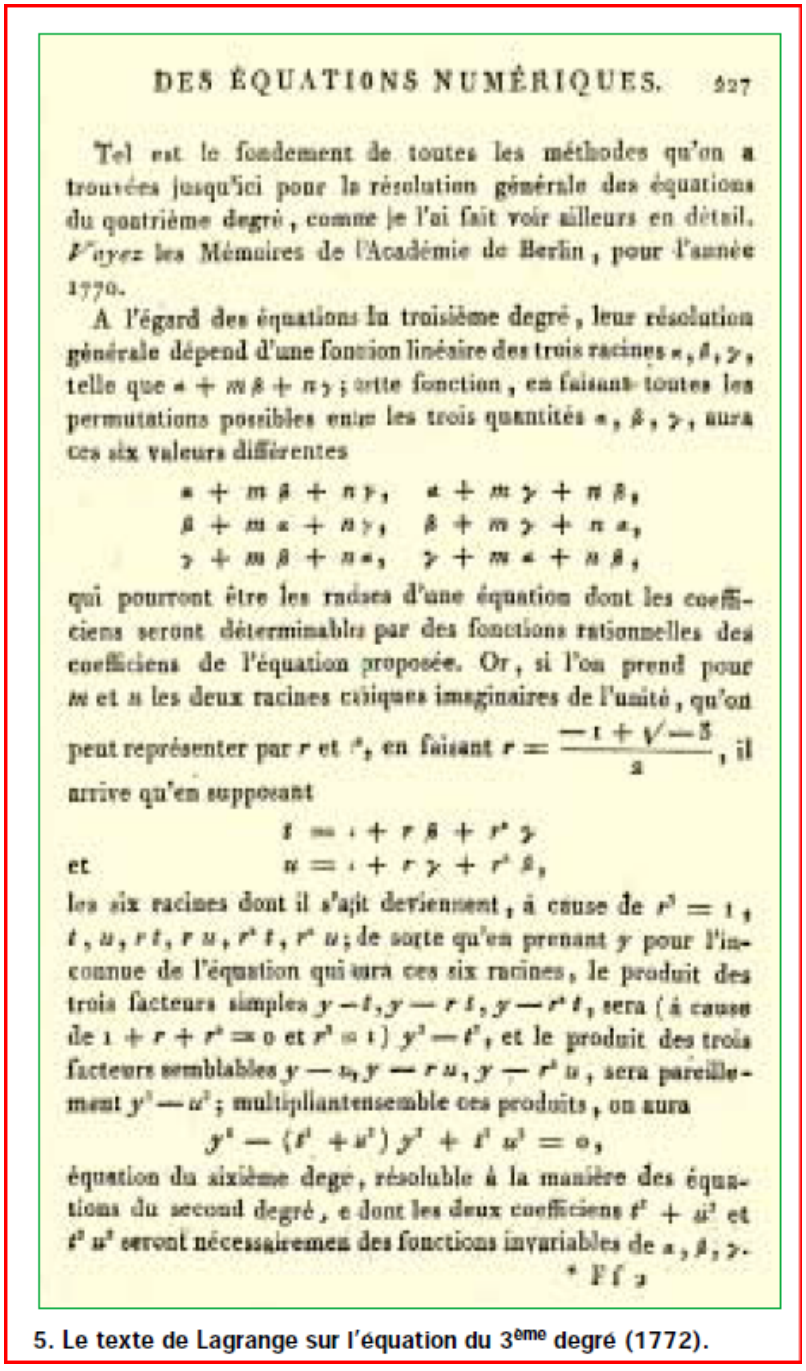
C'est à Joseph Louis Lagrange en 1770 et 1771 (publication en 1772, et dans une moindre mesure, à Alexandre Vandermonde dans un mémoire publié en 1774, mais également rédigé vers 1770, ainsi qu'à Edward Waring dans ses *Meditationes algebrica* de 1770 et à Francesco Malfatti) que l'on doit la mise en lumière du rôle fondamental des permutations sur les racines $a, b, c...$ et sur les quantités auxiliaires α, $\beta...$ d'ailleurs aujourd'hui justement appelées "résolvantes de Lagrange".

Ces résolvantes ne sont pas uniques (ainsi aurait-on également pu poser $\alpha = (a + b - c - d)^2$ dans le cas du quatrième degré, ce qui correspond à la solution de Descartes), mais elles fournissent la clef de toutes les résolutions générales par radicaux.

Abel et Galois

Il était normal de désirer aller plus loin : Descartes a certainement essayé et avec lui bien des chercheurs. L'étape suivante est évidemment celle du cinquième degré. Elle a toujours opposé des obstacles infranchissables, et nous savons depuis Abel et Galois (qui obtiennent leurs résultats aux alentours de 1830), pourquoi cette quête était vaine. Dans tous les cas précédents, nous avions pu associer à une famille de n nombres $a, b, c, d...$ (avec n inférieur ou égal à 4) une famille de

$n-1$ nombres $\alpha, \beta, \gamma...$ s'exprimant comme des polynômes en $a, b, c, d...$ et dont l'ensemble était globalement invariant par chacune des permutations de ces lettres. Plus précisément, notons S_n le groupe des bijections de l'ensemble $(a, b, c, d...)$ dans lui-même ; ce qui est possible pour n strictement inférieur à 5 c'est de définir une application de S_n sur S_{n-1}, respectant la composition des permutations.



DES ÉQUATIONS NUMÉRIQUES. 527

Tel est le fondement de toutes les méthodes qu'on a trouvées jusqu'ici pour la résolution générale des équations du quatrième degré, comme je l'ai fait voir ailleurs en détail. *Voyez* les Mémoires de l'Académie de Berlin, pour l'année 1770.

A l'égard des équations du troisième degré, leur résolution générale dépend d'une fonction linéaire des trois racines α, β, γ, telle que $\alpha + m\beta + n\gamma$; cette fonction, en faisant toutes les permutations possibles entre les trois quantités α, β, γ, aura ces six valeurs différentes

$$\begin{array}{ll} \alpha + m\beta + n\gamma, & \alpha + m\gamma + n\beta, \\ \beta + m\alpha + n\gamma, & \beta + m\gamma + n\alpha, \\ \gamma + m\beta + n\alpha, & \gamma + m\alpha + n\beta, \end{array}$$

qui pourront être les racines d'une équation dont les coefficiens seront déterminables par des fonctions rationnelles des coefficiens de l'équation proposée. Or, si l'on prend pour m et n les deux racines cubiques imaginaires de l'unité, qu'on peut représenter par r et r^2, en faisant $r = \frac{-1+\sqrt{-3}}{2}$, il arrive qu'en supposant

$$t = 1 + r\beta + r^2\gamma$$

et

$$u = 1 + r\gamma + r^2\beta,$$

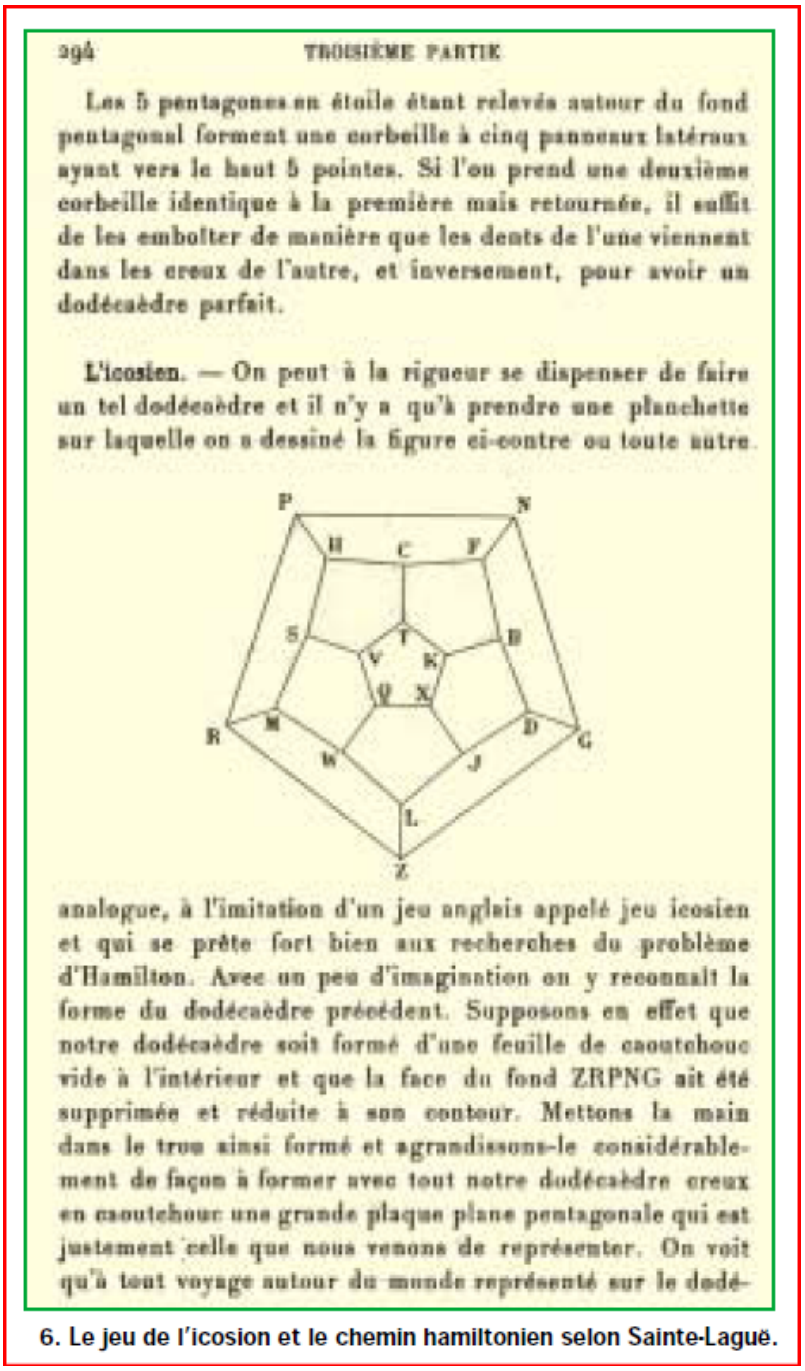
les six racines dont il s'agit deviennent, à cause de $r^3 = 1$, t, u, rt, ru, r^2t, r^2u; de sorte qu'en prenant y pour l'inconnue de l'équation qui aura ces six racines, le produit des trois facteurs simples $y-t, y-rt, y-r^2t$, sera (à cause de $1+r+r^2=0$ et $r^3=1$) y^3-t^3, et le produit des trois facteurs semblables $y-u, y-ru, y-r^2u$, sera pareillement y^3-u^3; multipliantensemble ces produits, on aura

$$y^6 - (t^3+u^3)y^3 + t^3u^3 = 0,$$

équation du sixième degré, résoluble à la manière des équations du second degré, et dont les deux coefficiens t^3+u^3 et t^3u^3 seront nécessairemen des fonctions invariables de α, β, γ.

* Ff 2

5. Le texte de Lagrange sur l'équation du 3ème degré (1772).



394 TROISIÈME PARTIE

Les 5 pentagones en étoile étant relevés autour du fond pentagonal forment une corbeille à cinq panneaux latéraux ayant vers le haut 5 pointes. Si l'on prend une deuxième corbeille identique à la première mais retournée, il suffit de les emboîter de manière que les dents de l'une viennent dans les creux de l'autre, et inversement, pour avoir un dodécaèdre parfait.

L'icosien. — On peut à la rigueur se dispenser de faire un tel dodécaèdre et il n'y a qu'à prendre une planchette sur laquelle on a dessiné la figure ci-contre ou toute autre

analogue, à l'imitation d'un jeu anglais appelé jeu icosien et qui se prête fort bien aux recherches du problème d'Hamilton. Avec un peu d'imagination on y reconnaît la forme du dodécaèdre précédent. Supposons en effet que notre dodécaèdre soit formé d'une feuille de caoutchouc vide à l'intérieur et que la face du fond ZRPNG ait été supprimée et réduite à son contour. Mettons la main dans le trou ainsi formé et agrandissons-le considérablement de façon à former avec tout notre dodécaèdre creux en caoutchouc une grande plaque plane pentagonale qui est justement celle que nous venons de représenter. On voit qu'à tout voyage autour du monde représenté sur le dodé-

6. Le jeu de l'icosion et le chemin hamiltonien selon Sainte-Laguë.

On sait depuis le début du XIXe siècle que l'existence d'une telle application du groupe S_n sur S_{n-1}, ou même une telle application (non constante) du groupe A_n des permutations paires (produits de deux, quatre, six transpositions) dans un groupe S_m avec m inférieur à n, est impossible pour n plus grand que 4. Cela démontre que la méthode de Lagrange ne peut être étendue à n égal à 5 ni aux valeurs supérieures, mais c'est naturellement insuffisant pour démontrer qu'une résolution d'une équation générale de degré supérieur à 4 n'est pas possible par radicaux - il se pourrait que d'autres méthodes, plus générales, réussissent là où Lagrange aurait échoué. Aujourd'hui, nous savons, toujours d'après Abel et Galois, que cette généralisation même est impossible. Ce problème fondamental et complexe intéressera de nombreux mathématiciens des plus célèbres, parmi lesquels

Leonhard Euler qui y reviendra à plusieurs reprises et surtout Karl Friedrich Gauss (1801) et Louis-Augustin Cauchy (1813).

Arrêtons-nous au cas du degré cinq, pour lequel Descartes par exemple, persuadé qu'il n'existait pas de formule analogue à celle de Cardano, avait proposé en 1637, dans *La Géométrie*, une méthode graphique de résolution grâce à l'intersection de cercles et de cubiques qu'il avait inventée pour l'occasion. Entre 1799 et 1813 (date de l'édition de ses *Riflessioni intorno alla solutione delle equazioni algebraiche generali*), Paolo Ruffini a publié diverses tentatives de démonstrations, de plus en plus affinées, visant à établir l'impossibilité de résoudre l'équation générale du cinquième degré par radicaux. À toute fonction rationnelle des racines, il a eu l'idée juste d'associer le groupe des permutations de ces racines qui laissent cette fonction invariante, mais il a cru à tort que les radicaux intervenant dans la résolution de l'équation, comme les racines cubiques pour le degré trois, étaient nécessairement des fonctions rationnelles des racines.

Il faudra attendre 1824 pour que Niels Abel justifie l'intuition de Ruffini dans son *Mémoire sur les équations algébriques*. Abel, après avoir cru trouver au contraire une méthode de résolution générale, prouve l'impossibilité de résoudre l'équation générale du cinquième degré par radicaux, en 1826 dans le *Mémoire sur une classe particulière d'équations résolubles algébriquement*, où il amorce une théorie générale qui ne s'épanouira que dans les écrits de Galois, vers 1830. Les travaux de Galois inaugurent une ère nouvelle des mathématiques, où les calculs font place à la réflexion sur leur potentialité et les concepts, tels celui de groupe abstrait ou d'extension algébrique occupent le devant de la scène.

L'idée lumineuse de Galois consiste d'abord à associer à une équation arbitraire un groupe de permutations qu'il définit en ces termes :

Soit une équation donnée dont $a, b, c...m$ sont les racines. Il y aura toujours un groupe de permutations des lettres $a, b, c...m$ qui jouira de la propriété suivante :

1) *que toute fonction des racines, invariante par les substitutions de ce groupe soit rationnellement connue* ;

2) *réciproquement, que toute fonction des racines, déterminée rationnellement, soit invariante par ces substitutions.*

Puis Galois étudie comment ce groupe "d'ambiguïté" se trouve modifié par l'adjonction de quantités auxi-liaires considérées dès lors comme "rationnelles". Résoudre une équation par radicaux revient alors à résoudre son groupe de Galois.

L'impossibilité de réduire l'équation du cinquième degré à des équations de degré inférieur provient alors de la "simplicité" du groupe A_5 des soixante permutations paires (produits d'un nombre pair de transpositions) des cinq racines a, b, c, d, e d'une telle équation. On dit qu'un groupe abstrait est "simple" si l'on ne peut l'envoyer (par une application non constante) dans un groupe plus petit tout en préservant la loi de groupe. Le groupe A_5 est le plus petit groupe simple non commutatif et il apparaît très souvent en mathématiques. Ce groupe se présente très économiquement : il est engendré par deux éléments u et v vérifiant les relations $u^2 = 1$, $v^3 = 1$ et $(uv)^5 = 1$, ce qui nous

donne l'occasion d'en venir aux icosions d'Hamilton.

Les icosions d'Hamilton

Après avoir découvert les quaternions, William Hamilton a tenté de construire en 1857 une nouvelle algèbre, formée de nombres généralisés qu'il appelait les icosions. Deux d'entre eux, notés u et v, que Hamilton dénommait racines non commutatives de l'unité, devaient vérifier $u^2 = 1, v^3 = 1$ et $(uv)^5 = 1$. Un calcul enfantin montre que si $uv = vu$, on a $v = 1v = u^5v^5v = u^5v^6 = (u^2)^2u(v^3)^2 = u$ puis $u = v = vu^2 = v^3 = 1$. Ainsi l'on ne peut représenter u et v dans aucun des groupes S_n avec n inférieur ou égal à 4. Pour représenter u et v dans le groupe A_5, des permutations paires des cinq lettres (a, b, c, d, e), il suffit de poser $u = (b, a, d, c, e)$, permutation qui laisse fixe e et échange a et b, c et d, et $v = (e, b, a, d, c)$ la permutation qui laisse fixe b et d, et qui change a en $e = v(a)$, c en $a = v(c)$ et e en $c = v(e)$. Le produit uv est alors la permutation cyclique (e, a, b, c, d) qui est bien d'ordre cinq. L'on peut ainsi représenter u et v de 120 manières différentes (mais deux à deux isomorphes) dans le groupe A_5.

Le groupe A_5 est isomorphe au groupe des rotations qui conservent un icosaèdre ou, ce qui revient au même, un dodécaèdre (ces deux corps sont les plus intéressants des cinq solides platoniciens, qui - avec le tétraèdre régulier, le cube et l'octaèdre formé par les six centres des faces d'un cube - sont les seuls polyèdres convexes réguliers existant dans notre espace habituel).

Pour obtenir l'isomorphisme cherché, il suffit d'associer à u l'une des 15 rotations d'ordre deux (une symétrie dont l'axe est l'une des 15 médiatrices communes à deux arêtes parallèles) et à v l'une des 20 rotations d'ordre trois (dont l'axe relie l'un des dix couples de deux sommets diamétralement opposés du dodécaèdre ou des centres de deux faces parallèles de l'icosaèdre) de telle sorte que le produit uv soit l'une des 24 rotations d'ordre cinq (dont l'axe relie l'un des six couples de centres de deux faces parallèles du dodécaèdre ou de deux sommets diamétralement opposés de l'icosaèdre) ; les 60 rotations conservant ce solide peuvent toutes s'exprimer simplement comme produits des générateurs u et v.

Bien que les deux icosions u, v engendrent le groupe A_5 et vérifient les relations $u^2 = 1, v^3 = 1$ et $(uv)^5 = 1$, il n'est pas immédiat que ces relations constituent une présentation de ce groupe, c'est-à-dire que toute autre relation entre u et v s'en déduise. Il y a deux façons de s'en convaincre, algébrique ou géométrique (voir les figures 4 et 7).

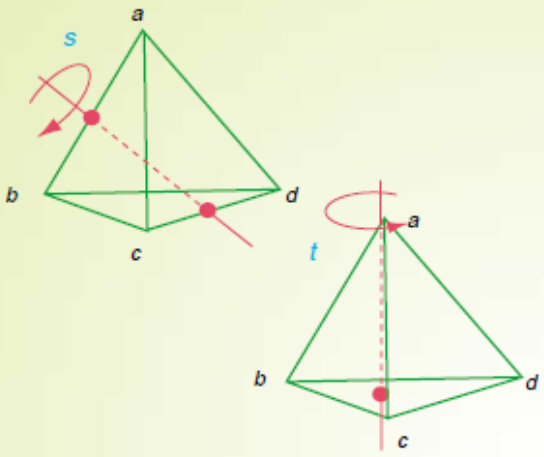
C'est à propos du graphe des arêtes du dodécaèdre, qui a les mêmes symétries que celui de l'icosaèdre, qu'Hamilton mit au point le "jeu de l'icosaèdre" qu'il appelait aussi "jeu des racines non commutatives de l'unité". Ce jeu constitue le premier exemple de ce que l'on appelle maintenant la recherche d'un circuit hamiltonien, concept très important dans la théorie moderne des graphes (voir la figure 6). Il s'agit d'un défi concernant les 20 sommets d'un dodécaèdre, qu'il s'agit de parcourir en suivant les arêtes du polyèdre de façon à passer par chaque sommet une fois et une seule, les sommets de départ et d'arrivée étant eux-mêmes liés par une arête qui permet de fermer le circuit. On pourra lire à ce sujet le remarquable essai de 1937 d'André Sainte-Laguë *Avec des nombres et des lignes*, réédité par Vuibert en 1994.

4. ÉTUDE DES GROUPES A_4 ET A_5

A) LE GROUPE A_4

1) Le groupe A_4 est le groupe des permutations paires sur les quatre lettres *(a,b,c,d)*. Ce groupe est engendré par les permutations $s = \begin{bmatrix} a & b & c & d \\ b & a & d & c \end{bmatrix}$, qui transforme *a* en *b*, *b* en *a*, *c* en *d* et *d* en *c*, *et* $t = \begin{bmatrix} a & b & c & d \\ a & c & d & b \end{bmatrix}$, qui transforme *a* en *a*, *b* en *c*, *c* en *d* et *d* en *b*. Celles-ci vérifient les règles : $s^2=1$, $t^3=1$, $(st)^3=1$.

2) Il existe une représentation géométrique du groupe A_4 : Ce groupe est le groupe des rotations conservant le tétraèdre régulier *a,b,c,d* .



s est représentée par la symétrie par rapport à la médiatrice commune à *ab* et *cd*.

t est représentée par la rotation d'angle 2π/3 autour de l'axe du tétraèdre passant par *a*.

$st = \begin{bmatrix} a & b & c & d \\ b & d & c & a \end{bmatrix}$ est la rotation d'angle 2π/3 autour de l'axe du tétraèdre passant par *c*.

Le lecteur patient vérifiera que les règles de simplification $s^2=1$, $t^3=1$, $(st)^3=1$ constituent une présentation de ce groupe, c'est-à-dire suffisent pour montrer qu'en les combinant avec la loi de groupe, il existe seulement douze "mots" différents constitués des lettres *s* et *t*.

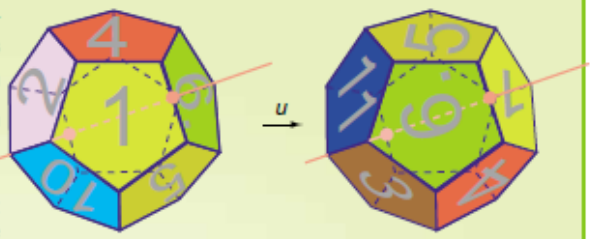
B) LE GROUPE A_5

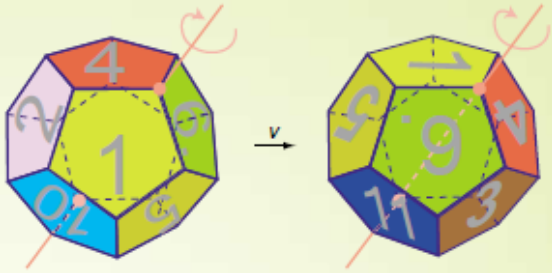
1) Le groupe A_5 est le groupe des permutations paires sur les cinq lettres *(a,b,c,d,e)*. Ce groupe est engendré par les permutations $u = \begin{bmatrix} a & b & c & d & e \\ b & a & d & c & e \end{bmatrix}$, qui transforme *a* en *b*, *b* en *a*, *c* en *d* , *d* en *c*, *et e en e, et* $v = \begin{bmatrix} a & b & c & d & e \\ e & b & a & d & c \end{bmatrix}$, qui transforme *a* en *e*, *b* en *b*, *c* en *a d* en *d et e en c*. Celles-ci vérifient les règles : $u^2=1$, $v^3=1$, $(uv)^5=1$ (bien sûr *u* et *v* ne commutent pas).

2) Ce groupe a 60 éléments et est isomorphe au groupe des rotations du dodécaèdre régulier.

Ainsi *u* est l'une des 15 symétries relatives à la médiatrice commune à deux arêtes elles-mêmes symétriques par rapport au centre.

De même, *v* est l'une des 20 rotations d'angle 2π/3 autour d'une droite joignant deux sommets symétriques par rapport au centre du dodécaèdre.





C) PRÉSENTATION DE A_5

Le lecteur patient vérifiera que les règles de simplification $u^2=1$, $v^3=1$, $(uv)^5=1$ suffisent avec la loi de groupe pour montrer qu'il existe seulement soixante mots différents constitués des lettres *u* et *v*. On commencera, en posant $s = u$, $t = k^{-2}uk$ (où $k = uv$), par montrer que *s* et *t* vérifient la présentation de A_4, c'est-à-dire les règles de simplification $s^2=1$, $t^3=1$, $(st)^3=1$. On montrera ensuite que tout mot avec les lettres *u* et *v* s'écrit grâce aux règles de simplification ci-dessus sous la forme $k^m h$, *m* étant égal à 0,1,2,3,4 et *h* étant un mot écrit avec les lettres *s* et *t*. Comme il existe exactement 12 éléments *h*, on trouve que le groupe A_5 est bien présenté par les relations ci-dessus.

D) A_5, GROUPE DE MATRICES

1) Notons $F_5 = Z/5Z$ le corps des entiers relatifs modulo 5. Dans ce corps, 4 + 2 =1, 3 + 2 =0, 4 x 2 = 3, 3 x 2 =1, etc.

2) Représentons u et v comme les transformations suivantes de l'espace projectif $P_1(F_5)$. Cet espace projectif contient, outre les cinq éléments de F_5, un point "à l'infini" noté 1/0. Posons $u(z) = -1/z$ pour *z* élément de $P_1(F_5)$. Nous avons clairement $u^2(z)=z$, c'est-à-dire $u^2=1$. Posons maintenant $v(z) = -1/(z+1)$: nous pouvons vérifier que $v^3=1$. Nous vérifions la présentation de A_5 puisque $k=uv$ est donné par $k(z) = z+1$, et $k^m(z) = z+m$, de sorte que $k^5=1$ car, dans F_5, 5 est égal à 0.

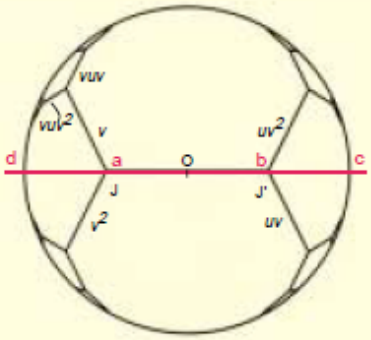
3) Donnons une représentation matricielle des éléments *u* et *v*. Étant donné des éléments *a,b,c,d* de F_5, *avec* $ad - bc = 1$, on associe à la matrice $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, la transformation *f de* $P_1(F_5)$, donnée par:

$$\begin{bmatrix} f(z) \\ 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} z \\ 1 \end{bmatrix}.$$

Le groupe de transformation ainsi obtenu est noté $PSL(2,F_5)$, pour groupe spécial linéaire projectifié de F_5. Ainsi *u, v, k,* et *t,* y sont représentés par les matrices:

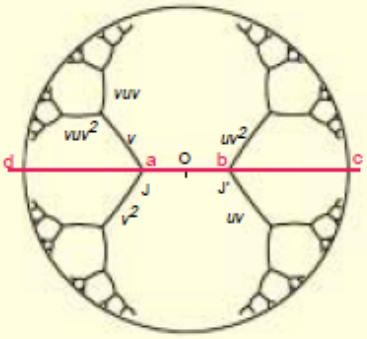
$$u = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad v = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \quad k^m = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \text{ puis } t = \begin{bmatrix} -2 & -3 \\ 1 & 1 \end{bmatrix}$$

7. REVÊTEMENT UNIVERSEL ET GÉOMÉTRIE NON EUCLIDIENNE



A **MODÈLE DE KLEIN**

Longueur du segment [a,b] = Log $\frac{ac \times bd}{ad \times bc}$



B **MODÈLE DE POINCARÉ**

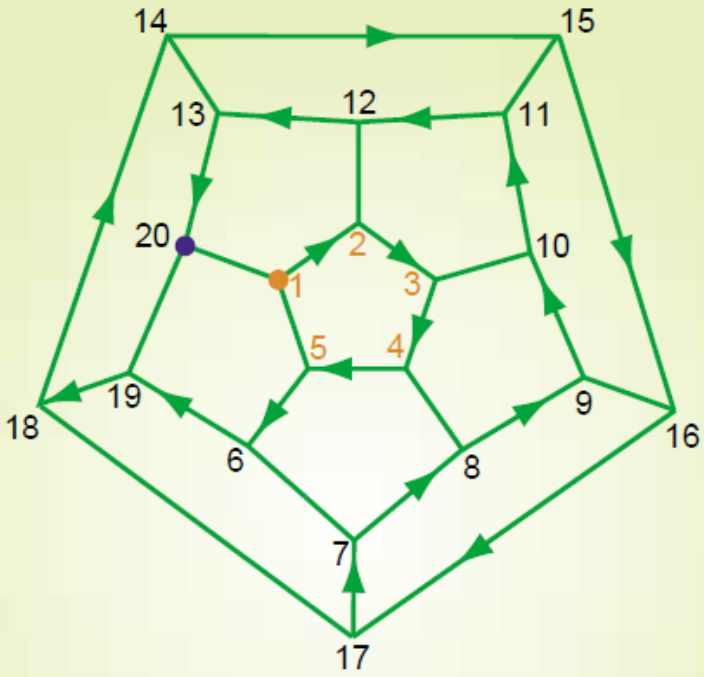
Pour comprendre géométriquement le groupe engendré par deux éléments *u* et *v* et présenté par les relations $u^2=1$, $v^3=1$, $(uv)^5=1$, l'on commence par considérer simplement les deux premières relations ($u^2=1$, $v^3=1$). Le groupe ainsi obtenu est le groupe PSL(2,Z) que l'on comprend en visualisant son action sur un arbre infini T dont trois arêtes partent de chaque sommet. La troisième relation ($(uv)^5=1$) se comprend alors en identifiant l'arbre T avec le revêtement universel du graphe de la figure 6 (ce revêtement universel, au sens de Poincaré, est obtenu en considérant tous les chemins qui suivent les arêtes du dodécaèdre régulier). L'arbre infini T est représenté selon deux modèles de la géométrie non-euclidienne, le modèle de Klein *(A)* et le modèle de Poincaré *(B)*. Dans les deux modèles l'ensemble des points de la géométrie plane est l'intérieur d'un disque. Dans le modèle de Klein le segment reliant deux points n'est autre que le segment de la géométrie euclidienne ; seule change la longueur de ce segment. Dans ce modèle, la longueur d'un segment ab est donnée par le logarithme du birapport *(ab, cd)* de *ab*, avec les points d'intersections *c* et *d* de la droite *ab* avec le cercle C. Ainsi : [a,b] = log $\frac{ac \times bd}{ad \times bc}$. Les arêtes de l'arbre T sont des segments de droite de longueurs égales.

Dans le modèle de Poincaré, les droites sont les arcs de cercles orthogonaux au cercle *C*, et la notion d'angle y est la même que dans la géométrie euclidienne. Les distances sont données par 2 Log*(ab, cd)* où le birapport *(ab, cd)* est calculé sur le cercle passant par *(a,b,c,d)* et où le facteur 2 est visible en comparant *(A)* et *(B)*.

Le groupe PSL(2, Z) est représenté par des isométries de la géométrie non euclidienne. Ce groupe a pour présentation les relations $u^2=1$ et $v^3=1$. L'élément *u* est donné par la symétrie par rapport à l'origine O, et l'élément *v*, par la rotation non euclidienne de centre J et d'angle $2\pi/3$. En appliquant, à l'arête JJ', les opérations représentées par les mots (tels que *uvvuuuvuv*...) dont les lettres sont les éléments *u* et *v*, on obtient exactement l'arbre T du revêtement universel du graphe du jeu de l'icosion d'Hamilton. En particulier, chacun des chemins hamiltoniens est un point de ce revêtement universel.

On obtient le dodécaèdre en identifiant les arêtes de l'arbre T qui sont congrues modulo 5. Cette congruence signifie que l'on passe de l'une à l'autre de ces arêtes par une isométrie non euclidienne donnée par un élément $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ du groupe PSL(2, Z) vérifiant $a = 1$ (modulo 5), $b = 0$ (modulo 5), $c = 0$ (modulo 5), $d = 1$ (modulo 5). Ainsi la présentation du groupe A_5 qui impose la relation supplémentaire $(uv)^5 = 1$ revient à quotienter PSL(2, Z) par le sous-groupe normal G engendré par $(uv)^5$. Le quotient de T par G n'est autre que le graphe formé par les arêtes du dodécaèdre. Le groupe quotient PSL(2, Z)/G est le groupe PSL(2, F_5) de la figure 4.

8.LE JEU DE L'ICOSION

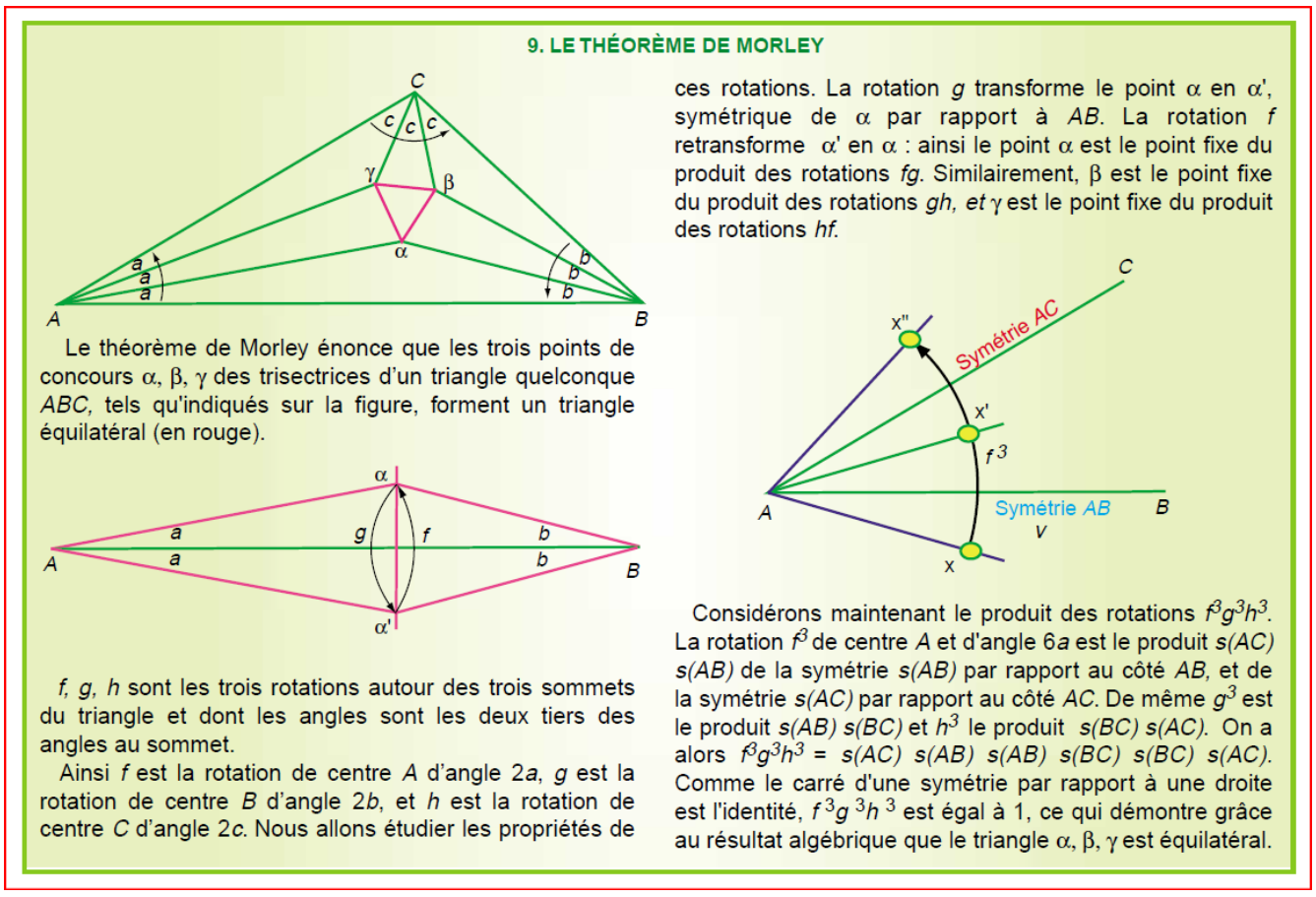


Sainte-Laguë dans son livre *Avec des nombres et des lignes,*, a fait revivre le jeu de l'icosion inventé par le mathématicien irlandais Hamilton (1805-1865). Le jeu consiste à compléter le circuit passant par tous les sommets d'un icosaèdre une fois et une seule ; on donne au départ, les cinq premiers sommets. En voici un exemple : (1, 2, 3, 4, 5, 6, 19, 18, 14, 15, 16, 17, 7, 8, 9, 10, 11, 12, 13, 20).

Le triangle de Morley

Il n'y a pas d'"ange de la géométrie" en rivalité avec le "diable de l'algèbre", mais une connivence fructueuse entre les aires visuelles du cerveau, qui décèlent d'un coup d'œil l'harmonie d'une configuration, et celles du langage qui la distille en écritures algébriques. Nous terminerons cette initiation au concept de symétrie par un bel exemple de cette connivence en évoquant le théorème de Morley. Il constitue également un domaine où les symétries, concrètes d'origine géométrique, et

abstraites et algébriques quand on le regarde sous un nouvel angle, se conjuguent de façon forte et laissent une réelle impression de beauté.



Le mathématicien britannique Frank Morley fut l'un des premiers enseignants des universités américaines. C'est au tournant du siècle précédent qu'à l'occasion de recherches sur les familles de cardioïdes tangentes aux trois côtés d'un triangle donné, il dégagea la propriété suivante : les trois couples de trissectrices intérieures de ses trois angles (c'est-à-dire des droites qui découpent ces angles en trois angles égaux, à la manière des bissectrices bien connues) se coupent en six points dont trois forment un triangle équilatéral.

La démonstration originale, assez difficile, est basée sur d'ingénieux calculs à base de géométrie analytique superbement maîtrisée. Il existe de nombreuses preuves de ce résultat, ainsi que des généralisations portant jusqu'à 18, voire 27 (et même davantage) triangles équilatéraux que l'on peut dégager à partir des 108 points d'intersections des 18 trissectrices obtenues à partir des trissectrices intérieures par des rotations d'angle $2\theta/3$. Parmi ces preuves, il en existe par le calcul trigonométrique, mais aussi par la géométrie pure, comme celle qu'a donnée Raoul Bricard en 1922.

Il en existe une de toute autre nature, qui l'éclaire sous un angle intéressant puisqu'elle permet d'étendre ce résultat a priori fortement euclidien à la géométrie de la droite affine sur un corps k arbitraire. Le résultat d'algèbre pure qui contient (et étend) la propriété des trissectrices est d'une telle généralité que sa démonstration devient une simple vérification (un énoncé très général est

souvent plus simple à démontrer qu'un cas particulier, car le nombre d'hypothèses que l'on doit utiliser est d'autant plus réduit). Il s'énonce ainsi :

Si G est le groupe affine d'un corps commutatif k (c'est-à-dire des applications g de k dans k qui peuvent s'écrire sous la forme $g(x) = ax + b$, où a, noté $a(g)$, est non nul), alors pour tout triplet (f, g, h) d'éléments de G tels que $j = a(fgh)$ soit différent de 1 et que fg, gh et hf ne soient pas des translations, il y a équivalence entre les deux assertions suivantes :

a) $f^3g^3h^3 = 1$ (transformation identique) ;

b) $j^3 = 1$ et $\alpha + j\beta + j^2\gamma = 0$ où α est l'unique point fixe de fg, β celui de gh et γ celui de hf.

Reste à montrer comment cette propriété algébrique très abstraite permet de mieux comprendre (et de prouver par la même occasion) le théorème de Morley. Nous prendrons pour k le corps des nombres complexes, pour lequel le groupe affine est celui des similitudes directes, et dont un sous-groupe est celui des rotations (il faut et il suffit que a soit de module 1 pour que g soit une rotation). Nous prendrons pour f, g, h les trois rotations autour des trois sommets du triangle et dont les angles sont les deux tiers des angles au sommet. Ainsi f est la rotation de centre A d'angle $2a/3$, g celle de centre B et d'angle $2b/3$ et h celle de centre C et d'angle $2c/3$. Le produit des cubes $f^3g^3h^3$ est égal à 1, car f^3 par exemple est le produit de deux symétries par rapport aux côtés de l'angle en A, de sorte que ces symétries se simplifient deux à deux dans le produit $f^3g^3h^3$.

L'équivalence ci-dessus montre donc que $\alpha + j\beta + j^2\gamma = 0$, où α, β, γ sont les points fixes de fg, gh et hf et où le nombre $j = a(fgh)$ est la première racine cubique de l'unité, que nous avons déjà rencontrée dans le cours de cet article. La relation $\alpha + j\beta + j^2\gamma = 0$ est une caractérisation bien connue des triangles équilatéraux. (Elle peut encore s'écrire sous la forme $(\alpha - \beta)/(\gamma - \beta) = -j^2$, ce qui montre que l'on passe du vecteur $\beta\gamma$ au vecteur $\beta\alpha$ par une rotation d'angle $\pi/3$).

Une vieille recette, connue des personnes ayant reçu une forte imprégnation de géométrie classique, montre que le point α défini par $f(g(\alpha)) = \alpha$ n'est autre que l'intersection de la trissectrice issue de A et de la trissectrice issue de B les plus proches du côté AB. Le lecteur pourra s'en persuader en vérifiant que la rotation g de centre B et d'angle $2b$ transforme ce point d'intersection en son symétrique par rapport au côté AB, et que la rotation f de centre A et d'angle $2a$ le remet exactement à sa place. Il en va de même pour les points β et γ. Nous avons donc démontré que le triangle (α, β, γ) est équilatéral. Nous voyons même en prime que, dans cet ordre, il est décrit dans le sens positif (opposé à celui des aiguilles d'une montre). Cette preuve s'applique tout autant aux autres triangles équilatéraux de Morley : les 18 trissectrices obtenues à partir des trissectrices intérieures par des rotations d'angle $\neq \pi/3$ permettent de modifier f, g et h sans changer le produit de leurs cubes et donnent de nouvelles solutions de l'équation a) et autant de triangles équilatéraux !

La dualité entre algèbre et géométrie, évidente dans les exemples ci-dessus, permet de repousser plus loin les limites de nos concepts géométriques, déjà libérés du carcan euclidien par l'avènement des géométries non euclidiennes (voir la figure 7).

La découverte de la mécanique quantique et de la non-commutativité des coordonnées sur l'espace des phases d'un système atomique a engendré dans les 20 dernières années une évolution largement

aussi radicale des concepts géométriques, libérant la notion d'espace de la commutativité des coordonnées.

En géométrie non commutative la notion de symétrie devient plus subtile, les groupes évoqués dans cet article étant remplacés par des algèbres inventées par le mathématicien Heinz Hopf, illustrant la belle définition d'Hermann Weyl extraite de son livre *Symétrie et mathématique moderne* :

> "*La symétrie n'est en aucune façon restreinte aux objets qui occupent un certain espace. Symétrique veut dire quelque chose comme bien proportionné, bien équilibré, et la symétrie indique alors cette sorte d'harmonie entre les diverses parties grâce à quoi elles s'intègrent dans un tout : la beauté est liée à cette symétrie-là*".

Alain Connes, Médaille Fields et Prix Crafoord, est professeur au Collège de France et à l'Institut des Hautes Études Scientifiques. Il tient à remercier André Warusfel de son aide très précieuse pour la rédaction de la conférence organisée par Jean-Pierre Bourguignon en septembre 2000 au centre Georges Pompidou. La Revue de Mathématiques de l'Enseignement Supérieur publiera, dans l'un de ses numéros de l'année universitaire 2001-2002, un exposé d'André Warusfel sur les configurations de Morley et quelques preuves des symétries sous-tendant ces objets spectaculaires, dont celles de Morley et de l'auteur de cet article.

Note de la transcriptrice : l'article dans le magazine avait pour titre le graphisme ci-dessous. En omettant la couleur et l'accent, une petite erreur s'est glissée parmi les droites (ou centres) de symétrie des différentes lettres.

Jouer avec les valeurs propres de l'opérateur de Dirac

Michael Creutz
Département de physique, Laboratoire nationale de Brookhaven
Upton, NY 11973, États-Unis

Résumé : On parle souvent de la physique des basses énergies en théorie de réseau de jauge en fonction des petites valeurs propres de l'opérateur de Dirac du réseau. Je m'intéresse aux pièges qui découlent de cette pratique dans l'interprétation de ces spectres de valeurs propres.

1 Introduction

Dans la communauté des réseaux de jauge, il est devenu assez populaire récemment d'étudier la distribution des valeurs propres de l'opérateur de Dirac en présence de champs de jauge sous-jacents engendrés dans les simulations. Il y a plusieurs motivations à cela. D'abord, dans la théorie classique, Banks et Casher[1] ont relié la densité des petites valeurs propres de l'opérateur de Dirac à la brisure spontanée de la symétrie chirale. Ensuite, les discrétisations du réseau de l'opérateur de Dirac basées sur la relation de Ginsparg-Wilson [2] ont les valeurs propres correspondantes qui sont sur des cercles dans le plan complexe. La validité des diverses approximations d'un tel opérateur peut être attestée qualitativement en regardant les valeurs propres. Troisièmement, utiliser la méthode du chevauchement de régions pour construire un opérateur de Dirac avec la bonne symétrie chirale présente des difficultés si l'opérateur de Wilson des fermions a de petites valeurs propres. Cela peut influencer la sélection des paramètres de la simulation, tels que l'action de jauge[4]. Finalement, puisque les petites valeurs propres entravent les méthodes de gradient conjugué, séparer ces valeurs propres explicitement peut potentiellement être utile pour développer des algorithmes de simulation dynamique.[5]

Malgré cet intérêt pour les distributions des valeurs propres, il y a quelques dangers inhérents à l'interprétation de ces observations. Les résultats physiques proviennent de l'intégrale de chemin à la fois sur les champs bosoniques et fermioniques. Calculer ces intégrales une par une est bien, mais essayer d'interpréter les résultats intermédiaires est dangereux de façon inhérente. Alors que les valeurs propres de l'opérateur de Dirac dépendent du champ de jauge donné, il est important de se rappeler que dans une simulation dynamique, la distribution du champ de jauge elle-même dépend des valeurs propres. Ce comportement circulaire donne un système hautement non linéaire, et de tels systèmes sont de façon notoire difficiles à interpréter.

Étant données ces gaies circonstances, je présenterai certain de ces problèmes en fonction d'un ensemble amusant de puzzles provenant des interprétations naïves des valeurs

Référence : https://arxiv.org/pdf/hep-lat/0511052https://arxiv.org/pdf/hep-lat/0511052.
Traduction : Denise Vella-Chemla, août 2025.

propres de l'opérateur de Dirac sur le réseau. La discussion sera un mélange de pensées provoquantes et d'idées qui ajoutent de la confusion. Elle ne sera pas nécessairement particulièrement profonde ou nouvelle.

2 Le modèle

Pour commencer, j'ai besoin d'établir le contexte de la discussion. Je considère une intégrale de chemin générique pour une théorie de jauge

$$Z = \int (dA)(d\psi)(d\overline{\psi})\; e^{-S_G(A)+\overline{\psi}D(A)\psi}. \tag{1}$$

Ici A et ψ représentent des champs de jauge et de quarks, respectivement, $S_G(A)$ est la partie purement jauge de l'action et $D(A)$ représente l'opérateur en usage pour les quarks. Comme l'action est quadratique dans les champs de fermions, une intégration formelle donne

$$Z = \int (dA)\; |D(A)|\; e^{-S_G(A)}. \tag{2}$$

En travaillant sur un réseau fini, le réseau $D(A)$ est une matrice de dimension finie, et pour un champ de jauge donné, je peux considérer formellement ses valeurs et ses vecteurs propres

$$D(A)\psi_i = \lambda_i \psi_i. \tag{3}$$

Le déterminant apparaissant dans l'éq. (2) est le produit de ces valeurs propres ; donc, l'intégrale de chemin prend la forme

$$Z = \int (dA)\; e^{-S_G(A)} \prod_i \lambda_i. \tag{4}$$

Faire la moyenne sur les champs de jauge définit la densité des valeurs propres

$$\rho(x+iy) = \frac{1}{NZ} \int (dA)\; |D(A)|\; e^{-S_G(A)} \sum_i \delta(x - \mathrm{Re}\lambda_i(A))\delta(y - \mathrm{Im}\lambda_i(A)). \tag{5}$$

Ici, N est la dimension de l'opérateur de Dirac, qui inclut le volume, la jauge, le spin et les indices de saveur.

Dans les situations où le déterminant des fermions n'est pas positif, ρ peut être négatif ou complexe. Pourtant, je continue de faire référence à lui comme à une densité. Je supposerai que ρ est réel ; les situations dans lesquelles cela n'est pas vrai, comme avec un potentiel chimique fini,[6] sont hors du champ du présent exposé.

Au potentiel chimique zéro, toutes les actions utilisées en pratique satisfont une herméticité "γ_5"

$$\gamma_5 D \gamma_5 = D^\dagger. \tag{6}$$

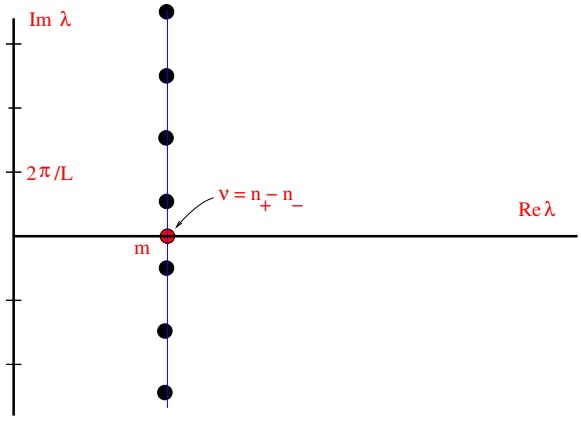


Figure 1: Dans le dessin continu naïf, toutes les valeurs propres de l'opérateur de Dirac sont le long d'une droite parallèle à l'axe imaginaire. Dans un volume fini, ces valeurs propres deviennent discrètes. Les valeurs propres réelles se séparent selon différentes chiralités et définissent un invariant topologique.

Avec cette condition, toutes les valeurs propres non réelles adviennent par paires de complexes conjugués, ce qui implique que pour la densité, on a

$$\rho(z) = \rho(z^*). \tag{7}$$

Cette propriété sera partagée par tous les opérateurs considérés dans la discussion ci-dessous.

L'objet de la recherche consiste à trouver des énoncés généraux liant le comportement de la densité des valeurs propres à des propriétés physiques de la théorie. Je répète la mise en garde que l'on a faite plus tôt ; ρ dépend de la distribution du champ de jauge A qui en retour est pondéré par ρ qui dépend de la distribution de A...

2.1 Le continuum

Bien sûr, la théorie du continu est seulement définie réellement comme la limite de la théorie du réseau. Pourtant, il est parfois utile de rappeler l'image standard, où l'opérateur de Dirac

$$D = \gamma_\mu(\partial_\mu + igA_\mu) + m$$

est la somme d'une partie anti-hermitienne et de la masse du quark m. Toutes les valeurs propres ont la même partie réelle m

$$\rho(x + iy) = \delta(x - m)\widetilde{\rho}(y).$$

Les valeurs propres appartenant à une droite parallèle à l'axe imaginaire, avec la condition d'herméticité de l'éq. (6), cela implique qu'elles apparaissent comme paires de

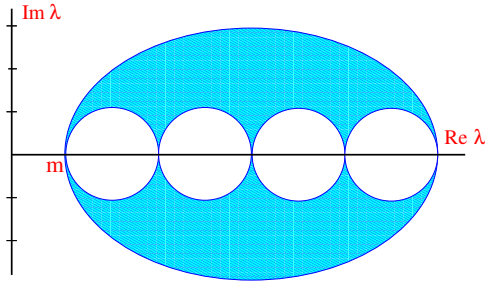


Figure 2: des fermions de Wilson libres montrent un spectre de valeurs propres avec une partie réelle dépendant du moment. Cela enlève les doublons en leur donnant une grande masse effective.

complexes conjugués.

En se restreignant au sous-espace des valeurs propres réelles, γ_5 commute avec D et par conséquent, ces vecteurs propres peuvent être séparés selon leur chiralité.

La différence entre le nombre de valeurs propres positives et négatives de γ_5 dans ce sous-espace définit un indice relié à la structure topologique du champ de jauge.[7] La structure de base est schématisée dans la fig. 1.

L'argument de Banks et Casher lie un $\widetilde{\rho}(0)$ ne s'évanouissant pas au condensat chiral qui apparaît quand la masse tend vers zéro. J'en dirai plus sur cela dans le contexte du réseau.

Notons que le dessin naïf suggère une symétrie entre les masses négatives et positives. À cause des anomalies, ceci est faux. Avec un nombre impair de saveurs, la théorie obtenue en échangeant les signes de toutes les masses des fermions est physiquement non équivalente à la théorie initiale.

2.2 Fermions de Wilson

Le réseau révèle que la situation véritable est considérablement plus embrouillée du fait de l'anomalie chirale. Avec les infinis ultraviolets, toutes les symétries naïves de l'action du réseau sont des symétries réelles. Les fermions naïfs ne peuvent pas avoir d'anomalies, qui sont supprimées par les états extraordinaires appelés doublons. Les fermions de Wilson[8] évitent ce problème en donnant une grande partie réelle aux valeurs propres correspondant à de tels doublons. Pour les fermions de Wilson libres, la structure des valeurs propres montre une forme simple telle que celle fournie par la Fig. 2.

Lorsque le champ de jauge est lancé, cette forme disparaît. Une complication additionnelle est que l'opérateur D n'est alors plus normal, i.e. $[D, D^\dagger] \neq 0$ et les vecteurs

propres ne sont plus nécessairement orthogonaux.

Les valeurs propres complexes vont toujours par paires, bien que, comme le champ de jauge varie, les paires complexes de valeurs propres puissent être en collision et se séparer le long de l'axe réel. En général, les valeurs propres réelles formeront une distribution continue.

Comme dans le continu, un indice peut être défini à partir du spectre de l'opérateur de Wilson-Dirac. À nouveau, l'herméticité γ_5 permet de trier les valeurs propres par chiralité. Pour supprimer la contribution des valeurs propres des doublons, sélectionnons un point à l'intérieur du cercle ouvert le plus à gauche de la Fig. 2. Définissons alors l'indice du champ de jauge comme étant la chiralité de réseau de toutes les valeurs propres sous ce point. Pour un champ de jauge lisse, cela est en accord avec le nombre topologique d'enroulements obtenu à partir de leur interpolation dans le continu. Cela correspond également au nombre d'enroulement sous l'opérateur de chevauchement.

2.3 Le chevauchement

Les fermions de Wilson ont un comportement assez compliqué selon des transformations chirales. Le formalisme du chevauchement (*overlap*)[3] simplifie cela en projetant d'abord la matrice de Wilson D_W sur un opérateur unitaire

$$V = (D_W D_W^\dagger)^{-1/2} D_W. \tag{8}$$

On doit comprendre cela comme le fait d'aller dans une base qui diagonalise $D_W D_W^\dagger$, puis d'effectuer l'inversion, puis de revenir dans la base initiale. En fonction de cette quantité unitaire, la matrice de chevauchement est

$$D = 1 + V. \tag{9}$$

Le processus de projection est schématisé dans la Fig. 2.3. La masse utilisée dans l'opérateur de Wilson de départ est prise comme une valeur négative qu'on sélectionne de telle façon que les états de moment faible soient projetés sur les valeurs propres basses, alors que les états des doublons sont envoyés vers $\lambda \sim 2$.

L'opérateur de chevauchement a quelques belles propriétés. D'abord, il satisfait la relation de Ginsparg-Wilson,[2] qu'on écrit succinctement comme l'unitaire de V couplé avec son herméticité γ_5

$$\gamma_5 V \gamma_5 V = 1. \tag{10}$$

Comme il est construit à partir d'un opérateur unitaire, la normalité de D est garantie. Mais, plus important encore, il exhibe une version réseau d'une symétrie chirale exacte.[9]

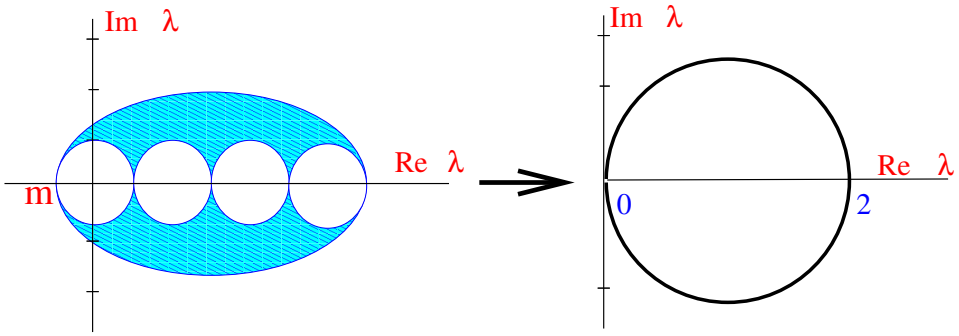


Fig. 3 : L'opérateur de chevauchement est constuit en projetant l'opérateur de Wilson-Dirac sur un opérateur unitaire.

L'action fermionique $\overline{\psi}D\psi$ est invariante selon la transformation

$$\begin{array}{l}\psi \to e^{i\theta\gamma_5}\psi \\ \overline{\psi} \to \overline{\psi}e^{i\theta\widehat{\gamma}_5}\end{array} \tag{11}$$

où

$$\widehat{\gamma}_5 = V\gamma_5. \tag{12}$$

Comme avec γ_5, cette quantité est hermitienne et son carré est 1. Par conséquent, ses valeurs propres sont ± 1. La trace définit un indice

$$\nu = \frac{1}{2}\mathrm{Tr}\widehat{\gamma}_5 \tag{13}$$

qui joue exactement le rôle de l'indice dans le continuum.

Il est important de noter que l'opérateur de chevauchement n'est pas unique. Sa forme précise dépend de l'opérateur particulier initial choisi pour se projeter sur la forme unitaire. En utilisant l'opérateur de Wilson-Dirac dans ce but, le résultat dépend encore de la masse utilisée en entrée. Du fait de ses origines historiques dans le formalisme du mur du domaine, cette quantité est parfois appelée la "hauteur du mur du domaine".

Comme le chevauchement n'est pas unique, il peut rester une ambiguité pour déterminer le nombre d'enroulements d'une configuration de jauge donnée. Des problèmes surgissent quand $D_W D_W^\dagger$ n'est pas inversible, et pour un champ de jauge donné, cela peut arriver pour des valeurs spécifiques du point de projection. Ce problème peut être évité pour les champs de jauge "lisses". En effet, une "condition d'admissibilité", [10,11] requérant que toutes les valeurs des plaquettes restent suffisamment proches de l'identité, supprime l'ambiguité. Malheureusement, cette condition est incompatible avec la positivité de la réflexion.[12] À cause de ces problèmes, on ne sait pas si la sensibilité topologique est en

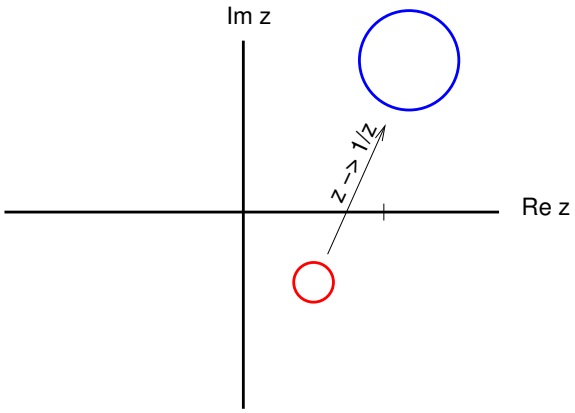


Figure 3: L'inversion d'un cercle complexe engendre un autre cercle.

fait une observable physique bien définie. D'un autre côté, comme la façon de mesurer cette sensibilité est maintenant claire dans une expérience de diffusion, il semble y avoir peu de raison de s'intéresser au fait que ça soit une observable ou pas.

3 Un condensat chiral de Cheshire

Maintenant que j'ai revu le paradigme de base, il est temps de s'amuser un peu. Je calculerai le condensat chiral dans le formalisme de chevauchement. Je dois vous prévenir du fait que pour vous amuser, je commence d'une façon intentionnellement très décevante.

3.1 Il est ici

Je commence avec la théorie du chevauchement standard sans masse. Je souhaite calculer la quantité $\langle\overline{\psi}\psi\rangle$. De façon remarquable, on peut faire ce calcul de manière exacte. Je commence avec

$$\langle\overline{\psi}\psi\rangle = \langle \mathrm{Tr} D^{-1}\rangle = \left\langle \sum_i \frac{1}{\lambda_i}\right\rangle = \left\langle \sum \mathrm{Re}\frac{1}{\lambda_i}\right\rangle \tag{14}$$

où j'ai utilisé l'appariement complexe des valeurs propres pour éliminer les parties imaginaires. À la fin, la moyenne doit être calculée sur les configurations de jauge adéquatement pondérées.

Maintenant, la caractéristique cruciale de l'opérateur de chevauchement est que ses valeurs propres sont toutes sur un cercle du plan complexe. Une propriété intéressante d'un cercle complexe et que les inverses de tous ses points engendrent un autre cercle, comme

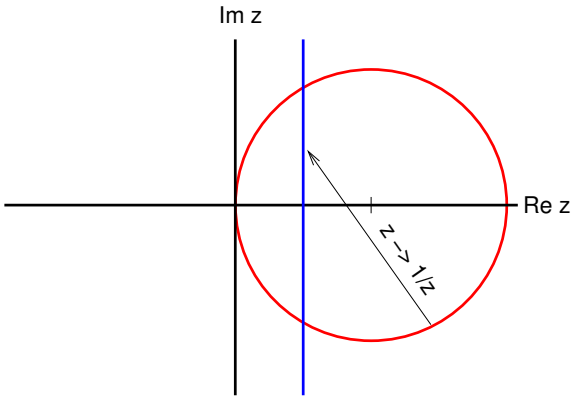


Figure 4: L'inversion de l'opérateur de chevauchement engendre une droite de partie réelle $1/2$.

montré sur la Fig. 3.

Ce processus est, pourtant, assez singulier pour l'opérateur de chevauchement lui-même puisque le cercle correspondant contient l'origine. Dans ce cas, l'inverse du cercle est de rayon infini, i.e. il dégénère en une droite. Pour le cercle de l'opérateur de chevauchement, avec son centre en $z = 1$ et son rayon 1, l'inverse du cercle est une droite de partie réelle $1/2$ et parallèle à l'axe imaginaire. C'est ce qui est montré sur la Fig. 4.

Ce placement des valeurs propres permet un calcul immédiat du condensat

$$\langle\overline{\psi}\psi\rangle = \sum \mathrm{Re}\frac{1}{\lambda_i} = \sum \frac{1}{2} = \frac{N}{2}. \tag{15}$$

Ici, N est la dimension de la matrice, et inclut le facteur de volume attendu.

Ainsi le condensat, supposé être un signal pour la brisure de symétrie chirale spontanée, ne s'évanouit pas ! Mais quelque chose est équivoque, je n'ai utilisé aucune dynamique. Le résultat est aussi indépendant de la configuration de jauge.

3.2 Il s'en est allé

Donc sophistiquons un peu. Sur le réseau, la symétrie chirale est plus compliquée que dans le continuum, faisant intervenir à la fois γ_5 et $\widehat{\gamma}_5$ d'une façon assez imbriquée. En particulier, l'opérateur $\overline{\psi}\psi$ ne se transforme pas de façon simple selon aucune rotation chirale. Une combinaison potentiellement plus jolie est $\overline{\psi}(1 - D/2)\psi$. Si je considère la rotation de l'Eq. (11) avec $\theta = \pi/2$, cette quantité devient son opposée. Mais il est aussi facile de calculer ce qui est attendu de cela aussi bien. Le second terme fait intervenir

$$\langle\overline{\psi}D\psi\rangle = \mathrm{Tr}D^{-1}D = \mathrm{Tr}I = N. \tag{16}$$

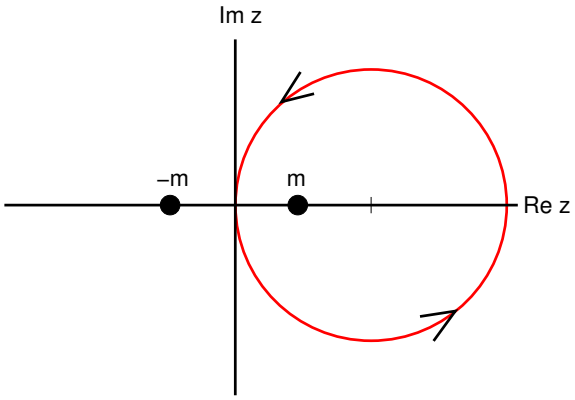


Figure 5: Comme la masse change de signe, un pôle va de l'intérieur à l'extérieur du cercle de chevauchement. Cela engendre un saut dans le condensat.

En mettant les deux morceaux ensemble

$$\langle\overline{\psi}(1-D/2)\psi\rangle = N/2 - N/2 = 0. \tag{17}$$

Donc, j'ai perdu le condensat chiral dont j'avais si facilement montré qu'il ne s'évanouissait pas il y a un instant. Comment s'est-il évaporé ?

3.3 Il est de retour

Le problème provient d'un traitement des limites sans faire suffisamment attention. Dans un volume fini, $\langle\overline{\psi}(1-D/2)\psi\rangle$ doit s'évanouir juste à partir de la symétrie chirale exacte du réseau. Cet évanouissement a lieu pour toutes les configurations de jauge. Pour procéder, introduisons une petite masse et faisons tendre le volume à l'infini d'abord, et puis alors, faisons tendre la masse vers zéro. Dans ce but, considérons la quantité

$$\langle\overline{\psi}\psi\rangle = \sum_i \frac{1}{\lambda_i + m}. \tag{18}$$

Le signal de la brisure de symétrie chirale est un saut vers cette quantité quand la masse passe à travers zéro.

Lorsque le volume tend vers l'infini, remplaçons la somme ci-dessus par une intégrale de contour autour du cercle de chevauchement en utilisant $z = 1 + e^{i\theta}$. Au facteur de volume trivial près, je devrais évaluer

$$i\int_0^{2\pi} d\theta \frac{\rho(\theta)}{1 + e^{i\theta} + m}. \tag{19}$$

Lorsque la masse passe à travers zéro, le pôle en $z = -m$ passe de l'extérieur à l'intérieur du cercle, comme montré dans la Fig. 5. Alors qu'il passe à travers le cercle, le résidu du pôle est $\rho(0) = \lim_{\theta \to 0} \rho(\theta)$.

Donc en général, les sauts s'effectuent par valeurs de $2\pi\rho(0)$. Ceci est la version de chevauchement de la relation de Banks-Casher [1] ; un saut non trivial dans le condensat est corrélé à un $\rho(0)$ qui ne s'évanouit pas.

Notons que les modes zéros exacts reliés à la topologie sont supprimés par la masse et ne contribuent pas à ce saut. Pour une saveur, pourtant, les modes zéros donnent effectivement naissance à une contribution ne s'évanouissant pas mais lisse dans le condensat [13]. On en dira plus sur ce point ultérieurement.

4 Un autre puzzle

Pour deux saveurs des quarks de lumière, on s'attend à une brisure de symétrie spontanée. C'est l'explication de la masse lumineuse du pion, qui est une approximation du boson de Goldstone. Dans le schéma ci-dessus, la théorie des deux saveurs devrait avoir un $\rho(0)$ qui ne s'évanouit pas.

Maintenant considérons la théorie à une seule saveur. Dans ce cas, il devrait ne pas y avoir de symétrie chirale. La célèbre anomalie $U(1)$ brise la symétrie naïve. On s'attend à ce qu'aucune des particules physiques soit sans masse quand la masse du quark s'évanouit. De plus, des arguments de lagrangien chiral simple [14,15] pour les théories à saveurs multiples indiquent qu'on s'attend à ce qu'il n'y ait aucune singularité quand seulement l'un des quarks passe à travers la masse nulle. De la discussion ci-dessus, on est amené à la conclusion que pour la théorie à une seule saveur, $\rho(0)$ doit s'évanouir.

Mais considérons maintenant l'intégrale de chemin originale après que les fermions aient été intégrés à l'extérieur [a] . En changeant le nombre de saveurs, N_f se manifeste dans la puissance du déterminant

$$\int dA \, |D|^{N_f} \, e^{-S_g(A)}. \tag{20}$$

Naïvement, cela suggère que lorsqu'on augmente le nombre de saveurs, la densité des valeurs propres basses devrait décroître. Mais je viens juste de dire qu'avec deux saveurs, $\rho(0) \neq 0$ alors qu'avec une seule saveur, $\rho(0) = 0$. Comment peut-il se faire que le fait d'augmenter le nombre de saveurs augmente effectivement la densité des petites valeurs propres ?

[a] *Note de la traductrice : to integrate out : sortir de l'intégration ??*

Ceci est un exemple clair de la façon dont la nature non-linéaire du problème peut produire des résultats contre-intuitifs. La densité des valeurs propres dépend de la distribution du champ de jauge, mais la distribution du champ de jauge dépend de la densité des valeurs propres . Ce ne sont pas seulement les valeurs propres basses qui sont importantes dans ce problème. Le champ fermionique tend vers un champ de jauge lisse, et ce processus fait intervenir toutes les échelles de valeurs. Un champ de jauge plus lisse peut donner en retour davantage de valeurs propres basses. Ainsi, les valeurs propres élevées influencent les valeurs propres basses, et cet effet peut outrepasser de manière évidente la suppression naïve de davantage de puissances du déterminant.

5 Instantons éthérés

À travers le théorème de l'indice, la structure topologique du champ de jauge se manifeste dans les modes zéros de l'opérateur de Dirac sans masse. Insérons à nouveau une petite masse et considérons l'intégrale de chemin avec les fermions intégrés à l'extérieur

$$Z = \int dA\, e^{-S_g} \prod_i (\lambda_i + m). \tag{21}$$

Si je fais tendre la masse vers zéro, toute configuration qui contient un mode propre nul aura un poids nul dans l'intégrale de chemin. Cela suggère que pour la théorie sans masse, je peux ignorer tous les effets instantons puisque ces configurations ne contribuent pas à l'intégrale de chemin.

Qu'est-ce qui est faux dans cet argument ? Le problème n'est pas de se demander si les modes zéros contribuent ou pas à l'intégrale de chemin, mais s'ils peuvent contribuer à des fonctions de corrélation physiques. Pour voir comment ça se passe, ajoutons quelques sources à l'intégrale de chemin

$$Z(\eta, \overline{\eta}) = \int dA\, d\psi\, d\overline{\psi}\, e^{-S_g + \overline{\psi}(D+m)\psi + \overline{\psi}\eta + \overline{\eta}\psi}. \tag{22}$$

La différentiation (au sens de Grassmann) par rapport à η et $\overline{\eta}$ donne les fonctions de corrélation fermioniques. Maintenant intégrons les fermions dehors selon

$$Z = \int dA\, e^{-S_g - \overline{\eta}(D+m)^{-1}\eta} \prod_i (\lambda_i + m). \tag{23}$$

Si je considère une source qui chevauche l'un des vecteurs propres de mode zéro, i.e.

$$(\psi_0, \eta) \neq 0, \tag{24}$$

la contribution de la source introduit un facteur $1/m$. Cela annule le m du déterminant, laissant une contribution finie lorsque m tend vers zéro.

Avec des saveurs multiples, le déterminant aura un facteur de masse à partir de chacune d'elles. Quand on fait tendre plusieurs masses vers zéro ensemble, on aura besoin d'un facteur similaire à partir des sources pour chacune d'elles. Ce produit de termes sources est la fameux "sommet de 't Hooft"[16]. Alors qu'il est correct de sortir les instantons de Z, ils perdurent dans les fonctions de corrélation.

Alors que ces problèmes sont bien compris théoriquement, ils peuvent amener de nouvelles difficultés lorsqu'on en effectue des simulations numériques. La procédure numérique habituelle engendre des configurations de jauge pondérées comme dans la fonction de partition. Pour une masse de quark petite, les configurations topologiques non triviales seront supprimées. Mais dans ces configurations, de grandes corrélations peuvent apparaître dues aux effets instantons. Cette combinaison de petits poids et de grandes corrélations peut donner naissance à de grandes erreurs statistiques, compliquant ainsi les extrapolations à partir des petites masses. Le problème deviendra particulièrement sévère pour des quantités dominées par des effets anomaux, comme la masse η'. Une stratégie possible pour éviter cet effet est de générer des configurations avec un poids modifié, peut-être selon les droites d'algorithmes multicanoniques.[17]

Notons que lorsque seulement une masse de quark tend vers zéro, le sommet de 't Hooft est une forme quadratique des sources de fermions. Cela donnera une contribution finie mais lisse au condensat $\langle\overline{\psi}\psi\rangle$. En effet, cela représente un décalage additif non perturbatif à la masse du quark. La valeur du décalage dépend généralement de détails concernant l'échelle et le régulateur. Même avec la condition de Ginsparg-Wilson, l'opérateur de Dirac du réseau n'est pas unique, et il n'y a pas de preuve que deux formes différentes doivent donner la même limite continue pour des masses de quarks s'évanouissant. À cause de cela, le concept de quark unique sans masse n'est pas un concept physique,[18], ceci invalidant une solution populaire proposée comme solution du problème difficile CP. Cette ambiguité a été notée pour des quarks lourds dans un contexte plus perturbatif[19] et on y fait souvent référence par le terme "problème du renormalon". Ce problème est intimement lié aux problèmes mentionnés précédemment de définition de la sensibilité topologique.

6 Résumé

En résumé, penser aux valeurs propres de l'opérateur de Dirac dans un champ de jauge peut donner quelques éclairages, par exemple l'image élégante de Banks-Casher de brisure de la symétrie chirale. Pourtant, il faut être précautionneux car le problème est hautement non linéaire. Cela se manifeste dans l'exemple contre-intuitif selon lequel l'ajout de saveur augmente plutôt que supprime les valeurs propres de valeurs faibles.

Les problèmes impliquant la suppression du mode nul représentent une facette d'un ensemble de problèmes non résolus liés entre eux. Y a-t-il des ambiguités non perturbatives

dans les quantités telles que la sensibilité topologique ? Est-ce que les champs de jauge rugueux sont importants, i.e. les champs de jauge sur lesquels le nombre d'enroulements est ambigu ? Comment ces problèmes sont-ils reliés à la masse du quark ? J'espère que les idées présentées ici stimuleront la réflexion le long de ces chemins.

Remerciements

Ce manuscrit a été écrit sous le contrat n DE-AC02-98CH10886 du département américain de l'Énergie des États-Unis.

Références

1. T. Banks and A. Casher, Nucl. Phys. B **169** (1980) 103.
2. P. H. Ginsparg and K. G. Wilson, Phys. Rev. D **25** (1982) 2649.
3. H. Neuberger, Phys. Lett. B **417** (1998) 141 [arXiv:hep-lat/9707022].
4. Y. Aoki *et al.*, Phys. Rev. D **69** (2004) 074504 [arXiv:hep-lat/0211023].
5. A. Duncan, E. Eichten and H. Thacker, Phys. Rev. D **59** (1999) 014505 [arXiv:hep-lat/9806020].
6. J. C. Osborn, K. Splittorff and J. J. M. Verbaarschot, Phys. Rev. Lett. **94** (2005) 202001 [arXiv:hep-th/0501210].
7. S. R. Coleman, in *C77-07-23.7* HUTP-78/A004 *Lecture delivered at 1977 Int. School of Subnuclear Physics, Erice, Italy, Jul 23-Aug 10, 1977.*
8. K. G. Wilson, in *New Phenomena In Subnuclear Physics. Part A. Proceedings of the First Half of the 1975 International School of Subnuclear Physics,* Erice, Sicily, July 11 - August 1, 1975, ed. A. Zichichi, Plenum Press, New York, 1977, p. 69.
9. M. Luscher, Phys. Lett. B **428** (1998) 342 [arXiv:hep-lat/9802011].
10. M. Luscher, Commun. Math. Phys. **85** (1982) 39.
11. P. Hernandez, K. Jansen and M. Luscher, Nucl. Phys. B **552** (1999) 363 [arXiv:hep-lat/9808010].
12. M. Creutz, Phys. Rev. D **70** (2004) 091501 [arXiv:hep-lat/0409017].
13. P. H. Damgaard, Nucl. Phys. B **556** (1999) 327 [arXiv:hep-th/9903096].
14. P. Di Vecchia and G. Veneziano, Nucl. Phys. B **171** (1980) 253.
15. M. Creutz, Phys. Rev. Lett. **92**, 201601 (2004) [arXiv:hep-lat/0312018].
16. G. 't Hooft, Phys. Rev. Lett. **37** (1976) 8.
17. B. A. Berg and T. Neuhaus, Phys. Rev. Lett. **68** (1992) 9 [arXiv:hep-lat/9202004].
18. M. Creutz, Phys. Rev. Lett. **92** (2004) 162003.
19. I. I. Y. Bigi, M. A. Shifman, N. G. Uraltsev and A. I. Vainshtein, Phys. Rev. D **50** (1994) 2234 [arXiv:hep-ph/9402360].

Ajouter des unités mod n

Marian Deaconescu

Marian Deaconescu est originaire de Roumanie, mais il travaille maintenant à l'étranger, au Koweit. Ses principaux centres d'intérêt en mathématiques sont reliés à la théorie des groupes. Ses deux petites filles, la photographie noir et blanc, la pêche et le temps passé à nourrir son chien sont les raisons qui font qu'il fait moins de mathématiques qu'il ne devrait.

dédié à Nicolae Popescu

Soit un entier $n \geq 2$ et dénotons par $U(Z_n)$ le groupe des unités de l'anneau Z_n des classes résiduelles modulo n. Ainsi $U(Z_n) = \{k \in Z | (k, n) = 1\}$. $U(Z_n)$ n'est pas clos par addition ; par exemple, $1 \in U(Z_2)$, mais $1 + 1 = 0 \notin U(Z_2)$.

Si l'on joue un peu avec les tables d'*addition* pour $U(Z_n)$, on observe que si n est impair, alors tout élément de Z_n apparaît dans la table comme un résultat. Dit autrement, l'équation $x + y = k$ semble avoir des solutions $x, y \in U(Z_n)$ pour tout $k \in Z_n$.

Si n est pair, pourtant, on observe rapidement que les classes de résidus impairs ne sont jamais sommes d'unités dans $U(Z_n)$; la raison est simple à voir ; n étant pair, les classes résiduelles sont contraintes d'être impaires et donc la somme de deux unités n'est jamais une classe résiduelle impaire.

Il est bien connu que pour un nombre premier p, la congruence $x + y = 0 \pmod{p}$ a exactement p solutions qui peuvent être représentées par les couples $(0, 0), (1, p - 1), ..., (p - 1, 1)$. À part la solution triviale $(0, 0)$, les composantes des solutions restantes sont toutes des classes de résidus non nulles dans le corps F_p à p éléments. [...][1] Dans le présent article, M. Deaconescu traite la variante suivante du problème décrit au début : il répond à la question du nombre de solutions x qui sont des nombres premiers à n et de la congruence $x + y = k \pmod{n}$, où k, n sont des nombres naturels quelconques.

Ces remarques élémentaires suggèrent le problème naturel de trouver, étant donnée une classe $k \in Z_n$, combien de fois cette classe k apparaît comme résultat dans la table d'addition de $U(Z_n)$. Selon une terminologie différente : fixons un certain entier naturel $n \geq 2$ et pour tout entier naturel k tel que $0 \leq k \leq n - 1$, déterminer le nombre $s(k)$ défini comme suit :

$$s(k) = |\{(x, y) \in U(Z_n) \times U(Z_n) \mid x + y = k\}|.$$

Bien sûr, ça n'est pas tout à fait un exercice évident. Car si on essaie de construire les tables d'addition des $U(Z_n)$ pour des nombres n de plus en plus compliqués (utiliser un ordinateur aide

Elem. Math. 55 (2000) 123-127, © Birkhäuser Verlag. Basel, 2000, Elemente der Mathematik.
Pendant l'écriture de cet article, l'auteur était financé par la subvention de recherche K.U. SM177.

[1] Je ne peux vérifier la traduction de l'allemand proposée par Google : "*En particulier, cela prouve que le nombre de points F_p-rationnels de l'espace projectif à une dimension est p. La question analogue pour les systèmes de polynômes de degré supérieur à plusieurs variables conduit aux conjectures d'A. Weil, résolues par P. Deligne dans les années 1970.*

à réaliser cette tâche fastidieuse), de plus en plus insaisissables, une conjecture de travail semble apparaître.

La réponse à notre question semble dépendre, de façon inattendue, de considérations liées au nombre de points fixes des automorphismes du groupe additif $(Z_n, +)$.

Théorème. *Soit $n \geq 2$ un entier naturel, soit k tel que $0 \leq k \leq n-1$, et dénotons par $s(k)$ le nombre de solutions $(x, y) \in U(Z_n) \times U(Z_n)$ de l'équation $x + y = k$. Alors*

$$s(k) = \frac{\varphi(n)}{\varphi(n/d)} \Psi(d, n)$$

où $d = (k, n)$ et $\Psi(d, n)$ est le nombre de ces automorphismes du groupe additif Z_n ayant exactement d points fixes.

Dans l'énoncé du théorème, (k, n) désigne le plus grand commun diviseur de k et n, alors que $\varphi(n)$ est la valeur de la fonction indicatrice d'Euler de n.

Preuve. Soit α un automorphisme du groupe additif Z_n. Alors $Fix(\alpha) = \{k \in Z_n \mid \alpha(k) = k\}$ est un sous-groupe de Z_n, et par conséquent, par le théorème de Lagrange, $|Fix(\alpha)|$ est un diviseur de n. Pour un diviseur d de n, $\Psi(d, n)$ dénote le nombre de ces automorphismes du groupe cyclique (additif) Z_n, qui ont d points fixes.

Observons d'abord que

$$\Psi(d, n) = |\{u \in U(Z_n) | (u–1, n) = d\}|. \tag{1}$$

Dans le but de prouver (1), notons qu'on peut identifier tout automorphisme $\alpha \in Aut(Z_n, +)$ avec une unité fixée $u \in U(Z_n)$ de telle façon que $\alpha(k) = ku$. Par conséquent

$$|Fix(\alpha)| = |Fix(u)| = |\{k \in Z_n \mid ku = k\}| = |\{k \in Z_n \mid n|k(u-1)\}| = (u-1, n).$$

Cela prouve l'hypothèse. □

Rappelons que nous voulons compter le nombre $s(k)$ de solutions dans $U(Z_n)$ de l'équation

$$x + y = k. \tag{*}$$

Soit $d = (k, n)$, de telle façon que $k = dt^{-1}$ pour une certaine unité $t \in U(Z_n)$ fixée. Transformons maintenant (*) dans des formes successives (et de plus en plus horribles) :

$$\begin{aligned} x + y = dt^{-1} &\iff xt + yt = d \iff x + y = d \iff xy^{-1} + 1 = dy^{-1} \\ &\iff xy + 1 = dy \iff -xy + 1 = dy. \end{aligned}$$

On doit ici attirer l'attention : quand on passe d'une équation à une autre, le signe d'équivalence est utilisé pour indiquer que les deux équations ont le même nombre de solutions.

Revenons à la longue liste d'équivalences : la première équation a le même nombre de solutions que (*), mais elle a deux avantages. Notons d'abord que $d = (dy, n) = (xy - 1, n)$. Ensuite, observons

que lorsque y parcourt $U(Z_n)$, l'expression dy prend exactement $\varphi(n/d)$ valeurs distinctes dans Z_n. En combinant ces remarques avec la formule (1), on voit que $s(k) = \dfrac{\varphi(n)}{\varphi(n/d)}\Psi(d,n)$, comme affirmé.

Supposons qu'on peut trouver la première décomposition de n (facile à supposer, mais habituellement difficile à réaliser en pratique - un fait sur lequel on devrait toujours insister !), i.e. $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ et soit $d = \prod_{i=1}^{s} p_i^{\beta_i}$ un diviseur de n. Il a été déterminé dans [1] que

$$\Psi(d,n) = \prod_{\substack{p_i \mid n/d \\ p_i \mid d}} p_i^{\alpha_i - \beta_i - 1}(p_i - 1) \prod_{\substack{p_j \mid n/d \\ p_j \nmid d}} p_j^{\alpha_j - 1}(p_j - 2) \tag{2}$$

Selon le théorème et selon la formule (2), les nombres $s(k)$ peuvent être effectivement calculés en supposant qu'on dispose d'une décomposition en facteurs premiers de n. La formule (2) permet également de dériver une première conséquence immédiate du théorème :

Corollaire 1 : *Soit $n \geq 2$ un entier naturel ;*

i) *Si n est impair, alors tout élément de Z_n est une somme de deux unités.*

ii) *Si n est pair, alors $k \in Z_n$ est une somme de deux unités si et seulement si k est pair.*

Preuve.

i) Si n est impair, la formule (2) indique que $\Psi(d,n) \neq 0$ pour tous les diviseurs d de n et le résultat découle du théorème.

ii) Par (2) et par le théorème, $s(k) \neq 0 \iff \Psi(d,n) \neq 0$, où $d = (k,n) \iff d$ est pair $\iff k$ est pair.

Le théorème a une autre conséquence moins évidente dans le domaine des entiers positifs - une inégalité qui identifie les nombres premiers comme une "empreinte digitale" dans son cas extrême.

De telles inégalités ne sont pas du tout courantes. Considérons juste celle-ci : si $n \geq 2$ est un entier naturel, alors $\varphi(n) \leq n-1$ et l'égalité a lieu si et seulement si n est un nombre premier. Certes, ces résultats sont jolis, mais ils ont une valeur pratique limitée et on se demande pourquoi en ajouter un de plus à la collection de ceux existant déjà.

Voici quelques raisons : l'inégalité suivante fait intervenir une fonction arithmétique moins habituelle, notamment $\Psi(1,n)$, cela suggère une conjecture naturelle que je pense être vraie, mais qui est très difficile à démontrer et sa preuve utilise les nombres $s(k)$.

Corollaire 2 : Soit $n \geq 2$ un entier naturel et soit $\Psi(1,n)$ le nombre d'automorphismes sans point fixe du groupe additif Z_n. Alors

$$\varphi(n)(\varphi(n) - 1) \geq (n-1)\Psi(1,n)$$

et l'égalité est vérifiée si et seulement si n est un nombre premier.

Preuve. Comme le suggère la notation $\Psi(1,n)$, un automorphisme sans point fixe du groupe additif Z_n est un automorphisme qui fixe seulement la classe identité 0.

Prenons $d=1$ dans la formule (2) pour obtenir

$$\Psi(1,n)=\prod_{i=1}^{s} p_i^{\alpha_i-1}(p_i-1). \tag{3}$$

Observons alors que, par définition de $s(k)$, on obtient :

$$\sum_{k=0}^{n-1} s(k)=\varphi(n)^2. \tag{4}$$

En effet, $U(Z_n)$ a $\varphi(n)$ éléments et sa table d'addition a $\varphi(n)^2$ entrées.

Appliquons le théorème deux fois pour obtenir :

$$s(0)=\varphi(n) \tag{5}$$

et

$$s(k)=\Psi(1,n) \qquad \text{à chaque fois que } (k,n)=1. \tag{6}$$

Maintenant, utilisons (2) et (3) pour obtenir, après un calcul plutôt long - mais élémentaire, que

(7) Pour n impair et pour d un diviseur propre de n, $\varphi(n)\Psi(d,n)>\varphi(n/d)\Psi(1,n)$.

Après cette préparation, on est prêt à prouver le corollaire 2. Soit d'abord n pair ≥ 4, de telle façon que par (3), $\Psi(1,n)=0$. L'énoncé est correct dans ce cas.

Supposons ensuite que n est impair et composé ; alors il existe un certain k, $0<k<n-1$ avec $(k,n)>1$ et on obtient :

$$\varphi(n)(\varphi(n)-1)=\varphi(n)^2-\varphi(n)= \qquad \text{(par (4) et (5))}$$

$$\sum_{k=1}^{n-1} s(k)=\sum_{(k,n)=1} s(k)+\sum_{(k,n)>1} s(k)= \qquad \text{(par (6))}$$

$$\varphi(n)\Psi(1,n)+\sum_{(k,n)>1} s(k)> \qquad \text{(par (7) et par théorème)}$$

$$\varphi(n)\Psi(1,n)+(n-1-\varphi(n))\Psi(1,n)=(n-1)\Psi(1,n).$$

Finalement, soit n un nombre premier. Alors (3) donne que $\Psi(1,n)=n-2$ et puisque clairement $\varphi(n)=n-1$, on vérifie aisément que l'égalité est vérifiée dans ce cas. La preuve est complète. □

Remarque. L'inégalité dans le corollaire 2 peut être prouvée directement, par des inégalités de force brute, mais c'est un peu bizarre de faire ça.

Il devrait être clair à partir de maintenant que les nombres $\Psi(1,n)$ ont une forte ressemblance avec $\varphi(n)$: considérons juste leur valeur si n est un nombre premier ou un nombre sans carré. Une conjecture bien connue (et autant que je sache non résolue à ce jour) de D.H. Lehmer [3] affirme

que si $n \geq 2$ et si $\varphi(n)$ divise $n-1$, alors n doit être un nombre premier.

Par analogie et inspiré par le corollaire 2, on peut conjecturer que les entiers $n \geq 2$ pour lesquels $\Psi(1,n)$ divise $\varphi(n)-1$ doivent être des nombres premiers. Je m'attends à ce que cette conjecture soit aussi difficile que celle de Lehmer. Le lecteur qui souhaite lire davantage de résultats partiels en lien avec la conjecture de Lehmer devrait consulter [2] pour une bibliographie partielle.

Je voudrais ici étendre mes remerciements à mon bon ami Vali Filip. Infirmier de formation et vocation, avec la patience d'un ange, il a été capable de comprendre la plupart de ce matériau, bien qu'à l'occasion j'aie dû lui expliquer ce qu'est un groupe et un automorphisme de groupe.

Bibliographie

[1] M. Deaconescu and H.K. Du, *Counting similar automorphisms of finite cyclic groups*, Math. Japonica 46 (1997), 345-348.

[2] R.K. Guy, *Unsolved problems in Number Theory*, Springer Verlag, 1981.

[3] D.H. Lehmer, *On Euler's totient function*, Bull. Amer. Math. Soc. 38 (1932), 745-751.

Marian Deaconescu
Département de mathématiques et informatique
Université du Koweit
P.O. Box 5969
Safat 13060
Kuwait
e-mail: DEACON@math-1.sci.kuniv.edu.kw

Sur le théorème de Pythagore

de Edsger W. Dijkstra

Pour le théorème de Pythagore, je commence à partir de la formulation de Coxeter ("*Introduction to Geometry*", p. 8) :

"Dans un triangle rectangle, le carré de l'hypothénuse est égal à la somme des carrés des deux autres côtés (les catheti)."

Jouons un peu avec cette formulation. Dans un triangle de côtés a, b, et c - différents de 0 pour que les angles du triangle soient bien définis - on introduit la notation habituelle α, β et γ pour les angles opposés respectifs des côtés. (Nous avons introduit un nom d'angle pour pouvoir exprimer le fait qu'un angle est droit, et les noms des deux autres angles pour des raisons de symétrie.)

Une expression formelle de la formulation de Coxeter est

$$\gamma = \pi/2 \implies a^2 + b^2 = c^2$$

En plus de la notation que nous avons introduite, cette formulation contient la constante (transcendentale !) π. Heureusement, on peut l'éliminer grâce à

$$\pi = \alpha + \beta + \gamma$$

L'arithmétique élémentaire amène la formulation équivalente

$$\alpha + \beta = \gamma \quad \implies \quad a^2 + b^2 = c^2.$$

N'est-ce pas joliment symétrique ? Cela suggère immédiatement - au moins à moi - le renforcement

(0) $$\alpha + \beta = \gamma \quad \equiv \quad a^2 + b^2 = c^2.$$

(Cela s'avèrera être un théorème.) On obtient une formulation équivalente en prenant la négation des deux côtés :

$$\alpha + \beta \neq \gamma \quad \equiv \quad a^2 + b^2 \neq c^2$$

Mais $x \neq y \;\equiv\; x < y \;\vee\; x > y$, et les termes de cette dernière disjonction sont mutuellement exclusifs. En se rappelant que l'angle le plus grand est opposé au côté le plus grand, il est audacieux d'imaginer

(1) $$\alpha + \beta < \gamma \quad \equiv \quad a^2 + b^2 < c^2$$ et

(2) $$\alpha + \beta > \gamma \quad \equiv \quad a^2 + b^2 > c^2?$$

Audacieux peut-être, mais pas déraisonnable.

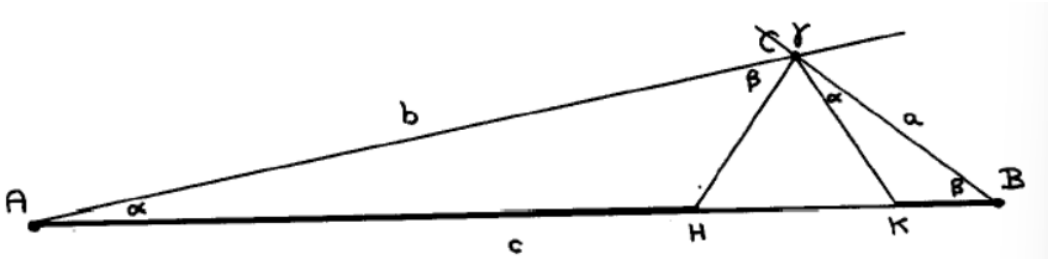
Notons que les assertions (0), (1) et (2) ne sont pas indépendantes : de deux quelconques d'entre elles, la troisième peut être déduite. On peut toutes les formuler en utilisant la fonction sgn - lire "signum" - par

EWD975-0, https://www.nieuwarchief.nl/serie5/pdf/naw5-2009-10-2-094.pdf.
Traduction : Denise Vella-Chemla, décembre 2023.

$$\text{sgn}.0 = 0 \quad \wedge (\text{sgn}.x = 1 \quad \equiv \quad x > 0) \wedge (\text{sgn}.x = -1 \quad \equiv \quad x < 0),$$

plus exactement $\text{sgn}.(\alpha + \beta - \gamma) = \text{sgn}.(a^2 + b^2 - c^2)$

Considérons maintenant la figure suivante.



On a dessiné le cas $\alpha + \beta < \gamma$, dans lequel les triangles ΔCKB et ΔAHC, d'aires disjointes, ne couvrent pas l'entièreté de ΔACB ; en notant "XYZ" l'aire de ΔXYZ, on a dans ce cas

$$CKB + AHC < ACB$$

Dans le cas $\alpha + \beta = \gamma$, H et K coïncident et on a

$$CKB + AHC = ACB$$

et dans le cas $\alpha + \beta > \gamma$, les deux triangles se chevauchent et on a

$$CKB + AHC > ACB$$

En résumé

$$\text{sgn}.(\alpha + \beta - \gamma) = \text{sgn}.(CKB + AHC - ACB).$$

Les trois aires sur le côté droit sont celles de triangles semblables et par conséquent, elles sont dans les mêmes ratios que les carrés des segments correspondant, en particulier

$$\frac{CKB}{a^2} = \frac{AHC}{b^2} = \frac{ACB}{c^2} > 0 \ ;$$

donc

$$\text{sgn}.(CKB + AHC - ACB) = \text{sgn}.(a^2 + b^2 - c^2).$$

Par conséquent, on a prouvé

$$\text{sgn}.(\alpha + \beta - \gamma) = \text{sgn}.(a^2 + b^2 - c^2)$$

un théorème, disons, 4 fois plus riche que celui que nous avions cité de Coxeter.

* *
*

Le titre de cette note peut faire se demander "Pourquoi perdrais-je mon temps à fouetter un cheval aussi mort que le théorème de Pythagore ?". Donc essayons de résumer ce que nous pourrions apprendre de cet exercice.

- Trois hourras pour la formalisation ! Au lieu d'entreprendre de prouver $a^2 + b^2 = c^2$ pour un triangle rectangle, on a inclus l'antécédent $\gamma = \pi/2$ dans l'énoncé formel de ce qui était à démontrer. C'est seulement après l'introduction de π qu'on a pu l'éliminer et rencontrer la formulation "joliment symétrique".

- Trois hourras pour l'équivalence ! Il semble assez clair que le théorème n'est pas à propos des triangles rectangles, mais à propos des triangles en général.

- Trois hourras pour les avantages de notation qu'offre la fonction sgn. Si on n'avait pas fait attention, on aurait fini par prouver

$$(\alpha + \beta) \underline{\mathrm{R}}\, \gamma \quad \equiv \quad (a^2 + b^2) \underline{\mathrm{R}}\, c^2$$

  pour $\underline{\mathrm{R}}$ n'importe laquelle des six relations $=, \neq, <, \leq, >$ and $\geq$.

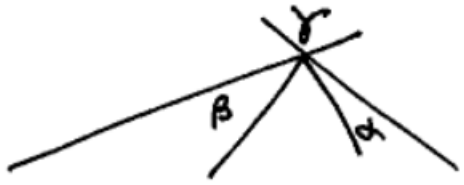
- Aucun hourra du tout pour cette étape de l'argumentation dans laquelle le manque d'axiomatisation nous a forcés à recourir à un dessin. Les dessins sont presque inévitablement ultra-spécifiques et nous forcent souvent à une analyse de cas. Notons que j'ai soigneusement évité les dessins pour $\alpha + \beta > \gamma$; il y en a 9 : K à droite de A, coïncidant avec A, et à gauche de A, et similairement pour la paire H et B. Pour l'argumentation, ces distinctions sont non pertinentes mais, quand on dessine, on peut difficilement les éviter.

- Un de ces jours, j'aimerais trouver une explication convaincante du fait que l'on continue d'éduquer les jeunes avec le théorème de Pythagore dans sa forme diluée telle que celle fournie par Coxeter. Notons que les 9 figures auraient pu être évitées en démontrant également

$$\begin{array}{lll} CKB + AHC < ACB & \Longrightarrow \alpha + \beta < \gamma & \text{et} \\ CKB + AHC = ACB & \Longrightarrow \alpha + \beta = \gamma \ , & \end{array}$$

  i.e. en prouvant (0) et (1) en entier.

- Notons que notre figure n'est pas sortie d'un chapeau de magicien ! Dès que $\mathrm{sgn}.(\alpha + \beta - \gamma)$ apparaît dans la démonstration, il est doucement raisonnable de construire cette différence. Pour ne pas détruire la symétrie entre α et β, on commence avec γ et on soustrait α d'un côté et β de l'autre :



  et ceci est le germe de la figure que nous avons dessinée.

Épilogue. Je suis dans une situation paradoxale. Je suis convaincu que parmi les personnes qui connaissent le théorème de Pythagore, presqu'aucune ne peut lire ce qui a précédé sans être surpris au moins une fois. De plus, je pense que toutes ces surprises sont pertinentes (parce qu'elles

témoignent de leur éducation au raisonnement). Pourtant, je ne connais pas un seul journal respectable dans lequel je pourrais fouetter ce cheval mort.

Austin, 7 septembre 1986

Prof. Dr. Edsger W. Dijkstra
Département d'Informatique
Université du Texas à Austin
Austin, TX 78712-1188 , USA.

La preuve géométrique mal comprise qu'a faite Eisenstein de la loi de réciprocité quadratique

R.C. Laubenbacher, D.J.Pengelley,
traduction : D. Chemla

30/8/2011

1 Introduction

La Loi de Réciprocité Quadratique a joué un rôle central dans le développement de la théorie des nombres et a constitué la première loi profonde gouvernant les nombres premiers. Ses nombreuses preuves de nombreux points de vue distincts attestent de sa position au coeur de ce sujet. Le théorème a été découvert par Euler et reformulé par Legendre en utilisant le symbole qui porte maintenant son nom mais a été prouvé pour la première fois par Gauss. Les huit preuves différentes de ce théorème, que Gauss publia au début des années 1800, en appellant la Loi de Réciprocité Quadratique le théorème fondamental, furent suivies de douzaines d'autres avant que ce dix-neuvième siècle ne s'achève, en incluant quatre de Gotthold Eisenstein dans les années 1844-1845. Notre but est de porter un nouveau regard sur la preuve géométrique d'Eisenstein, dans laquelle il présente une adaptation particulièrement belle et économique de la troisième preuve de Gauss et d'amener ainsi l'attention sur tous les avantages de sa preuve sur celle de Gauss, la plupart de ces avantages n'ayant apparemment pas été perçus jusqu'à présent.
Il est difficile d'imaginer aujourd'hui la sensation causée par Eisenstein quand il surgit dans le monde mathématique. A l'automne 1843, à 20 ans, ce mathématicien autodidacte avait tout juste reçu son certificat de Hautes Etudes et était entré à l'université de Berlin lorsqu'il produisit un flot de publications faisant immédiatement de lui un des mathématiciens majeurs du début du dix-neuvième siècle. Le 14 juillet 1844, Gauss écrivit à C.Gerling :

> *J'ai récemment fait la connaissance d'un jeune mathématicien, Eisenstein de Berlin, qui est venu ici avec une lettre de recommandation de Humboldt. Cet homme, qui est encore très jeune, montre un talent remarquable et il fera certainement de grandes choses.*

En 1844, Eisenstein contribua à pas moins de 16 des 27 articles mathématiques du volume 27 du Journal de Crelle et lors de son troisième semestre en tant qu'étudiant, il avait reçu un doctorat honorable de Breslau. Gauss et le grand scientifique et explorateur Alexandre Von Humboldt tous deux firent de gros efforts, pour la plupart en vain, pour obtenir la reconnaissance et la sécurité financière d'Eisenstein appauvri. Gauss écrivit à Humboldt que le talent d'Eisenstein était de ceux que la Nature ne crée que quelques fois dans un siècle. Il obtint un poste de Privatdozent (assistant non rémunéré) à l'université de Berlin et fut finalement admis à l'Académie des Sciences de Berlin début 1852. Mais sa santé s'étant alors sérieusement détériorée, il mourut la même année à l'âge de 29 ans, de la tuberculose. Gotthold Eisenstein reste avec Abel et Galois un autre génie mathématique du dix-neuvième siècle à avoir eu une vie courte et tragique.
La preuve géométrique d'Eisenstein parut dans le Journal de Crelle sous le titre *Démonstration géométrique du théorème fondamental des restes quadratiques.* Elle est très liée à la troisième preuve de Gauss. Plusieurs exposés de la preuve d'Eisenstein ont observé seulement un de ses trois aspects géométriques et ont omis les autres différences importantes entre les deux preuves. Le résultat en a été un échec à reconnaître et apprécier pleinement la manière dont Eisenstein organise grandement et éclaire la preuve de Gauss et ce-faisant révèle l'essence de cette troisième démonstration de Gauss. Par exemple, la troisième démonstration est basée sur un résultat appelé le Lemme de Gauss. Eisenstein était particulièrement satisfait du raccourci qu'il a trouvé pour éviter la technique nécessitée par l'application de ce Lemme.

Je ne me reposai pas tant que je ne réussis pas à libérer cette preuve géométrique du lemme dont elle dépendait encore et cela est maintenant si simple qu'on peut le communiquer en deux lignes.

Nous croyons que l'élégance de la preuve d'Eisenstein mérite une large attention et nous la présentons ci-dessous en la comparant à la troisième preuve de Gauss.

2 Preuve d'Eisenstein

Pour commencer, nous rappelons quelques conséquences du fait que les classes de restes modulo un nombre premier p forment un corps Z_p. Le Petit Théorème de Fermat $b^{p-1} \equiv 1 \ (mod\ p)$ pour tout entier b non divisible par p découle du fait que les classes de restes non-nulles forment un groupe (cyclique) d'ordre $p-1$ selon la multiplication. Quand p est impair, l'application $x \to x^2$ a comme noyau $\{-1, 1\}$ et donc son image, les carrés (ou résidus quadratiques) modulo p, forment un sous-groupe d'ordre $\frac{p-1}{2}$ et les non-résidus forment son coset. Le caractère de résiduosité quadratique d'une classe de restes $b \in Z_p^*$ est spécifié en utilisant le symbole de Legendre : $\left(\frac{b}{p}\right) = 1$ si b est un résidu quadratique mod p et $\left(\frac{b}{p}\right) = -1$ sinon. De $\left(b^{\frac{p-1}{2}}\right)^2 = 1$, il résulte que $b^{\frac{p-1}{2}} = \pm 1$ pour tout $b \in Z_p^*$. Mais si $b = c^2$, alors $b^{\frac{p-1}{2}} = c^{p-1} = 1$, et alors les résidus quadratiques sont toutes les racines du polynome $x^{\frac{p-1}{2}} = 1$. Puisque ce polynome ne peut avoir plus de $\frac{p-1}{2}$ racines dans le corps Z_p, nous concluons que ses racines sont exactement les résidus quadratiques. C'est à dire que nous avons le *critère d'Euler* : $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}}$ pour tout b non divisible par p. Le théorème de la réciprocité quadratique compare le caractère quadratique de deux nombres premiers l'un par rapport à l'autre.
Loi de Réciprocité Quadratique : Si p et q sont deux nombres premiers impairs distincts alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Voici la preuve d'Eisenstein, en suivant au plus près ses propre langage et notation (dont il a lui-même abusé avec convenance et succès).

Considérons l'ensemble $a = 2, 4, 6, \ldots, p-1$. Appelons r le reste modulo p d'un multiple arbitraire qa. Alors il apparaît clairement que la liste des nombres $(-1)^r r$ concorde avec la liste des nombres a, jusqu'aux multiples de p (car clairement chacun des nombres $(-1)^r r$ a un plus petit résidu positif pair et que s'il y avait une duplication parmi ces restes, on aurait

$$(-1)^{qa}.qa = (-1)^{qa'}.qa',$$

mais alors $a \equiv \pm a'$. Puisque les a sont distincts, on en déduit que $a + a' \equiv 0$ ce qui ne peut avoir lieu puisque $0 < a + a' < 2p$ et $a + a'$ est pair). Mais alors :

$$q^{\frac{p-1}{2}} \prod a \equiv \prod r \ (mod\ p) \ \ et \ \ \prod a \equiv (-1)^{\sum r} \prod r \ (mod\ p),$$

d'où il résulte que $q^{\frac{p-1}{2}} \equiv (-1)^{\sum r} \ (mod\ p)$. En rappelant que selon le critère d'Euler $\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \ (mod\ p)$, cela entraîne que

$$\left(\frac{q}{p}\right) = (-1)^{\sum r}, \qquad (1)$$

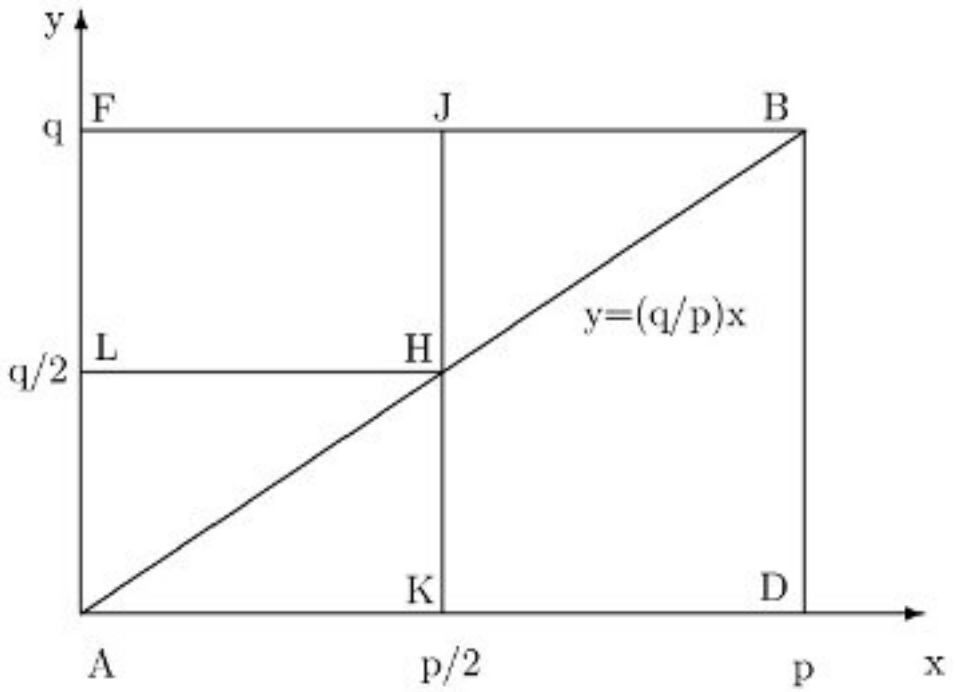
ainsi on peut se concentrer seulement sur la parité de l'exposant. Clairement,

$$\sum qa = p \sum \left[\frac{qa}{p}\right] + \sum r, \qquad (2)$$

où $[\,]$ est la fonction *plus grand entier inférieur à*. Puisque les éléments a sont tous pairs, et que p est impair, il s'ensuit que $\sum r \equiv \sum [\frac{qa}{p}] \ (mod\ 2)$ et donc que

$$\left(\frac{q}{p}\right) = (-1)^{\sum [\frac{qa}{p}]}.$$

(Ici, Eisenstein remarque que puisque jusque là, q ne nécessite pas d'être un nombre premier impair, mais plutôt un nombre premier à p, on peut facilement obtenir le caractère de résiduosité de 2 : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ de la formule ci-dessus. On laisse ceci en exercice au lecteur.)



Eisenstein utilise alors une représentation géométrique de l'exposant dans cette dernière équation pour la transformer deux fois en étudiant sa parité : cet exposant est précisément le nombre de points entiers du réseau d'abscisses paires à l'intérieur du triangle ABD sur la Figure (notez qu'il n'y a aucun point du réseau sur la ligne AB). Considérons une abscisse paire $a > p/2$. Puisque le nombre de points du réseau associé à chaque abscisse à l'intérieur du rectangle $ADBF$ est pair, le nombre $[\frac{qa}{p}]$ de points du réseau d'abscisse sous AB a la même parité que le nombre de points du réseau au-dessus de AB. Celui-ci en retour est le même que le nombre de points du réseau sous AB d'abscisse impaire $p - a$. Cette correspondance un-à-un entre les abscisses paires dans le triangle BHJ et les abscisses impaires dans AHK implique maintenant que $\sum \left[\frac{qa}{p}\right] \equiv \mu \ (mod\ 2)$, où μ est le nombre de points à l'intérieur du triangle AHK, et donc $\left(\frac{q}{p}\right) = (-1)^{\mu}$.

En inversant les rôles de p et q, on aboutit à $\left(\frac{p}{q}\right) = (-1)^{\nu}$, où ν est le nombre de points à l'intérieur du triangle AHL. Puisque le nombre total de points à l'intérieur des deux triangles est simplement $\frac{p-1}{2}.\frac{q-1}{2}$, on peut maintenant conclure que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\nu+\mu} = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}. \qquad \square$$

Même l'habituellement modeste Eisenstein ne put retenir sa joie face à cette démonstration :

> *Comme Euler se serait trouvé chanceux s'il avait été en possession de ces lignes il y a quelques soixante-dix ans.*

3 Eisenstein contre Gauss

Gauss lui-même considérait sa troisième preuve comme la plus directe et la plus naturelle de ses démonstrations. En l'introduisant, il disait :

Une année entière, ce théorème m'a tourmenté et a absorbé mes plus gros efforts jusqu'à ce qu'enfin j'obtienne une démonstration... Plus tard, je trouvai trois autres preuves qui étaient construites sur des principes complètement différents... Je n'hésite pas à dire que jusqu'à présent, aucune preuve naturelle n'a été produite. Je laisse les autorités juger si la preuve suivante que j'ai été assez chanceux de découvrir mérite cette description.

Tandis qu'Eisenstein suit essentiellement la même structure que Gauss, chaque caractéristique de son approche est d'une grande clarté, et offre une vision élégante tout en raccourcissant le chemin pris par Gauss.
La troisième preuve de Gauss commence par son Lemme, qui dit que :

$$\left(\frac{q}{p}\right) = (-1)^{\alpha}, \qquad (3)$$

avec α obtenu de la manière suivante. Posons

$$A = 1, 2, \ldots, \frac{p-1}{2} \; et \; B = \frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1.$$

Alors α est défini comme le nombre de *résidus minima absolus* positifs de l'ensemble qA qui appartiennent à B.
Plutôt que d'utiliser le Lemme de Gauss, Eisenstein dérive l'équation (1), avec l'expression algébrique $\sum r$ en exposant, qui est alors plus facilement convertie en l'équation clef

$$\left(\frac{q}{p}\right) = (-1)^{\sum[\frac{qa}{p}]}, \qquad (4)$$

commune aux deux démonstrations, ce qui n'est pas le cas de l'équation (3). Alors que l'exposant algébrique d'Eisenstein est facilement transformé en l'exposant dans (4) via (2), Gauss doit établir un certain nombre de propriétés de la fonction plus grand entier et les appliquer pour relier α à l'exposant dans (4). L'utilisation par Eisenstein de l'ensemble $a = 2, 4, 6, \ldots, p-1$, par opposition à l'ensemble A de Gauss, lui permet de compter les mêmes éléments que le Lemme de Gauss, mais via l'expression $\sum r$, l'amenant rapidement à (4) :

La principale différence entre mon argument et celui de Gauss est que je ne divise pas les nombres moindres que p en ceux moindres que $p/2$ et ceux supérieurs à $p/2$, mais plutôt en pairs et impairs.

Eisenstein applique maintenant ses deux intelligentes transformations géométriques pour convertir l'exposant $\sum[\frac{qa}{p}]$ en nombre de points du réseau dans le triangle AHK (*mod* 2). Après avoir fait la même chose pour $\left(\frac{p}{q}\right)$, calculant le nombre de points du réseau du triangle AHL, la preuve est complétée en comptant le nombre de points du réseau du rectangle $AKHL$[1]. Gauss, de son côté, fait essentiellement les deux mêmes transformations, et calculs, sans avoir recours à l'approche géométrique. Il compte vraiment les points en utilisant des propriétés algébriques de la fonction plus grand entier. Cela rend le reste de la preuve longue et non-intuitive, et le force à considérer des cas séparés dépendant des classes de congruence de p et q (mod 4).

[1]La plupart des exposés modernes de la preuve d'Eisenstein présentent seulement cet argument de comptage final, en remplaçant ses deux transformations géométriques par de l'algèbre.

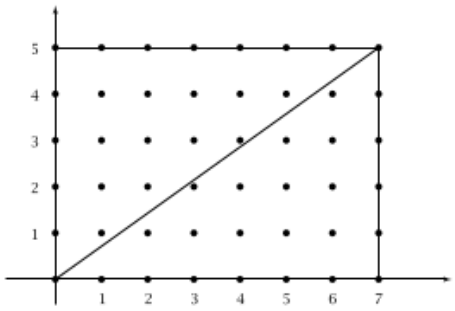
Traduction de l'explication de la preuve géométrique par Eisenstein de la loi de réciprocité quadratique de Gauss trouvée dans le livre Topologie des nombres de Allen Hatcher

On rappelle la loi de réciprocité quadratique de Gauss (si on note $\left(\frac{p}{q}\right)$ le caractère de résiduosité quadratique de p à q, qui exprime que p est un carré modulo q) :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

1. Ici notre but est d'exprimer le symbole de Legendre $\left(\frac{p}{q}\right)$ en termes géométriques.

Pour commencer, considérons un rectangle dans le premier quadrant du plan cartésien qui est de largeur égale à p unités et de hauteur égale à a unités, avec un coin à l'origine et l'autre coin au point (p, a). Par exemple pour $p = 7$ et $a = 5$, on a le schéma



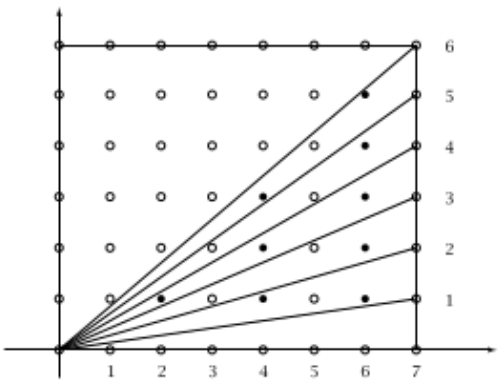
Nous allons nous intéresser aux points qui sont strictement à l'intérieur du rectangle dont les coordonnées sont entières. Les points satisfaisant cette dernière condition sont appelés *points du réseau*. Le nombre de points du réseau à l'intérieur du rectangle est donc $(p-1)(a-1)$ puisque leur abscisse est comprise entre 1 et $p-1$ and leur ordonnée est comprise entre 1 et $a-1$, indépendamment.

La diagonale du rectangle de $(0, 0)$ à (p, a) ne passe par aucun point du réseau intérieur au rectangle puisque nous avons supposé que p ne divise pas a, ainsi la fraction a/p, qui est la pente de la diagonale, est irréductible (s'il y avait un point intérieur du réseau sur la diagonale, la pente de la diagonale serait une fraction avec un numérateur et un dénominateur plus petits que a et p). Puisqu'il n'y a pas de points intérieurs au réseau sur la diagonale, exactement la moitié des points du réseau à l'intérieur du rectangle sont de chaque côté de la diagonale, et du coup, le nombre de points du réseau sous la diagonale est $\frac{1}{2}(p-1)(a-1)$. Ce nombre est un entier puisque p est impair, ce qui rend $p-1$ pair.

librement téléchargeable ici https://pi.math.cornell.edu/ hatcher/TN/TNbook.pdf.

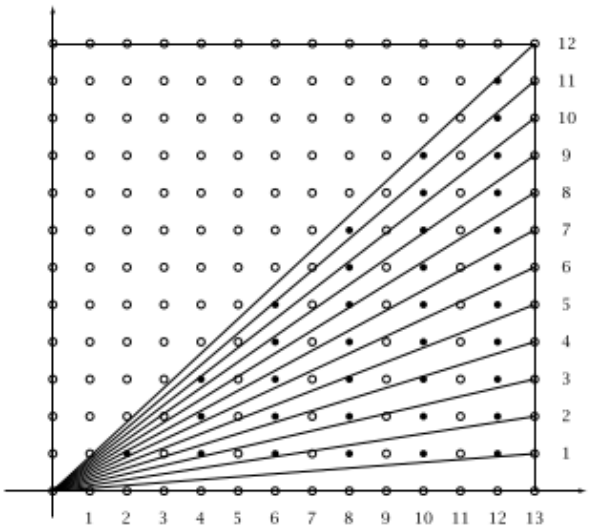
Une question plus précise que l'on peut se poser est de savoir combien de points du réseau sous la diagonale ont une abscisse (coordonnée x) paire et combien ont une abscisse impaire. Ici, il n'y a pas de garantie que ces deux nombres doivent être égaux, et si par exemple ils étaient égaux, ils devraient être égaux à $\frac{1}{4}(p-1)(a-1)$ mais cette fraction pourrait ne pas être entière, par exemple quand $p = 7$ et $a = 4$.

Nous dénotons le nombre de points du réseau qui sont sous la diagonale et ont une abscisse paire par la lettre e. La figure ci-dessous montre les valeurs de e quand $p = 7$ et quand a est compris entre 1 et 6.



a	e	$\left(\frac{a}{7}\right)$
6	9	−1
5	7	−1
4	6	+1
3	3	−1
2	2	+1
1	0	+1

Un exemple un petit peu plus compliqué pour p = 13 et a compris entre 1 et 12



a	e	$\left(\frac{a}{13}\right)$
12	36	+1
11	33	−1
10	30	+1
9	26	+1
8	23	−1
7	21	−1
6	15	−1
5	13	−1
4	10	+1
3	6	+1
2	3	−1
1	0	+1

La manière dont e varie en fonction de a semble quelque peu imprévisible. Ce que nous allons montrer c'est que connaître simplement la parité de e suffit déjà pour déterminer la valeur du symbole de Legendre via la formule

$$\left(\frac{a}{p}\right) = (-1)^e$$

Pour prouver cela, on trouve d'abord une formule pour e. Le segment de la ligne verticale $x = u$ allant de l'axe des abscisses jusqu'à la diagonale a pour longueur $\frac{ua}{p}$ puisque la pente de la diagonale est a/p. Si u est un entier positif, le nombre des points du réseau sur ce segment de droite est $\left\lfloor \frac{ua}{p} \right\rfloor$, le plus grand entier $n \leq \frac{ua}{p}$. Maintenant si on ajoute ces nombres de points du réseau pour l'ensemble des nombres pairs $E = \{2, 4, \ldots, p-1\}$, on obtient

$$e = \sum_E \left\lfloor \frac{ua}{p} \right\rfloor .$$

La manière de calculer $\left\lfloor \frac{ua}{p} \right\rfloor$ est d'appliquer l'algorithme de division entière en divisant ua par p pour obtenir $\left\lfloor \frac{ua}{p} \right\rfloor$ comme quotient et un reste que nous notons $r(u)$. Du coup, nous avons la formule

$$ua = p \left\lfloor \frac{ua}{p} \right\rfloor + r(u) \tag{1}$$

Cette formule implique que le nombre $\left\lfloor \frac{ua}{p} \right\rfloor$ a la même parité que $r(u)$ puisque u est pair et p est impair. Cette relation entre les parités implique que le nombre $(-1)^e$ qui nous intéresse peut aussi être calculé comme

$$(-1)^e = (-1)^{\sum_E \left\lfloor \frac{ua}{p} \right\rfloor} = (-1)^{\sum_E r(u)} \tag{2}$$

Avec cette dernière expression à l'esprit, nous allons nous focaliser sur les restes $r(u)$.

Le nombre $r(u)$ est strictement compris entre 0 et p et peut être soit pair soit impair, mais dans les deux cas, nous pouvons dire que $(-1)^{r(u)} r(u)$ est congruent à un nombre pair dans l'intervalle $(0, p)$ puisque si $r(u)$ est impair, $(-1)^{r(u)} r(u)$ l'est aussi et alors en ajoutant p à cela, on obtient un nombre pair entre 0 et p. Ainsi, il y a toujours un nombre pair $s(u)$ entre 1 et p qui est congruent à $(-1)^{r(u)} r(u)$ $mod\ p$. De façon évidente, $s(u)$ est unique puisqu'il n'y a pas deux nombres dans l'intervalle $(0, p)$ qui sont congruents mod p.

Un fait clef à propos de ces nombres pairs $s(u)$ est qu'ils sont tous distincts lorsque u varie dans l'ensemble E. Car supposons que nous ayons $s(u) = s(v)$ pour un autre nombre pair v dans E. Alors $r(u) = \pm r(v)$ $mod\ p$, ce qui implique $au = \pm av$ $mod\ p$ au regard de l'équation (1) ci-dessus. Nous pouvons éliminer les a des deux côtés de la congruence pour obtenir $u \equiv \pm v$. Pourtant, nous ne pouvons avoir $u \equiv -v$ parce que le nombre entre 0 et p qui est congruent à $-v$ est $p - v$, du coup, nous devrions avoir $u = p - v$ ce qui est impossible puisque ce sont des nombres strictement compris entre 0 et p. Cela montre que les nombres $s(u)$ sont tous distincts.

Maintenant considérons le produit de tous les nombres $(-1)^{r(u)}r(u)$ lorsque u^r parcourt E. Ecrivons-le : c'est

$$\left[(-1)^{r(2)}r(2)\right]\left[(-1)^{r(4)}r(4)\right]\ldots\left[(-1)^{r(p-1)}r(p-1)\right] \tag{3}$$

Par l'équation (1), nous avons $r(u) = ua \ mod \ p$, du coup, ce produit est congruent mod p à

$$\left[(-1)^{r(2)}2a\right]\left[(-1)^{r(4)}4a\right]\ldots\left[(-1)^{r(p-1)}(p-1)a\right]$$

D'un autre côté, par la définition des nombres $s(u)$, le produit (3) est congruent mod p à

$$[s(2)][s(4)]\ldots[s(p-1)]$$

Il y a $\frac{p-1}{2}$ facteurs ici et ce sont tous des nombres pairs distincts de l'intervalle $[0..p]$ comme nous l'avons montré au paragraphe précédent, de telle façon qu'ils sont juste un réarrangement des nombres $2, 4, \ldots, p-1$. Ainsi nous avons la congruence

$$\left[(-1)^{r(2)}2a\right]\left[(-1)^{r(4)}4a\right]\ldots\left[(-1)^{r(p-1)}(p-1)a\right] \equiv (2)(4)\ldots(p-1) \ mod \ p$$

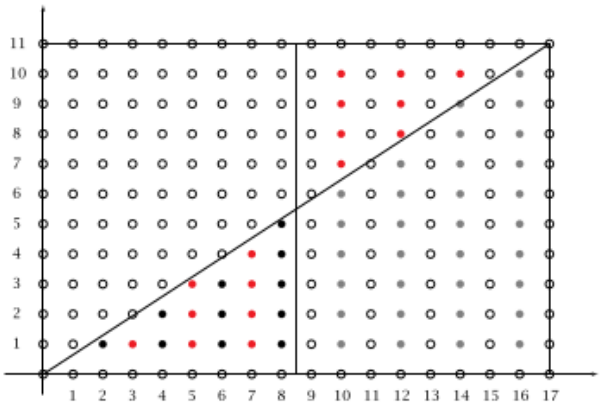
Nous pouvons éliminer les facteurs $2, 4, \ldots, p-1$ des deux côtés de la congruence pour obtenir

$$(-1)^{\sum_E r(u)} a^{\frac{p-1}{2}} \equiv 1 \ mod \ p$$

Les facteurs $(-1)^{\sum_E r(u)}$ et $a^{\frac{p-1}{2}}$ sont à la fois égaux à $\pm 1 \ mod \ p$ et leur produit est 1, ce qui fait qu'ils doivent être égaux mod p (en utilisant le fait que 1 et -1 ne sont pas congruents modulo un nombre premier impair). Par la formule d'Euler, on a $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \ mod \ p$, du coup, de la formule précédente (2), nous concluons que $\left(\frac{a}{p}\right) = (-1)^e$. Cela termine cette première étape de la preuve géométrique de la loi de réciprocité quadratique.

2. Maintenant nous traitons le cas où $a = q$ avec q un nombre premier impair distinct de p. Comme dans l'étape 1, nous considérons un triangle de taille $p \times q$.

Nous savons que $\left(\frac{a}{p}\right) = (-1)^e$ où e est le nombre de points du réseau d'abscisse paire à l'intérieur du rectangle et au-dessous de la diagonale. Supposons que nous divisions le rectangle en deux moitiés égales séparées par un ligne verticale $x = \frac{p}{2}$. Cette ligne ne passe par aucun point du réseau puisque p est impair Cette ligne verticale coupe deux triangles plus petits dans chacun des deux grands triangles au-dessus et au-dessous de la diagonale du rectangle. Appelons le petit triangle du bas L et celui du haut U, et les variables l et u pour le nombre de points du réseau d'abscisse paire dans L et U respectivement. On remarque que u a la même parité que le nombre de



points du réseau d'abscisse paire dans le quadrilatère sous U dans la moitié droite du rectangle puisque chaque colonne de points du réseau dans le rectangle contient $q-1$ points, un nombre pair. Du coup, e a la même parité que $l+u$, et par conséquent $(-1)^e = (-1)^{l+u}$.

La chose suivante à remarquer est qu'en tournant le rectangle U de 180 degrés autour du centre du rectangle l'amène sur le triangle L. Cette rotation amène les points du réseau dans U d'abscisse paire sur les points du réseau dans L sur les points d'abscisse impaire. Ainsi nous obtenons la formule $\left(\frac{q}{p}\right) = (-1)^t$ où t est le nombre total de points du réseau dans le triangle L.

En inversant les rôles de p et q, nous pouvons aussi dire que $\left(\frac{q}{p}\right) = (-1)^{t'}$ où t' est le nombre de points du réseau à l'intérieur du triangle L' au-dessus de la diagonale et au-dessous de la ligne horizontale $y = \frac{q}{2}$ qui coupe le rectangle en deux horizontalement. Alors $t + t'$ est le nombre des points du réseau dans le petit rectangle formé par L et L' ensemble. Ce nombre est juste $\frac{p-1}{2}.\frac{q-1}{2}$. Ainsi nous avons

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^t(-1)^{t'} = (-1)^{t+t'} = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}$$

qui finalement termine la preuve de la loi de réciprocité quadratique.

DÉCOUVERTE D'UNE LOI TOUT EXTRAORDINAIRE DES NOMBRES PAR RAPPORT À LA SOMME DE LEURS DIVISEURS

Leonhard Euler [1]

Commentatio 175 indicis Enestroemiani
Bibliothèque impartiale 3, 1751, p. 10-31

1. Les Mathematiciens ont tâché jusqu'ici en vain de découvrir quelque ordre dans la progression des nombres premiers, et on a lieu de croire que c'est un mystère que l'esprit humain ne saurait jamais pénétrer. Pour s'en convaincre, on n'a qu'à jeter les yeux sur les tables des nombres premiers, que quelques-uns se sont donnés la peine de continuer au-delà de cent mille et on s'apercevra d'abord qu'il n'y règne aucun ordre ni règle. Cette circonstance est d'autant plus surprenante, que l'Arithmétique nous fournit des règles sûres, par le moyen desquelles on est en état de continuer la progression de ces nombres aussi loin qu'on souhaite, sans pourtant nous y laisser la moindre marque de quelque ordre. Je me crois aussi bien éloigné de ce but, mais je viens de découvrir une loi fort bizarre parmi les sommes des diviseurs des nombres naturels, qui, au premier coup d'œil, paraissent aussi irrégulières que la progression des nombres premiers, et qui semblent même envelopper celle-ci. Cette règle, que je vais expliquer, est à mon avis d'autant plus importante qu'elle appartient à ce genre dont nous pouvons nous assurer de la vérité, sans en donner une démonstration parfaite. Néanmoins, j'en apporterai de telles preuves, qu'on pourra presque les envisager comme équivalentes à une démonstration rigoureuse.

2. Les nombres premiers se distinguent des autres nombres en ce qu'ils n'admettent d'autres diviseurs que l'unité et eux-mêmes. Ainsi 7 est un nombre premier, parce qu'il n'est divisible que par l'unité et lui-même. Les autres nombres qui ont, outre l'unité et eux-mêmes, encore d'autres diviseurs, sont nommés composés, comme par exemple le nombre 15 qui, outre l'unité et lui-même, est divisible par 3 et 5. Donc en général, si le nombre p est premier, il ne sera divisible que par 1 et par p ; mais si p est un nombre composé, il aura, outre 1 et p, encore d'autres diviseurs; et partant, dans le premier cas, la somme des diviseurs $= 1 + p$ et dans l'autre cas, elle sera plus grande que $1 + p$. Comme mes réflexions suivantes rouleront sur la somme des diviseurs de chaque nombre, je me servirai d'un certain caractère pour la marquer. La lettre $\int$ qu'on emploie dans l'analyse des infinis pour indiquer les intégrales, étant mise devant un nombre, me marquera la somme de ses diviseurs [2] : ainsi $\int 12$ signifiera la somme de tous les diviseurs du nombre 12 qui

[1] Ce mémoire a été également publié, comme "ineditum", d'après un manuscrit de l'Académie de Berlin dans les *Commentationes arithmeticae* 2, 1849, p. 639, et ensuite dans les *Opera postuma* 1, 1862, p. 76, les éditeurs, P. H. et N. Fuss, n'ayant pas eu connaissance de la publication antérieure, faite dans la Bibliothèque impartiale. Cf. *Comment. arithm.* Prooemium, p. XVIII, No. 57, Suppl. Prooem., No. 1, et t. II, p. VIII; en outre P. Stäckel et W. Ahrens, *Der Briefwechsel zwischen* C. G. J. JACOBI *und* P. H. von Fuss *Über die Herausgabe der Werke* Leonhard Euler, Leipzig 1908, p. 59 et 83. Il faut remarquer que le texte de la Bibliothèque impartiale diffère sur plusieurs points de celui des *Comment. arithm.* et des *Op. post.* Nous avons reproduit intégralement dans notre édition le texte de la Bibliothèque impartiale. Voir aussi le mémoire 243 de ce volume. F. R.
Leonhardi Euleri Opera omnia $I_2 Commentationesarithmeticae 31$.

[2] Voir les mémoires 152, 243 et surtout le mémoire 244 de ce volume. Voir aussi la lettre d'Euler à Goldbach du 1er avr. 1747, *Correspondance math. et phys. publiée par* P. H. Fuss, St.-Pétersbourg 1843, t. I, p. 407, et la lettre d'Euler à D'Alembert du 15 février 1748 publiée par P. Stäckel, Biblioth. Mathem. 115, 1910/1, p. 220 ; Leonhardi Euleri, *Opera omnia*, series III. F. R.

sont $1+2+3+4+6+12=28$ de sorte que $\int 12 = 28$. Cela posé, on verra que $\int 60 = 168$ et $\int 100 = 217$. Mais, comme l'unité n'a d'autre diviseur qu'elle-même, on aura $\int 1 = 1$. Or la chiffre 0, étant divisible par tout nombre, la valeur de $\int 0$ sera infinie. Cependant, dans la suite, je lui assignerai, pour chaque cas proposé, une valeur déterminée, convenable à mon dessein.

3. Ayant donc établi ce signe $\int$ pour marquer la somme des diviseurs du nombre devant lequel il est posé, il est clair que si p marque un nombre premier, la valeur de $\int p$ sera $= 1 + p$; excepté le cas où $p = 1$ dans lequel il y a $\int 1 = 1$, et non pas $\int 1 = 1 + 1$ d'où l'on voit qu'on doit exclure l'unité de la suite des nombres premiers, de sorte que l'unité étant le commencement des nombres entiers, n'est ni premier ni composé. Or, si le nombre p n'est pas premier, la valeur de $\int p$ sera plus grande que $1 + p$. Dans ce cas, on trouvera aisément la valeur de $\int p$ par les facteurs du nombre p. Car soient a, b, c, d, etc. des nombres premiers différents entre eux, on verra aisément que

$$\int ab = 1 + a + b + ab = (1 + a)(1 + b) = \int a \cdot \int b,$$

$$\int abc = (1 + a)(1 + b)(1 + c) = \int a \cdot \int b \cdot \int c,$$

$$\int abcd = \int a \cdot \int b \cdot \int c \cdot \int d,$$

etc.

Pour les puissances des nombres premiers, on a besoin de règles particulières, comme

$$\int a^2 = 1 + a + a^2 = \frac{a^3 - 1}{a - 1},$$

$$\int a^3 = 1 + a + a^2 + a^3 = \frac{a^4 - 1}{a - 1},$$

et généralement

$$\int a^n = \frac{a^{n+1} - 1}{a - 1}$$

Et par le moyen de celles-ci, on pourra assigner la somme des diviseurs de chaque nombre, tout composé qu'il puisse être ; ce qui sera clair par les formules suivantes :

$$\int a^2 b = \int a^2 \cdot \int b$$

$$\int a^3 b^2 = \int a^3 \cdot \int b^2,$$

$$\int a^3 b^4 c = \int a^3 \cdot \int b^4 \cdot \int c,$$

et généralement

$$\int a^\alpha b^\beta c^\gamma d^\beta e^\epsilon = \int a^\alpha \cdot \int b^\beta \cdot \int c^\gamma \cdot \int d^\beta \cdot \int e^\epsilon.$$

Ainsi, pour trouver la valeur de $\int 360$, puisque 360 se résout dans ces facteurs $2^3.3^2.5$, j'aurai

$$\int 360 = \int 2^3 \cdot 3^2 \cdot 5 = \int 2^3 \cdot \int 3^2 \cdot \int 5 = 15 \cdot 13 \cdot 6 = 1170.$$

4. Pour mettre devant les yeux la progression des sommes des diviseurs, j'ajouterai la table suivante qui contient les sommes des diviseurs des nombres naturels depuis l'unité jusqu'à 100 :

$\int 1 = 1$	$\int 21 = 32$	$\int 41 = 42$	$\int 61 = 62$	$\int 81 = 121$
$\int 2 = 3$	$\int 22 = 36$	$\int 42 = 96$	$\int 62 = 96$	$\int 82 = 126$
$\int 3 = 4$	$\int 23 = 24$	$\int 43 = 44$	$\int 63 = 104$	$\int 83 = 84$
$\int 4 = 7$	$\int 24 = 60$	$\int 44 = 84$	$\int 64 = 127$	$\int 84 = 224$
$\int 5 = 6$	$\int 25 = 31$	$\int 45 = 78$	$\int 65 = 84$	$\int 85 = 108$
$\int 6 = 12$	$\int 26 = 42$	$\int 46 = 72$	$\int 66 = 144$	$\int 86 = 132$
$\int 7 = 8$	$\int 27 = 40$	$\int 47 = 48$	$\int 67 = 68$	$\int 87 = 120$
$\int 8 = 15$	$\int 28 = 56$	$\int 48 = 124$	$\int 68 = 126$	$\int 88 = 180$
$\int 9 = 13$	$\int 29 = 30$	$\int 49 = 57$	$\int 69 = 96$	$\int 89 = 90$
$\int 10 = 18$	$\int 30 = 72$	$\int 50 = 93$	$\int 70 = 144$	$\int 90 = 234$
$\int 11 = 12$	$\int 31 = 32$	$\int 51 = 72$	$\int 71 = 72$	$\int 91 = 112$
$\int 12 = 28$	$\int 32 = 63$	$\int 52 = 98$	$\int 72 = 195$	$\int 92 = 168$
$\int 13 = 14$	$\int 33 = 48$	$\int 53 = 54$	$\int 73 = 74$	$\int 93 = 128$
$\int 14 = 24$	$\int 34 = 54$	$\int 54 = 120$	$\int 74 = 114$	$\int 94 = 144$
$\int 15 = 24$	$\int 35 = 48$	$\int 55 = 72$	$\int 75 = 124$	$\int 95 = 120$
$\int 16 = 31$	$\int 36 = 91$	$\int 56 = 120$	$\int 76 = 140$	$\int 96 = 252$
$\int 17 = 18$	$\int 37 = 38$	$\int 57 = 80$	$\int 77 = 96$	$\int 97 = 98$
$\int 18 = 39$	$\int 38 = 60$	$\int 58 = 90$	$\int 78 = 168$	$\int 98 = 171$
$\int 19 = 20$	$\int 39 = 56$	$\int 59 = 60$	$\int 79 = 80$	$\int 99 = 156$
$\int 20 = 42$	$\int 40 = 90$	$\int 60 = 168$	$\int 80 = 186$	$\int 100 = 217$

Je ne doute pas que, pour peu qu'on regarde la progression de ces nombres, on ne désespère presque d'y découvrir le moindre ordre, vu que l'irrégularité de la suite des nombres premiers s'y trouve

entremêlée tellement, qu'il semblera d'abord impossible d'indiquer quelque loi que ces nombres observent entre eux, sans qu'on sache celle des nombres premiers. Il semble même qu'il y a ici beaucoup plus de bizarrerie que dans les nombres premiers.

5. Néanmoins, j'ai remarqué [3] que cette progression suit une loi bien réglée et qu'elle est même comprise dans l'ordre des progressions que les géomètres nomment *récurrentes*, de sorte qu'on peut toujours former chacun de ces termes par quelques-uns des précédents, suivant une règle constante. Car si $\int n$ marque un terme quelconque de cette irrégulière progression, et $\int(n-1), \int(n-2), \int(n-3), \int(n-4), \int(n-5)$, etc. des termes précédents, je dis que la valeur de $\int n$ est toujours composée de quelques-uns des précédents suivant cette formule :

$$\begin{aligned}\int n = {} & \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15) \\ & - \int(n-22) - \int(n-26) + \int(n-35) + \int(n-40) - \int(n-51) - \int(n-57) \\ & + \int(n-70) + \int(n-77) - \int(n-92) - \int(n-100) + \text{etc.}\end{aligned}$$

Dans cette formule, il y a à remarquer :

I. Que dans l'altération des signes + et -, chacun se trouve toujours mis deux fois de suite.

II. La progression des nombres 1, 2, 5, 7, 12, 15, etc. qu'il faut successivement retrancher du nombre proposé n, deviendra évidente, en prenant leurs différences :

N.	1,	2,	5,	7,	12,	15,	22,	26,	35,	40,	51,	57,	70,	77,	92,	100, etc.
Diff.	1,	3,	2,	5,	3,	7,	4,	9,	5,	11,	6,	13,	7,	15,	8,	etc.

Car alternativement, on aura tous les nombres naturels 1, 2, 3, 4, 5, 6, etc. et les nombres impairs 3, 5, 7, 9, 11, etc., d'où l'on pourra continuer la suite de ces nombres aussi loin qu'on voudra.

III. Quoique cette suite aille à l'infini, on n'en doit prendre, dans chaque cas, que les termes depuis le commencement où le nombre mis après le signe $\int$ est encore positif, en omettant ceux qui renferment des nombres négatifs.

IV. S'il arrive que le terme $\int 0$ se rencontre dans cette formule, comme sa valeur est indéterminée en elle-même, il faut, dans chaque cas, au lieu de $\int 0$, mettre le nombre même proposé.

6. Ces choses remarquées, il ne sera pas difficile de faire l'application de cette formule à chaque nombre proposé et de se convaincre de sa vérité, par autant d'exemples qu'on voudra développer. Et comme je dois avouer que je ne suis pas en état d'en donner une démonstration rigoureuse, j'en ferai voir sa justesse par un assez grand nombre d'exemples :

[3] Voir la lettre d'Euler à Goldbach citée p. 242. F. R.

$$\int 1 = \int 0 = 1$$

$$\int 2 = \int 1 + \int 0 = 1 + 2 = 3,$$

$$\int 3 = \int 2 + \int 1 = 3 + 1 = 4,$$

$$\int 4 = \int 3 + \int 2 = 4 + 3 = 7,$$

$$\int 5 = \int 4 + \int 3 - \int 0 = 7 + 4 - 5 = 6,$$

$$\int 6 = \int 5 + \int 4 - \int 1 = 6 + 7 - 1 = 12,$$

$$\int 7 = \int 6 + \int 5 - \int 2 - \int 0 = 12 + 6 - 3 - 7 = 8,$$

$$\int 8 = \int 7 + \int 6 - \int 3 - \int 1 = 8 + 12 - 4 - 1 = 15,$$

$$\int 9 = \int 8 + \int 7 - \int 4 - \int 2 = 15 + 8 - 7 - 3 = 13,$$

$$\int 10 = \int 9 + \int 8 - \int 5 - \int 3 = 13 + 15 - 6 - 4 = 18,$$

$$\int 11 = \int 10 + \int 9 - \int 6 - \int 4 = 18 + 13 - 12 - 7 = 12,$$

$$\int 12 = \int 11 + \int 10 - \int 7 - \int 5 + \int 0 = 12 + 18 - 8 - 6 + 12 = 28,$$

$$\int 13 = \int 12 + \int 11 - \int 8 - \int 6 + \int 1 = 28 + 12 - 15 - 12 + 1 = 14,$$

$$\int 14 = \int 13 + \int 12 - \int 9 - \int 7 + \int 2 = 14 + 28 - 13 - 8 + 3 = 24,$$

$$\int 15 = \int 14 + \int 13 - \int 10 - \int 8 + \int 3 + \int 0 = 24 + 14 - 18 - 15 + 4 + 15 = 24,$$

$$\int 16 = \int 15 + \int 14 - \int 11 - \int 9 + \int 4 + \int 1 = 24 + 24 - 12 - 13 + 7 + 1 = 31,$$

$$\int 17 = \int 16 + \int 15 - \int 12 - \int 10 + \int 5 + \int 2 = 31 + 24 - 28 - 18 + 6 + 3 = 18,$$

$$\int 18 = \int 17 + \int 16 - \int 13 - \int 11 + \int 6 + \int 3 = 18 + 31 - 14 - 12 + 12 + 4 = 39,$$

$$\int 19 = \int 18 + \int 17 - \int 14 - \int 12 + \int 7 + \int 4 = 39 + 18 - 24 - 28 + 8 + 7 = 20,$$

$$\int 20 = \int 19 + \int 18 - \int 15 - \int 13 + \int 8 + \int 5 = 20 + 39 - 24 - 14 + 15 + 6 = 42.$$

Je crois ces exemples suffisants pour ne pas s'imaginer que c'est par un pur hasard que ma règle se trouve d'accord avec la vérité.

7. Si l'on doutait encore, si la loi des nombres à retrancher 1, 2, 5, 7, 12, 15, etc. était précisement celle que j'ai indiquée, vu que dans les exemples donnés, il n'entre que les six premiers de ces nombres par lesquels la loi ne pourrait pas encore paraître assez établie, je vais donner quelques exemples de plus grands nombres.

I. Soit proposé le nombre 101 dont on veuille chercher la somme de ses diviseurs, et on aura

$$\begin{aligned}\int 101 \;&= \int 100 + \int 99 - \int 96 - \int 94 + \int 89 + \int 86 - \int 79 - \int 75 + \int 66 + \int 61 \\ &\quad - \int 50 - \int 44 + \int 31 + \int 24 - \int 9 - \int 1 \\ &= +217 + 156 - 252 - 144 + 90 + 132 - 80 - 124 + 144 + 62 \\ &\quad - 93 - 84 + 32 + 60 - 13 - 1,\end{aligned}$$

ou joignant deux à deux $\int 101 = +373 - 396 + 222 - 204 + 206 - 177 + 92 - 14$, ce qui donne $\int 101 = 102$, d'où l'on connaitrait que 101 est un nombre premier, si on ne le savait d'ailleurs.

II. Soit proposé le nombre 301 dont on veut savoir la somme de ses diviseurs, et on aura

$$\begin{aligned}\int 301 \;&\overset{\text{differ.}}{=} \int 300 + \int 299 - \int 296 - \int 294 + \int 289 + \int 286 - \int 279 - \int 275 \\ &\quad + \int 266 + \int 261 - \int 250 - \int 244 + \int 231 + \int 224 - \int 209 - \int 201 \\ &\quad + \int 184 + \int 175 - \int 156 - \int 146 + \int 125 + \int 114 - \int 91 - \int 79 \\ &\quad + \int 54 + \int 41 - \int 14 - \int 0,\end{aligned}$$

où il est clair que par le moyen des différences, on peut aisément former cette suite pour chaque cas proposé. Or, prenant ces sommes de diviseurs, on trouvera

$$\begin{aligned}\int 301 \;&= +868 - 570 + 307 - 416 + 480 - 468 + 384 \\ &\quad + 336 - 684 + 504 - 372 + 390 - 434 + 504 \\ &\quad - 240 + 360 - 392 + 156 - 112 + 120 - 24 \\ &\quad - 272 + 248 - 222 + 240 - 80 + 42 - 301\end{aligned}$$

ou

$$\int 301 = +4939 - 4587 = 352,$$

d'où l'on connaît que 301 n'est pas premier. Or, puisque $301 = 7 \cdot 43$, on aura

$$\int 301 = \int 7 \cdot \int 43 = 8 \cdot 44 = 352,$$

comme la règle vient de montrer.

8. Ces exemples que je viens de développer, ôteront sans doute tout scrupule qu'on aurait pu encore avoir sur la vérité de ma formule. Or, par là-même, on sera d'autant plus surpris de cette belle propriété, ne voyant aucune liaison entre la composition de ma formule et la nature des diviseurs sur la somme desquels roule la proposition. La progression des nombres 1, 2, 5, 7, 12, 15, etc. ne paraît non seulement avoir nul rapport au sujet dont il s'agit, mais, comme la loi de ces nombres est interrompue et qu'ils sont mêlés de deux progressions régulières différentes, à savoir

$$\text{de } 1, 5, 12, 22, 35, 51, \quad \text{etc.} \quad \text{et de } 2, 7, 15, 26, 40, 57, \text{etc.},$$

il semble presque qu'une telle irrégularité ne saurait trouver lieu dans l'analyse. De plus, le défaut d'une démonstration n'en doit pas peu augmenter la surprise ; vu qu'il serait presque moralement impossible de parvenir à la découverte d'une telle propriété, sans y avoir été conduit par une méthode certaine qui pourrait tenir lieu d'une parfaite démonstration. J'avoue aussi que ce n'a pas été par un pur hasard que je suis tombé sur cette découverte ; mais une autre proposition d'une pareille nature qui doit être jugée vraie, quoique je n'en puisse donner une démonstration, m'a ouvert le chemin de parvenir à cette belle propriété. Et bien que cette chose ne roule que sur la nature des nombres à laquelle l'analyse des infinis ne paraît pas être applicable, c'est pourtant par le moyen des différentiations et plusieurs autres détours que j'ai été conduit à cette conclusion. Je souhaiterais qu'on trouvât un chemin plus court et plus naturel d'y parvenir, et peut-être que la considération de la route que j'ai suivie y pourra conduire.

9. Il y a longtemps [4] que je considérai, à l'occasion du problème de la partition des nombres, cette expression

$$(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)(1-x^8) \text{ etc.}$$

La supposant continuée à l'infini, j'ai multiplié actuellement un grand nombre de facteurs ensemble, pour voir la forme de la série qui en résulterait, et j'ai trouvé cette progression

$$1-x-x^2+x^5+x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+\text{etc.},$$

où les exposants de x sont les mêmes nombres qui entrent dans la formule précédente ; et aussi les signes + et - se trouvent doublés. On n'a qu'à entreprendre cette multiplication et à la continuer aussi loin qu'on jugera à propos, pour se convaincre de la vérité de cette série. Aussi n'ai-je point d'autre preuve pour cela qu'une longue induction que j'ai du moins poussée si loin, que je ne puis en aucune manière douter de la loi dont ces termes et leurs exposants sont formés. J'ai longtemps cherché en vain une démonstration rigoureuse que cette série doit être égale à l'expression proposée $(1-x)(1-x^2)(1-x^3)$ etc. et j'ai proposé la même demande à quelques-uns de mes amis [5] dont je connais la force dans ces sortes de questions ; mais tous sont tombés avec moi d'accord sur la vérité de cette conversion, sans en avoir pu déterrer aucune source de démonstration. Ce sera donc une vérité connue, mais pas encore démontrée, que si l'on pose

$$s=(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6) \text{ etc.},$$

la même quantité s se pourra aussi exprimer de la sorte

$$s=1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+\text{etc.}$$

Car chacun est en état de se convaincre de cette vérité par la résolution actuelle à tel point qu'il souhaitera ; et il paraît impossible que la loi qu'on a découverte dans 20 termes par exemple, ne soit point observée dans tous les suivants.

---

[4] Voir le mémoire 158 de ce volume, spécialement la note p. 191. F. R.

[5] Voir les lettres d'Euler à Goldbach du 15 oct. 1743, *Correspondance math, et phys. publiée par.* P. H. Fuss, St.-Pétersbourg 1843, t. I, p. 265, et à Nic. Bernoulli du 1er sept. et du 10 nov. 1742, L. Euleri, *Opera postuma*, t. I, p. 527 et p. 533; les réponses de ces savants se trouvent dans la Correspondance citée, t. I, p. 270 et t. II, p. 698; Leonhardi Euleri *Opera omnia*, series III. F. R.

10. Ayant donc découvert que ces deux expressions infinies sont égales, quoique l'égalité ne puisse être démontrée, toutes les conclusions qu'on pourra déduire de cette égalité seront de même nature, c'est-à-dire vraies sans être démontrées. Ou, si quelqu'une de ces conclusions pouvait être démontrée, on en pourrait réciproquement tirer une démonstration de l'égalité mentionnée ; et c'est en cette vue que j'ai manié en plusieurs manières ces deux expressions, par où j'ai été conduit entre autres à la découverte que je viens d'expliquer, et dont la vérité doit être aussi certaine que celle de l'égalité de ces deux expressions. Voilà de quelle manière j'ai opéré. Ces deux expressions étant égales

$$\text{I.} \quad s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7) \text{ etc.}$$

$$\text{II.} \quad s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} + \text{etc.},$$

pour délivrer la première des facteurs, j'en prends les logarithmes, d'où je tire

$$ls = l(1-x) + l(1-x^2) + l(1-x^3) + l(1-x^4) + l(1-x^5) + \text{etc.}$$

Maintenant, pour éliminer les logarithmes, j'en prends les différentielles, ce qui donnera cette équation

$$\frac{ds}{s} = -\frac{dx}{1-x} - \frac{2\,xdx}{1-x^2} - \frac{3\,x^2dx}{1-x^3} - \frac{4\,x^3dx}{1-x^4} - \frac{5\,x^4dx}{1-x^5} - \text{etc.}$$

que je divise par $-dx$ et multiplie par x, pour avoir

$$-\frac{xds}{sdx} = \frac{x}{1-x} + \frac{2\,x^2}{1-x^2} + \frac{3\,x^3}{1-x^3} + \frac{4\,x^4}{1-x^4} + \frac{5\,x^5}{1-x^5} + \text{etc.}$$

La seconde valeur de la même quantité s donne par la différentiation

$$ds = -dx - 2xdx + 5x^4dx + 7x^5dx - 12x^{11}dx - 15x^{14}dx + \text{etc.},$$

de laquelle, en la multipliant par $-x$ et divisant par sdx, on tirera une autre valeur de $-\dfrac{xds}{sdx}$ qui sera

$$-\frac{xds}{sdx} = \frac{x + 2\,x^3 - 5\,x^5 - 7\,x^7 + 12\,x^{12} + 15\,x^{15} - 22\,x^{22} - 26\,x^{26} + \text{etc.}}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.}}.$$

11. Soit la valeur de cette quantité $t - \dfrac{xds}{sdx} = t$ et nous aurons deux valeurs égales pour cette quantité t

$$\text{I.} \quad t = \frac{x}{1-x} + \frac{2x^2}{1-x^2} + \frac{3x^3}{1-x^3} + \frac{4x^4}{1-x^4} + \frac{5x^5}{1-x^6} + \frac{6x^6}{1-x^6} + \text{etc.}$$

$$\text{II.} \quad t = \frac{x + 2x^2 - 5x^5 - 7x^7 + 12x^{12} + 15x^{15} - 22x^{22} - 26x^{26} + \text{etc.}}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.}}.$$

De la première, je résous chaque terme dans une progression géométrique par la division ordinaire, et j'aurai

$$
\begin{array}{rcl|llllllllllll}
t & = & x & +x^2 & +x^3 & +x^4 & +x^5 & +x^6 & +x^7 & +x^8 & +x^9 & +x^{10} & +x^{11} & +x^{12} & +\text{etc.} \\
 & & & +2x^2 & & +2x^4 & & +2x^6 & & +2x^8 & & +2x^{10} & & +2x^{12} & +\text{etc.} \\
 & & & & +3x^3 & & & +3x^6 & & & +3x^9 & & & +3x^{12} & +\text{etc.} \\
 & & & & & +4x^4 & & & & +4x^8 & & & & +4x^{12} & +\text{etc.} \\
 & & & & & & +5x^5 & & & & & +5x^{10} & & & +\text{etc.} \\
 & & & & & & & +6x^6 & & & & & & +6x^{12} & +\text{etc.} \\
 & & & & & & & & +7x^7 & & & & & & +\text{etc.} \\
 & & & & & & & & & +8x^8 & & & & & +\text{etc.} \\
 & & & & & & & & & & +9x^9 & & & & +\text{etc.} \\
 & & & & & & & & & & & +10x^{10} & & & +\text{etc.} \\
 & & & & & & & & & & & & +11x^{11} & & +\text{etc.} \\
 & & & & & & & & & & & & & +12x^{12} & +\text{etc.}
\end{array}
$$

où il est aisé de voir que chaque puissance de x se trouve autant de fois que son exposant a de diviseurs, puisque chaque diviseur devient un coefficient de la même puissance de x. Ainsi, recueillant tous les termes homogènes dans une somme, le coefficient de chaque puissance de x sera la somme de tous les diviseurs de son exposant. Et partant, exprimant ces sommes de diviseurs par la préposition du signe $\int$, comme j'ai fait ci-dessus, j'obtiendrai pour t la série qui suit :

$$t = \int 1x + \int 2 \cdot x^2 + \int 3 \cdot x^3 + \int 4 \cdot x^4 + \int 5 \cdot x^5 + \int 6 \cdot x^6 + \int 7 \cdot x^7 + \text{etc.}$$

dont la loi de progression est tout à fait manifeste ; et, quoiqu'il semble que l'induction ait quelque part dans la détermination de ces coefficients, qu'on considere l'expression infinie précédente, on s'assurera aisément de la nécessité de cette loi de progression.

12. Substituons cette valeur au lieu de t dans la seconde expression de cette même lettre t qui, étant délivrée de fractions, se réduit en cette forme

$$t\,(1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.})$$

$$-x - 2x^2 + 5x^5 + 7x^7 - 12x^{12} - 15x^{15} + 22x^{22} + 26x^{26} - \text{etc.} = 0.$$

Maintenant, la valeur précédente de t étant mise dans cette équation, nous trouverons :

$$
\begin{array}{rl|llllllll}
0 & = \int 1 \cdot x & + \int 2 \cdot x^2 & + \int 3 \cdot x^3 & + \int 4 \cdot x^4 & + \int 5 \cdot x^5 & + \int 6 \cdot x^6 & + \int 7 \cdot x^7 & + \int 8 \cdot x^8 & + \int 9 \cdot x^9 & + \text{etc.} \\
 & -x & - \int 1 \cdot x^2 & - \int 2 \cdot x^3 & - \int 3 \cdot x^4 & - \int 4 \cdot x^5 & + \int 5 \cdot x^6 & - \int 6 \cdot x^7 & - \int 7 \cdot x^8 & - \int 8 \cdot x^9 & - \text{etc.} \\
 & & -2x^2 & - \int 1 \cdot x^3 & - \int 2 \cdot x^4 & - \int 3 \cdot x^5 & - \int 4 \cdot x^6 & - \int 5 \cdot x^7 & 6 \cdot x^8 & - \int 7.x^9 & - \text{etc.} \\
 & & & & & +5x^5 & + \int 1 \cdot x^6 & + \int 2 \cdot x^7 & + \int 3 \cdot x^8 & + \int 4 \cdot x^9 & + \text{etc.} \\
 & & & & & & & +7x^7 & + \int 1 \cdot x^8 & + \int 2 \cdot x^9 & + \text{etc.}
\end{array}
$$

Ici, il est aisé d'observer que les coefficients de chaque puissance de x sont les sommes des diviseurs, premièrement de l'exposant de cette puissance même, et ensuite des autres nombres plus petits qui résultent si l'on ôte successivement de l'exposant les nombres 1, 2, 5, 7, 12, 15, 22, 26, etc. Ensuite, si l'exposant de la puissance de x est égal à un terme de cette série numérique, alors ce même terme accompagne encore les coefficients. En troisième lieu, l'ordre des signes n'a besoin d'aucun éclaircissement. Ainsi, on conclura en général que la puissance x aura ces coefficients :

$$\int n - \int (n-1) - \int (n-2) + \int (n-5) + \int (n-7) - \int (n-12) - \int (n-15) + \text{etc.},$$

jusqu'à ce qu'on parvienne à des nombres négatifs. Mais, si quelqu'un de ces nombres devant lesquels se trouve le signe $\int$ devient 0, alors il faut mettre en sa place le nombre n même, de sorte que dans ce cas, il y a $\int 0 = n$ et le signe de ce terme suit l'ordre général des autres.

13. Puisque donc l'expression infinie du § précédent doit être égale à zéro, quelque valeur qu'on donne à la quantité x, il faut de nécessité que les coefficients de chaque puissance à part, soient égaux ensemble à zero, et partant, nous aurons les équations suivantes :

I.	$\int 1 - 1 = 0,$	ou	$\int 1 = 1,$
II.	$\int 2 - \int 1 - 2 = 0,$		$\int 2 = \int 1 + 2,$
III.	$\int 3 - \int 2 - \int 1 = 0,$		$\int 3 = \int 2 + \int 1,$
IV.	$\int 4 - \int 3 - \int 2 = 0,$		$\int 4 = \int 3 + \int 2,$
V.	$\int 5 - \int 4 - \int 3 + 5 = 0,$		$\int 5 = \int 4 + \int 3 - 5,$
VI.	$\int 6 - \int 5 - \int 4 + \int 1 = 0,$		$\int 6 = \int 5 + \int 4 - \int 1,$
VII.	$\int 7 - \int 6 - \int 5 + \int 2 + 7 = 0,$		$\int 7 = \int 6 + \int 5 - \int 2 - 7,$
	etc.		etc.

et généralement nous aurons :

$$\int n - \int (n-1) - \int (n-2) + \int (n-5) + \int (n-7) - \int (n-12) - \int (n-15) + \text{etc.} = 0$$

et par conséquent

$$\int n = \int (n-1) + \int (n-2) - \int (n-5) - \int (n-7) + \int (n-12) + \int (n-15) - \text{etc.}$$

qui est la même expression que j'ai donnée ci-dessus et qui exprime la loi selon laquelle les sommes des diviseurs des nombres naturels sont continuées. Outre la raison des signes et la nature de la progression des nombres

$$1, 2, 5, 7, 12, 15, 22, 26, 35, 40, 51, 57, 70, 77, \text{etc.},$$

on voit aussi, par ce que je viens d'avancer, la raison pourquoi, dans les cas où se trouve le terme $\int 0$, il faut mettre en sa place le nombre n même, ce qui aurait pu paraître le plus étrange dans mon expression. Ce raisonnement, quoiqu'il soit encore fort éloigné d'une démonstration parfaite [6], ne laissera pas pourtant de lever plusieurs doutes sur la forme bizarre de l'expression que je viens d'expliquer.

[6] Voir le mémoire 244 de ce volume. F.R.

Le théorème des deux carrés de Fermat

D. R. Heath-Brown

Pierre de Fermat (1601-1665) était un magistrat français. On l'a décrit comme le plus grand mathématicien amateur de tous les temps, pour ses contributions à l'optique, aux probabilités, et, plus notablement, à la théorie des nombres. Peut-être est-il davantage connu pour le "dernier théorème de Fermat", l'assertion (toujours non démontrée[1]) que $x^n + y^n = z^n$ n'a pas de solutions x, y, z dans les entiers positifs pour tout $n \geq 3$. Les étudiants de première année d'université rencontrent un autre théorème de Fermat (authentique !) énonçant que $x^p \equiv x \pmod{p}$ pour tout entier x et tout nombre premier p, comme conséquence du théorème de Lagrange pour les groupes finis.

Le théorème de Fermat des deux carrés est le suivant :

Si $p \equiv 1 \pmod{4}$ est un nombre premier,
alors p est la somme de deux carrés.

Ce résultat est remarquable en cela qu'il relie les nombres premiers - des objets dont la définition ne fait intervenir que la multiplication et la division - à la structure *additive* des entiers. Comme exemples d'illustrations de ce théorème, on a $5 = 1 + 4, 13 = 4 + 9, 17 = 1 + 16$, etc. *Exercice :* Montrer que si $p \equiv 3 \pmod{4}$ alors p ne peut pas être la somme de deux carrés (considérer le reste de la division lorsqu'on divise un carré par 4).

Plus de 50 démonstrations différentes du théorème ont été publiées. Les étudiants non diplômés peuvent rencontrer eux-mêmes deux preuves : l'une utilisant la propriété de factorisation unique de $\mathbb{Z}[\sqrt{-1}]$ et l'autre, dans le livre de cours *Elementary Number Theory*, utilisant le théorème d'approximation de Dirichlet. La grande majorité des preuves publiées, et en effet, les deux preuves qui viennent d'être mentionnées, ont de nombreux points communs. En particulier, elles dépendent du fait suivant :

Si $p \equiv 1 \pmod{4}$ est un nombre premier, il existe un entier x pour lequel $x^2 + 1 \equiv 0 \pmod{p}$ - par exemple $x = \left(\frac{(p-1)}{2}\right)!$.

Je décrirai une preuve nouvelle et complètement différente, utilisant les actions de groupes sur les ensembles. Soit

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, C = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 2 & -1 \end{pmatrix}$$

et

$$M = \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Référence du fichier original :
https://ora.ox.ac.uk/objects/uuid:c91a3bdd-7d8a-4bea-9734-28caf66f0914.
Traduction : Denise Vella-Chemla, février 2023.

[1] i.e. à l'époque de l'écriture de l'article d'Heath-Brown. Le dernier théorème de Fermat a été démontré, ultérieurement à l'écriture du présent article, en 1994 par Andrew Wiles.

On vérifie aisément que $A^2 = B^2 = C^2 = I$, et que $A^T MA = B^T MB = C^T MC = M$. En particulier A^{-1}, B^{-1}, et C^{-1} existe, par conséquent, les applications linéaires produites par A, B, C sont bijectives.

Définissons

$$S = \{\mathbf{v} = (x, y, z) \in \mathbb{Z}^3 : \mathbf{v}^T M\mathbf{v} = p \text{ et } x, y > 0\}$$

(on pense à $\mathbf{v}$ comme à un vecteur colonne) et soit

$$T = \{(x, y, z) \in S : z > 0\}, \quad U = \{(x, y, z) \in S : x + z > y\}.$$

Notons que $\mathbf{v}^T M\mathbf{v} = p$ signifie simplement que $4xy + z^2 = p$. Il en découle que S est un ensemble fini, puisque $x, y > 0$. On aura besoin de savoir que A envoie S dans lui-même, B envoie T dans lui-même, et C envoie U dans lui-même. On ne regardera que le dernier cas, les autres étant plus faciles. Si $\mathbf{v} = (x, y, z) \in S$ avec $x + z > y$, alors $C\mathbf{v} = (x - y + z, y, 2y - z) = (x', y', z')$, disons. Donc $x' > 0$, parce que $x + z > y$; $y' > 0$, parce que $y > 0$; et $x' + z' > y'$, parce que $x > 0$. De plus

$$(C\mathbf{v})^T M(C\mathbf{v}) = \mathbf{v}^T (C^T MC)\mathbf{v} = \mathbf{v}^T M\mathbf{v} = p,$$

donc C envoie U dans lui-même.

Ensuite on montre que S est l'union disjointe de T et AT, et aussi de U et AU. À nouveau, on vérifiera juste la dernière assertion. Si $(x, y, z) \in S$ alors soit $x + z > y$ (donc $(x, y, z) \in U$) ou $x + z = y$, ou $x + z < y$. Le cas $x + z = y$ ne peut advenir, puisque $\mathbf{v}^T M\mathbf{v} = p$ implique $p = 4xy + z^2 = 4x(x + z) + z^2 = (2x + z)^2$, contredisant la primalité de p. On montrera que si

$$U' = \{(x, y, z) \in S : x + z < y\}$$

alors $U' = AU$; cela donne le résultat requis.

Si $\mathbf{v} = (x, y, z) \in U$ alors $\mathbf{v} \in S$, donc $A\mathbf{v} \in AS = S$. De plus $A\mathbf{v} = (y, x, -z) = (x', y', z')$, disons, avec $x' + z' = y - z < x = y'$ donc $A\mathbf{v} \in U'$. Alors $AU \subseteq U'$. De façon similaire $AU' \subseteq U$, donc $U' = A^2 U \subseteq AU$. Ainsi $U' = AU$.

On atteint maintenant le cœur de la preuve. Puisque A est 1-1, on a $\#T = \#AT, \#U = \#AU$. De plus, comme S est l'union disjointe de T et AT on a $\#S = \#T + \#AT = 2\#T$. De façon similaire $\#S = 2\#U$, donc $\#T = \#U$.

Puisque $C^2 = I$, l'action de C sur U produit des orbites de longueur 1 ou 2. Si (x, y, z) est un point fixe de C alors $x - y + z = x, y = y, 2y - z = z$, donc $y = z$, et puisque $4xy + z^2 = p$ on a $p = 4xy + y^2 = y(4x + y)$. En utilisant le fait que p est un nombre premier et le fait que $p \equiv 1 \pmod 4$, on voit que cela arrive si et seulement si $y = 1$ et $x = (p - 1)/4$. Par conséquent, C a exactement un point fixe dans son action sur U. Puisque toutes les autres orbites ont pour longueur 2, on en déduit que $\#U$ est impair.

On argumente maintenant de façon similaire avec l'action de B sur T. Puisque $\#T(= \#U)$ est impair, il en découle que B doit avoir un nombre impair de points fixes sur U. Il y a donc au moins

un point fixe. Pourtant, un point fixe de B doit avoir $x = y$, et donc $p = 4xy + z^2$ aura une solution pour laquelle $x = y$. Il en découle que $p = (2x)^2 + z^2$ comme requis.

Appendice - Janvier 2008

Invariant était une publication occasionnelle de la société Invariant (la société mathématique des élèves non encore diplômés de l'université d'Oxford). Comme l'article original n'était pas disponible électroniquement, je l'ai réécrit en LaTeX, en corrigeant quelques coquilles.

L'histoire de l'argument utilisé ici a peut-être de l'intérêt. J'ai été amené à cet argument à partir de l'étude d'une présentation des articles de Liouville au sujet des identités pour les fonctions de parité, présentée dans le livre de Uspensky et Heaslet [1]. Mes notes originales datent de 1971. J'ai donné un exposé dans un groupe dissident[2] au colloque mathématique britannique en 1980 (ou 1979 ?), après quoi les notes semblent s'être propagées à travers le monde par le bouche à oreille. Cela devint un exercice pour entraîner les professeurs en France (Varouchas [2]). Plus tard, l'intérêt pour ces éléments a été engendré par la version de la preuve de Zagier en une seule phrase [3].

Références

[1] J.V. Uspensky and M.A. Heaslet, *Elementary Number Theory*, (McGraw-Hill Book Company, Inc., New York, 1939).

[2] I. Varouchas, Une démonstration élementaire du théorème des deux carrés, *I.R.E.M., Bull.*, n° 6 (1984), 31-39.

[3] D. Zagier, A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, *Amer. Math. Monthly*, 97 (1990), 144.

Mathematical Institute,
24-29, St. Giles',
Oxford
OX1 3LB
UK

rhb@maths.ox.ac.uk

[2] ?

À propos de l'application continue d'une ligne vers un morceau de surface.[1]

par

David Hilbert à Königsberg[2]

Peano a récemment montré dans les Annales Mathématiques[3], à travers une observation arithmétique, comment les points d'une ligne peuvent être envoyés continûment sur les points d'une surface. Les fonctions requises pour une telle application peuvent être réalisées de manière plus claire si l'on utilise la vue géométrique suivante. Divisons d'abord la ligne à représenter, un segment de droite de longueur 1, en 4 parties égales 1, 2, 3, 4 et divisons l'aire, que nous supposons avoir la forme d'un carré de côté 1, en 4 carrés égaux 1, 2, 3, 4 (Fig. 1), par deux lignes droites perpendiculaires. Deuxièmement, divisons chacune des sections 1, 2, 3, 4 en 4 parties égales, de sorte que nous ayons 16 sections sur la ligne droite, numérotées $1, 2, 3, \ldots, 16$. Dans le même temps, chacun des 4 carrés 1, 2, 3, 4 est divisé en 4 carrés égaux et les nombres 1, 2, 3,..., 16 sont écrits dans les 16 carrés résultants, l'ordre des carrés devant être choisi de la manière suivante : chaque carré partage un côté avec le carré précédent (Fig. 2). Si nous poursuivons ce processus, la figure 3 illustrant l'étape suivante, il est facile de voir comment on peut attribuer un seul point spécifique du carré à chaque point donné de la ligne. Il suffit de déterminer la partie de la ligne sur laquelle se situe le point donné. Les carrés marqués des mêmes numéros se trouvent nécessairement à la suite les uns des autres et délimitent la zone dans laquelle se trouve un certain point. Le point obtenu est l'image du point donné. *L'image ainsi obtenue est claire et continue et, à l'inverse, à chaque point du carré correspondent un, deux ou quatre points de la ligne. Il semble également remarquable qu'en modifiant de manière appropriée les lignes partielles du carré, on puisse facilement trouver une image claire et continue, dont l'inverse n'est nulle part plus ambigue.*

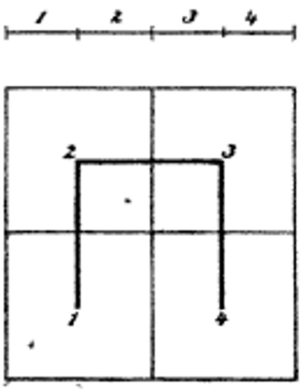


Fig. 1.

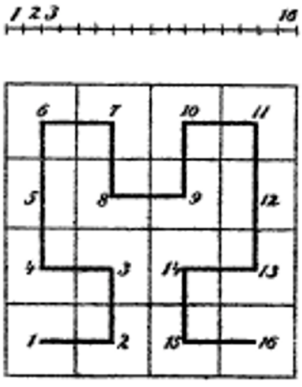


Fig. 2.

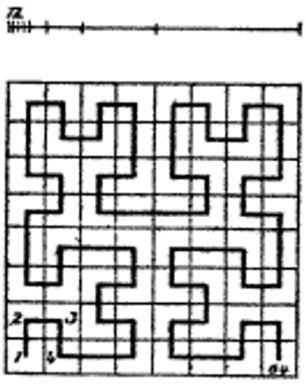


Fig. 3.

---

[1] À comparer à une communication sur le même sujet dans les Comptes-rendus de la Société allemande des chercheurs en sciences naturelles et médecins. Brême 1890.

Référence : (de) D. Hilbert, "*Über die stetige Abbildung einer Linie auf ein Flächenstück*", Math. Ann., vol. 38, 1891, p. 459-460.

https://gdz.sub.uni-goettingen.de/id/PPN235181684$_0$038?$tify$ = %7B%22$pages$%22%3A%5B476%5D%7D.

Transcription Latex : Denise Vella-Chemla, mars 2024.

Traduction : google translate de l'allemand au français.

[2] suivi des lettres i. Pr. qui signifient peut-être à Prague.

[3] Vol. 36, page 157.

Les applications présentées ci-dessus sont des exemples simples de fonctions à la fois continues partout et différenciables nulle part.

La signification mécanique de l'illustration discutée est la suivante : un point peut se déplacer continûment de telle manière qu'il passe par tous les points d'une surface pendant un temps fini. En modifiant de manière appropriée les lignes partielles du carré, on peut également garantir qu'un nombre infini de points densément répartis du carré sont parcourus selon une certaine direction de mouvement, à la fois vers l'avant et vers l'arrière.

En ce qui concerne la représentation analytique des fonctions représentatives, elle résulte de leur continuité, selon un théorème général [4] prouvé par K. Weierstrass, qui énonce que ces fonctions peuvent se développer en séries infinies qui progressent selon des fonctions rationnelles entières, qui convergent absolument et uniformément tout au long de l'intervalle.

Königsberg[5], le 4 Mars 1891.

[4]Comparez ce résultat à celui de l'article des Actes de l'Académie des Sciences de Berlin, du 9 juillet 1885.
[5]suivi également des lettres i. Pr. pour à Prague, peut-être.

Sur une courbe, qui remplit toute une aire plane.

G. Peano à Turin.

Dans cette Note on détermine deux fonctions x et y, uniformes et continues d'une variable (réelle) t, qui, lorsque t varie dans l'intervalle $(0, 1)$, prennent tous les couples de valeurs tels que $0 \leq x \leq 1, 0 \leq y \leq 1$. Si l'on appelle, suivant l'usage, *courbe continue* le lieu des points dont les coordonnées sont des fonctions continues d'une variable, on a ainsi un arc de courbe qui passe par tous les points d'un carré. Donc, étant donné un arc de courbe continu, sans faire d'autres hypothèses, il n'est pas toujours possible de le renfermer dans une aire arbitrairement petite.

Adoptons pour base de numération le nombre 3 ; appelons *chiffre* chacun des nombres 0, 1, 2 ; et considérons une suite illimitée de chiffres $a_1, a_2, a_3, \ldots$, que nous écrirons

$$T = 0, a_1 a_2 a_3 \ldots .$$

(Pour le moment, T est seulement une suite de chiffres).

Si a est un chiffre, désignons par $\mathbf{k}a$ le chiffre $2 - a$, *complémentaire de* a ; c'est-à-dire, posons

$$\mathbf{k}0 = 2, \mathbf{k}1 = 1, \mathbf{k}2 = 0.$$

Si $b = \mathbf{k}a$, on deduit $a = \mathbf{k}b$; on a aussi $\mathbf{k}a \equiv a \pmod 2$.

Désignons par $\mathbf{k}^n a$ le résultat de l'opération $\mathbf{k}$ répétée n fois sur a.

Si n est pair, on a $\mathbf{k}^n a = a$; si n est impair, $\mathbf{k}^n a = \mathbf{k}a$. Si $m \equiv n \pmod 2$, on a $\mathbf{k}^m a = \mathbf{k}^n a$.

Faisons correspondre à la suite T les deux suites

$$X = 0, b_1 b_2 b_3 \ldots , \quad Y = 0, c_1 c_2 c_3 \ldots ,$$

où les chiffres b et c sont donnés par les relations

$$b_1 = a_1, \quad c_1 = \mathbf{k}^{a_1} a_2, \quad b_2 = \mathbf{k}^{a_2} a_3, \quad c_2 = \mathbf{k}^{a_1 + a_2} a_4, \quad b_3 = \mathbf{k}^{a_2 + a_4} a_5, \ldots$$

$$b_n = \mathbf{k}^{a_2 + a_4 + \ldots + a_{2n-2}} a_{2n-1}, \quad c_n = \mathbf{k}^{a_1 + a_3 + \ldots + a_{2n-1}} a_{2n}.$$

Donc b_n, $n^{\text{ième}}$ chiffre de X, est égal à a_{2n-1}, $n^{\text{ième}}$ chiffre de rang impair dans T, ou à son complementaire, selon que la somme $a_2 + \ldots + a_{2n-2}$ des chiffres de rang pair, qui le précèdent, est paire ou impaire. Analoguement pour Y. On peut aussi écrire ces relations sous la forme :

$$a_1 = b_1, \quad a_2 = \mathbf{k}^{b_1} c_1, \quad a_3 = \mathbf{k}^{c_1} b_2, \quad a_4 = \mathbf{k}^{b_1 + b_2} c_2, \ldots ,$$

$$a_{2n-1} = \mathbf{k}^{c_1 + c_2 + \ldots + c_{n-1}} b_n, \quad a_{2n} = \mathbf{k}^{b_1 + b_2 + \ldots + b_n} c_n.$$

Transcription en LaTeX : Denise Vella-Chemla, juin 2025.

Si l'on donne la suite T, alors X et Y résultent déterminées, et si l'on donne X et Y, la T est déterminée.

Appelons *valeur* de la suite T la quantité (analogue à un nombre décimal ayant même notation)

$$t = \text{val. } T = \frac{a_1}{3} + \frac{a_2}{3^2} + \ldots + \frac{a_n}{3^n} + \ldots .$$

À chaque suite T correspond un nombre t, et l'on a $0 \leq t \leq 1$. Réciproquement les nombres t, dans l'intervalle $(0, 1)$ se divisent en deux classes :

α) Les nombres, différents de 0 et de 1, qui, multipliés par une puissance de 3, donnent un entier. Ils sont représentés par deux suites, l'une

$$T = 0,\, a_1 a_2 \ldots a_{n-1} a_n\, 2\, 2\, 2 \ldots$$

où a_n est égal à 0 ou à 1 ; l'autre

$$T' = 0,\, a_1 a_2 \ldots a_{n-1} a'_n\, 0\, 0\, 0 \ldots$$

où $a'_n = a_n + 1$.

β) Les autres nombres ; ils sont représentés par une seule suite T.

Or la correspondance établie entre T et (X, Y) est telle que si T et T' sont deux suites de forme différente, mais val. T = val. T', et si X, Y sont les suites correspondantes à T, et X', Y' celles correspondantes à T', on a

$$\text{val. } X = \text{val. } X', \qquad \text{val. } Y = \text{val. } Y'.$$

En effet considérons la suite

$$T = 0,\, a_1 a_2 \ldots a_{2n-3} a_{2n-2} a_{2n-1} a_{2n} 2\, 2\, 2\, 2 \ldots$$

où a_{2n-1} et a_{2n} ne sont pas toutes deux égales à 2. Cette suite peut représenter tout nombre de la classe α. Soit

$$X = 0,\, b_1 b_{2n-1} b_n b_{n+1} \ldots$$

on a

$$b_n = \mathbf{k}^{a_2 + \ldots + a_{2n-2}} a_{2n-1}, \quad b_{n+1} = b_{n+2} = \ldots = \mathbf{k}^{a_2 + \ldots + a_{2n-2} + a_{2n}} 2.$$

Soit T' l'autre suite dont la valeur coïncide avec val. T,

$$T' = 0,\, a_1 a_2 \ldots a_{2n-3} a_{2n-2} a'_{2n-1} a'_{2n} 0\, 0\, 0\, 0 \ldots$$

et

$$X' = 0,\, b_1 \ldots b_{n-1} b'_n b'_{n+1} \ldots .$$

Les premiers $2n-2$ chiffres de T' coïncident avec ceux de T ; donc les premiers $n-1$ chiffres de X' co"incident aussi avec ceux de X ; les autres sont déterminés par les relations

$$b'_n = \mathbf{k}^{a_2 + \ldots + a_{2n-2}} a'_{2n-1}, \quad b'_{n+1} = b'_{n+2} = \ldots = \mathbf{k}^{a_2 + \ldots + a_{2n-2} + a'_{2n}} 0.$$

Nous distinguerons maintenant deux cas, suivant que $a_{2n} < 2$ ou $a_{2n} = 2$.

Si a_{2n} a la valeur 0 ou 1, on a $a'_{2n} = a_{2n} + 1, a'_{2n-1} = a_{2n-1}, b'_n = b_n$,
d'où

$$b'_{n+1} = b'_{n+2} = \ldots = b_{n+1} = b_{n+2} = \ldots = \mathbf{k}^{a_2+\ldots+a_{2n}}2.$$

Dans ce cas les deux séries X et X' coïncident en forme et en valeur.

Si $a_{2n} = 2$, on a $a_{2n-1} = 0$ ou 1, $a'_{2n} = 0,\ a'_{2n-1} = a_{2n-1} + 1$, et en posant

$$s = a_2 + a_4 + \ldots + a_{2n-2}$$

on a

$$b_n = \mathbf{k}^3 a_{2n-1},\ \ b_{n+1} = b_{n+2} = \ldots = \mathbf{k}^3 2,$$

$$b'_n = \mathbf{k}^3 a'_{2n-1},\ \ b'_{n+1} = b'_{n+2} = \ldots = \mathbf{k}^3 0.$$

Or, puisque $a'_{2n-1} = a_{2n-1} + 1$, les deux fractions 0, $a_{2n-2}2\,2\,2\ldots$ et 0, $a'_{2n-1}0\,0\,0\ldots$ ont la même valeur ; en faisant sur les chiffres la même opération $\mathbf{k}^3$ on obtient les deux fractions 0, $b_n b_{n+1} b_{n+2}\ldots$ et 0, $b'_n b'_{n+1} b'_{n+2}\ldots$, qui ont aussi, comme l'on voit facilement, la même valeur ; donc les fractions X et X', bien que de forme différente, ont la même valeur.

Analoguement on prouve que val. Y = val. Y'.

Donc si l'on pose x = val. X, et y = val. Y, on déduit que x et y sont deux fonctions uniformes de la variable t dans l'intervalle $(0, 1)$. Elles sont continues ; en effet si t tend vers t_0, les $2n$ premiers chiffres du développement de t finiront par coïncider avec ceux du développement de t_0, si t_0 est un β, ou avec ceux de l'un des deux développements de t_0, si t_0 est un α ; et alors les n premiers chiffres de x et y correspondant à t coïncideront avec ceux des x, y correspondant à t_0.

Enfin à tout couple (x, y) tel que $0 \leq x \leq 1, 0 \leq y \leq 1$ correspond au moins un couple de suites (X, Y), qui en expriment la valeur ; à (X, Y) correspond un T, et à celui-ci t ; donc on peut toujours déterminer t de manière que les deux fonctions x et y prennent des valeurs arbitrairement données dans l'intervalle $(0, 1)$.

On arrive aux mêmes conséquences si l'on prend pour base de numération un nombre impair quelconque, au lieu de 3. On peut prendre aussi pour base un nombre pair, mais alors il faut établir entre T et (X, Y) une correspondance moins simple.

On peut former un arc de courbe continu qui remplit entièrement un cube. Faisons correspondre à la fraction (en base 3)

$$T = 0,\, a_1 a_2 a_3 a_4 \ldots$$

les fractions

$$X = 0,\, b_1 b_2 \ldots, \quad Y = 0,\, c_1 c_2 \ldots, \quad Z = 0,\, d_1 d_2 \ldots$$

où

$$b_1 = a_1, \quad c_1 = \mathbf{k}^{b_1}\, a_2, \quad d_1 = \mathbf{k}^{b_1+c_1}\, a_3, \quad b_2 = \mathbf{k}^{c_1+d_1}\, a_4, \ldots$$
$$b_n = \mathbf{k}^{c_1+\ldots+c_{n-1}+d_1+\ldots+d_{n-1}}\, a_{3n-2},$$
$$c_n = \mathbf{k}^{d_1+\ldots+d_{n-1}+b_1+\ldots+b_n}\, a_{3n-1},$$
$$d_n = \mathbf{k}^{b_1+\ldots+b_n+c_1+\ldots+c_n}\, a_{3n}.$$

On prouve que $x = \text{val. } X, y = \text{val. } Y, z = \text{val. } Z$ sont des fonctions uniformes et continues de la variable $t = \text{val. } T$; et si t varie entre 0 et 1, x, y, z prennent tous les ternes de valeurs qui satisfont aux conditions $0 \leq x \leq 1, 0 \leq y \leq 1, 0 \leq z \leq 1$.

M. Cantor, (Journal de Crelle, t. 84, p. 242) a démontré qu'on peut établir une correspondance univoque et réciproque (unter gegenseitiger Eindeutigkeit) entre les points d'une ligne et ceux d'une surface. Mais M. Netto (Journal de Crelle, t. 86, p. 263), et d'autres ont démontré qu'une telle correspondance est nécessairement discontinue. (Voir aussi G. Loria, *La definizione dello spazio ad n dimensioni secondo le ricerche di G. Cantor*, Giornale di Matematiche, 1877). Dans ma Note on démontre qu'on peut établir d'un coté l'uniformité et la continuité, c'est-à-dire, aux points d'une ligne on peut faire correspondre les points d'une surface, de façon que l'image de la ligne soit l'entière surface, et que le point sur la surface soit fonction continue du point de la ligne. Mais cette correspondance n'est point univoquement réciproque, car aux points (x, y) du carré, si x et y sont des β, correspond bien une seule valeur de t, mais si x, ou y, ou toutes les deux sont des α, les valeurs correspondantes de t sont en nombre de 2 ou de 4.

On a démontré qu'on peut enfermer un arc de courbe plane con-tinue dans une aire arbitrairement petite :

1) Si l'une des fonctions, p. ex. la x coïncide avec la variable indépendante t ; on a alors le théorème sur l'intégrabilité des fonctions continues.

2) Si les deux fonctions x et y sont à variation limitée (Jordan, Cours d'Analyse, III, p. 599). Mais, comme démontre l'exemple précédent, cela n'est pas vrai si l'on suppose seulement la continuité des fonctions x et y.

Ces x et y, fonctions continues de la variable t, manquent toujours de dérivée.

Turin, Janvier 1890.

Note de la transcriptrice : ci-dessous, un programme en python, utilisant un système de réécriture de Lindenmayer, et la tortue python-Logo, [1] *du dessin des 3 premiers niveaux de la courbe dite "de Peano".*

```
import numpy as np
import turtle
from turtle import *

def substitue(chaine):
      nouvellechaine = ''
      for k in range(len(chaine)):
            if chaine[k] == 'G':
                  nouvellechaine += 'GADAG-A-DAGAD+A+GADAG'
            else:
                  if chaine[k] == 'D':
                        nouvellechaine += 'DAGAD+A+GADAG-A-DAGAD'
                  else:
                        if chaine[k] in ['+','-','A']:
                              nouvellechaine += chaine[k]
      return(nouvellechaine)

niveau = 3 ; axiome = 'G' ; chaine = axiome ; mouvements = []
for k in range(niveau):
      chaine = substitue(chaine)
      mouvements.append(chaine)
print('Mouvements par niveau') ; up() ; setposition(-300,0)
down()
for k in range(niveau):
      print(k,' --> ',mouvements[k])
      setup() ; speed(0)
      chaine = mouvements[k]
      for m in range(len(chaine)):
            if (chaine[m] == '+'):
right(90)
            else:
                  if chaine[m] == '-':
                        left(90)
                  else:
                        if chaine[m] == 'A':
                              forward(100/(3**(k+1)-1))
      up()
      setposition(-300+150*(k+1),0) ; setheading(0)
      down()
exitonclick()
```

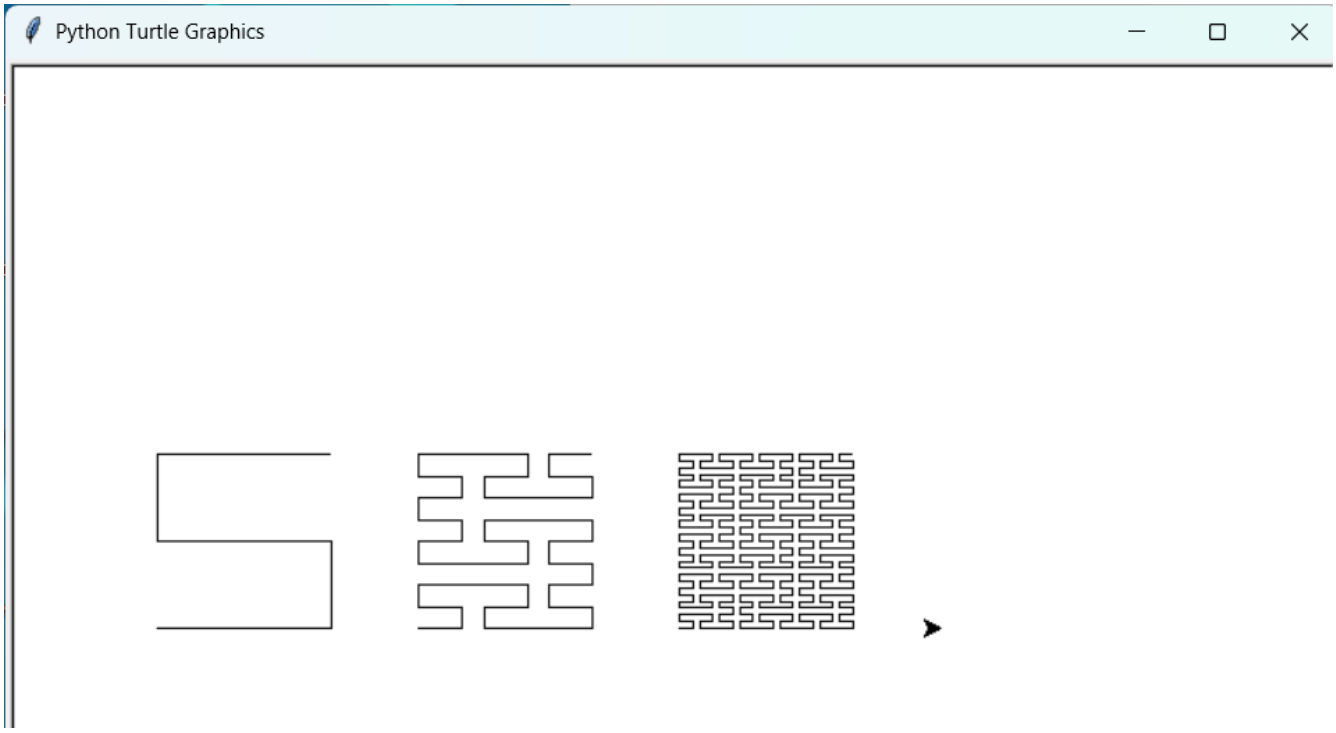
Les mots des mouvements et appels récursifs créés par niveaux :
0 −− > `GADAG-A-DAGAD+A+GADAG`

1 −− > `GADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A`

[1] Logo, le premier langage informatique explicitement conçu pour les enfants, a été inventé par Seymour Papert, Wallace Feurzeig, Daniel Bobrow et Cynthia Solomon en 1966 chez Bolt, Beranek and Newman, Inc. (BBN).

-DAGADAGADAG-A-DAGAD+A+GADAG

2 −− > GADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGAD+A+GADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGAD+A+GADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGAD+A+GADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGAD+A+GADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAG-A-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A-DAGAD+A+GADAG-A-DAGAD+A+GADAGADAGAD+A+GADAG-A
-DAGADAGADAG-A-DAGAD+A+GADAG



Traduction d'un article paru en mai 1965 dans Le professeur de mathématiques (Denise Vella-Chemla, 29.10.2020)

Utilisation des transformations pour trouver les équations de figures géométriques simples

Clarence R. Perisho

Un traitement clair de transformations géométriques utiles

Le signe de valeur absolue peut être utilisé pour écrire les équations de figures contenant des coins pointus ou des discontinuités, comme les carrés ou les parallélogrammes[1], des fonctions en escalier [2], et des fonctions en dents-de-scie[3]. La dérivation systématique de nombreuses telles équations peut être facilitée en utilisant certaines transformations de coordonnées. Cet article décrit cinq telles transformations de coordonnées et inclut des exemples de leur application.

Transformations de coordonnées

Les deux premières transformations de coordonnées dont on parlera, la translation et la rotation, sont des transformations métriques bien connues[4]. Des transformations moins connues sont les transformations qui étirent ou étendent une figure dans une direction parallèle à l'un des axes de coordonnées, les transformations qui ont un effet de cisaillement sur une figure, et les transformations qui produisent des formes symétriques des deux côtés d'un axe de coordonnées. L'étirement et le cisaillement sont des exemples de transformations affines[5].

Translation

Les équations habituelles d'une translation des axes sont

$$x = x' + h$$
$$y = y' + k,$$

où x et y sont les coordonnées d'un point en relation avec l'ensemble des anciens axes, et x' et y' sont les coordonnées du même point par rapport aux nouveaux axes. Les nouveaux axes sont parallèles aux anciens, mais la nouvelle origine est située au point (h, k) relativement aux anciens axes. Si h et k sont positifs, les *axes* sont transportés à droite de h unités et

Article original : *"The use of transformations in deriving equations of common geometric figures,"* The mathematics teacher, vol. 58, issue 5, p. 386., may 1965, ©The National Council of Teachers of Mathematics.

Clarence R. Perisho : Lycée d'état de Mankato, Mankato, Minnesota.

[1] John L. Spence, "Equations of Some Common Geometric Figures," *School Science and Mathematics*, LVIII (décembre 1958), p. 674-676.

[2] John. L. Spence, "Step Function Notation," *School Science and Mathematics*, LX (mars 1960), p. 179-180.

[3] John L. Spence, "Periodic Absolute Value Functions", *School Science and Mathematics*, LXI (décembre 1961), p. 664-666.

[4] Une *transformation métrique* préserve les distances et les angles ; les figures gardent leur taille et leur forme.

[5] Une *transformation affine* est une transformation qui peut être représentée par les équations

$$x' = a_1 x + b_1 y + c_1$$
$$y' = a_2 x + b_2 y + c_2,$$

où a, b et c sont des nombres réels. (Si $a_1 b_2 - a_2 b_1 = 0$, le plan entier s'effondre en une ligne ou un point.)

En général, une transformation affine ne préserve pas la taille et la forme des figures. Les transformations métriques, pourtant, peuvent être considérées comme une classe spéciale des transformations affines où la taille et la forme des figures sont préservées. Voir Felix Klein, *Elementary Mathematics from an Advanced Standpoint: Geometry*, trans. E.R. Hedrick and C.A. Noble (New York: The Macmillan Company, 1999), p. 70-86, 131.

vers le haut de k unités. On peut, pourtant, imaginer les axes fixes et voir cela comme une translation de la figure. Dans ce cas, pour h et k positifs, la *figure* est transportée sur la gauche de h unités et vers le bas de k unités. Si l'origine est translatée au point (h, k), cela signifie que le point de la figure situé en $(0, 0)$ est transporté au point $(-h, -k)$.

Si nous souhaitons bouger la figure de telle façon que le point initialement en (0, 0) soit transporté au point (h, k), nous devrions écrire notre transformation comme

$$\begin{aligned} x &= x' - h \\ y &= y' - k, \end{aligned}$$

Pour des raisons de convenance, nous oublierons les premiers et dirons que pour translater une figure de telle façon que le point initialement à l'origine soit déplacé au point (h, k), on transforme l'équation en utilisant la règle :

$$\textbf{remplacer } x \textbf{ par } x - h$$

et

$$\textbf{remplacer } y \textbf{ par } y - k. \tag{1}$$

En d'autres termes, $f(z, y) = 0$ devient $f(x - h, y - k) = 0$.

Exemple. L'équation $x^2 + y^2 = 9$ représente un cercle avec un rayon de 3 et centré à l'origine. Si nous souhaitons bouger le cercle de façon à ce que son centre soit le point (2, 4), nous utilisons la transformation (1) et remplaçons x par $x - 2$ et y par $y - 4$. Cela donne

$$(x - 2)^2 + (y - 4)^2 = 9$$

comme équation du cercle de rayon 3 et de centre le point (2, 4).

Rotation

Faire tourner une *figure* dans le sens des aiguilles d'une montre selon un angle θ autour de l'origine est la même chose que faire tourner les *axes* dans le sens inverse des aiguilles d'une montre d'un angle θ. Pour faire cela, on peut

$$\textbf{remplacer } x \textbf{ par } x\cos\theta - y\sin\theta$$

et

$$\textbf{remplacer } y \textbf{ par } x\sin\theta + y\cos\theta. \tag{2}$$

Par exemple, pour faire tourner une figure dans le sens des aiguilles d'une montre d'un angle de 45°, on utilise $\theta = 45°$ dans la transformation (2) et on obtient la règle :

$$\textbf{remplacer } x \textbf{ par } \tfrac{1}{2}\sqrt{2}(x - y)$$

et

$$\textbf{remplacer } y \textbf{ par } \frac{1}{2}\sqrt{2}(x + y) \tag{3}$$

Exemple. L'équation $x = 5$ représente une ligne parallèle à l'axe des y décalée de 5 unités sur sa droite. En tournant la figure de 45° en utilisant la transformation (3), nous obtenons

$$\frac{1}{2}\sqrt{2}(x - y) = 5$$

ou

$$y = x - 5\sqrt{2}$$

comme équation d'une droite (toujours à 5 unités de l'origine) avec une pente de 1 et telle que les points $(5\sqrt{2}, 0)$ et $(0, -5\sqrt{2})$ appartiennent à cette droite.

Étirement

Pour étirer, ou agrandir une figure selon un facteur p dans une direction parallèle à l'axe des x,

$$\textbf{remplacer } x \textbf{ par } \frac{x}{p} \tag{4}$$

Si $p > 1$, on a un agrandissement ; si $0 < p < 1$, on a une contraction; si $-1 < p < 0$, on a une réflexion et une contraction ; si $p < -1$, on a une réflexion et une expansion. Si $p = 1$, la figure est inchangée ; si $p = -1$, on a une réflexion selon l'axe des y sans changement de taille.

Similairement, pour étirer une figure selon un facteur q dans la direction parallèle à l'axe des y,

$$\textbf{remplacer } y \textbf{ par } \frac{y}{q} \tag{5}$$

Exemple. Un cercle peut être étiré en une ellipse. En remplaçant x par $\frac{x}{2}$, l'équation du cercle

$$x^2 + y^2 = 9$$

devient

$$x^2 + 4y^2 = 36,$$

qui est l'équation d'une ellipse d'axe le plus long horizontal et deux fois plus grand que l'axe le plus court.

Cisaillement

Si une translation bouge les points dans une direction parallèle à l'un des axes de coordonnées, tous les points sont translatés de la même distance. Un cisaillement bouge les points dans une direction parallèle à l'un des axes de coordonnées, mais les points à différentes distances de l'axe sont, en général, bougés à des distances différentes.

Pour cisailler une figure dans une direction parallèle à l'axe des x,

$$\textbf{remplacer } x \textbf{ par } x - cy. \tag{6}$$

Les points sont translatés horizontalement d'une distance proportionnelle à leur distance à l'axe des x. Les points de l'axe des x ne sont pas translatés, mais les points au-dessus de lui sont translatés vers la droite lorsque $c > 0$ et vers la gauche lorsque $c < 0$. Les points sous l'axe des x sont translatés dans la direction opposée. Une ligne parallèle à l'axe des y est déviée de façon à avoir une pente de $\frac{1}{c}$. Les ordonnées des points (coordonnées y) restent inchangées. Par exemple, les points de l'axe des y restent à la même distance de l'axe des x mais pas à la même distance les uns des autres.

Similairement, un cisaillement peut être réalisé parallèlement à l'axe des y ; pour cela, il faut

$$\textbf{remplacer } y \textbf{ par } y - dx. \tag{7}$$

Exemple. Si x est remplacé par $x - 2y$ dans l'équation du cercle d'équation

$$x^2 + y^2 = 9,$$

nous obtenons

$$(x - 2y)^2 + y^2 = 9.$$

Développé, cela devient

$$x^2 - 4xy + 5y^2 = 9$$

dont on peut démontrer que c'est l'équation d'une ellipse dont les axes ne sont parallèles ni à l'axe des x ni à l'axe des y.

Symétrie

Pour produire une figure symétrique selon l'axe des y

$$\textbf{remplacer } x \textbf{ par } |x|. \tag{8}$$

Cela retire toute partie située à gauche de l'axe des y (où x est négatif) et la remplace par son symétrique à droite de l'axe des y. Tous les éléments sur l'axe des y sont inchangés. Pour produire une figure symétrique selon l'axe des x

$$\textbf{remplacer } y \textbf{ par } |y|. \tag{9}$$

Cela retire toute partie située sous l'axe des x (où y est négatif) et la remplace par son symétrique qui est au-dessus de l'axe des x. Les points situés sur l'axe des x restent inchangés. En utilisant simultanément les deux transformations, on détruit toute partie située en dehors du premier quadrant et on la remplace par des réflexions des points de cette portion à partir de leur position initiale dans le premier quadrant.

Exemple. L'équation

$$(x-2)^2 + (y-3)^2 = 9$$

représente un cercle de rayon 3 et de centre (2, 3); il est tangent à l'axe des x mais intersecte l'axe des y en $(0, 3+\sqrt{5})$ et $(0, 3-\sqrt{5})$. En utilisant la transformation (8), on remplace x par $|x|$ et on obtient

$$(|x|-2)^2 + (y-3)^2 = 9,$$

qui représente les portions de deux cercles qui s'intersectent (Fig. 1). Si l'on appliquait également la transformation (9), la figure serait dupliquée sous l'axe des x.

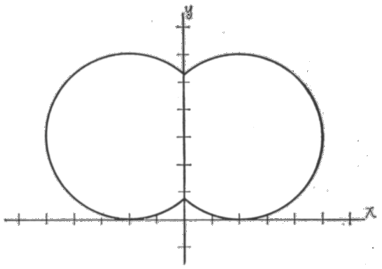


Figure 1

Applications

Les équations d'un certain nombre de figures géométriques communes peuvent être trouvées par l'utilisation de ces transformations. Comme exemples, les équations d'un carré, d'un triangle équilatéral, d'un hexagone régulier et d'un angle en position standard vont être trouvées ci-après.

Carré

Pour développer l'équation d'un carré, on commence avec la droite

$$x + y = a.$$

La droite croise les axes des coordonnées en $(a, 0)$ et $(0, a)$. La seule portion de la droite qui est dans le premier quadrant est le segment entre ces deux points. D'abord, on applique les transformations de symétrie (8) et (9); le remplacement de x par $|x|$ et de y par $|y|$ élimine la portion initiale de la ligne à gauche de l'axe des y et sous l'axe des x et place dans les second, troisième et quatrième quadrants les réflexions du segment de droite dans le premier quadrant. Ainsi, nous avons

$$|x| + |y| = a \tag{10}$$

comme équation du carré (Fig. 2) de sommets $(a, 0)$, $(0, a)$, $(-a, 0)$, et $(0, -a)$. Chaque côté est de longueur $\sqrt{2}a$.

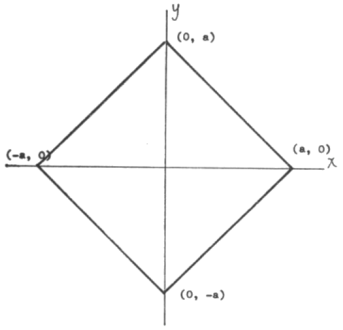


Figure 2

Si l'on souhaite que le carré ait ses côtés parallèles aux axes des coordonnées, on peut faire tourner la figure d'un angle de 45°. Après avoir appliqué la transformation (3) et avoir multiplié par $\sqrt{2}$, on obtient

$$|x+y| + |x-y| = \sqrt{2}a.$$

Ceci est l'équation d'un carré dont les côtés sont parallèles aux axes des coordonnées et dont les sommets sont $(\frac{1}{2}\sqrt{2}a, \frac{1}{2}\sqrt{2}a), (-\frac{1}{2}\sqrt{2}a, \frac{1}{2}\sqrt{2}a), (-\frac{1}{2}\sqrt{2}a, -\frac{1}{2}\sqrt{2}a)$ et $(\frac{1}{2}\sqrt{2}a, -\frac{1}{2}\sqrt{2}a)$. Chaque côté est toujours de longueur $\sqrt{2}a$.

Par expansion ou contraction, le carré peut être agrandi ou rétréci à la taille désirée. En particulier, l'utilisation des transformations (4) et (5) avec $p = q = \frac{1}{2}\sqrt{2}$ rétrécit le carré de telle façon que ses côtés soient de longueur a (Fig. 3). L'équation est alors

$$|x+y| + |x-y| = a. \tag{11}$$

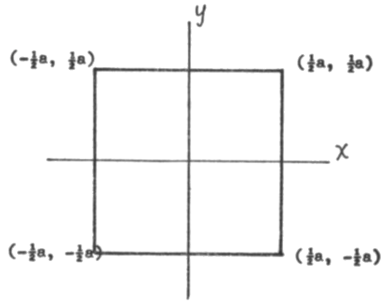


Figure 3

Si une figure quelconque est agrandie symétriquement (étirée d'un même montant parallèlement aux deux axes de coordonnées), la figure sera d'une taille différente mais elle sera similaire à la figure originale. En général, si la figure est agrandie assymétriquement (étirée plus dans une direction que dans une autre, ou étirée seulement dans une direction), la figure résultante aura une forme différente. En appliquant un agrandissement assymétrique à l'équation (10) au moyen des transformations (4) et (5), le carré sera changé en un losange de n'importe quelles dimensions données. En appliquant un agrandissement assymétrique à l'équation (11), le carré peut être changé en un rectangle de n'importe quelles dimensions spécifiées. Une combinaison d'agrandissement et de cisaillement produit un parallélogramme de toute taille et forme spécifiée.

Triangle équilatéral

Pour que ce soit plus pratique, dans le but d'obtenir l'équation d'un triangle équilatéral, nous choisissons $2a$ comme longueur des 3 côtés et situons les sommets en $(a, 0), (0, \sqrt{3}a)$, et $(-a, 0)$. On commence avec l'équation d'un carré de côté a, centré à l'origine, et dont les côtés sont parallèles aux axes des coordonnées (Fig. 3). Comme vu dans l'équation (11), cette équation est

$$|x+y| + |x-y| = a.$$

D'abord nous translatons le carré de façon à ce que son côté du bas coïncide avec l'axe des x. Cela se fait par la transformation (1) ; on remplace y par $y - \frac{1}{2}a$, ce qui donne

$$|x + y - \frac{1}{2}a| + |x - y + \frac{1}{2}| = a.$$

Deuxièmement, on agrandit la figure horizontalement par un facteur 2 et verticalement par un facteur $\sqrt{3}$. Selon la transformation (4), on remplace x par $\frac{x}{2}$; selon la transformation (5), on remplace y par $\frac{y}{\sqrt{3}}$.

Cela donne

$$|x + \frac{2}{3}\sqrt{3}y - a| + |x - \frac{2}{3}\sqrt{3}y + a| = 2a$$

comme équation du rectangle (Fig. 4) de base $2a$ (la même que celle du triangle équilatéral) et hauteur $\sqrt{3}a$ (la même que celle du triangle).

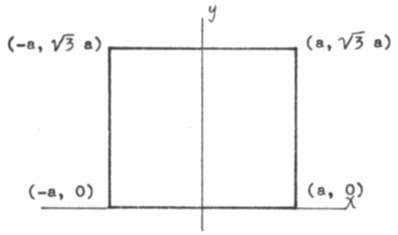


Figure 4

Troisièmement, le rectangle est penché sur la gauche de telle façon que son côté droit ait une pente de $-\sqrt{3}$. En utilisant la transformation (6), x est remplacé par $x + \frac{1}{3}\sqrt{3}y$, ce qui donne

$$|x + \sqrt{3}y - a| + |x - \frac{1}{3}\sqrt{3}y + a| = 2a$$

qui est l'équation d'un parallélogramme (Fig. 5) avec un côté sur l'axe des x et un côté allant du point $(a, 0)$ vers le haut à gauche jusqu'au point $(0, \sqrt{3}a)$.

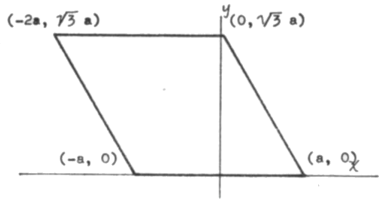


Figure 5

Quatrièmement, on remplace x par $|x|$ selon la transformation (8); cela enlève la portion du parallélogramme à gauche de l'axe des y et la remplace par la réflexion de la portion à droite de l'axe des y. Cela donne

$$||x| + \sqrt{3}y - a| + ||x| - \frac{1}{3}\sqrt{3}y + a| = 2a,$$

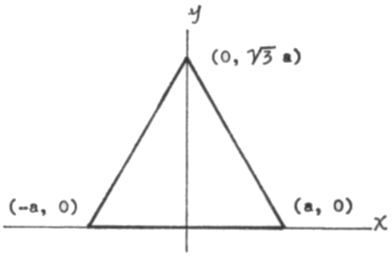


Figure 6

qui est l'équation requise d'un triangle équilatéral (Fig. 6) de côté $2a$ et de sommets $(a, 0), (0, \sqrt{3}a)$, et $(-a, 0)$.

L'équation n'est pas unique, car l'équation du triangle peut être produite en appliquant la transformation (8) à l'équation de n'importe quelle figure qui coïncide avec cette portion du triangle à droite de l'axe des y. D'un choix différent de figures peut résulter une équation différente.

Hexagone régulier

Si un hexagone régulier a son centre à l'origine, il peut être orienté de telle façon que deux de ses sommets soient sur l'axe des x, deux au-dessus, et deux en-dessous. La figure sera alors symétrique selon le premier axe et selon le deuxième axe. Si les côtés sont de longueur a, les sommets seront les points $(a, 0), (\frac{1}{2}a, \frac{1}{2}\sqrt{3}a), (-\frac{1}{2}a, \frac{1}{2}\sqrt{3}a), (-a, 0), (-\frac{1}{2}a, -\frac{1}{2}\sqrt{3}a)$, et $(\frac{1}{2}a, -\frac{1}{2}\sqrt{3}a)$.

On commence par écrire l'équation d'une courbe qui coïncide avec cette portion de l'hexagone située dans le premier quadrant. Cette courbe est constituée de deux segments de droites (Fig. 7) avec un coin en $(\frac{1}{2}a, \frac{1}{2}\sqrt{3}a)$. À gauche de ce point, la pente est 0 ; à droite de ce point, la pente est $-\sqrt{3}$. L'équation requise est [6]

$$y = -\frac{1}{2}\sqrt{3}x - \frac{1}{2}\sqrt{3}|x - \frac{1}{2}a| + \frac{3}{4}\sqrt{3}a.$$

Quand les transformations de symétrie (8) et (9) sont appliquées, les réflexions de cette courbe sont trouvées dans les second, troisième, et quatrième quadrants pour compléter l'hexagone (Fig. 8). L'équation devient alors

$$|y| = -\frac{1}{2}\sqrt{3}|x| - \frac{1}{2}\sqrt{3}||x| - \frac{1}{2}a| + \frac{3}{4}\sqrt{3}a.$$

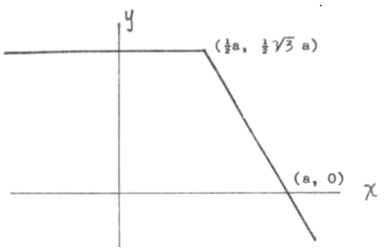


Figure 7

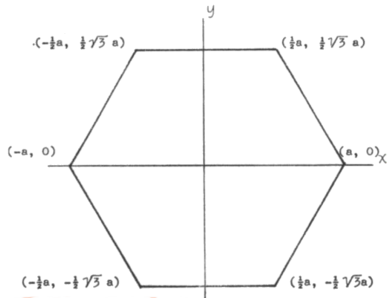


Figure 8

Angle en position standard

D'abord, nous plaçons un angle A symétrique selon l'axe des y avec son sommet à l'origine, son côté initial à droite de l'axe des y et son côté terminal à gauche de l'axe des y. Si $0^o < A < 180^o$, la figure formera un V s'ouvrant vers le haut avec son côté initial dans le premier quadrant et son côté terminal dans le second quadrant (Fig. 9). Si $180^o < A < 360^o$, la figure formera un V inversé avec le côté initial dans le quatrième quadrant et son côté terminal dans le troisième quadrant.

[6] Pour une explication de la méthode générale, voir Clarence E. Perisho, "Curves with corners", *The mathematics teacher*, LV (May 1962), 326-329 ; et Charles P. Seguin, "Equations of Polygonal Paths", *The American Mathematical Monthly*, LXIX (June-July, 1962), p. 548-549.

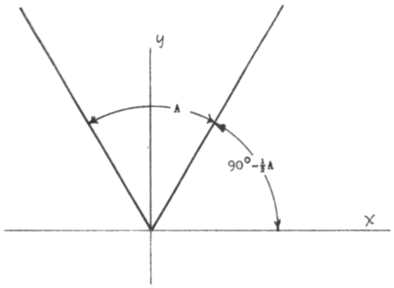


Figure 9

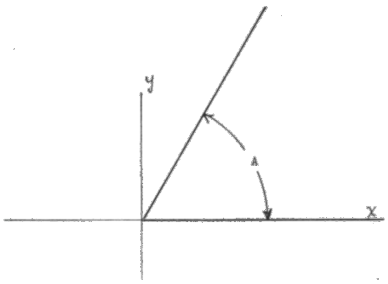


Figure 10

Dans les deux cas, si nous utilisons des angles orientés, l'inclinaison de la courbe à droite de l'axe des y est $90^\circ - \frac{1}{2}A$, et la pente est $\tan(90^\circ - \frac{1}{2}A) = \cot\frac{1}{2}A$. L'équation pour la moitié droite de la figure est ainsi

$$y = x\cot\frac{1}{2}A.$$

En appliquant la transformation (8), nous obtenons l'équation de l'angle qui est

$$y = |x|\cot\frac{1}{2}A. \tag{12}$$

Alors nous plaçons l'angle dans la *position standard*, i.e. de telle façon que son sommet soit à l'origine et que le côté initial coïncide avec la portion positive de l'axe des x (la Figure 10 montre un angle aigu en position standard). Si $0^\circ < A < 180^\circ$, l'angle est placé en position standard en le faisant tourner dans le sens des aiguilles d'une montre d'un angle de $90^\circ - \frac{1}{2}A$. Si $180^\circ < A < 360^\circ$, on fait tourner l'angle dans le sens inverse des aiguilles d'une montre d'un angle de $\frac{1}{2}A - 90^\circ$. Si on utilise des angles orientés, on peut dire dans les deux cas que la figure est tournée dans le sens des aiguilles d'une montre d'un angle de $90^\circ - \frac{1}{2}A$ ou que les axes sont tournés selon le sens inverse des aiguilles d'une montre d'un angle égal à $90^\circ - \frac{1}{2}A$.

Quand on applique la transformation (2) avec $\theta = 90^\circ - \frac{1}{2}A$ à l'équation (12), on obtient

$$x\sin(90^\circ - \frac{1}{2}A) + y\cos(90^\circ - \frac{1}{2}A) = \cot\frac{1}{2}A|x\cos(90^\circ - \frac{1}{2}A) - y\sin(90^\circ - \frac{1}{2}A)|$$

comme équation de l'angle A en position standard. Cela peut être simplifié en

$$x + y\tan\frac{1}{2}A = \frac{1}{\sin\frac{1}{2}A}|x\sin\frac{1}{2}A - y\cos\frac{1}{2}A|.$$

Puisque $\sin\frac{1}{2}A$ est toujours positif pour $0^\circ < A < 360^\circ$, on peut faire entrer l'expression $\sin\frac{1}{2}A$ à l'intérieur de la valeur absolue, et l'équation est simplifiée encore en

$$x + y\tan\frac{1}{2}A = |x - y\cot\frac{1}{2}A|. \tag{13}$$

Cette équation est valide pour tous les angles tels que $0^\circ < A < 360^\circ$, sauf pour $A = 180^\circ$. L'angle peut être translaté de façon que son sommet soit en n'importe quel endroit du plan, et il peut être tourné de telle façon que son côté initial prenne n'importe quelle direction donnée.

Les équations des angles des second et troisième quadrant en position standard peuvent s'écrire plus simplement par d'autres méthodes[7], puisque y est une fonction à une seule valeur de x, l'équation (13) est applicable aux angles du second et du troisième quadrant, où y est une fonction à valeur unique de x, et aussi aux angles des premier et quatrième quadrants, où y est une fonction à deux valeurs de x.

[7] Joseph F. Santner, "A Note on Curve Fitting.", The Mathematics Teacher, LVI (avril 1963), p. 218-221.

Une preuve géométrique du théorème de Wilson.

Écrit par
Dr. K. Petr.

Le théorème de Wilson nous dit que le nombre $1.2.3\ldots(p-1)+1$ (ou autrement, écrit $(p-1)!+1$) est divisible par p, si p est premier. Pour prouver ce théorème, imaginons dans le plan les p points $A_1, A_2, \ldots, A_p$ sommets d'un polygone régulier et considérons d'abord de combien de façons il est possible de connecter ces p points avec une ligne brisée constituée de p segments ayant ces points comme extrémités. Il y a probablement autant de façons qu'il y a de permutations de $p-1$ éléments différents, c'est-à-dire qu'il y en a $(p-1)!$ parce qu'à partir d'un point, par exemple du point A_x, on peut parcourir le reste des points dans n'importe quel ordre. Ce faisant, nous considérons deux lignes qui se chevauchent mais qui vont dans la direction opposée comme différentes. Ces lignes brisées fermées sont de deux types, les régulières ou les irrégulières. Les régulières sont celles qui, si on les fait tourner autour du centre correspondant aux points $A_1, A_2, \ldots, A_p$ d'un angle $\dfrac{2\pi}{p}$ ou par des multiples de cet angle $\dfrac{2\pi}{p}, \dfrac{4\pi}{p}, \ldots, \dfrac{2(p-1)\pi}{p}$, vont se recouvrir elles-mêmes. Les irrégulières ont alors la propriété que si nous faisons tourner les points $A_1, A_2, \ldots, A_p$, de n'importe lequel des angles, nous obtenons une ligne brisée, reliant les points mais dans un ordre différent de celui dont nous sommes partis. Par conséquent, les lignes discontinues irrégulières peuvent être assemblées en groupes de p membres chacun. D'une ligne brisée irrégulière, on obtient toutes les autres du même groupe, si l'on fait tourner cette ligne brisée autour du centre d'angles successifs

$$\frac{2\pi}{p}, \frac{4\pi}{p}, \ldots, \frac{p-1}{p}2\pi$$

Il n'y a pas d'autres lignes brisées. Car supposons que nous ayons une ligne brisée qui se couvrirait si nous la tournions autour du centre q d'un angle $q\dfrac{2\pi}{p}$, et supposons que q serait le plus petit nombre ayant cette propriété $\quad(1 < q < p)$.

Alors, cette ligne se couvrirait également lorsqu'on la tournerait d'un angle égal à

$$\frac{2.q2\pi}{p}, \quad \frac{3.q2\pi}{p}, \ldots, \frac{\lambda.q2\pi}{p}.$$

Soit λ un entier tel que

$$(\lambda-1)q < p \quad \text{et} \quad \lambda q > p,$$

Retranscription en Latex et correction de la traduction par Google : Denise Vella-Chemla, août 2022.

alors

$$\lambda q = p + q_1,$$

où, puisque p est premier

$$0 < q_1 < q \ ;$$

et la ligne brisée se chevaucherait à l'angle

$$\frac{\lambda.q2\pi}{p} = 2\pi + \frac{q_1 2\pi}{p}$$

c'est-à-dire à un angle $\frac{q_1 2\pi}{p}$, ce qui est contraire à l'hypothèse que q est le plus petit nombre ayant cette propriété.

Il y a $p-1$ lignes brisées régulières, car une ligne brisée régulière est complètement définie par une ligne de connexion, et nous pouvons relier le point 1 par exemple avec seulement $(p-1)$ points différents. Soit N le nombre de groupes à p éléments de lignes brisées irrégulières. Alors on a

$$(p-1)! = p - 1 + Np$$

ou

$$(p-1)! + 1 = p(N+1)$$

ce qui prouve le théorème de Wilson.

Sur la loi de réciprocité quadratique

G. Rousseau

Résumé : une version de la cinquième preuve de Gauss de la loi de réciprocité quadratique est donnée qui utilise seulement des considérations simples de théorie des groupes (en se passant même du lemme de Gauss) et qui rend manifeste que la loi de réciprocité quadratique est une conséquence simple du théorème des restes chinois.

Comme on le sait, le critère d'Euler et les théorèmes de Fermat et Wilson peuvent être démontrés de manière très simple en déterminant de deux manières le produit des éléments d'un groupe abélien fini adéquat (cf. Dirichlet [2]). On montre qu'il en est de même pour la loi de réciprocité quadratique. Cette loi est ainsi vue comme ne dépendant de rien de plus mystérieux que du théorème des restes chinois, sans nécessiter de lemmes particuliers ou de considérations auxiliaires qui vont au-delà du domaine des simples congruences.

Pour un entier m, soit $\mathbb{Z}_m^*$ le groupe multiplicatif des restes réduits modulo m. Soient p et q deux nombres premiers impairs distincts. On détermine le produit π des éléments du groupe $G = (\mathbb{Z}_p^* \times \mathbb{Z}_q^*)/U$, où $U = \{(1,1),(-1,-1)\}$.

Clairement, $\{(i,j) : i = 1,2,...,p-1; j = 1,2,...,(q-1)/2\}$ est un système de représentants pour les cosets de U. Le produit des (i,j) est $((p-1)!^{(q-1)/2}, ((q-1)/2)!^{p-1})$, et $((q-1)/2)!^2 \equiv (-1)^{(q-1)/2}(q-1)! \pmod q$, donc

$$\pi = ((p-1)!^{(q-1)/2},\ \ (q-1)!^{(p-1)/2}(-1)^{((p-1)/2)((q-1)/2)})U.$$

L'ensemble $\{(k \bmod p, k \bmod q) : k = 1,2,...,(pq-1)/2 \ \ ; \ \ (k,pq) = 1\}$ est aussi un système de représentants pour les cosets de U parce que $\mathbb{Z}_{pq}^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ (théorème des restes chinois). Le produit des k, modulo p, est

$$\frac{\left(\prod_{i=1}^{p-1} i\right)\left(\prod_{i=1}^{p-1} p+i\right)\cdots\left(\prod_{i=1}^{p-1}\left(\frac{q-1}{2}-1\right)p+i\right)\left(\prod_{i=1}^{p-1}\frac{q-1}{2}p+i\right)}{1.q.2q\ldots\frac{p-1}{n}q} \equiv \frac{(p-1)!^{(q-1)/2}}{q^{(p-1)/2}},$$

avec une expression similaire pour le produit modulo q, donc par le critère d'Euler

$$\pi = ((p-1)!^{(q-1)/2}(q|p),\ \ (q-1)!^{(p-1)/2}(p|q))U.$$

Comparer les deux expressions pour π donne

$$(1,(-1)^{((p-1)/2)((q-1)/2)})U = ((q|p),(p|q))U$$

(Reçu le 21 décembre 1989),
Communiqué par J. H. Loxton.

J. Austral. Math. Soc. (Série A) 51 (1991), 423-425.

et par conséquent la loi de réciprocité quadratique,

$$(q|p) = (-1)^{((p-1)/2)((q-1)/2)}(p|q)$$

On note que, puisque la première expression pour π est symétrique en p et q, prendre $\{(i,j) : i = 1, 2, ..., (p-1)/2 \ ; \ j = 1, 2, ..., q-1\}$ comme système de représentants amènerait à la même expression. On obtient également la valeur réelle sans appliquer le théorème de Wilson :

$$\pi = (1, (-p|q)(-q|p))U = \begin{cases} (1,1)U & \text{si } p \equiv q \equiv 1 \pmod 4 \\ (1,-1)U & \text{sinon.} \end{cases}$$

La preuve ci-dessus nous a été suggérée par l'étude de la seconde preuve de H. Schmidt [4], qui est en retour (comme noté dans [1]) une variante de la cinquième preuve de Gauss [3]. La caractéristique remarquable de la preuve de Schmidt est qu'elle se dispense du lemme de Gauss alors qu'elle retient en effet l'idée implicite de ce dernier de considérer les quotients $\mathbb{Z}_m^*/\{1,-1\}$.

Références

[1] P. Bachmann, *Niedere Zahlentheorie* I, (Teubner, Leipzig, 1910, reprinted Chelsea, New York, 1968).

[2] P. G. L. Dirichlet, Démonstrations nouvelles de quelques théorèmes relatifs aux nombres, *J. Reine Angew. Math.* **3** (1828), 390-393.

[3] C. F. Gauss, *Werke* II, (K. Gesell. Wiss., Göttingen, 1870), 47-64.

[4] H. Schmidt, Drei neue Beweise des Reciprocitätssatzes in der Theorie der quadratischen Reste, *J. Reine Angew. Math.* **111** (1893), 107-120.

Université de Leicester,
LE1 7RH
Royaume uni

Traduction des pages 306 à 308 extraites du chapitre "Types d'algèbres de von Neumann et traces", du livre (en anglais) Théorie des algèbres d'opérateurs I, de Masamichi Takesaki, 1979, aux éditions Springer Verlag New York-Heidelberg-Berlin, Denise Vella-Chemla, mars 2023.

Nous allons maintenant analyser la position relative de deux projections sur un espace de Hilbert $\mathfrak{H}$. Soient e et f des projections non nulles sur $\mathfrak{H}$. Pour abréger, on écrira $e^\perp = 1 - e$ et $f^\perp = 1 - f$. On a alors

$$e = e \wedge f + e \wedge f^\perp + (e - e \wedge f - e \wedge f^\perp),$$
$$f = e \wedge f + e^\perp \wedge f + (f - e \wedge f - e^\perp \wedge f).$$

Posons

$$e_0 = e - e \wedge f - e \wedge f^\perp, \qquad e_1 = e \wedge f + e \wedge f^\perp,$$
$$f_0 = f - e \wedge f - e^\perp \wedge f, \qquad f_1 = e \wedge f + e^\perp \wedge f.$$

Il est évident de vérifier que e et f_1 (resp. e_1 et f) commutent et que

$$1 = e \wedge f + e \wedge f^\perp + e^\perp \wedge f + e^\perp \wedge f^\perp + e_0 \vee f_0,$$
$$e_0 \wedge f_0 = e_0 \wedge f_0^\perp = e_0^\perp \wedge f_0 = 0.$$

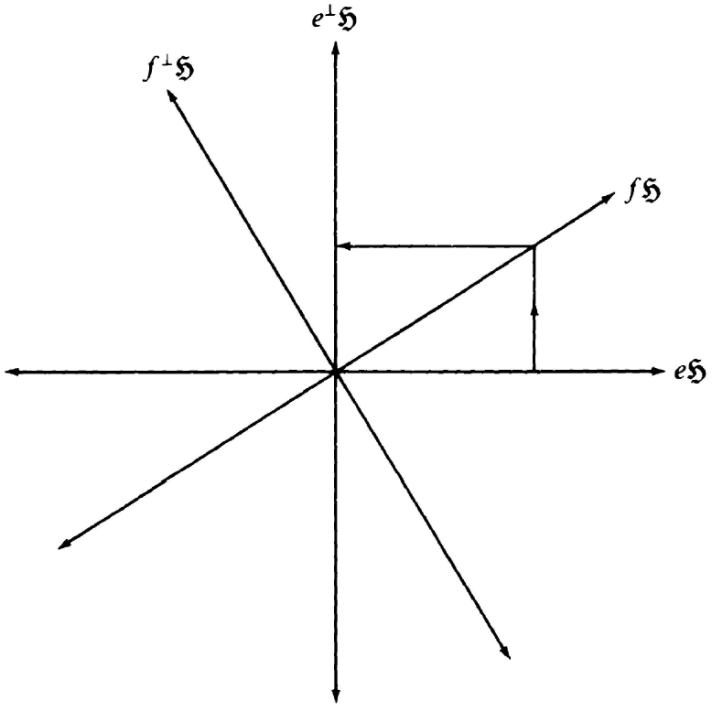
Puisque la position relative de e_1 et f (resp. e et f_1) est si simple que les décompositions $e_1 = e_1 f + (e_1 - e_1 f)$ et $f = e_1 f + (f - e_1 f)$ fournissent une description complète de la paire e_1 et f, l'analyse de e_0 et f_0 suffit pour comprendre la paire e et f. Par conséquent, en remplaçant e et f par e_0 et f_0, et en oubliant $(e \vee f)^\perp$, on arrive à :

$$(*) \qquad \begin{cases} e \wedge f = e^\perp \wedge f = e \wedge f^\perp = 0 \ ; \\ e \vee f = 1, \qquad \text{par conséquent} \qquad e^\perp \wedge f^\perp = 0. \end{cases}$$

On a alors

$$1 = e \vee f = e^\perp \vee f = e \vee f^\perp = e^\perp \vee f^\perp.$$

La situation de e et f peut être illustrée par la figure suivante :



On a alors, dans l'algèbre de von Neumann $\mathscr{M}$ engendrée par e et f,

$$\begin{aligned} e &= e - e \wedge f^{\perp} \sim e \vee f^{\perp} - f^{\perp} = f = f - e \wedge f \sim e \vee f - e \\ &= e^{\perp} = e^{\perp} - e^{\perp} \wedge f \sim e^{\perp} \vee f - f = f^{\perp}. \end{aligned}$$

Par conséquent, $e, e^{\perp}, f$, et $f^{\perp}$ sont toutes équivalentes dans $\mathscr{M}$. Donc il existe une isométrie partielle $u \in \mathscr{M}$ avec $u^*u = e$ et $uu^* = e^{\perp}$. Mais, on veut avoir une isométrie partielle spécifique qui soit directement reliée à cette situation. À partir de la relation spéciale (*) entre e et f, il s'ensuit que $e^{\perp}fe$ envoie $e\mathfrak{H}$ injectivement sur un sous-espace dense de $e^{\perp}\mathfrak{H}$. Soit $a = e^{\perp}fe$ et $a = uh$ la décomposition polaire. Il découle alors de ce qui précède que $u^*u = e$ et $uu^* = e^{\perp}$. On utilise alors cet u pour fabriquer une matrice unitaire $\{e_{11}, e_{12}, e_{21}, e_{22}\}$. Posons

$$e_{11} = e, \qquad e_{21} = u, \qquad e_{12} = u^*, \qquad e_{22} = e^{\perp}.$$

Avec cette matrice unitaire, on a une représentation par une matrice 2×2 de $\mathscr{M}$ sur $\mathscr{M}_e$. En d'autres termes, tout élément de $\mathscr{M}$ est représenté par une matrice 2×2 avec ses entrées prises dans $\mathscr{M}_e$, et $\{e_{ij}\}$ est donné par les égalités suivantes :

$$e = e_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \; ; \qquad e_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \; ;$$

$$e_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \qquad e_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = e^{\perp}.$$

Soit

$$f = \begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix}$$

la matrice de f. Puisque $a = e^{\perp}ae$, on a $ehe = h$; ainsi, on obtient

$$\begin{bmatrix} 0 & 0 \\ f_{21} & 0 \end{bmatrix} = e^{\perp}fe = uh = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} h & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ h & 0 \end{bmatrix},$$

où

$$h \qquad \text{et} \qquad \begin{bmatrix} h & 0 \\ 0 & 0 \end{bmatrix},$$

sont identifiés. Ainsi on obtient $f_{21} = h$; du fait du caractère auto-adjoint de f, $h = f_{12}$. Par conséquent, on obtient

$$f = \begin{bmatrix} f_{11} & h \\ h & f_{22} \end{bmatrix}$$

À partir de l'égalité $f = f^2$, on obtient

$$\begin{cases} f_{11}^2 + h^2 = f_{11}, & f_{11}h + hf_{22} = h \\ hf_{11} + f_{22}h = h, & h^2 + f_{22}^2 = f_{22} \end{cases}$$

Par conséquent f_{11} et f_{22} commutent tous les deux avec h, et donc, on obtient $h(f_{11} + f_{22} - 1) = 0$. Puisque h est injective dans $e\mathfrak{H}$, on obtient $f_{11} + f_{22} = 1$. Puisque $f_{11} \geq 0$ et $f_{22} \geq 0$, on pose $c = f_{11}^{1/2}$ et $s = f_{22}^{1/2}$. Alors on obtient

$$h = (f_{11} - f_{11}^2)^{1/2} = cs.$$

Ainsi on obtient l'expression suivante :

$$\begin{cases} e = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \ ; \\ \\ f = \begin{bmatrix} c^2 & cs \\ cs & s^2 \end{bmatrix} \ ; \quad 0 \leq c \leq 1 \ ; \quad 0 \leq s \leq 1 \ ; \quad c^2 + s^2 = 1. \end{cases}$$

Dans le cas où $\dim \mathfrak{H} = 2$, les variables c et s ci-dessus sont les cosinus et sinus de l'angle entre $e\mathfrak{H}$ et $f\mathfrak{H}$. Par conséquent c et s sont des généralisations des cosinus et sinus de l'angle entre $e\mathfrak{H}$ et $f\mathfrak{H}$. On observe également que

$$|e - f| = \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}, \qquad |e - f^\perp| = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}.$$

Maintenant, résumons les arguments ci-dessus :

Théorème 1.41. *Si e et f sont deux projections sur un espace de Hilbert $\mathfrak{H}$, et si $\mathscr{M}$ est l'algèbre de von Neumann engendrée par e et f, alors*

(i) $\mathscr{M}$ est de type I,

(ii) il existe une projection centrale unique $z \in \mathscr{M}$ telle que $\mathscr{M}z$ est de type I_2, et $\mathscr{M}(1-z)$ est abélienne et $\dim \mathscr{M}(1-z) \leq 4$.

Définition 1.42. Pour deux projections e et f, on écrit $s(e,f) = |e - f|$ et $c(e,f) = |e - f^\perp|$, et on les appelle le *sinus* et le *cosinus* de e et f, respectivement.

Sur une surface de révolution du quatrième degré dont les lignes géodésiques sont algébriques

par M. Jules Tannery

Dans la Note XV du *Traité de Mécanique* de Despeyrous, M. Darboux a donné une méthode pour obtenir les surfaces de révolution dont les lignes géodésiques sont fermées. En appliquant cette méthode, j'ai rencontré la surface dont l'équation est

$$16a^2(x^2+y^2)-z^2(2a^2-z^2);$$

les lignes géodésiques de cette surface sont, non seulement fermées, mais encore *algébriques*.

Les calculs qui permettent de vérifier ce fait sont d'une nature trop élémentaire pour qu'il vaille la peine de les développer ici ; je me contenterai d'indiquer les résultats.

La surface présente un point conique à l'origine et se compose de deux parties symétriques par rapport au plan des $x,\ y$; il suffira de considérer l'une d'elles, celle du bas, par exemple, qui a la forme d'une poire allongée dont la pointe serait tournée vers le haut. Le plan du parallèle maximum a pour équation $z=-a$. Si, en conservant l'axe des z, on prend pour plan des $x,\ y$ ce plan du parallèle maximum, on reconnaît que les différents points de la surface s'obtiennent en faisant varier u de $-\frac{\pi}{2}$ à $+\frac{\pi}{2}$ et θ de 0 à 2π dans les formules

$$\begin{aligned} x &= \frac{a}{i}\cos u\cos\theta,\\ y &= \frac{a}{i}\cos u\sin\theta,\\ z &= a\left(1-\cos\frac{u}{2}+\sin\frac{u}{2}\right); \end{aligned}$$

l'élément linéaire de la surface est alors

$$ds^2=\frac{a^2}{16}[(a+\sin u)^2\ du^2+\cos^2 u\ d\theta^2]$$

et l'équation différentielle des lignes géodésiques est

$$\frac{d\theta}{du} = \frac{\cos\alpha}{\cos u}\frac{\alpha+\sin u}{\sqrt{\sin^2\alpha-\sin^2 u}},$$

en désignant par α l'angle sous lequel la ligne géodésique coupe le parallèle maximum.

L'intégration se fait sans peine au moyen de la substitution

$$\sin u=\sin\alpha\sin\varphi$$

et la même substitution permet de rectifier la courbe.

On parvient ainsi aux équations suivantes dont l'une ou l'autre peut définir la ligne géodésique qui passe par le point où la partie positive du nouvel axe des x rencontre la surface : la constante d'intégration a, en effet, été déterminée de façon que θ et u puissent s'annuler en même temps

$$\sin(\theta-\alpha)=\frac{\sqrt{\sin^2\alpha-\sin^2 u}}{\sin^2\alpha}\ \frac{2\sin u-\sin^2\alpha(1+\sin u)}{\cos u(1-\sin u)},$$

$$\cos(\theta-\alpha)=\frac{\cos\alpha}{\sin^2\alpha}\ \frac{\sin^2\alpha(1+\sin u)-\alpha\sin^2 u}{\cos u(1-\sin u)}.$$

Retranscription de l'article du Bulletin des Sciences Mathématiques, Paris, 1892, p. 190-192

Supposons que l'on parte de la valeur $u = 0$, que α soit compris entre 0 et $\frac{\pi}{2}$, et que le radical soit d'abord positif ; quand u croît de 0 à α, θ croît de 0 à $\pi + \alpha$, z augmente continuellement et l'on obtient une première branche de courbe C_1 qui, en contournant la surface, s'élève au-dessus du parallèle maximum ; lorsque u décroît de α à 0, on doit changer le signe du radical, pour que θ continue de croître ; θ croît alors de $\pi + \alpha$ à $2\pi + 2\alpha$; la portion de courbe C_2 que l'on obtient ainsi est symétrique de C_1 par rapport au plan méridien de longitude $\pi + \alpha$; C_1 et C_2 se croisent en un point pour lequel on a

$$\theta = \alpha \qquad\qquad \sin u = \frac{\sin^2 \alpha}{2 - \sin^2 \alpha}.$$

Lorsque u décroît de 0 à $-\alpha$, θ croît de $2\pi + 2\alpha$ à $3\pi + \alpha$; on obtient ainsi une portion de courbe C_3 qui descend au-dessous du plan des x, y jusqu'à ce que l'on soit dans le plan de symétrie : le point le plus bas de C_3 est sur la même parallèle à l'axe des z que le point le plus haut où se raccordent C_1 et C_2 : enfin, quand u croît de $-\alpha$ à 0, il faut encore changer le signe du radical ; θ croît de $3\pi + \alpha$ à 4π ; et l'on obtient une portion de courbe symétrique de C_3 ; la courbe totale est fermée. Elle présente la forme d'un 8 gauche : on peut se figurer le point double du 8 sur la partie antérieure de la surface, chacune des boucles passant derrière la surface, l'une en haut, l'autre en bas. Il est très aisé d'imaginer un fil fermé affectant cette forme et tendu sur la surface ; mais il y a plus : on vérifie sans peine que la longueur totale de la courbe est indpendante de α et qu'elle est, par conséquent, égale à deux fois la circonférence du parallèle maximum, ou encore à la longueur de la courbe méridienne : parallèle et méridienne sont en effet des courbes géodésiques limites, qui correspondent aux hypothèses $\alpha = 0; \alpha = \frac{\pi}{2}$. En sorte que le *même* fil, en se déformant de manière à rester tendu sur la surface, permettra de représenter toutes les lignes géodésiques. La construction d'un modèle qui permettrait de constater expérimentalement ces résultats n'offrirait évidemment aucune difficulté.

Enfin, si l'on projette la ligne géodésique sur son plan de symétrie, on trouve, en conservant le même axe des z et en prenant pour axe des x l'intersection du plan de symétrie avec le plan du parallèle maximum, l'équation

$$x = \frac{1}{4} \frac{\cos \alpha}{\sin^2 \alpha} \frac{[a^2 + z(\alpha a - z)] a^2 \sin^2 \alpha - \alpha (a^2 - z^2)^2}{a(a - z)^2} ;$$

la seule partie de cette courbe qu'il convienne de garder est celle qui est contenue à l'intérieur de la courbe méridienne ; il est à peine utile de dire que les deux courbes sont tangentes au point qui correspond au point double de la ligne géodésique.

Une approche moderne du casse-tête des 15

Aaron F. Archer

1. Introduction. Dans les années 1870, le malicieux inventeur de casse-têtes Sam Loyd fit sensation aux États-Unis, en Grande-Bretagne et en Europe avec son désormais célèbre casse-tête des 15. Dans sa version originale, ce casse-tête se compose de quinze blocs carrés numérotés de 1 à 15, par ailleurs identiques, et d'un plateau carré suffisamment grand pour contenir 16 blocs. Les 15 blocs sont placés dans le plateau comme indiqué sur la figure 1, le coin inférieur droit étant laissé vide. Un mouvement autorisé consiste à glisser un bloc adjacent à l'espace vide dans cet espace. Ainsi, à partir de la position initiale, les blocs 12 ou 15 peuvent être glissés dans l'espace vide. Le but du jeu est d'effectuer une suite de mouvements autorisés pour échanger les positions des blocs 14 et 15 tout en remettant tous les autres blocs à leur position initiale.

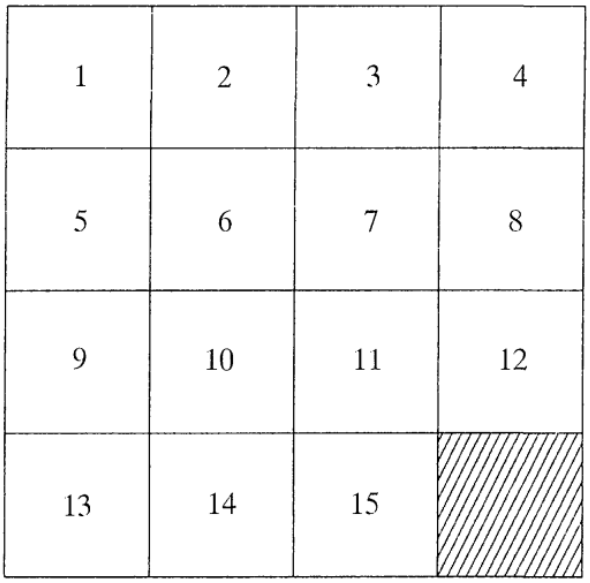


FIGURE 1. Position de départ du taquin. La case grisée est laissée vide.

Loyd écrit comment il a "rendu le monde entier fou" et que "le prix de 1000 $ offert pour la première solution correcte au problème n'a jamais été réclamé, bien que des milliers de personnes prétendent avoir accompli l'exploit". Il poursuit :

> Les gens sont devenus fascinés par l'énigme et l'on raconte des histoires rocambolesques de commerçants qui ont négligé d'ouvrir leurs magasins ; d'un ecclésiastique distingué qui est resté sous un lampadaire toute une nuit d'hiver à essayer de se rappeler comment il avait accompli l'exploit… On dit que des pilotes ont fait s'écraser leurs avions et que des conducteurs de train ont fait passer leurs trains à toute vitesse devant les gares. Un célèbre rédacteur en chef de Baltimore raconte comment, parti déjeuner, il a été retrouvé par son équipe frénétique bien après minuit en train de faire rouler des petits morceaux de tarte sur une assiette ! [9]

Référence : Archer, A. F. (1999). A Modern Treatment of the 15 Puzzle. The American Mathematical Monthly, 106(9), 793–799.
Traduction : Denise Vella-Chemla, novembre 2025.

La raison de cette hystérie est, bien sûr, que le casse-tête de Loyd est insoluble. Chaque déplacement entraîne une transposition des 16 blocs (la case vide étant considérée comme contenant un bloc blanc), et pour que ce bloc blanc se retrouve dans le coin inférieur droit, il faut un nombre pair de déplacements, la permutation résultante est donc paire. Or, la position finale souhaitée est une permutation impaire de la configuration initiale, et est par conséquent impossible à obtenir. On peut supposer que Sam Loyd le savait, et l'on ne peut qu'imaginer le plaisir qu'il a pu prendre à rendre le public américain fou.

Ce casse-tête a inspiré de nombreux articles et références dans la littérature mathématique. Parmi ceux-ci, on peut citer deux articles publiés dans l'*American Journal of Mathematics* en 1879 par W. W. Johnson [7] et W. E. Story [13]. L'article de Johnson explique pourquoi les permutations impaires du puzzle sont impossibles à obtenir, tandis que celui de Story prouve que toutes les permutations paires sont possibles. Les rédacteurs étaient apparemment si réticents et sur la défensive à l'idée de publier des articles sur ce que certains pourraient qualifier de sujet futile qu'ils ont ajouté la justification suivante à la fin de l'article de Story :

> Le casse-tête des "15" a occupé une place prépondérante dans le débat public américain ces dernières semaines, et l'on peut affirmer sans risque d'erreur qu'il a captivé l'attention de neuf personnes sur dix, tous sexes et toutes conditions confondus. Pourtant, cela n'aurait pas incité les rédacteurs de l'*American Journal of Mathematics* à publier un article sur ce sujet si le principe de ce jeu ne reposait pas sur ce que tous les mathématiciens contemporains considèrent comme la conception la plus subtile et caractéristique de l'algèbre moderne : la loi de dichotomie applicable à la séparation des termes de tout système complet de permutations en deux groupes naturels et indéfectibles, une loi du monde intérieur de la pensée, qui préfigure en quelque sorte la relation polaire entre les vis à gauche et à droite, ou encore entre les objets dans l'espace et leurs reflets dans un miroir. En conséquence, les rédacteurs ont estimé qu'en présentant cette loi polaire a priori sous une forme concrète, par le biais d'un jeu qui a tellement marqué la pensée nationale qu'on pourrait presque le qualifier d'institution nationale, ils ne desserviraient pas leur science, mais qu'ils en promouvraient au contraire les intérêts. Quiconque s'y est adonné a sans doute reçu sa première leçon de théorie des déterminants. [13, p. 404]

Le casse-tête est un sujet populaire dans les ouvrages de mathématiques récréatives ou de pot-pourri mathématique, tels que [1], [2], [4], [5], [9] et [12], qui l'utilisent pour la plupart comme exemple afin d'illustrer les conséquences des permutations paires et impaires, à l'instar de [14]. Diverses sources ont proposé des variantes du casse-tête à 15 chiffres, notamment [3], [4], [6], [8], [10] et [15]. Aujourd'hui, ce casse-tête apparaît sur certains écrans de veille d'ordinateur, et une version est distribuée avec chaque ordinateur Macintosh.

La plupart des références au taquin expliquent l'impossibilité d'obtenir des permutations impaires et beaucoup énoncent le résultat de Story selon lequel toute permutation paire est possible, mais l'auteur de ces lignes n'a trouvé que trois démonstrations. R. M. Wilson [15] a publié un résultat plus général en 1974, que nous abordons à la fin de cet article. L'ouvrage de Ball et Coxeter [1] renvoie à [10] pour une démonstration, mais l'article ne tient pas sa promesse. La terminologie complexe de l'article de Story [13] le rend difficile à appréhender, et il ne tire évidemment pas parti des notations modernes développées depuis. Spitznagel [11] a publié une démonstration en 1967, mais a écrit plus tard : "Au fil des années, de nombreuses explications inutilement compliquées

du taquin ont été publiées. J'avoue avoir moi-même publié l'une de ces explications excessivement compliquées" [12]. En effet, Herstein et Kaplansky [5] écrivent qu"'il ne semble pas exister de démonstration vraiment simple". Cet article vise à combler cette lacune.

2. Solution. Il convient de noter que la démonstration présentée ici a été élaborée indépendamment des démonstrations précédentes, mais partage par ailleurs certaines idées avec la démonstration de Story [13].

Nous appelons chacun des 15 blocs des pièces, et les 16 cases différentes du plateau, des cellules. Pour des raisons qui deviendront évidentes, nous numérotons les cellules selon le motif en serpentin illustré à la figure 2. Nous pouvons considérer la cellule vide comme étant occupée par un bloc blanc. Chaque coup légal consiste alors à "déplacer le bloc blanc", c'est-à-dire à échanger le bloc blanc avec l'un de ses voisins horizontaux ou verticaux. Un placement est une bijection de l'ensemble des blocs (y compris le bloc blanc) vers l'ensemble des cellules ; en d'autres termes, une image instantanée du plateau entre deux coups. Étant donné un placement initial, nous cherchons à déterminer quels autres placements sont possibles par une suite de coups légaux.

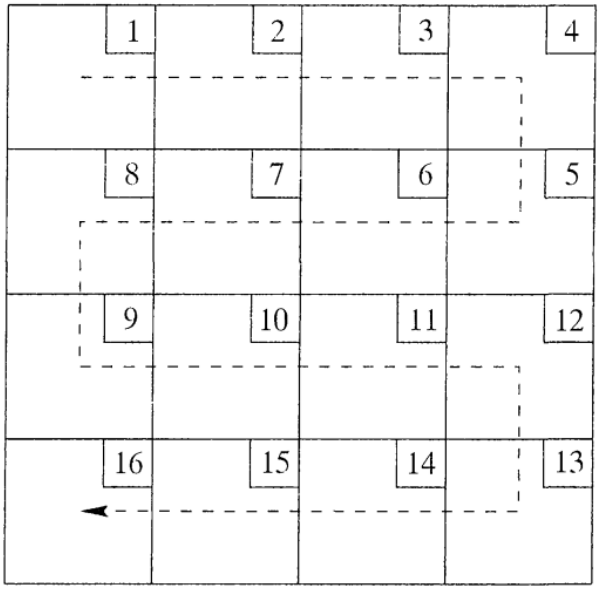


FIGURE 2. La ligne pointillée et les chiffres dans le coin de chaque cellule indiquent un ordre particulier des cellules que nous utilisons pour définir les classes d'équivalence des placements.

Remarquez qu'en déplaçant le bloc vide le long du chemin sinueux de la figure 2, on peut le placer dans n'importe quelle cellule sans modifier l'ordre des autres blocs sur ce chemin. Ceci nous amène à définir une relation d'équivalence sur l'ensemble des placements : deux placements sont équivalents si l'on peut obtenir l'un à partir de l'autre en déplaçant le bloc vide le long du chemin sinueux. Chaque classe d'équivalence est appelée une configuration et contient 16 placements, un pour chaque cellule que le bloc vide peut occuper. Si le bloc i occupe la cellule j et que le bloc vide occupe une cellule de numéro supérieur, alors on dit que le bloc i est dans l'emplacement j ; sinon, il est dans l'emplacement $(j-1)$. Voir la figure 3 pour un exemple. Tous les placements d'une configuration donnée ont les 15 blocs dans les mêmes emplacements ; on peut donc noter une

configuration par $[a_1, \ldots, a_{15}]$, où a_i est l'emplacement occupé par le bloc i dans la configuration.

Chaque déplacement du bloc vide entraîne une permutation des emplacements occupés par les blocs. Par exemple, déplacer le bloc vide de la case 10 à la case 15 provoque la permutation (10, 11, 12, 13, 14) car le bloc initialement en case 15 (emplacement 14) est déplacé en case 10 (qui devient l'emplacement 10) et les blocs des cases 11 à 14 sont décalés d'un emplacement vers le haut. Une configuration $[a_1, \ldots, a_{15}]$ soumise à la permutation est transformée en la configuration $[a_1, \ldots, a_{15}]\sigma = [a_1\sigma, \ldots, a_{15}\sigma]$; comme nos permutations agissent à droite, nous les multiplions de gauche à droite. Voir la figure 3 pour un exemple.

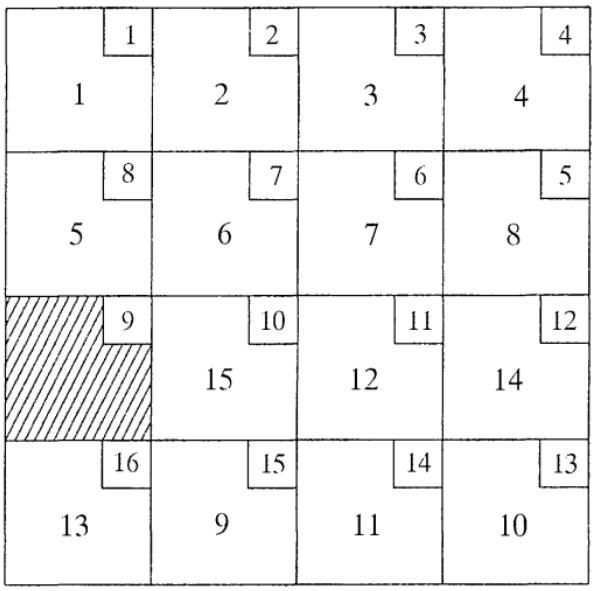


FIGURE 3. La disposition illustrée ici correspond à la configuration $C = [1, 2, 3, 4, 8, 7, 6, 5, 14, 12, 13, 10, 15, 11, 9]$. Puisque la disposition initiale de la figure 1 correspond à $I = [1, 2, 3, 4, 8, 7, 6, 5, 9, 10, 11, 12, 15, 14, 13]$, la permutation de la configuration initiale $\sigma = (9, 14, 11, 13)(10, 12)$ donne C. Cette permutation étant paire, d'après le théorème 3, C peut être obtenue à partir de I.

Soit $\sigma_{i,j}$ la permutation obtenue en déplaçant le marqueur vide de la case i à la case j. On a clairement $\sigma_{i,i+1}$ est l'élément neutre et $\sigma_{j,i} = \sigma_{i,j}^{-1}$. Il nous reste donc 9 permutations à déterminer. Celles-ci sont répertoriées dans le tableau 1. L'élément clé est que l'on peut déplacer le marqueur vide le long du chemin sinueux de la figure 2 vers n'importe quelle case sans modifier la configuration. Par conséquent, les neuf premières permutations listées dans le tableau 1 et leurs inverses peuvent être appliquées dans n'importe quel ordre, de sorte que le problème se ramène à identifier le sous-groupe de S_{15} (le groupe symétrique sur les 15 cases) engendré par ces permutations. Nous démontrons que ces permutations engendrent A_{15} (toutes les permutations paires).

TABLEAU 1. Récapitulatif de toutes les permutations possibles des emplacements obtenues en déplaçant le bloc vide. Le déplacement du bloc vide de la case i à la case j induit la permutation $\sigma_{i,j}$.

$\sigma_{1,8}$	$= (1,2,3,4,5,6,7)$
$\sigma_{2,7}$	$= (2,3,4,5,6)$
$\sigma_{3,6}$	$= (3,4,5)$
$\sigma_{5,12}$	$= (5,6,7,8,9,10,11)$
$\sigma_{6,11}$	$= (6,7,8,9,10)$
$\sigma_{7,10}$	$= (7,8,9)$
$\sigma_{9,16}$	$= (9,10,11,12,13,14,15)$
$\sigma_{10,15}$	$= (10,11,12,13,14)$
$\sigma_{11,14}$	$= (11,12,13)$
$\sigma_{n,n+1}$	$= id,$ $\quad n = 1,2,\ldots,15$
$\sigma_{i,j}$	$= \sigma_{j,i}^{-1}$ $\quad$ pour tout $i > j$ adequat

Lemme 1. *Pour $n \geq 3$, les 3-cycles engendrent A_n.*

Démonstration : Par définition, tout élément de A_n peut s'écrire comme le produit d'un nombre pair de transpositions. Si a, b, c et d sont distincts, alors $(a,b)(c,d) = (a,b,c)(a,d,c)$, $(a,b)(b,c) = (a,c,b)$ et $(a,b)(a,b) = id$. □

Pour $n \geq 5$, le lemme 1 découle également directement du fait que A_n est simple, puisque l'ensemble des 3-cycles est stable par conjugaison. Appelons un 3-cycle consécutif s'il est de la forme $(k, k+1, k+2)$.

Lemme 2. *Pour $n \geq 3$, les 3-cycles consécutifs $\{(1,2,3),(2,3,4),\ldots,(n-2,n-1,n)\}$ engendrent A_n.*

Démonstration : Puisque les 3-cycles engendrent A_n, il suffit de montrer que les 3-cycles consécutifs engendrent tous les 3-cycles. Ceci est trivial pour $n = 3$. Pour $n \geq 4$, on montre par récurrence qu'on peut engendrer tous les 3-cycles ne contenant pas à la fois 1 et n. Pour engendrer $(1,x,n)$, posons $y \in \{1,\ldots,n\}\backslash\{1,x,n\}$. Alors $(1,x,n) = (y,x,n)(1,x,y)$. Bien sûr, $(1,n,x) = (1,x,n)^2$. □

Théorème 3. *Les cycles listés dans le Tableau 1 engendrent A_{15}.*

Démonstration : Puisque tous les cycles sont impairs, ce sont des permutations paires, donc ils engendrent un sous-groupe de A_{15}. Notons que pour toute permutation σ, on a

$$\sigma^{-1}(a_1,\ldots,a_k)\sigma = (a_1\sigma,\ldots,a_k\sigma).$$

Ainsi,

$$\begin{array}{l}(1,2,\ldots,7)^{-n}(3,4,5)(1,2,\ldots,7)^n \quad \text{donne} \quad (1,2,3),\ldots,(5,6,7)\ ; \\ (5,6,\ldots,11)^{-n}(7,8,9)(5,6,\ldots,11)^n \quad \text{donne} \quad (5,6,7),\ldots,(9,10,11) \quad \text{et} \\ (9,10,\ldots,15)^{-n}(11,12,13)(9,10,\ldots,15)^n \quad \text{donne} \quad (9,10,11),\ldots,(13,14,15)\end{array}$$

lorsque n prend les valeurs $-2, -1, 0, 1$ et 2, cela constitue tous les 3-cycles consécutifs de S_{15}, donc d'après le lemme 2, cela engendre A_{15}.

Ainsi, étant donné deux placements quelconques Pl_1 et Pl_2 appartenant respectivement aux configurations Cf_1 et Cf_2, Pl_2 est obtenu à partir de Pl_1 si et seulement si Cf_2 est une permutation paire de Cf_1. En termes de placement, si Pl_1 et Pl_2 ont la case vide dans la même cellule, alors Pl_2 est obtenu à partir de Pl_1 si et seulement si Pl_2 est une permutation paire des 15 blocs numérotés de Pl_1. Soit n le nombre de déplacements entre la case vide de Pl_1 et la case vide de Pl_2. Chaque déplacement de la case vide entraînant une transposition de deux blocs, alors pour n impair (respectivement pair), Pl_2 est obtenu à partir de Pl_1 si et seulement si Pl_2 est une permutation impaire (respectivement paire) des 16 blocs de Pl_1.

3. Généralisations. Ce qui suit constitue, en un sens, la généralisation la plus large du taquin. Étant donné un graphe connexe quelconque à n sommets, nous pouvons étiqueter ces sommets avec n étiquettes, dont l'une est appelée étiquette vide. Chaque mouvement consiste à échanger l'étiquette vide avec l'étiquette d'un sommet adjacent. Nous cherchons alors à déterminer, parmi les $n!$ étiquetages possibles, lesquels peuvent être obtenus à partir d'un étiquetage initial donné par une suite de mouvements. Plus précisément, nous cherchons à déterminer quelles permutations des $(n-1)$ étiquettes ordinaires (un sous-groupe de S_{n-1}) peuvent être obtenues par une suite de mouvements qui replace l'étiquette vide sur son sommet d'origine v (puisque les sous-groupes obtenus pour différents choix de v sont isomorphes). Le jeu du taquin (ou casse-tête des 15) en est un cas particulier, correspondant au graphe $P_4 \times P_4$ (le produit cartésien du chemin à quatre sommets avec lui-même) représenté sur la figure 4. Les sommets correspondent aux cellules, les étiquettes (non représentées) correspondent aux blocs, et les arêtes indiquent quelles cellules sont adjacentes.

Le principe de la méthode présentée dans la section 2 repose sur l'induction de classes d'équivalence et la définition des emplacements par la position de l'élément vide le long d'un chemin hamiltonien (un chemin qui visite chaque sommet du graphe exactement une fois). Cette méthode est applicable à tout graphe contenant un chemin hamiltonien, quel que soit le chemin utilisé. Ainsi, pour le taquin, on aurait pu utiliser une spirale au lieu du motif en serpentin de la figure 2. Le graphe de Petersen en est un autre exemple. En numérotant les sommets comme sur la figure 5, on constate que le groupe recherché est engendré par $\sigma_{1,9}, \sigma_{1,5}, \sigma_{2,7}, \sigma_{3,10}, \sigma_{4,8}$ et $\sigma_{6,10}$, où $\sigma_{i,j} = (i, i+1, \ldots, j-1)$ représente la permutation des emplacements obtenue en déplaçant l'étiquette vide du sommet i au sommet j. Des calculs montrent que le groupe engendré correspond à l'ensemble S_9 ; [15] explique pourquoi ce résultat n'est pas fortuit.

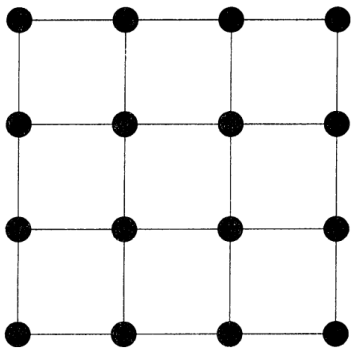


FIGURE 4. Le graphe $P_4 \times P_4$.

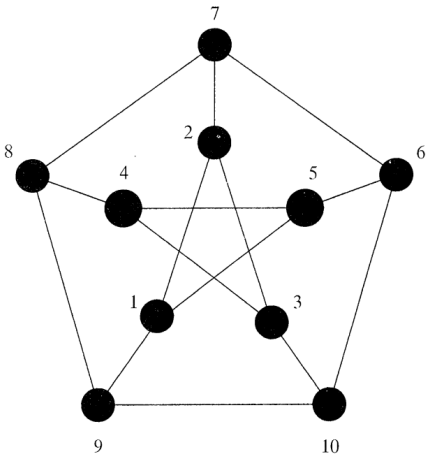


FIGURE 5. Dans le célèbre graphe de Petersen, chaque étiquetage est possible à partir de tous les autres par une suite de mouvements autorisés. Les sommets sont numérotés pour indiquer un chemin hamiltonien.

Nous abordons maintenant le cas général, où le graphe peut contenir ou non un chemin hamiltonien. Si le graphe contient un sommet de coupure v, alors aucune des étiquettes, à l'exception de l'étiquette vide, ne peut être déplacée à travers v, ce qui décompose le problème en deux parties. Il suffit donc de considérer les graphes ne contenant aucun sommet de coupure.

Dans [15], R. M. Wilson résout complètement ce problème. Son résultat remarquable est que, hormis les cycles C_n et le graphe θ_0 représenté sur la figure 6, le groupe contient A_{n-1}. Il est clair que le groupe contient une permutation impaire si et seulement si le graphe contient un cycle impair, c'est-à-dire si le graphe n'est pas biparti. Ainsi, pour les graphes bipartis, le groupe est exactement A_{n-1}, et sinon, il est entièrement S_{n-1}. Par conséquent, mis à part ces deux cas exceptionnels, on peut obtenir soit exactement la moitié, soit la totalité des $n!$ étiquetages, selon que le graphe est biparti ou non. Pour θ_0, le groupe recherché est $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ agissant sur la droite projective au-dessus de $\mathbb{Z}/5\mathbb{Z}$ (un groupe d'ordre 120 agissant 3-transitivement sur un ensemble de six éléments), ce qui donne six étiquetages non équivalents. Pour C_n, le groupe est $\langle(1, 2, \ldots, n-1)\rangle$, ce qui donne $(n-2)!$ étiquetages non équivalents. L'existence d'une caractérisation complète aussi simple est surprenante. Cependant, la démonstration de Wilson, bien qu'élégante, requiert des mathématiques considérablement plus sophistiquées que la démonstration simple et élémentaire présentée ici pour le cas particulier du taquin.

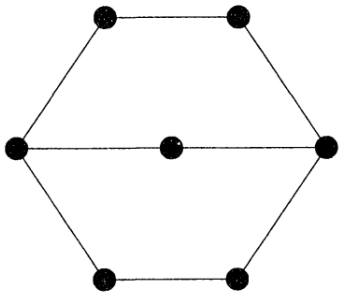


FIGURE 6. Le graphe 60.

Remerciements. L'auteur remercie les professeurs Alan J. Goldman et Arthur T. Benjamin de lui avoir signalé ce problème, et ce dernier pour ses nombreuses suggestions pertinentes. Ce travail a bénéficié du soutien de la Fondation Fannie et John Hertz.

Références

1. W. W. R. Ball, H. S. M. Coxeter, *Mathematical Recreations and Essays*, 12th ed., U. of Toronto Press, Toronto & Buffalo, 1974, pp. 313-316.
2. J. D. Beasley, *The Mathematics of Games*, Oxford U. Press, Oxford & New York, 1989, pp. 80-81.
3. A. L. Davies, Rotating the fifteen puzzle, *Math. Gazette* 54 (1970) 237-240.
4. M. Gardner, *Martin Gardner's Sixth Book of Mathematical Diversions from Scientific American*, U. of Chicago Press, Chicago, 1971, pp. 64-70.
5. 1. N. Herstein, I. Kaplansky, *Matters Mathematical*, Chelsea, New York, 1978, pp. 114-115.
6. S. Hurd, D. Trautman, The knight's tour on the 15-puzzle, *Math. Mag.* 66 (1993) 159-166.
7. W. W. Johnson, Note on the "15" puzzle, *Amer. J. Math.* 2 (1879) 397-399.
8. H. Liebeck, Some generalizations of the 14-15 puzzle, *Math. Mag.* 44 (1971) 185-189.
9. S. Loyd, *Mathematical Puzzles of Sam Loyd*, sélectionné et édité par Martin Gardner, Dover, New York, 1959, pp. 19-20.
10. H. V. Mallison, An array of squares, *Math. Gazette* 24 (1940) 119-121.
11. E. L. Spitznagel, Jr., A new look at the fifteen puzzle, *Math. Mag.* 40 (1967) 171-174.
12. E. L. Spitznagel, Jr., *Selected Topics in Mathematics*, Holt, Rinehart & Winston, New York, 1971, pp. 143-148.
13. W. E. Story, Note on the "15" puzzle, *Amer. J. Math.* 2 (1879) 399-404.
14. F. J. W. Whipple, The sign of a term in the expansion of a determinant, *Math. Gazette* 13 (1926) 126.
15. R. M. Wilson, Graph puzzles, homotopy, and the alternating group, *J. Combin. Theory* (Series B) 16 (1974) 86-96.

Aaron Archer a obtenu sa licence en mathématiques au Harvey Mudd College en 1998, où ses recherches en théorie des graphes chromatiques lui ont valu une mention honorable pour le prix Morgan (AMS/MAA/SIAM). Ancien participant aux programmes d'été de mathématiques du Hampshire College et aux semestres de mathématiques de Budapest, son séjour en Hongrie l'a inspiré à rédiger un guide de restaurants en ligne pour Budapest. Aaron est actuellement boursier Hertz et prépare un doctorat en recherche opérationnelle à l'Université Cornell. Ses recherches portent sur l'optimisation combinatoire et les algorithmes d'approximation.

Département de Recherche opérationnelle, Université de Cornell, Ithaca, NY 14853
Harvey Mudd College, Claremont, CA 91711

Un extrait de *Mathematics and the Imagination*, de Edward Kasner et James Newman, illustrations Rufus Isaac, Dover Publications, Mineola, New York, 1940

Aucune discussion sur les casse-têtes, même brève, ne saurait omettre le plus célèbre des nombreux jeux inventés par Sam Lloyd. “Puzzle 15”, “Puzzle du Patron”, “Jeu du Taquin” ne sont que quelques-uns de ses noms. Pendant plusieurs années après son apparition en 1878, ce casse-tête connut une popularité, notamment en Europe, supérieure à celle aujourd'hui du bridge swing et du bridge contract réunis. En Allemagne, on y jouait dans les rues, dans les usines, dans les palais royaux et au Reichstag. Les employeurs étaient contraints d'afficher des avis interdisant à leurs employés de jouer au “Puzzle 15” pendant les heures de travail, sous peine de licenciement. Les électeurs, ne bénéficiant pas de tels privilèges, devaient assister, impuissants, à la pratique du “Puzzle du Patron” par leurs représentants dûment élus au Reichstag, tandis que Bismarck jouait lui-aussi au puzzle. En France, le “Jeu du Taquin” se pratiquait sur les boulevards parisiens et dans chaque village, des Pyrénées à la Normandie. Le “Jeu du Taquin” était un fléau pour l'humanité, selon un journaliste français de l'époque, pire que le tabac et l'alcool, “responsable d'innombrables maux de tête, névralgies et névroses”.

Pendant un temps, l'Europe était folle de ce “casse-tête des 15”. Des tournois étaient organisés et des prix faramineux offerts pour la résolution de problèmes en apparence simples. Mais le plus étrange, c'est que personne ne remportait jamais ces prix, et que ces problèmes apparemment simples restaient irrésolus.

Le “casse-tête des 15” (figure ci-dessous) se compose d'une boîte carrée peu profonde en bois ou en métal contenant 15 petits blocs carrés numérotés de 1 à 15. La boîte peut en réalité contenir 16 blocs, ce qui permet de déplacer les 15 blocs et d'intervertir leurs positions. Le nombre de positions possibles est de $16\,! = 20\,922\,789\,888\,000$. Un problème consiste à obtenir une disposition spécifique des blocs à partir d'une position initiale donnée, souvent la position normale illustrée sur la figure 57.

Peu après l'invention du casse-tête, deux mathématiciens américains ont démontré que, quelle que soit la disposition initiale, seule la moitié des positions possibles peut être obtenue. Ainsi, il existe toujours environ 10 000 milliards de positions possibles pour le possesseur d'un “casse-tête des 15”, et 10 000 milliards de positions impossibles à obtenir.

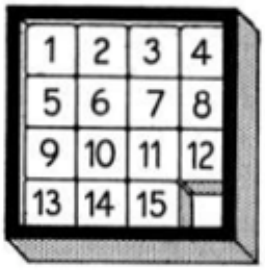


FIG. 57. Le “Puzzle 15” (également “Puzzle du Patron” ou “Jeu du Taquin”) en position normale.

L'existence de positions impossibles explique aisément pourquoi Lloyd et d'autres offraient des prix aussi généreux, puisque les problèmes récompensés impliquaient systématiquement des positions impossibles. Il est navrant d'imaginer les maux de tête, les névralgies et les névroses qui auraient

pu être épargnés, sans parler des retombées économiques pour le Reichstag, si l'*American Journal of Mathematics* avait connu la même diffusion que le casse-tête lui-même. Avec dix mille milliards de solutions possibles, il y aurait eu largement de quoi s'amuser.

Dans la position normale (FIG. 57), l'espace vide se trouve dans le coin inférieur droit. Pour analyser mathématiquement le casse-tête, il est utile de considérer qu'un réarrangement des blocs consiste simplement à déplacer l'espace vide selon un parcours précis, en veillant toujours à ce qu'il arrive dans le coin inférieur droit de la boîte. Pour ce faire, l'espace vide doit traverser autant de cases vers la gauche que vers la droite, et autant de cases vers le haut que vers le bas. Autrement dit, l'espace vide doit traverser un nombre pair de cases. Si, en partant de la position initiale, la position souhaitée peut être atteinte tout en respectant cette condition, alors cette position est possible ; sinon, elle est impossible.

En se basant sur ce principe, la méthode pour déterminer si une position est possible ou impossible est très simple. Dans la position normale, chaque bloc numéroté apparaît dans son ordre numérique correct, c'est-à-dire que, pour chaque rangée de cases, de gauche à droite, aucun nombre ne précède un nombre inférieur. Pour obtenir une position différente de la position normale, l'ordre numérique des blocs doit être modifié. Certains nombres, voire tous, précéderont d'autres nombres inférieurs. Chaque cas où un nombre précède un autre nombre inférieur est appelé une inversion. Par exemple, si le nombre 6 précède les nombres 2, 4 et 5, il s'agit d'une inversion à laquelle on attribue la valeur 3, car 6 précède trois nombres inférieurs. Si la somme des valeurs de toutes les inversions dans une position donnée est paire, la position est possible, c'est-à-dire qu'elle peut être obtenue à partir de la position normale. Si la somme des valeurs des inversions est impaire, la position est impossible et ne peut être obtenue à partir de la configuration normale.

La position illustrée sur la figure 58 peut être obtenue à partir de la position normale puisque la somme des valeurs des inversions est égale à six, un nombre pair.

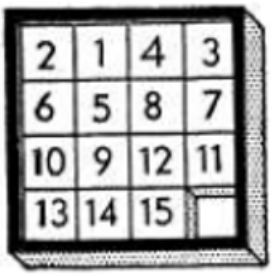


FIG. 58.

Mais la position représentée sur la figure 59 est impossible, puisque, comme on peut facilement le constater, la somme des valeurs des inversions produites est impaire :

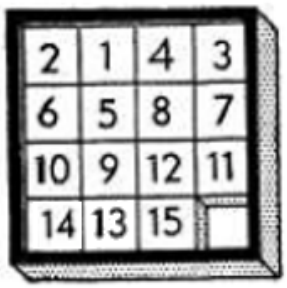


FIG. 59.

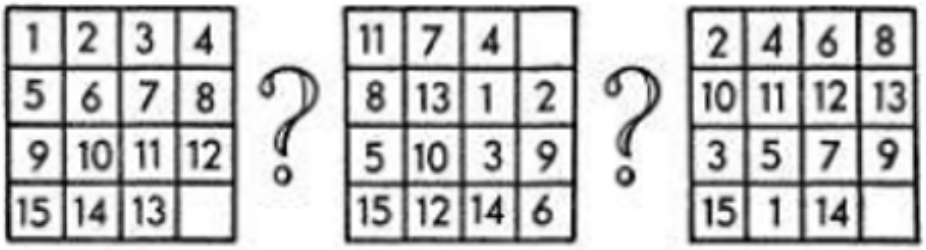


FIG. 60.

Les figures 60 a, b et c illustrent trois autres positions. Sont-elles possibles ou impossibles à obtenir à partir de l'ordre normal ?

L'invariant du pouss-pouss
Traduction d'un extrait de *Mathématiques en instantanés*
Hugo Steinhaus

Il n'existe pas de théorie mathématique du jeu d'échecs, mais il y en a une pour certains jeux plus simples. Par exemple, celui de la figure 1, le jeu du "taquin", qui utilise une boîte, avec 15 pions carrés numérotés, laissant vide l'emplacement d'un pion supplémentaire. Il s'agit de disposer les pions dans la boîte selon un ordre choisi quelconque (fig. 2) puis, par une suite de déplacements convenables, de les remettre dans leur ordre primitif. La théorie est la suivante : désignons par "16" l'emplacement vide ; dès lors, chaque arrangement des pions est une permutation des nombres 1, 2, 3, ..., 15, 16. Or, à partir des nombres 1 . . . 16, écrits dans leur ordre naturel, on peut obtenir n'importe quel ordre choisi d'avance par une série adéquate d'opérations qui consistent à échanger deux nombres voisins. Par exemple, pour obtenir l'arrangement 2, 1, 3, 4, 5, 16, il faut un échange entre 1 et 2. Appelons "coup" un tel échange.

FIG. 1

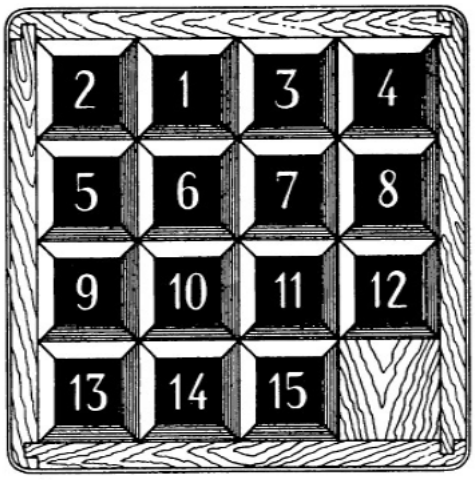


FIG. 2

éditions Flammarion, 1964.

Transcription en LaTeX: Denise Vella-Chemla, mars 2025. [Petit encart de la transcriptrice : J'ai vécu de multiples émois mathématiques, durant mon enfance, de l'étude de ma petite maison aux formes géométriques, à celle du pouss-pouss (taquin) que m'avait offert mon père, ou encore à celle de ma petite étoile de Galilée en plastique noir et blanc.]

Certains arrangements nécessitent un nombre impair de coups, d'autres un nombre pair. Mais, si un arrangement doit être atteint par un nombre impair de coups, il est impossible de l'obtenir aussi par un nombre pair. Imaginons le contraire, c'est-à-dire un arrangement qui s'obtiendrait aussi bien par un nombre pair que par un nombre impair de coups. Partant de l'ordre naturel, si on réalisait le nombre pair de coups, puis le nombre impair, cette fois en sens inverse, on devrait revenir à l'ordre naturel. Ainsi, on pourrait partir de l'ordre naturel et y revenir par un nombre de coups qui, au total, serait impair, chose impossible, car chaque coup est un échange de deux nombres voisins. Considérons d'abord les seuls coups qui échangent 5 et 6. Le premier coup de cette sorte fait passer de 56 à 65, le second de 65 à 56, et ainsi de suite ; lorsqu'en fin de compte, on doit rétablir l'ordre naturel 56, le nombre des coups considérés est pair. Le même raisonnement s'applique aux couples 1-2, 2-3,..., jusqu'à 15-16 : pour chaque couple, il faut un nombre pair de coups. Ainsi, le nombre total de coups permettant de partir de l'ordre naturel et d'y revenir est forcément pair, puisque c'est une somme de nombres pairs.

Nous pouvons ainsi classer tous les arrangements en deux catégories : les arrangements "pairs" et les arrangements "impairs". Considérons la disposition des pions dans la boîte comme un arrangement de nombres, en convenant de les lire ligne par ligne, de haut en bas. Quand nous déplaçons les pions dans la boîte, nous ne pouvons échanger l'emplacement vide "16" qu'avec l'un des pions voisins. Si ce pion est le voisin de droite ou celui de gauche, l'échange est un "coup" au sens déjà défini, car tout se passe comme si l'ensemble des lignes horizontales formait une seule ligne. Par contre, si nous échangeons le pion "16" avec son voisin supérieur ou son voisin inférieur, l'opération équivaut à échanger deux pions qui, dans la ligne globale, sont distants de 4. Un tel échange requiert 7 coups, c'est à dire 7 échanges de pions voisins. Pour résoudre notre problème, nous devons dans tous les cas ramener le pion "16" à la position initiale qu'il occupait dans la boîte : le coin inférieur droit ; on doit donc déplacer ce pion le même nombre de fois vers le haut et vers le bas, le même nombre de fois vers la droite ou vers la gauche. Le nombre de déplacements horizontaux est par conséquent un nombre pair $2h$ et le nombre de déplacements verticaux également un nombre pair, $2v$. L'ensemble du processus est de la sorte équivalent à $2h$ coups plus $2v \times 7$ coups $= 2h + 14v$ coups et ce dernier nombre est pair.

Par conséquent, si un arrangement a été obtenu à partir de l'arrangement fondamental par un nombre impair de "coups", le problème de rétablir l'ordre naturel est insoluble. Par exemple, nous ne pouvons pas, en déplaçant les pions, passer de l'arrangement de la figure 2 à celui de la figure 1, pas plus que nous ne pouvons passer de 1 à 2. Pourquoi ? L'ensemble des arrangements qui peuvent être obtenir par un nombre pair de "coups" définit les problèmes solubles ; le lecteur peut essayer de démontrer ce point.

Logique propre dans l'esprit de George Boole

Zeno Toffano

Résumé : Ce travail présente une approche opérationnelle et géométrique de la logique. Il part de la décomposition élective multilinéaire des fonctions logiques binaires sous la forme originale introduite par George Boole. Une justification sur des bases historiques est présentée, reliant la théorie de Boole et l'utilisation de ses fonctions logiques arithmétiques avec les axiomes de l'algèbre booléenne utilisant des ensembles et la logique quantique. On montre que cette formulation polynomiale algébrique peut être naturellement étendue à des opérateurs dans des espaces vectoriels finis. Les opérateurs logiques apparaîtront comme des opérateurs de projection qui commutent et les valeurs de vérité, qui prennent les valeurs binaires (0, 1), sont les valeurs propres respectives. Dans cette optique, la solution d'une proposition logique résultant de l'opération sur une combinaison d'arguments apparaîtra comme une sélection dont le résultat ne peut être que l'une des valeurs propres. Ainsi la logique propositionnelle peut être formalisée en algèbre linéaire en utilisant des développements électifs qui correspondent ici à des combinaisons d'opérateurs de projection élémentaires tensoriels. La motivation originale et principale de ce travail, ce sont les applications dans le nouveau domaine de l'information quantique ; les différences sont soulignées avec des approches de logique quantique plus traditionnelles.

1. Introduction

L'année 2015 a célébré en toute discrétion le 200^{e} anniversaire de la naissance de George Boole (1815-1864). Son approche visionnaire de la logique a conduit à formaliser en langage mathématique simple ce qui était avant lui une discipline orientée vers le langage et la philosophie. Sa motivation initiale telle qu'elle apparaît clairement dans son premier ouvrage sur la logique en 1847, *Mathematical Analysis of Logic* [1], était de proposer une formulation algébrique capable de générer toutes les propositions logiques possibles, d'exprimer toute proposition logique par une équation, et de trouver les conséquences les plus générales de tout ensemble fini de propositions logiques par un raisonnement algébrique appliqué aux équations correspondantes. Il rédige ensuite la synthèse de toutes ses investigations en logique en 1854 avec *Les Lois de la pensée* [2].

En 1847, George Boole était déjà un mathématicien exceptionnel, il reçut la médaille d'or de la Royal Society en 1844 pour ses mémoires *On a General Method in Analysis*. Il était un expert dans la résolution des équations différentielles non linéaires et il a introduit de nombreuses nouvelles méthodes utilisant l'algèbre symbolique comme indiqué par Maria Panteki [3]. De toute évidence, George Boole s'est pris d'affection pour les opérateurs en raison de ses succès dans l'application de l'algèbre des opérateurs différentiels dans les années 1841-1845.

Son approche peut être considérée comme opérationnelle, cette caractéristique est rarement considérée de nos jours, comme le souligne Theodeore Hailperin [4, 5]. George Boole (voir [1] p. 16) utilise X, Y, Z... pour représenter les éléments individuels de classes. Il introduit ensuite le symbole x, qu'il nomme le *symbole électif*, agissant sur tout objet comprenant des individus ou des classes en sélectionnant tous les X qu'il contient. Il s'ensuit que le produit des symboles électifs "xy représentera successivement la sélection de la classe Y, puis dans la sélection de la classe Y, des objets de la classe X que la sélection de la classe Y contient, le résultat étant la classe commune

Centrale-Supelec - Laboratoire des Signaux et Systèmes (L2S-UMR8506) - CNRS - Université Paris-Saclay, 3 rue Joliot-Curie, F-91190 Gif-sur-Yvette, FRANCE.
Référence : https://arxiv.org/pdf/1512.06632.pdf.
Traduction Denise Vella-Chemla : mars 2023.

aux X et aux Y". En langage logique, c'est l'opération de conjonction `AND`.

Une expression dans laquelle interviennent les symboles électifs, $x, y, z...$, ne devient une fonction élective que si elle peut être considérée comme "interprétable" en logique. George Boole n'a pas donné une définition précise de ce qu'il entendait par une fonction élective, il semble probable qu'il voulait dire que toute fonction algébrique des symboles électifs $x, y, z...$, serait une fonction élective. C'est le cas lorsque l'expression se résume aux deux valeurs possibles 0 et 1. En logique, les nombres 0 et 1 correspondent respectivement à faux et vrai. Ainsi, selon George Boole, toutes les quantités deviennent interprétables lorsqu'elles prennent les valeurs 0 et 1.

La logique de George Boole utilisant l'algèbre symbolique était différente et nouvelle parce qu'il était convaincu que la logique n'avait pas seulement à voir avec la "quantité", mais devait posséder un "système de relations plus profond" qui avait à voir avec l'activité de "raisonnement déductif". Or avec ces prémisses il était capable d'utiliser toutes les opérations courantes de l'algèbre ordinaire mais en introduisant une condition spéciale sur les symboles : la loi d'idempotence. Cette loi ne peut être satisfaite que par les nombres 0 et 1 et était par lui considérée comme la loi particulière de la logique. Dans son deuxième livre sur la logique [2], il donne à cette loi le statut de "loi fondamentale de la pensée".

Pour George Boole, tous les arguments et fonctions en logique peuvent être considérés comme des symboles électifs. Par exemple il déclare (p. 63 dans [1]) : "Il est évident que si le nombre de symboles électifs est n, le nombre des modules sera 2^n, et que leurs valeurs séparées seront obtenues en interchangeant de chaque manière possible les valeurs 1 et 0 à la place des symboles électifs de la fonction donnée. n représente le nombre de symboles électifs qui correspondent au nombre d'arguments du système logique ou en langage moderne son arité (la lettre m dans le texte original est ici remplacée par la lettre n). Les modules, pour George Boole, sont les cofacteurs du développement (p. 62 dans [1]). De ce qui a été dit ci-dessus, une conclusion évidente est qu'il y a 2^{2^n} extensions possibles des fonctions électives, mais curieusement George Boole ne tire pas explicitement cette conclusion.

Avec l'introduction des tables de vérité par Charles Sanders Peirce au début des années 1880 [6], peu remarquées à l'époque, comme l'affirme Karl Menger dans [9] et successivement, vers 1920, redécouvertes simultanément et indépendamment par Emil Post [7] et par Ludwig Wittgenstein (5,101 dans le *Tractatus* [8]), le comptage du nombre de propositions logiques élémentaires possibles (connectifs) est devenu une évidence. D'ailleurs, Emil Post dans [7] a étendu le comptage aux alphabets supérieurs au binaire ($m > 2$) conduisant au nombre combinatoire m^{m^n} de connecteurs logiques multivalués élémentaires avec m valeurs et n arguments.

L'aspect de la méthode de Boole qui a été beaucoup discuté était son interprétation donnée aux deux nombres particuliers : 1 et 0. Le nombre 1 représentait pour lui la classe de tous les objets concevables, c'est-à-dire l'univers entier, et naturellement le nombre 0 aurait dû représenter la classe vide. Mais il n'est pas clair de savoir dans [1, 2] si George Boole a jamais fait référence à 0 comme étant une classe, ou était-ce juste une partie de sa machinerie algébrique ? Quant à l'objection à l'usage de 1, c'est à l'exigence qu'il renvoie à l'univers entier par opposition à un *univers de discours* (étendue du champ dans lequel se trouvent tous les objets de notre discours) [10].

George Boole introduit un flou considérable dans [1] quant à savoir à quel moment on travaille dans une logique de classes, et à quel moment on travaille dans une logique de propositions. Dans son calcul propositionnel, il a limité son attention aux énoncés qui étaient toujours vrais ou toujours faux, ce qui réduit les propositions hypothétiques à des propositions catégoriques. En 1854 [2] George Boole remplace plus explicitement l'algèbre des opérateurs de sélection par l'algèbre des classes.

Dans cet article, les propositions hypothétiques ne seront pas considérées, l'analyse se limitera à ce qu'on appelle couramment la *logique propositionnelle* (aussi appelée *logique sententielle*) et ne traitera pas de la *logique des prédicats* (également appelée *logique du premier ordre*) qui utilise des quantificateurs (le quantificateur existentiel $\exists$ et le quantificateur universel $\forall$) sur les propositions.

Comme l'a souligné Theodore Hailperin dans [4], les symboles et fonctions électives dénotent des opérateurs et il sera souligné dans ce travail que l'algèbre des symboles électifs peut également être interprétée comme une algèbre d'opérateurs de projection qui commutent et utilisée pour développer la logique propositionnelle dans un cadre d'algèbre linéaire par l'isomorphisme des symboles et fonctions électives de Boole avec les opérateurs de projection qui commutent.

2. Symboles et fonctions électifs

Idempotence et théorème de développement de Boole

Ici sont brièvement présentés les concepts de base qui sous-tendent la méthode de décomposition élective, à partir de la toute première intuition de George Boole concernant sa numérisation de la logique.

Les symboles électifs obéissent aux lois suivantes, celles-ci sont suffisantes pour construire une algèbre.

La loi (1) dit que les symboles électifs sont distributifs. Cela signifie, selon Boole, que "le résultat d'un acte d'élection est indépendant du groupement ou de la classification du sujet".

$$x(u+v) = xu + xv \tag{1}$$

La loi (2) dit que les symboles électifs commutent, ceci parce que : "l'ordre dans lequel s'accomplissent deux actes successifs d'élection est indifférent.".

$$xy = yx \tag{2}$$

La loi (3) appelée *loi d'indice* par George Boole représente l'idempotence d'un symbole électif, elle stipule : "le résultat d'un acte d'élection donné, effectué deux fois de suite, ou un nombre quelconque de fois de suite, est le résultat du même acte effectué une seule fois".

$$x^n = x \tag{3}$$

En conséquence de cette loi, George Boole a formulé les deux équations équivalentes suivantes.

$$\begin{aligned} x^2 &= x \\ x(1-x) &= 0 \end{aligned} \tag{4}$$

L'équation (4) montre explicitement que les nombres 0 et 1 sont les seuls possibles. Il indique également l'orthogonalité entre le symbole électif x et $(1-x)$, qui représente le complément ou la négation de x. Aussi:

$$x + (1 - x) = 1 \tag{5}$$

cette équation montre que le symbole x et son complément $(1-x)$ forment la classe d'univers.

Maintenant, avec ces lois et ces symboles, les fonctions électives peuvent être calculées. Il est intéressant d'illustrer comment George Boole est arrivé à une expression générale d'une fonction élective en utilisant le développement de Mac Laurin de la fonction $f(x)$ autour du nombre 0 (voir [1] p. 60). Du fait de la loi d'indice (3) ou de la loi d'idempotence (4) le symbole x devient un facteur de la série commençant au deuxième terme dans le développement de Mac Laurin, cela donne :

$$f(x) = f(0) + x\left[f'(0) + \frac{1}{2!}f''(0) + \frac{1}{3!}f'''(0) + ...\right] \tag{6}$$

Puis en calculant la fonction à la valeur 1, f(x = 1), à l'aide de l'équation (6), n trouve un expression différente de la série. En remplaçant cette expression en retour dans l'équation (6) on obtient finalement :

$$\begin{aligned} f(x) &= f(0) + x(f(1) - f(0)) \\ &= f(0)(1-x) + f(1)x \end{aligned} \tag{7}$$

De façon plus simple ces expressions peuvent être obtenues directement par des méthodes d'interpolation classiques utilisant par exemple des polynômes d'interpolation de Lagrange pour un nombre fini m de points distincts x_i. Les polynômes de Lagrange sont alors de degré $m-1$ et sont donnés par :

$$\pi_{x_i}(x) = \prod_{j\ (j\neq i)}^{m} \frac{(x - x_j)}{(x_i - x_j)} \tag{8}$$

La fonction d'interpolation $f(x)$ d'une fonction donnée $g(x)$ s'exprime alors à l'aide du développement polynomial fini sur les m points distincts choisis x_i :

$$f(x) = \sum_{i=1}^{m} g(x_i)\,\pi_{x_i}(x) \tag{9}$$

Pour un système binaire ($m = 2$) de valeurs sur l'alphabet $\{0, 1\}$, les deux polynômes d'interpolation se calculent facilement à partir de (8), donnant respectivement : $\pi_{x_0=0}(x) = (1-x)$ et $\pi_{x_1=1}(x) = x$, qui sont les mêmes qu'en (7), et pour cet alphabet, l'équation (9) est équivalente à l'équation (7) car bien entendu aux points d'interpolation $g(0) = f(0)$ et $g(1) = f(1)$. De cette manière, la démonstration du théorème de développement électif ne nécessite pas de séries de puissances polynomiales infinies, par exemple le développement de Maclaurin, comme cela a été fait avec la preuve en séries de puissances de George Boole dans [1].

Il faut souligner que les polynômes de Lagrange (8) sont par construction des fonctions idempotentes aux points d'interpolation, plus précisément : $\pi_{x_i}(x = x_i) = 1$ et $\pi_{x_i}(x = x_j \neq x_i) = 0$.

La même méthode d'interpolation peut être étendue à d'autres alphabets binaires, par exemple $\{+1, -1\}$, ainsi qu'aux systèmes multivalués avec $m > 2$ (pour les développements, voir [11]).

L'équation (7) montre qu'une fonction élective peut être développée de manière unique en utilisant les deux symboles électifs orthogonaux x et $(1 - x)$. Maintenant, si la fonction doit être "interprétable" en logique, elle ne doit prendre que les valeurs 0 et 1, ce qui signifie que les deux cofacteurs $f(0)$ et $f(1)$ (les *moduli* de George Boole) prennent également les valeurs 0 ou 1. Ces coefficients représentent les valeurs de vérité pour la fonction logique.

Combien de possibilités, ou exprimées en langage logique, combien de fonctions logiques différentes pouvons-nous construire en utilisant n arguments ? Nous avons déjà dit que les combinaisons possibles sont au nombre de 2^{2^n}. Considérant donc un symbole unique, $n = 1$, on obtient 4 fonctions électives distinctes. Celles-ci sont présentés dans le tableau 1.

Une procédure similaire peut être utilisée (voir p. 62 dans [1]) pour les fonctions électives de deux arguments $f(x, y)$, cela donne le développement multilinéaire suivant utilisant 4 polynômes orthogonaux et idempotents :

$$f(x, y) = f(0, 0)\,(1 - x)(1 - y) + f(0, 1)\,(1 - x)y + f(1, 0)\,x(1 - y) + f(1, 1)\,xy \tag{10}$$

Et ainsi de suite pour n croissant. Pour $n = 2$ on a $2^{2^{n=2}} = 16$ fonctions électives différentes (données dans le tableau 2) et pour $n = 3$, $2^{2^{n=3}} = 256$. Toutes les fonctions électives sont idempotentes : $f_{el}^2 = f_{el}$. Ici aussi, les méthodes d'interpolation finie pourraient être utilisées en utilisant cette fois-ci des fonctions à plusieurs variables.

L'équation (10) représente le développement électif canonique d'une fonction élective à deux arguments et a la même structure que la forme canonique de disjonction *minterme* en algèbre booléenne [4] qui représente la disjonction de conjonctions mutuellement exclusives (voir ci-après).

Ainsi à partir de l'équation (10) toutes les fonctions logiques peuvent être exprimées comme une combinaison de polynômes multilinéaire de degré 1. On peut montrer que cette décomposition est unique.

George Boole a également développé une méthode de résolution de ce qu'il appelait les *équations électives* où par exemple, la question est : "pour quelles valeurs une fonction élective est-elle vraie ?" (voir [1] p. 70).

Une méthode très simple utilisée pour résoudre les équations électives utilise l'orthogonalité des différents polynômes électifs qui sont multipliés par les cofacteurs respectifs (*moduli*) $f^{[n]}(a, b, c, ...)$ dans le développement, on appelle ces polynômes $\pi^{[n]}_{(a,b,c...)}$ pour une combinaison donnée de valeurs fixes $(a, b, c, ...)$. Cela donne l'équation suivante pour sélectionner les cofacteurs individuels pour une fonction élective à n symboles :

$$f^{[n]}(x, y, z, ...) \cdot \pi^{[n]}_{(a,b,c,...)} = f^{[n]}(a, b, c, ...)\,\pi^{[n]}_{(a,b,c,...)} \tag{11}$$

L'équation (11) peut être utilisée quel que soit le nombre de symboles et aussi lorsque les fonctions ne sont pas explicitement mises sous la forme canonique. Par exemple si l'on veut sélectionner le

coefficient $f(0,1)$ parmi $f(x,y)$ dans l'équation (10), on multiplie simplement la fonction par le polynôme orthogonal correspondant $(1-x)y$. Sans doute est-il la plupart du temps plus facile d'évaluer directement $f(0,1)$.

3. Logique symbolique élective

3.1. Tables de vérité et fonctions électives

Dans cette section, le lien des fonctions électives avec la logique propositionnelle ordinaire est présenté. Les fonctions et les symboles prendront exclusivement les deux valeurs binaires 0 et 1 représentant respectivement le caractère faux (F) et vrai (T) d'une proposition donnée. Les fonctions logiques sont classées selon leurs tables de vérité.

En partant des propositions très simples dérivées du symbole électif unique x, selon le développement de la fonction dans l'équation (7), on voit qu'il y a 4 fonctions possibles selon les valeurs prises respectivement par $f(0)$ et $f(1)$. C'est ce que montre le tableau 1 :

fonction. $f_i^{[1]}$	proposition logique	valeur de vérité $f(0)$ $f(1)$	forme canonique $(1-x)$, x	forme polynomiale
$f_0^{[1]}$	F	0 0	0	0
$f_1^{[1]}$	$\bar{A}$	1 0	$(1-x)$	$1-x$
$f_2^{[1]}$	A	0 1	x	x
$f_3^{[1]}$	V	1 1	$(1-x)+x$	1

Table 1: Les 4 fonctions électives logique à un seul argument

Dans ce cas, les deux propositions non triviales sont la projection logique A et sa négation $\bar{A}$. Les deux autres donnent des sorties constantes : `Faux` (`F`) et `Vrai` (`V`) quelle que soit la valeur de l'argument.

Dans le tableau 2, on montre les 16 fonctions électives, $f_i^{[2]}$, pour $n = 2$ arguments. Les polynômes électifs correspondants peuvent être obtenus directement en substituant les valeurs de vérité respectives aux quatre termes polynomiaux dans l'équation (10). Selon la classification standard, donnée par exemple par Donald Knuth [12], les fonctions logiques sont ordonnées par nombre binaire croissant dans la table de vérité (l'ordre de comptage va de gauche à droite : le digit le plus bas est à gauche). La représentation utilisée ici correspond à ce que l'on appelle souvent le vecteur de vérité de la fonction : $(f(0,0), f(0,1), f(1,0), f(1,1))$.

Quelques précisions sur d'autres connecteurs logiques : l'expression $A \Rightarrow B$ signifie "A implique B", et l'inverse $A \Leftarrow B$ signifie "B implique A" ; le symbole $\not\Rightarrow$ représente la non-implication. L'expression pour `NAND` qui est "not `AND`" est donnée selon les lois de de Morgan [12] par $\bar{A} \vee \bar{B}$. Il en est de même pour `NOR`, "non `OR`", donné par $\bar{A} \wedge \bar{B}$.

La négation s'obtient en complémentant la fonction en soustrayant du nombre 1.

fonct. $f_i^{[2]}$	connecteur logique pour A et B	valeur de vérité $f(0,0)\ f(0,1)\ f(1,0)\ f(1,1)$	forme canonique $(1-x)(1-y)\ ,\ (1-x)y\ ,\ x(1-y)\ ,\ xy$	forme polynomiale
$f_0^{[2]}$	F	0 0 0 0	0	0
$f_1^{[2]}$	NOR , $\bar{A} \wedge \bar{B}$	1 0 0 0	$(1-x)(1-y)$	$1-x-y+xy$
$f_2^{[2]}$	$A \not\Leftarrow B$	0 1 0 0	$(1-x)y$	$y-xy$
$f_3^{[2]}$	$\bar{A}$	1 1 0 0	$(1-x)(1-y)+(1-x)y$	$1-x$
$f_4^{[2]}$	$A \not\Rightarrow B$	0 0 1 0	$x(1-y)$	$x-xy$
$f_5^{[2]}$	$\bar{B}$	1 0 1 0	$(1-x)(1-y)+x(1-y)$	$1-y$
$f_6^{[2]}$	XOR , $A \oplus B$	0 1 1 0	$(1-x)y+x(1-y)$	$x+y-2xy$
$f_7^{[2]}$	NAND , $\bar{A} \vee \bar{B}$	1 1 1 0	$(1-x)(1-y)+(1-x)y+x(1-y)$	$1-xy$
$f_8^{[2]}$	AND , $A \wedge B$	0 0 0 1	xy	xy
$f_9^{[2]}$	$A \equiv B$	1 0 0 1	$(1-x)(1-y)+xy$	$1-x-y+2xy$
$f_{10}^{[2]}$	B	0 1 0 1	$(1-x)y+xy$	y
$f_{11}^{[2]}$	$A \Rightarrow B$	1 1 0 1	$(1-x)(1-y)+(1-x)y+xy$	$1-x+xy$
$f_{12}^{[2]}$	A	0 0 1 1	$x(1-y)+xy$	x
$f_{13}^{[2]}$	$A \Leftarrow B$	1 0 1 1	$(1-x)(1-y)+x(1-y)+xy$	$1-y+xy$
$f_{14}^{[2]}$	OR , $A \vee B$	0 1 1 1	$(1-x)y+x(1-y)+xy$	$x+y-xy$
$f_{15}^{[2]}$	V	1 1 1 1	$(1-x)(1-y)+(1-x)y+x(1-y)+xy$	1

Table 2: Les seize fonctions électives logiques à deux arguments

La conjonction, AND, correspond à la fonction élective suivante :

$$f_8^{[2]}(x,y) = f_{\texttt{AND}}^{[2]}(x,y) = xy \tag{12}$$

et sa négation NAND est simplement :

$$f_7^{[2]}(x,y) = 1 - xy = 1 - f_{\texttt{AND}}^{[2]}(x,y) = f_{\texttt{NAND}}^{[2]}(x,y) \tag{13}$$

$f_0^{[2]}$ a les valeurs de vérité $(0,0,0,0)$ et représente la contradiction, $f_1^{[2]}$ est NOR avec les valeurs de vérité $(1,0,0,0)$ et etc... Par exemple la fonction (AND, $\wedge$) est $f_8^{[2]}$ avec $(0,0,0,1)$, la disjonction (OR, $\vee$) est $f_{14}^{[2]}$ avec $(0,1,1,1)$ et la disjonction exclusive (XOR, $\oplus$) est $f_6^{[2]}$ avec $(0,1,1,0)$.

Dans le tableau 2 sont également présentées les formes polynomiales canoniques issues directement de l'éq. (10) et les expressions polynomiales respectives simplifiées.

En complémentant les symboles en entrée, i.e. en remplaçant les symboles x et y par $1-x$ et $1-y$ respectivement, on obtient d'autres fonctions logiques. Par exemple, considérons :

$$\begin{aligned} f_1^{[2]}(x,y) &= (1-x)(1-y) = 1-x-y-xy = 1-(x+y-xy) \\ &= 1 - f_{14}^{[2]}(x,y) = 1 - f_{\texttt{OR}}^{[2]}(x,y) = f_{\texttt{NOR}}^{[2]}(x,y) \end{aligned} \tag{14}$$

c'est le complément de la disjonction OR nommé NOR. Ce résultat correspond à la loi de de Morgan [12] qui stipule que la conjonction AND des compléments est le complément de la disjonction OR.

$$f_{14}^{[2]}(x,y) = f_{\texttt{OR}}^{[2]}(x,y) = x + y - xy \tag{15}$$

remarquez que l'expression de la disjonction OR est donnée par une expression polynomiale contenant un signe moins, ceci est propre aux fonctions électives, et il doit en être ainsi pour que les fonctions soient "interprétables".

L'expression de la disjonction exclusive XOR est donnée par :

$$f_{6}^{[2]}(x,y) = f_{\texttt{XOR}}^{[2]}(x,y) = x + y - 2xy \tag{16}$$

cette forme diffère de ce que l'on utilise habituellement en logique où le dernier terme est omis du fait que l'opération d'addition est considérée comme une somme modulo 1 en algèbre booléenne. Cette fonction représente la fonction de parité donnant 1 lorsque le nombre total de 1 des arguments est impair.

La fonction d'implication (appelée *implication matérielle*) peut également être obtenue par la même méthode, la fonction correspondant à $A \Rightarrow B$ sera $f_{\Rightarrow}^{[2]}$ et l'inverse $f_{\Leftarrow}^{[2]}$. Selon la 2 :

$$f_{\Rightarrow}^{[2]}(x,y) = f_{11}^{[2]}(x,y) = 1 - x + xy \qquad f_{\Leftarrow}^{[2]}(x,y) = f_{13}^{[2]}(x,y) = 1 - y + xy \tag{17}$$

En utilisant le théorème de de Morgan et en complétant les arguments, il est facile de vérifier que $f_{\Rightarrow}^{[2]}$ se transforme en $f_{\Leftarrow}^{[2]}$.

Les cas de non-implication seront respectivement $f_{\not\Rightarrow}^{[2]}$ et $f_{\not\Leftarrow}^{[2]}$ et sont donnés par :

$$f_{\not\Rightarrow}^{[2]}(x,y) = f_{4}^{[2]}(x,y) = x - xy = 1 - f_{\Rightarrow}^{[2]} \qquad f_{\not\Leftarrow}^{[2]}(x,y) = f_{2}^{[2]}(x,y) = y - xy = 1 - f_{\Leftarrow}^{[2]} \tag{18}$$

On peut bien sûr continuer en augmentant le nombre d'arguments n d'une manière évidente. Considérons le cas $n = 3$, la conjonction devient :

$$f_{\texttt{AND}}^{[3]}(x,y,z) = xyz \tag{19}$$

L'expression de la disjonction est obtenue de la même manière que dans l'équation (10) mais avec trois choix de symboles x, y et z. Un calcul simple en utilisant les 8 valeurs de vérité $(0,1,1,1,1,1,1,1)$ donne :

$$f_{\texttt{OR}}^{[3]}(x,y,z) = x + y + z - xy - xz - yz + xyz \tag{20}$$

qui représente la règle d'inclusion-exclusion bien connue, et peut être étendue à toute arité n par récurrence.

Pour la fonction XOR avec $n = 3$ on obtient, en utilisant les valeurs de vérité $(0,1,1,0,1,0,0,1)$:

$$f_{\texttt{XOR}}^{[3]}(x,y,z) = x + y + z - 2xy - 2xz - 2yz + 4xyz \tag{21}$$

cette dernière expression représente une règle spécifique qui peut être étendue directement à tout n par récurrence.

Une autre fonction très populaire pour $n = 3$ arguments est la majorité `MAJ` qui donne la valeur 1 lorsqu'il y a une majorité de 1 pour les arguments. La fonction est obtenue en utilisant les valeurs de vérité : $(0, 0, 0, 1, 0, 1, 1, 1)$:

$$f^{[3]}_{\texttt{MAJ}}(x, y, z) = xy + xz + yz - 2xyz \tag{22}$$

Ces deux derniers connecteurs logiques sont actuellement utilisés ensemble en électronique numérique pour construire un additionneur complet binaire à l'aide de portes logiques, les trois entrées `XOR` donnent la somme binaire et les trois entrées `MAJ` donnent la réalisation.

On voit donc que cette méthode est tout à fait générale et s'applique directement à tous les connecteurs quel que soit le nombre d'arguments.

3.2. Développements logiques

Une fonction élective idempotente $f(x, y, ...)$ peut être évaluée aux valeurs 0 et 1 en utilisant l'algèbre numérique ordinaire, et toutes les fonctions propositionnelles usuelles ont des tables de vérité qui peuvent être exprimées soit sous la forme canonique de Boole, soit sous la forme polynomiale ; par exemple, on a `XOR` exprimé par $x(1-y)+(1-x)y$ ainsi que $x+y-2xy$. Une remarque importante doit être faite sur l'utilisation des deux développements polynomiaux différents nommés respectivement "forme canonique" et "forme polynomiale" présentés dans les deux dernières colonnes du tableau 2. La forme canonique correspond à ce que l'on nomme en logique numérique moderne la décomposition minterme. Les mintermes correspondent ici à des produits de polynômes électifs. Par exemple, pour $n = 2$ arguments, les mintermes sont les 4 polynômes orthogonaux donnés dans l'équation (10) ; en langage logique chaque minterme est une des 4 conjonctions possibles obtenues en complétant aucun, un ou deux arguments.

On peut toujours mettre n'importe quelle fonction logique dans la forme canonique SOP (Sum Of Products), également appelée *forme normale conjonctive complète* [12] qui est une somme de *mintermes*. Un minterme étant formé d'un ensemble d'arguments en entrée, dans une combinaison donnée complémentée ou non, reliés par conjonction $\wedge$, et la "Somme" correspondant à la disjonction $\vee$ (également disjonction exclusive $\oplus$, comme discuté ci-après). Une autre décomposition canonique est POS (Product Of Sums) de *maxtermes*. Un maxterme étant formé d'un ensemble d'arguments en entrée, dans une combinaison donnée complémentée ou non, reliés par disjonction $\vee$, et le "Produit" correspondant à la conjonction $\wedge$, cette forme est aussi appelée *forme normale disjonctive*.

Un SOP avec quatre arguments d'entrée peut être considéré pour l'exemple de travail suivant :

$$F^{[4]}_{\Sigma m(5,7,10,15)}(A, B, C, D) =$$
$$(\overline{A} \wedge B \wedge \overline{C} \wedge D) \vee (\overline{A} \wedge B \wedge C \wedge D) \vee (A \wedge B \wedge \overline{C} \wedge D) \vee (A \wedge B \wedge C \wedge D) \tag{23}$$

L'expression $\Sigma m(5,7,10,15)$ est la notation minterme standard, où les nombres correspondent aux mintermes spécifiques utilisés dans le développement. Sous cette forme, on peut facilement vérifier qu'un seul parmi tous les mintermes peut être vrai à la fois, cela signifie que chaque disjonction est en fait une disjonction exclusive. Dans la décomposition minterme SOP, puisque tous les termes sont orthogonaux, la disjonction et la disjonction exclusive jouent le même rôle.

On peut écrire l'expression donnée dans l'équation (23) en utilisant le formalisme présenté dans cet article en écrivant directement la décomposition élective :

$$f^{[4]}_{\Sigma m(5,7,10,15)}(x,y,z,r) = (1-x)y(1-z)r + (1-x)yzr + xy(1-z)r + xyzr = yr \qquad (24)$$

On peut donc transformer cette expression en d'autres formes polynomiales afin d'obtenir une expression plus simple. Des simplifications importantes sont obtenues lorsqu'on peut factoriser un argument et son complément pour une même expression, par exemple x et $(1-x)$. Les cas les plus simples étant les projecteurs logiques eux-mêmes tels que A dans le tableau 2 où la forme canonique $x(1-y)+xy$ se réduit à x. Ce dernier argument est essentiellement ce qui est utilisé pour opérer la réduction de fonctions logiques en utilisant des cartes de Karnaugh [12].

3.3. Discussion au sujet de la logique arithmétique élective

La caractéristique de la méthode de George Boole est que si certains termes apparaissant dans des expressions logiques peuvent être ininterprétables, les équations le sont toujours lorsqu'elles sont convenablement interprétées, par les règles $(+,-,\times,0,1)$, conduisant in fine aux valeurs 0 et 1. Il reconnaît aussi des termes qui ne sont pas toujours interprétables, comme le terme $2xy$, qui apparaît dans les manipulations d'équations comme pour la fonction élective correspondant à `XOR` dans (16). La cohérence de l'ensemble de l'entreprise est justifiée dans ce que Stanley Burris a appelé plus tard la "règle des 0 et des 1" [13], qui justifie l'affirmation selon laquelle des termes ininterprétables ne peuvent pas être le résultat ultime de manipulations équationnelles à partir de formules de départ significatives. George Boole n'a fourni aucune preuve de cette règle, mais la cohérence de son système a ensuite été prouvée par Theodore Hailperin [4], qui a fourni une interprétation basée sur une construction assez simple d'anneaux à partir des entiers pour fournir une interprétation de la théorie de Boole (voir ci-après).

Même si cette procédure est simple et directe, il n'est pas dans les habitudes de la logique d'utiliser ces expressions arithmétiques, et la raison n'est pas si claire. Une explication pourrait être due aux habitudes axées sur la technologie : le développement d'ordinateurs utilisant des portes logiques comme blocs de construction et des chiffres binaires (bits) comme unités d'information a généralisé ce qu'on appelle "l'algèbre booléenne" formulée dans sa forme actuelle par Edward Huntington en 1904 [14], qui n'est pas l'algèbre élective de Boole [5]. Par exemple l'addition est considérée en algèbre booléenne comme une somme modulo 1 donnant : $x+x=x$. Pour un anneau booléen, nous avons même une règle différente : $x+x=0$. Alors que le calcul électif utilise l'addition et la soustraction arithmétiques normales comme vu précédemment.

Les expressions arithmétiques sont étroitement liées aux expressions polynomiales sur le corps de Galois $\mathrm{GF}_2 = \mathbb{Z}/\mathbb{Z}_2$, mais avec des variables et des valeurs de fonction interprétées comme des entiers 0 et 1 au lieu de valeurs logiques. De cette manière, les expressions arithmétiques peuvent

être considérées comme des homologues entiers d'expressions polynomiales sur GF_2. Pour deux variables booléennes x_1 et x_2 (en utilisant ici une notation plus standard correspondant à deux bits) les relations nécessaires sont :

$$\begin{aligned} \bar{x} &= 1 - x & x_1 \wedge x_2 &= x_1 x_2 \\ x_1 \vee x_2 &= x_1 + x_2 - x_1 x_2 & x_1 \oplus x_2 &= x_1 + x_2 - 2x_1 x_2 \end{aligned} \tag{25}$$

ceci résume toute la discussion de la section précédente, la partie droite des équations s'appelle l'*expression arithmétique*.

Il semble que, historiquement, seul John Venn ait explicitement utilisé le raisonnement original de George Boole pour construire ses schémas graphiques logiques [15]. Il a utilisé des surfaces sur un espace à 2 dimensions qui représentaient les différentes propositions logiques et plus précisément l'intersection et l'union correspondant à la conjonction et la disjonction. Ce faisant, il devait, dans certains cas, soustraire des portions de surfaces afin d'obtenir la mesure de surface correcte. Par exemple en considérant deux surfaces qui se chevauchent, la surface représentant la disjonction„ est obtenue par la somme des deux surfaces moins leur surface sécante (sans cette soustraction on compterait le double de la surface sécante), également pour la disjonction exclusive, il faut soustraire deux fois la surface d'intersection, cela conduit à des formules du type *inclusion-exclusion* comme illustré dans les équations (20) et (21). Les formes canoniques des fonctions électives idempotentes dans l'algèbre de Boole sont les mêmes que pour les fonctions de l'algébre booléenne, et le nombre de celles-ci était bien connu dans la seconde moitié des années 1800, et entièrement écrit pour trois variables par John Venn en 1881 (selon Ernst Schroder dans [16]).

En 1933, Hassler Whitney [17], a montré comment convertir l'algèbre moderne des classes (en utilisant l'union, l'intersection et le complément) en algèbre numérique, donnant trois formes normales différentes (polynômes en x, polynômes en $(1-x)$, et forme de Boole) pour les fonctions. Il n'a pas reconnu qu'il convertissait l'algèbre moderne des classes en algèbre des classes de Boole. Théodore Hailperin s'en rendra compte des décennies plus tard.

L'observation que l'on peut exprimer des fonctions propositionnelles, vues comme des fonctions de commutation, en utilisant des polynômes en algèbre numérique ordinaire, comme l'a fait George Boole, a été utilisée par Howard Aiken en 1951 dans [19], où l'on trouve des tables d'expressions algébriques numériques ordinaires minimales pour les fonctions de commutation $f : \{0,1\}^n \to \{0,1\}$ jusqu'à $n = 4$. Il est intéressant de noter que Howard Aiken, qui a fondé le "Laboratoire de calcul de Harvard", le premier laboratoire dédié à l'informatique à Havard à partir de 1937, développe le premier ordinateur, l'ASCC (Automatic Sequence Controlled Calculator), aussi appelé Harvard MARK 1 en 1944 avec IBM.

Il a d'abord découvert que les expressions arithmétiques peuvent être utiles dans la conception de circuits logiques et les a utilisées dans les ordinateurs successifs Harvard MARK 3 et MARK 4. Ce type de logique n'a pas percé principalement parce que la famille d'ordinateurs Harvard MARK a été remplacée par la génération d'ordinateurs ENIAC qui utilise des transistors à semi-conducteurs au lieu d'interrupteurs électro-mécaniques et de tubes à vide et il s'est appuyé sur le paradigme du *bit* et de la *porte logique* introduit à l'origine par Claude E. Shannon en 1938 [20] et il "a adapté"

la logique booléenne aux circuits de commutation.

De nos jours, ces développements arithmétiques sont encore utilisés pour décrire les fonctions de commutation et la conception de la logique de décision. Une bonne critique est donnée par Svetlana Yanushkevich dans [18]. Les représentations arithmétiques des fonctions booléennes (c'est-à-dire ici les fonctions électives) sont connues sous le nom de *formes au niveau du mot* et permettent de décrire le calcul parallèle de plusieurs fonctions booléennes à la fois. Une autre propriété utile de ces représentations arithmétiques est utilisée pour les techniques de linéarisation.

4. Logique de projecteur élective

La section suivante présente la véritable nouveauté de ce travail. On montrera que les résultats présentés ci-dessus peuvent être appliqués dans le cadre du formalisme à venir. Il faut souligner qu'à l'époque de George Boole, les méthodes d'algèbre linéaire matricielle n'en étaient qu'à leurs balbutiements. La plupart des méthodes ont été introduites vers 1850, des contributions majeures sont dues à Arthur Cayley et James Joseph Sylvester, ce dernier ayant introduit le terme *matrice*. La définition moderne d'un espace vectoriel a ensuite été introduite par Giuseppe Peano en 1888.

4.1. Parallèles au théorème de développement de Boole dans le domaine des opérateurs idempotents en algèbre linéaire

Une question se pose : pourquoi voudrait-on trouver des parallèles au théorème d'expansion de Boole pour les fonctions ou des symboles idempotents en algèbre linéaire ? L'une des principales motivations de ce travail est de rechercher les liens avec l'algèbre opérationnelle telle qu'elle est utilisée en mécanique quantique dans l'espace de Hilbert avec des applications dans le domaine émergent de l'*information quantique* et du *calcul quantique* [11].

Concernant les applications possibles à la mécanique quantique de la version algébrique en algèbre des opérateurs linéaires idempotents de l'algèbre des opérateurs de Boole, quelques éléments importants peuvent être rappelés. La mécanique quantique était un sujet brûlant à Harvard à partir de la fin des années 1920. Marshall H. Stone, un étudiant de Garret D. Birkhoff, a écrit un livre au début des années 1930 sur les opérateurs linéaires sur les espaces de dimension infinie [21] puis par la suite, à partir de 1934, il a entrepris un grand effort de recherche en logique aboutissant à deux articles sur les algèbres booléennes, les anneaux booléens et les espaces booléens [22, 23].

Marshall H. Stone a montré que toute algèbre booléenne est isomorphe à un corps d'ensembles, et il a motivé son approche algébrique de la logique par le fait qu'elle permet de relier de nombreux domaines différents des mathématiques. Comme le souligne Stanley Burris [13], il est intéressant de noter que sa motivation pour étudier l'algèbre booléenne provenait des mathématiques d'un domaines tel que la mécanique quantique : (citation de son article de 1936 [22]) "L'intérêt de l'écrivain pour le sujet, par exemple, est né en relation avec la théorie spectrale des transformations symétriques dans l'espace de Hilbert et certaines propriétés connexes des intégrales abstraites." Cela aurait pu signifier qu'il examinait des algèbres booléennes des transformations linéaires idempotentes et qu'il s'était rendu compte qu'il existait de nombreux exemples d'algèbres booléennes qui n'avaient pas été pris en compte auparavant. Il poursuit en démontrant que l'axiomatisation

de Huntington des algèbres booléennes [14] est équivalente à l'axiomatisation des anneaux commutatifs à élément unitaire, dans lesquels tout élément est idempotent et qu'on appelle des anneaux booléens ([22] p. 38).

Selon Dirk Schlimm dans [24], Marshall H. Stone a pu relier la théorie des anneaux booléens également à la topologie en prouvant que "la théorie des anneaux booléens est mathématiquement équivalente à la théorie des espaces topologiques localement bicompacts totalement déconnectés". Cette identification, également appelée *théorème de représentation fondamentale* permettant le transfert de méthodes topologiques à l'étude des algèbres booléennes, et vice-versa, est connue sous le nom de *dualité de Stone*.

Il y a également eu des travaux sur le développement d'une logique spécifique pour la mécanique quantique par Garrett Birkhoff et John von Neumann dans leur article fondateur de 1936 sur le sujet [25], ils ont proposé le remplacement des algèbres booléennes par le réseau de sous-espaces fermés d'un espace de Hilbert fini. La logique quantique est devenue une discipline indépendante avec de nombreux promoteurs et différentes déclinaisons, même si elle n'a pas encore atteint le statut d'"outil opérationnel" dans les domaines émergents de l'information et de l'informatique quantiques. Déjà en 1932, John von Neumann établissait des parallèles entre les projections dans l'espace de Hilbert et les propositions logiques (p. 249 : "Les projecteurs comme propositions" dans [26]). Comme l'indique clairement François David dans [27], John von Neumann a remarqué que les *observables* (nom donné aux opérateurs hermitiens en mécanique quantique) données par les opérateurs de projection $\mathbf{P}$, tels que $\mathbf{P}^2 = \mathbf{P} = \mathbf{P}^\dagger$, correspondent aux propositions avec un résultat *Oui* or *Non* i.e. `Vrai` ou `Faux`) dans un système logique.

Un opérateur de projection orthogonale $\mathbf{P}$ sur un sous-espace linéaire P, dans l'espace de Hilbert, est en effet une observable qui ne peut prendre que les valeurs propres 1 (si l'état quantique correspondant appartient au sous-espace P) ou 0 (si l'état quantique correspondant appartient au sous-espace orthogonal à P). Ainsi les deux valeurs 1 et 0 sont les seules valeurs propres possibles de l'opérateur de projection $\mathbf{P}$, et cette affirmation, qu'une mesure ne peut donner qu'une des valeurs propres, fait partie du postulat de mesure fondamental en Mécanique Quantique [26, 27, 28]. Ainsi mesurer l'observable $\mathbf{P}$ équivaut à effectuer un test sur le système, ou à vérifier la validité d'une proposition logique sur le système, qui ne peut être que vraie ou fausse, et non une combinaison de ces valeurs. Cela énonce en d'autres termes la *loi du tiers exclu* aristotélicienne pour une proposition.

Dans son livre de 1932 [26] John von Neumann cite le livre de Marshall H. Stone (p. 70 : "Projections" dans [21]) à propos des opérations conservant les propriétés des opérateurs de projection et donne les règles suivantes :
- $\mathbf{P}_1 \cdot \mathbf{P}_2$ est un opérateur de projection si et seulement si $\mathbf{P}_1 \cdot \mathbf{P}_2 \equiv \mathbf{P}_2 \cdot \mathbf{P}_1$ (i.e. ils commutent) ;
- $\mathbf{P}_1 + \mathbf{P}_2$ est un opérateur de projection si et seulement si $\mathbf{P}_1 \cdot \mathbf{P}_2 \equiv 0$ ou $\mathbf{P}_2 \cdot \mathbf{P}_1 \equiv 0$;
- $\mathbf{P}_1 - \mathbf{P}_2$ est un opérateur de projection si et seulement si $\mathbf{P}_1 \cdot \mathbf{P}_2 \equiv \mathbf{P}_2$ ou $\mathbf{P}_2 \cdot \mathbf{P}_1 \equiv \mathbf{P}_2$.

Cela montre que la propriété des opérateurs de projection, c'est-à-dire l'idempotence, est conservée sous les opérations (matricielles) que sont le produit $\mathbf{P}_1 \cdot \mathbf{P}_2$, la somme $\mathbf{P}_1 + \mathbf{P}_2$ et la différence $\mathbf{P}_1 - \mathbf{P}_2$ uniquement pour les opérateurs de projection qui commutent, cette condition est généralement ex-

primée en mécanique quantique par la relation de commutation $\mathbf{P}_1 \cdot \mathbf{P}_2 - \mathbf{P}_2 \cdot \mathbf{P}_1 = [\mathbf{P}_1, \mathbf{P}_2] = 0$. La somme n'est définie que pour les sous-espaces disjoints, $P_1 \cap P_2 \equiv 0$, et la différence avec l'inclusion des sous-espaces $P_2 \subseteq P_1$. Ces propriétés seront à la base du développement donné ci-après pour ce qu'on appellera la *logique propre* (Eigenlogic), qui permet d'établir le lien entre les valeurs propres et la logique parce que les matrices diagonales idempotentes n'ont que des 1 et des 0 sur la diagonale, et donc ce sont les seuls résultats possibles (valeurs propres).

Il est également intéressant de noter que la définition même d'un état quantique pur lorsqu'il est exprimé par une matrice de densité, également introduite par John von Neumann, est un *rayon* (un opérateur de projection idempotent de rang 1 traversant un sous-espace unidimensionnel). Tous ces concepts sont à la base de la théorie quantique.

Le travail présenté ici peut être compris dans ce cadre, même si l'on n'a pas besoin ici (du moins à ce stade) de l'algèbre non-commutative qui est à la base des aspects particuliers de la théorie quantique, ayant pour conséquence, par exemple, la non-distributivité de la logique quantique. L'approche ici peut être considérée comme *classique* dans le sens où la discussion se limite aux familles d'observables qui commutent qui sont ici des opérateurs de projection. Mais parce que cette approche utilise des observables, elle peut aussi être considérée comme étant partie intégrante de la "machinerie quantique" mondiale. La plupart des problèmes de physique quantique traditionnelle traitent de la recherche de fonctions propres et de valeurs propres de certaines observables physiques, les plus étudiées étant les observables hamiltoniennes dont les valeurs propres représentent les énergies d'un système physique et dont les états propres sont les états stationnaires représentant les solutions d'équilibre stables, sous la forme de fonctions d'onde, de l'équation de Schrödinger. Les aspects non traditionnels de la mécanique quantique, principalement la superposition, l'intrication et la non-commutativité, sont largement utilisés dans le domaine de l'information quantique et sont considérés comme une ressource pour l'informatique quantique [28]. Rien dans la formulation présentée ici n'interdit d'explorer en dehors de la famille des opérateurs logiques de projection qui commutent, ou de considérer des vecteurs qui ne sont pas des vecteurs propres de la même famille logique. C'est l'objet de recherches en cours (voir [11]).

4.2 Lien entre la formulation de George Boole et l'algèbre linéaire

Si l'on remonte à la motivation des symboles électifs de George Boole, on voit qu'il les applique comme opérateurs de sélection sur des classes d'objets. Comme indiqué dans [3], les expressions qui ne représentent pas des classes sont dites par George Boole "ininterprétables", et sont formellement reconnaissables comme celles qui ne satisfont pas la loi d'idempotence $x^2 = x$. La caractéristique de la méthode est qu'alors que des expressions peuvent être ininterprétables, les équations sont toujours interprétables lorsqu'elles sont interprétées adéquatement par les règles.

Mais dans son premier livre [1], Boole était limité par l'interprétation du nombre 1 qu'il considérait comme l'unique classe U représentant l'univers entier. De ce fait, sans entrer dans tous les détails, voir par exemple [4, 5], il modifie la méthode dans son deuxième livre en 1854 [2] et applique le formalisme à des sous-classes de la classe universelle U.

La terminologie moderne sera utilisée pour décrire ce que faisait George Boole : le mot *classe*

devrait être utilisé comme synonyme du mot moderne *ensemble*. Dans [1], il part de la classe d'univers U et regarde successivement dans [2] l'ensemble $P(U)$ des sous-classes. La définition de l'opérateur de sélection (i.e. électif) S_A défini pour $P(U) \to P(U)$ pour $A \in P(U)$ agissant pour $X \in P(U)$ est donnée par l'intersection :

$$S_A(X) \vDash A \cap X \tag{26}$$

Utilisant la composition d'opérateurs pour la multiplication, ses opérateurs étaient associatifs, commutatifs et idempotents. En appelant 0 la classe vide, 1 l'univers U, on a $S_0(X) = 0, S_1(X) = X$. L'addition était partiellement définie, à savoir $S_A + S_B$ était définie pour $A \cap B = 0$. De même la soustraction était également partiellement définie.

En considérant toutes les lois que George Boole utilise réellement $(+, -, \times, 0, 1)$ vues comme un ensemble d'axiomes pour une théorie mathématique, Theodore Hailperin trouve [3] que les interprétations ou modèles corrects sont obtenus si l'on considère les domaines auxquelles les variables appartiennent, non pas comme des classes, mais comme des multi-ensembles. Les opérateurs définis ci-dessus ont pour domaines images des *multi-ensembles signés*, qui s'expriment commodément par une application $f : U \to \mathbb{Z}$. Alors les classes de George Boole correspondent à des fonctions caractéristiques par l'intermédiaire de l'application $\alpha : \Lambda \to \widehat{\Lambda}$, où $\widehat{\Lambda}(u)$ vaut 1 si $u \in \Lambda$ et 0 sinon. La collection des applications de U dans $\mathbb{Z}$ s'écrit généralement $\mathbb{Z}^U$, un anneau de fonctions avec multiplication scalaire (par des éléments de $\mathbb{Z}$), où les opérations sont données en chaque point, c'est-à-dire pour $u \in U$. Les opérateurs d'élection de Boole S_A sur $P(U)$ peuvent donc être traduit en les opérateurs correspondants qui sont l'ensemble des éléments idempotents de l'anneau $\mathbb{Z}^U$.

Si l'on veut utiliser des opérations linéaires sur un espace vectoriel, il faut prolonger l'anneau $\mathbb{Z}^U$ à un corps F, puisque les espaces vectoriels sont définis sur les corps, ainsi l'ensemble des idempotents $\{0, 1\}^U$, l'anneau des multi-ensembles signés $\mathbb{Z}^U$ et l'algébre des fonctions F^U sur F vérifient :

$$\{0, 1\}^U \subseteq \mathbb{Z}^U \subseteq F^U \tag{27}$$

L'isomorphisme entre l'anneau $\mathbb{Z}^U$ restreint à ses éléments idempotents $\{0, 1\}^U$ et l'algèbre de Boole des classes sur $P(U)$ est due à Theodore Hailperin dans [3]. Sa percée fut de souligner cette équivalence : l'ensemble des éléments x d'une algèbre de multi-ensembles signés qui satisfont $x^2 = x$ constitue une algèbre booléenne. Mais plus important encore, tous les axiomes qui étaient nécessaires dans l'algèbre (partielle) de Boole de la logique sont vérifiés dans l'algèbre complète $\mathbb{Z}^U$. Cela signifie que les raisonnements équationnels de Boole étaient corrects dans $\mathbb{Z}^U$ et donc dans son algèbre partielle $P(U)$. Donc finalement, comme le souligne Stanley Burris [13], une grande partie du travail de Boole en logique a des fondations solides.

Il y a aussi un isomorphisme entre l'anneau des opérateurs linéaires sur F^U, restreint aux opérateurs linéaires définis par multiplication à gauche (i.e. le produit matriciel n'est pas commutatif) par un élément idempotent de F^U et l'algébre de Boole des opérateurs de sélection S_A sur $P(U)$. Un opérateur linéaire sur F^U défini par multiplication à gauche par un idempotent est le même que celui obtenu par multiplication à gauche par une matrice diagonale avec fonction caractéristique idempotente $\widehat{\Lambda}$ le long de la diagonale.

D'après le livre de Theodore Hailperin [4], il est clair qu'étant donné n'importe quel anneau commutatif R avec unité et sans éléments nilpotents, on a des parallèles avec tous les théorèmes de George Boole, pas seulement avec le théorème de développement, qui sont vérifiés dans l'anneau. On peut considérer un tel anneau comme un anneau d'opérateurs agissant par multiplication à gauche sur R. En effet, R peut être considéré comme un R-module unitaire à gauche. Ainsi, on a aussi des parallèles avec les résultats de Boole dans [1].

Si l'on prend pour anneau R l'anneau $\mathbb{Z}^N$ des N-uplets d'entiers, alors les éléments idempotents sont les N-uplets avec des entrées dans $\{0, 1\}$. En identifiant les opérateurs sur les N-uplets aux matrices $N \times N$ diagonales (un espace vectoriel de dimension $d = N$), et les éléments de l'anneau avec des vecteurs colonnes, on obtient la situation d'algèbre linéaire traitée ci-après. Il faut souligner qu'en raison de la cardinalité binaire, nous avons ici $d = N = 2^n$.

4.3. Le projecteur de semis et les opérateurs à un argument

Comme indiqué ci-dessus, les symboles électifs représentent des opérateurs agissant sur une classe donnée d'objets (une sous-classe $P(U)$ de la classe univers U). Ainsi l'opérateur électif représenté par le chiffre 1 deviendra simplement l'opérateur d'identité pour la sous-classe considérée. En utilisant le cadre de l'algèbre linéaire, les opérateurs sont définis sur un espace vectoriel dont la dimension dépend du nombre d'arguments (l'arité) dans le système propositionnel.

Alors quels opérateurs peuvent représenter la sélection d'éléments hors d'une classe ? La réponse directe fournie par l'algèbre linéaire est que ces opérateurs sont les opérateurs de projection qui ont la propriété d'idempotence.

En considérant le cas d'objets appartenant à une seule classe, l'opérateur de projection correspondant $\mathbf{\Pi}$ de cette classe agira sur les vecteurs. Maintenant, quels sont les résultats attendus lors de l'application de ce projecteur ? Si un vecteur $\overrightarrow{(a)}$ correspond exactement aux éléments de la classe, les équations matricielles suivantes seront vérifiées :

$$\mathbf{\Pi}_{(1)} \cdot \overrightarrow{(a)} = 1 \cdot \overrightarrow{(a)} \qquad\qquad \mathbf{\Pi}_{(0)} \cdot \overrightarrow{(a)} = 0 \cdot \overrightarrow{(a)} \tag{28}$$

Les valeurs 0 et 1 sont les deux valeurs propres des deux projecteurs associés au vecteur propre $\overrightarrow{(a)}$. Comme avant, si des résultats interprétables sont à considérer en logique, les seuls nombres possibles pour ces valeurs propres sont 0 et 1.

1 sera obtenu pour les objets appartenant à la classe considérée et 0 pour les objets n'appartenant pas à elle. Dans le second cas on peut aussi définir le vecteur complément $\overrightarrow{(\overline{a})}$.

La valeur propre *Vrai* (1) correspondra au vecteur propre $\overrightarrow{(a)}$, nommé $\overrightarrow{(1)}$, et la valeur propre *Faux* (0) correspondra au vecteur propre complément $\overrightarrow{(\overline{a})}$ appelé $\overrightarrow{(0)}$.

Lorsque ces propriétés sont exprimées sous forme matricielle, les opérateurs de projection $\mathbf{\Pi}_{(1)}$ et $\mathbf{\Pi}_{(0)}$ sont des matrices carrées 2×2 et les vecteurs $\overrightarrow{(a)}$ et $\overrightarrow{(\overline{a})}$ sont des vecteurs colonnes orthonormés

à 2 dimensions :

$$\mathbf{\Pi}_{(1)} = \mathbf{\Pi} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \qquad \mathbf{\Pi}_{(0)} = \mathbf{I}_2 - \mathbf{\Pi} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \tag{29}$$

$$\overrightarrow{(a)} = \overrightarrow{(1)} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \overrightarrow{(\overline{a})} = \overrightarrow{(0)} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{30}$$

Les deux projecteurs donnés dans l'équation (29) sont compléments et idempotents, cette dernière condition s'écrit :

$$\mathbf{\Pi} \cdot \mathbf{\Pi} = \mathbf{\Pi}^2 = \mathbf{\Pi} \tag{31}$$

On peut alors construire les 4 opérateurs logiques correspondant aux 4 fonctions électives données dans le tableau 1 correspondant au cas à un seul argument $n = 1$. Les majuscules en gras sont utilisées ici pour représenter les opérateurs.

$$\begin{aligned} \boldsymbol{A} \;\; &= \;\; \mathbf{\Pi} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \qquad \bar{\boldsymbol{A}} = \mathbf{I}_2 - \mathbf{\Pi} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \\ \boldsymbol{Vrai} &= \mathbf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \boldsymbol{Faux} = \mathbf{0}_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned} \tag{32}$$

$\boldsymbol{A}$ est le *projecteur logique* et $\bar{\boldsymbol{A}}$ est son complément. L'opérateur $\boldsymbol{Vrai}$ (tautologie) correspond ici à l'opérateur identité en 2 dimensions $\boldsymbol{I}_2$. $\boldsymbol{Faux}$ (contradiction) correspond ici à l'opérateur nul $\mathbf{0}_2$.

Remarquons que $\boldsymbol{I}_2$ et $\mathbf{0}_2$ sont aussi des opérateurs de projection (idempotents). Donc en général, pour un argument la forme matricielle de l'opérateur de projection correspondant à la fonction logique $f_i^{[1]}(x)$ donnée dans le tableau 1 est :

$$\boldsymbol{F}_i^{[1]} = f_i^{[1]}(0)\, \mathbf{\Pi}_{(0)} + f_i^{[1]}(1)\, \mathbf{\Pi}_{(1)} = \begin{pmatrix} f_i^{[1]}(0) & 0 \\ 0 & f_i^{[1]}(1) \end{pmatrix} \tag{33}$$

Cette équation représente la décomposition spectrale de l'opérateur et comme les valeurs propres sont réelles, l'opérateur logique est hermitien et peut donc être considéré comme une observable. Ainsi, en *logique propre* (eigenlogic), les valeurs de vérité de la proposition logique sont les valeurs propres de l'observable logique. Dans le cas très simple où 0 et 1 sont tous deux des valeurs propres non dégénérées, les opérateurs de projection relatifs à la base des vecteurs propres prennent la forme du projecteur logique $\boldsymbol{A}$ et de son complément $\bar{\boldsymbol{A}}$.

Comme cela se fait en mécanique quantique, on peut trouver l'ensemble des opérateurs de projection qui représentent complètement le système, notamment en levant l'éventuelle dégénérescence des valeurs propres. Ici les valeurs propres sont toujours égales à 0 ou 1 et la question de la multiplicité des valeurs propres est naturelle. Ce dernier point est important dans le modèle, car non seulement les opérateurs de projection mutuellement exclusifs sont représentatifs d'un système logique, mais la *famille complète* des opérateurs de projection qui commutent (la famille logique) doit être utilisée afin de définir complètement le système logique. Lorsque ces propriétés sont exprimées en termes matriciels, cela signifie que le produit matriciel des observables logiques n'est pas nécessairement

égal à 0.

4.4. Extension à plus d'arguments

Comme vu ci-dessus lors de la représentation de la logique avec n arguments (n-arité) en utilisant des opérateurs de projection idempotents, diverses possibilités sont intrinsèquement présentes dans une structure unique avec 2^{2^n} opérateurs de projection différents. Une fois la base propre choisie, la structure restante est intrinsèque, donc indépendante de la base.

L'extension à plus d'arguments peut être obtenue en augmentant la dimension, cela se fait en utilisant le produit de Kronecker $\otimes$. C'est une procédure standard en algèbre linéaire justifiée car on peut montrer (petit théorème de Wedderburn [27]) que tout anneau à division finie (un anneau à division est l'analogue d'un corps qui ne nécessite pas de commutativité) est un produit direct de corps de Galois $\mathrm{GF}_p = \mathbb{Z}/\mathbb{Z}_p$ (p un nombre premier), dans le cas binaire considéré ici $p = 2$. Le produit direct devient explicitement le tenseur ou produit de Kronecker d'opérateurs linéaires.

Dans notre travail, l'application de cette méthode s'est inspirée à l'origine de la règle de composition des états quantiques, qui a aujourd'hui le statut de postulat en mécanique quantique [28], cette règle étant que le vecteur d'état quantique correspondant à la composition de deux systèmes quantiques représentés par deux sous-espaces dans l'espace de Hilbert est le produit de Kronecker des vecteurs d'état quantiques respectifs. Les opérateurs agissant dans l'espace combiné sont des combinaisons des opérateurs quantiques dans les sous-espaces respectifs. Le fait intéressant est que pour le cas combiné, de nouvelles structures apparaissent, dites non locales, qui ne peuvent pas être mises là comme de simples produits de Kronecker, mais qui sont des combinaisons linéaires de ceux-ci. On montrera que plusieurs opérateurs de projection présentés ci-après correspondant à des observables logiques ne sont pas simplement des produits de Kronecker d'opérateurs de projection élémentaires.

Dans ce qui suit, comme précédemment pour les fonctions logiques électives, des exposants indiqueront combien d'arguments (arité) interviennent dans le système propositionnel.

On peut vérifier que dans l'équation (32), tous les quatre opérateurs logiques sont effectivement idempotents et ils commutent. La correspondance du symbole électif x avec le projecteur élémentaire de *semis* $\mathbf{\Pi}$ sera utilisée dans la suite pour construire des opérateurs logiques d'arité supérieure.

Pour 2 arguments (arité $n = 2$), il faut 4 opérateurs projecteurs orthogonaux de rang 1 qui commutent pour exprimer le développement de la même manière que dans l'équation (10).

Certaines propriétés du produit de Kronecker sur les opérateurs de projection idempotents doivent être décrites.
(i) Le produit de Kronecker de deux opérateurs de projection est aussi un opérateur de projection.
(ii) Si les opérateurs de projection sont de rang 1 (une seule valeur propre est 1, toutes les autres sont 0), alors leur produit de Kronecker est également un opérateur de projection de rang 1.

En utilisant ces deux propriétés, les 4 projecteurs orthogonaux de rang 1 qui commutent couvrant l'espace vectoriel à 4 dimensions peuvent être calculés de manière simple :

$$\mathbf{\Pi}^{[2]}_{(0,0)} = (\mathbf{I}_2 - \mathbf{\Pi}) \otimes (\boldsymbol{I}_2 - \mathbf{\Pi}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \mathbf{\Pi}^{[2]}_{(0,1)} = (\mathbf{I}_2 - \mathbf{\Pi}) \otimes \mathbf{\Pi} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathbf{\Pi}^{[2]}_{(1,0)} = \mathbf{\Pi} \otimes (\mathbf{I}_2 - \mathbf{\Pi}) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \mathbf{\Pi}^{[2]}_{(1,1)} = \mathbf{\Pi} \otimes \mathbf{\Pi} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{34}$$

Par la même procédure que dans l'équation (10), on peut écrire les opérateurs pour $n = 2$ arguments pour une fonction à deux arguments (voir le tableau 2) en utilisant les projecteurs donnés dans l'équation (34) :

$$\boldsymbol{F}^{[2]}_i = f^{[2]}_i(0,0)\, \mathbf{\Pi}^{[2]}_{(0,0)} + f^{[2]}_i(0,1)\, \mathbf{\Pi}^{[2]}_{(0,1)} + f^{[2]}_i(1,0)\, \mathbf{\Pi}^{[2]}_{(1,0)} + f^{[2]}_i(1,1)\, \mathbf{\Pi}^{[2]}_{(1,1)} \tag{35}$$

$$\boldsymbol{F}^{[2]}_i = \begin{pmatrix} f^{[2]}_i(0,0) & 0 & 0 & 0 \\ 0 & f^{[2]}_i(0,1) & 0 & 0 \\ 0 & 0 & f^{[2]}_i(1,0) & 0 \\ 0 & 0 & 0 & f^{[2]}_i(1,1) \end{pmatrix} \tag{36}$$

Les coefficients (cofacteurs) sont les valeurs de vérité de la fonction logique données dans le tableau 2.

Cette méthode peut être étendue à n'importe quel nombre d'arguments n en utilisant le même projecteur de semis $\mathbf{\Pi}$ et son complément $(\mathbf{I}_2 - \mathbf{\Pi})$.[1]

4.5. Observables logiques pour deux arguments

Pour l'arité $n = 2$, les expressions polynomiales ont déjà été calculées dans le tableau 2, on peut donc écrire directement les opérateurs correspondants. Il faut exprimer les projecteurs logiques correspondant aux deux arguments $x = a$ et $y = b$ et ceci est donné à l'aide de l'équation (35) en considérant les valeurs de vérité des fonctions $f^{[2]}_{12}$ et $f^{[2]}_{10}$, ces opérateurs sont :

$$\boldsymbol{A}^{[2]} = \boldsymbol{F}^{[2]}_{12} = 1 \cdot \mathbf{\Pi}^{[2]}_{(1,0)} + 1 \cdot \mathbf{\Pi}^{[2]}_{(1,1)} = \mathbf{\Pi} \otimes (\mathbf{I}_2 - \mathbf{\Pi}) + \mathbf{\Pi} \otimes \mathbf{\Pi} = \mathbf{\Pi} \otimes \mathbf{I}_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{37}$$

$$\boldsymbol{B}^{[2]} = \boldsymbol{F}^{[2]}_{10} = 1 \cdot \mathbf{\Pi}^{[2]}_{(0,1)} + 1 \cdot \mathbf{\Pi}^{[2]}_{(1,1)} = (\mathbf{I}_2 - \mathbf{\Pi}) \otimes \mathbf{\Pi} + \mathbf{\Pi} \otimes \mathbf{\Pi} = \mathbf{I}_2 \otimes \mathbf{\Pi} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{38}$$

[1] $\mathbf{I}_2$?

Voici quelques exemples : l'opérateur de conjonction pour $n = 2$ sera simplement le produit des deux projecteurs :

$$\boldsymbol{F}^{[2]}_{\texttt{AND}} = \boldsymbol{A}^{[2]} \cdot \boldsymbol{B}^{[2]} = (\boldsymbol{\Pi} \otimes \mathbf{I}_2) \cdot (\mathbf{I}_2 \otimes \boldsymbol{\Pi}) = \boldsymbol{\Pi} \otimes \boldsymbol{\Pi} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{39}$$

où la propriété suivante du produit de Kronecker a été utilisée : si $\boldsymbol{P}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ et $\boldsymbol{S}$ sont des opérateurs alors :

$$(\boldsymbol{P} \otimes \boldsymbol{Q}) \cdot (\boldsymbol{R} \otimes \boldsymbol{S}) = (\boldsymbol{P} \cdot \boldsymbol{R}) \otimes (\boldsymbol{Q} \cdot \boldsymbol{S}) \tag{40}$$

L'opérateur de disjonction peut s'écrire directement, à l'aide de l'équation (15) :

$$\boldsymbol{F}^{[2]}_{\texttt{OR}} = \boldsymbol{A}^{[2]} + \boldsymbol{B}^{[2]} - \boldsymbol{A}^{[2]} \cdot \boldsymbol{B}^{[2]} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{41}$$

La disjonction exclusive peut aussi s'écrire directement, à l'aide de l'équation (16) :

$$\boldsymbol{F}^{[2]}_{\texttt{XOR}} = \boldsymbol{A}^{[2]} + \boldsymbol{B}^{[2]} - 2\boldsymbol{A}^{[2]} \cdot \boldsymbol{B}^{[2]} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{42}$$

La négation s'obtient en soustrayant à l'opérateur d'identité (complémentation) donnant en général pour n arguments :

$$\bar{\boldsymbol{A}}^{[n]} \;\; = \;\; \mathbf{I}_{2^n} - \boldsymbol{A}^{[n]} \tag{43}$$

Cette équation peut être utilisée pour obtenir l'opérateur `NAND` :

$$\boldsymbol{F}^{[2]}_{\texttt{NAND}} = \mathbf{I}_4 - \boldsymbol{F}^{[2]}_{\texttt{AND}} = \mathbf{I}_4 - \boldsymbol{A}^{[2]} \cdot \boldsymbol{B}^{[2]} \tag{44}$$

En utilisant la loi de de Morgan :

$$\boldsymbol{F}^{[2]}_{\texttt{NOR}} = (\mathbf{I}_4 - \boldsymbol{A}^{[2]}) \cdot (\mathbf{I}_4 - \boldsymbol{B}^{[2]}) = \mathbf{I}_4 - \boldsymbol{A}^{[2]} - \boldsymbol{B}^{[2]} + \boldsymbol{A}^{[2]} \cdot \boldsymbol{B}^{[2]} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = (\mathbf{I}_2 - \boldsymbol{\Pi}) \otimes (\mathbf{I}_2 - \boldsymbol{\Pi}) \tag{45}$$

L'implication matérielle est aussi directement obtenue en utilisant l'expression donnée dans le tableau 2 :

$$\boldsymbol{F}^{[2]}_{\Rightarrow} = \mathbf{I}_4 - \boldsymbol{A}^{[2]} + \boldsymbol{A}^{[2]} \cdot \boldsymbol{B}^{[2]} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \mathbf{I}_4 - (\boldsymbol{\Pi}) \otimes (\mathbf{I}_2 - \boldsymbol{\Pi}) \tag{46}$$

Le tableau 3 donne les formes d'opérateurs logiques pour les 16 connecteurs logiques à deux arguments.

connecteur pour les booléens A, B	forme de l'opérateur diagonal $diag$(**valeurs de vrit**)	observable logique $\boldsymbol{F}_i^{[2]}$ forme arguments $\boldsymbol{A}$, $\boldsymbol{B}$	observable logique $\boldsymbol{F}_i^{[2]}$ forme opérateur semis $\boldsymbol{\Pi}$
Faux F	$diag(0,0,0,0)$	$\mathbf{0}$	$\mathbf{0}$
NOR ; $\overline{A \vee B}$	$diag(1,0,0,0)$	$\mathbf{I} - \boldsymbol{A} - \boldsymbol{B} + \boldsymbol{A} \cdot \boldsymbol{B}$	$(\mathbf{I} - \boldsymbol{\Pi}) \otimes (\mathbf{I} - \boldsymbol{\Pi})$
$A \not\Leftarrow 1B$	$diag(0,1,0,0)$	$\boldsymbol{B} - \boldsymbol{A} \cdot \boldsymbol{B}$	$\boldsymbol{\Pi} \otimes (\mathbf{I} - \boldsymbol{\Pi})$
$\overline{A}$	$diag(1,1,0,0)$	$\mathbf{I} - \boldsymbol{A}$	$\mathbf{I} - (\boldsymbol{\Pi} \otimes \mathbf{I})$
$A \not\Rightarrow B$	$diag(0,0,1,0)$	$\boldsymbol{A} - \boldsymbol{A} \cdot \boldsymbol{B}$	$(\mathbf{I} - \boldsymbol{\Pi}) \otimes \boldsymbol{\Pi}$
$\overline{B}$	$diag(1,0,1,0)$	$\mathbf{I} - \boldsymbol{B}$	$\mathbf{I} - (\mathbf{I} \otimes \boldsymbol{\Pi})$
$A \oplus B$	$diag(0,1,1,0)$	$\boldsymbol{A} + \boldsymbol{B} - 2\boldsymbol{A} \cdot \boldsymbol{B}$	$\boldsymbol{\Pi} \otimes (\mathbf{I} - \boldsymbol{\Pi}) + (\mathbf{I} - \boldsymbol{\Pi}) \otimes \boldsymbol{\Pi}$
NAND ; $\overline{A \wedge B}$	$diag(1,1,1,0)$	$\mathbf{I} - \boldsymbol{A} \cdot \boldsymbol{B}$	$\mathbf{I} - (\boldsymbol{\Pi} \otimes \boldsymbol{\Pi})$
AND ; $A \wedge B$	$diag(0,0,0,1)$	$\boldsymbol{A} \cdot \boldsymbol{B}$	$\boldsymbol{\Pi} \otimes \boldsymbol{\Pi}$
$A \equiv B$	$diag(1,0,0,1)$	$\mathbf{I} - \boldsymbol{A} - \boldsymbol{B} + 2\boldsymbol{A} \cdot \boldsymbol{B}$	$\boldsymbol{\Pi} \otimes \boldsymbol{\Pi} + (\mathbf{I} - \boldsymbol{\Pi}) \otimes (\mathbf{I} - \boldsymbol{\Pi})$
B	$diag(0,1,0,1)$	$\boldsymbol{B}$	$\mathbf{I} \otimes \boldsymbol{\Pi}$
$A \Rightarrow B$	$diag(1,1,0,1)$	$\mathbf{I} - \boldsymbol{A} + \boldsymbol{A} \cdot \boldsymbol{B}$	$\mathbf{I} - [(\mathbf{I} - \boldsymbol{\Pi}) \otimes \boldsymbol{\Pi}]$
A	$diag(0,0,1,1)$	$\boldsymbol{A}$	$\boldsymbol{\Pi} \otimes \mathbf{I}$
$A \Leftarrow B$	$diag(1,0,1,1)$	$\mathbf{I} - \boldsymbol{B} + \boldsymbol{A} \cdot \boldsymbol{B}$	$\mathbf{I} - [\boldsymbol{\Pi} \otimes (\mathbf{I} - \boldsymbol{\Pi})]$
OR ; $A \vee B$	$diag(0,1,1,1)$	$\boldsymbol{A} + \boldsymbol{B} - \boldsymbol{A} \cdot \boldsymbol{B}$	$\mathbf{I} - [(\mathbf{I} - \boldsymbol{\Pi}) \otimes (\mathbf{I} - \boldsymbol{\Pi})]$
Vrai V	$diag(1,1,1,1)$	$\mathbf{I}$	$\mathbf{I}$

Table 3: Les seize connecteurs à deux arguments et leurs observables logiques propres respectives

4.6. Observables logiques pour trois arguments

Pour une arité $n = 3$, on peut générer 8 projecteurs orthogonaux de rang 1 à 8 dimensions, par exemple deux d'entre eux sont donnés par

$$\boldsymbol{\Pi}^{[3]}_{(1,1,1)} = \boldsymbol{\Pi} \otimes \boldsymbol{\Pi} \otimes \boldsymbol{\Pi} \qquad \boldsymbol{\Pi}^{[3]}_{(0,1,0)} = (\mathbf{I}_2 - \boldsymbol{\Pi}) \otimes \boldsymbol{\Pi} \otimes (\mathbf{I}_2 - \boldsymbol{\Pi}) \tag{47}$$

et pour les projecteurs logiques on a :

$$\boldsymbol{A}^{[3]} = \boldsymbol{\Pi} \otimes \mathbf{I}_2 \otimes \mathbf{I}_2 \qquad \boldsymbol{B}^{[3]} = \mathbf{I}_2 \otimes \boldsymbol{\Pi} \otimes \mathbf{I}_2 \qquad \boldsymbol{C}^{[3]} = \mathbf{I}_2 \otimes \mathbf{I}_2 \otimes \boldsymbol{\Pi} \tag{48}$$

Pour l'arité $n = 3$, la conjonction AND devient alors carrément :

$$\boldsymbol{F}^{[3]}_{\texttt{AND}} = \boldsymbol{A}^{[3]} \cdot \boldsymbol{B}^{[3]} \cdot \boldsymbol{C}^{[3]} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{49}$$

Pour l'arité $n = 3$, l'opérateur majoritaire `MAJ` sera une matrice 8 x 8, son expression peut s'écrire directement à l'aide de l'équation (22) et de l'équation (48) :

$$\boldsymbol{F}^{[3]}_{\texttt{MAJ}} = \boldsymbol{A}^{[3]} \cdot \boldsymbol{B}^{[3]} + \boldsymbol{A}^{[3]} \cdot \boldsymbol{C}^{[3]} + \boldsymbol{B}^{[3]} \cdot \boldsymbol{C}^{[3]} - 2\boldsymbol{A}^{[3]} \cdot \boldsymbol{B}^{[3]} \cdot \boldsymbol{C}^{[3]} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{50}$$

4.7. Opérateurs de sélection

La méthode pour sélectionner les valeurs propres est similaire à celle pour les fonctions électives données dans l'équation (11). Comme les projecteurs de type $\boldsymbol{\Pi}^{[n]}_{(a,b,c...)}$ sont des projecteurs de rang 1, le produit (matriciel) avec n'importe quel autre opérateur de projection qui commute (par exemple l'opérateur logique $\boldsymbol{F}^{[n]}_i$) donnera aussi un projecteur de rang 1 et plus précisément, ce sera le même projecteur multiplié par la valeur propre. Donc pour n'importe quel opérateur logique $\boldsymbol{F}^{[n]}_i$ de la famille considérée, on a :

$$\boldsymbol{F}^{[n]}_i \cdot \boldsymbol{\Pi}^{[n]}_{(a,b,c...)} = f^{[n]}_i(a,b,c,...)\, \boldsymbol{\Pi}^{[n]}_{(a,b,c...)} \tag{51}$$

Du côté droit de l'équation (51), la valeur de vérité est multipliée par le projecteur de rang 1 correspondant.

Pour obtenir explicitement la valeur propre, on peut prendre la trace du produit des deux opérateurs à gauche de l'équation (51). On obtient ainsi la valeur de vérité $f^{[n]}_i(a,b,c...)$ correspondant à un cas de combinaison fixe des valeurs $(a,b,c,...)^{[n]}$ des arguments logiques (une *interprétation*).

La méthode de sélection des valeurs propres est similaire à celle des fonctions électives donnée dans l'équation (11). Comme les projecteurs de type $\boldsymbol{\Pi}^{[n]}_{(a,b,c...)}$ sont des projecteurs de rang 1, le produit (matriciel) avec n'importe quel autre projecteur (par exemple, l'opérateur logique $\boldsymbol{F}^{[n]}_i$) donnera aussi un projecteur de rang 1 et plus précisément, ce sera le même projecteur multiplié par la valeur propre. Donc pour n'importe quel opérateur $\boldsymbol{F}^{[n]}_i$ de la famille considérée, la valeur de vérité est multipliée par le projecteur de rang 1 correspondant.

5. Vecteurs propres, valeurs propres et valeurs de vérité

En commençant par le projecteur bidimensionnel de rang 1 $\boldsymbol{\Pi}$ pour le cas à un argument, les vecteurs $\overrightarrow{(0)}$ et $\overrightarrow{(1)}$ sont des vecteurs orthonormés bidimensionnels comme indiqué dans les équations (30).

Le choix de la position de la valeur 1 dans la colonne suit la convention d'information quantique pour un "qubit-1" [28]. La notation bra-ket de Dirac $|\psi\rangle$ pour représenter les vecteurs en mécanique quantique (i.e. on aurait eu ici : $|0\rangle \equiv \overrightarrow{(0)}$ et $|1\rangle \equiv \overrightarrow{(1)}$) n'a pas été utilisée exprès pour montrer

que cette méthode ne se limite pas aux problèmes liés à la physique quantique.

Pour le cas à deux arguments $n = 2$, les vecteurs auront la dimension $2^{n=2} = 4$ et la famille complète de 16 opérateurs de projection qui commutent représentera toutes les propositions logiques possibles et sera interprétable lorsqu'elle sera appliquée aux quatre vecteurs propres orthonormés possibles de cette famille qui forment la base canonique complète. Ces vecteurs seront représentés par la notation symbolique $\overrightarrow{(a,b)}$, où les arguments a, b prennent les valeurs $\{0, 1\}$ et représentent l'un des quatre cas possibles :

$$\overrightarrow{(0,0)} = \overrightarrow{(0)} \otimes \overrightarrow{(0)} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad \overrightarrow{(0,1)} = (0) \otimes \overrightarrow{(1)} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$
$$\overrightarrow{(1,0)} = \overrightarrow{(1)} \otimes \overrightarrow{(0)} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad \overrightarrow{(1,1)} = \overrightarrow{(1)} \otimes \overrightarrow{(1)} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{52}$$

Lors de l'application des opérateurs de projection logique sur ces vecteurs, la valeur propre résultante est la valeur de vérité de la proposition logique correspondante, ce qui signifie que les opérations sur l'espace propre d'une famille observable logique sont interprétables. Par exemple, pour $n = 2$ arguments, la famille complète de 16 observables logiques commutantes représente tous les connecteurs logiques possibles et les opérations sont interprétables lorsqu'elles sont appliquées à l'un des quatre vecteurs propres canoniques possibles de la famille. Ces vecteurs, correspondant à toutes les interprétations possibles, sont représentés par la base des vecteurs $\overrightarrow{(0,0)}$, $\overrightarrow{(0,1)}$, $\overrightarrow{(1,0)}$ et $\overrightarrow{(1,1)}$ formant une base orthonormée complète.

Que se passe-t-il maintenant lorsque le vecteur d'état n'est pas l'un des vecteurs propres du système logique ? On peut toujours exprimer un vecteur normalisé comme une décomposition sur une base orthonormée complète. En particulier on peut l'exprimer sur la base propre canonique de la famille observable logique. Pour deux arguments, ce vecteur peut s'écrire :

$$\overrightarrow{(\phi)} \;=\; C_{00}\,\overrightarrow{(0,0)} \,+\, C_{01}\,\overrightarrow{(0,1)} \,+\, C_{10}\,\overrightarrow{(1,0)} \,+\, C_{11}\,\overrightarrow{(1,1)}$$

Lorsqu'un seul des coefficients est non nul (dans ce cas sa valeur absolue doit prendre la valeur 1) alors on se retrouve dans la situation précédente d'une interprétation déterminée (cas propositionnel atomique à entrée déterminée). Mais lorsque plus d'un coefficient est non nul, on est dans un cas "mixte" ou "flou". Un tel état peut être considéré comme une superposition cohérente d'interprétations. Cela peut conduire à un traitement de logique floue comme cela a été proposé dans [11], la logique floue traite des valeurs de vérité qui peuvent être n'importe quel nombre entre 0 et 1, ici la vérité d'une proposition peut être comprise entre complètement vraie et complètement fausse.

Une remarque importante est que le choix de la base propre n'est pas fixe, ce qui signifie que pour chaque choix, il y a une famille complète d'opérateurs de projection logique, donc comme

indiqué ci-dessus, on pourrait imaginer travailler avec deux (ou plusieurs) systèmes logiques caractérisés chacun par leur famille d'opérateurs projectifs. Les opérateurs d'une famille ne commutent (généralement) pas avec les opérateurs d'une autre famille. Cette propriété de non-commutativité a son analogue dans le traitement mécanique quantique général. Sans étendre davantage cet argument, on voit la potentialité de considérer ce type d'approche en gardant à l'esprit qu'en algèbre linéaire, le changement de base est obtenu au moyen d'opérateurs unitaires et que c'est un peu au cœur du calcul quantique où toutes les opérations logiques sont effectuées au moyen de transformations unitaires et par mesures à l'aide d'opérateurs de projection.

6. Propriétés de la logique propre

Pour résumer, tous les opérateurs de projection logique ont les propriétés suivantes en logique propre (eigenlogic).

1. La dimension de l'espace vectoriel couvert par les opérateurs logiques est $d_n = 2^n$. Tous les opérateurs de projection logique de la même famille sont des matrices carrées $d_n \times d_n$.

2. Tous les opérateurs logiques sont des opérateurs de projection idempotents (voir (31)). Cela signifie que dans la base propre logique de la famille, les matrices sont diagonales avec des valeurs propres qui valent soit 0 soit 1.

3. Tous les opérateurs logiques de projection d'une famille donnée commutent deux à deux. Cela signifie que toutes les matrices respectives sont diagonales sur la base propre logique de la famille.

4. Les opérateurs de projection logique ne sont pas nécessairement orthogonaux. Cela signifie que le produit matriciel de deux opérateurs logiques n'est pas nécessairement l'opérateur nul.

5. Le nombre d'opérateurs de projection logique différents d'une famille donnée est de 2^{2^n}, représentant un sysème complet de propositions logiques. Ce nombre correspond au nombre de matrices diagonales différentes qui commutent, obtenues pour toutes les combinaisons de 0 et de 1 sur la diagonale des matrices.

6. Pour chaque famille, il existe 2^n opérateurs de projection orthogonale de rang 1 couvrant tout l'espace vectoriel. Les matrices correspondantes auront une seule valeur propre égale à 1, les autres valeurs propres étant égales à 0.

7. Tout opérateur logique peut être exprimé comme une décomposition élective en utilisant les 2^n opérateurs de projection orthogonale de rang 1, où les coefficients de la décomposition ne peuvent prendre que les valeurs 0 ou 1 (voir éq. (35) pour $n = 2$).

8. Tout projecteur de rang 1 de la famille peut être obtenu au moyen du produit de Kronecker, le projecteur de semis $\mathbf{\Pi}$ et son complément $(\mathbf{I}_2 - \mathbf{\Pi})$ (voir éq. (29), éq. (34) et éq. (47)).

9. La négation d'un opérateur logique, qui est son complément, s'obtient en soustrayant l'opérateur de l'opérateur d'identité (voir éq. (43)).

10. Les vecteurs propres de la famille des opérateurs logiques de projection d'arité n qui commutent forment une base complète orthonormée de dimension $d_n = 2^n$. Cette base correspond à la

base canonique et chaque vecteur propre correspond à une certaine combinaison d'arguments logiques, appelée une *interprétation*, du système propositionnel logique.

11. Les valeurs propres des opérateurs logiques sont les valeurs de vérité de la proposition logique respective et chaque valeur propre est associée à un vecteur propre donné correspondant à une interprétation de la proposition atomique en entrée.

12. La valeur de vérité d'un opérateur logique donné pour une interprétation donnée de n arguments peut être obtenue en utilisant l'équation (51).

7. Discussion et travaux connexes

Les tentatives de lier la géométrie à la logique sont très nombreuses et remontent aux premiers efforts de formalisation de la logique. Les plus célèbres sont par exemple le carré des oppositions d'Aristote pour les 4 propositions catégorielles (sujet-copule-prédicat), les diagrammes de Leonhard Euler (1707-1783) illustrant les propositions et les quantificateurs (tous, non, certains,...), les diagrammes de C. L. Dodgson (alias Lewis Carroll 1832-1898), des diagrammes recherchant la symétrie du vrai et du faux ayant une ressemblance frappante avec les cartes de Karnaugh modernes, et bien sûr les méthodes développées par John Venn [15] qui ont été évoquées plus haut.

Dans les méthodes de conception logique modernes, les tables de vérité, les cartes de Karnaugh, les hypercubes, les réseaux logiques et à seuil, les arbres de décision et les graphes de diagrammes sont largement utilisés pour représenter les structures de données booléennes [18]. La réduction logique basée sur la symétrie est un sujet très important qui utilise les diagrammes de Hesse, les développements de Shannon et Davio et les théorèmes de Post sur les symétries des fonctions booléennes. La vectorisation est également une procédure standard en logique utilisant par exemple des *vecteurs de vérité* et des *vecteurs porteurs* (vecteurs de vérité réduits de fonctions booléennes symétriques).

Dans ce qui suit sont brièvement citées des recherches récentes qui ont surgi au cours de cette enquête et qui soutiennent l'approche basée sur l'algèbre linéaire présentée dans cet article.

En commençant par *Matrix Logic* développé par August Stern [29] qui donne directement une formulation matricielle des opérateurs logiques, en mettant les valeurs de vérité sous forme de coefficients matriciels, à la manière des diagrammes de Karnaugh. Ainsi, par exemple, une fonction logique à deux arguments devient une matrice 2×2, c'est une différence fondamentale par rapport à la méthode donnée ci-dessus où des matrices 4×4 sont utilisées. Utilisant des produits scalaires sur des vecteurs et des valeurs moyennes sur des opérateurs, ce formalisme donne une méthode pour résoudre des équations logiques et permet d'agrandir l'alphabet des valeurs de vérité avec des antivaleurs en logique négative.

Une percée a sans aucun doute été faite par *Vector Logic* développé par Eduardo Mizraji [30]. Cette approche vectorise la logique où les valeurs de vérité sont envoyées par des applications sur des vecteurs orthonormés. Techniquement, cette approche est différente de celle présentée dans cet article car les opérateurs résultants pour 2 arguments sont représentés par des matrices 2×4 et ne représentent pas des opérateurs de projection. La logique vectorielle peut également gérer la

logique à trois valeurs et des applications ont été proposées pour les réseaux de neurones.

Un développement très pertinent, proche de l'approche de cet article, a été fait par Vannet Aggarwal et Robert Caldebrabnk [31] dans le cadre de la théorie quantique du codage d'erreurs, leur travail a également été justifié par la formulation *Projection Logic* de David Cohen [33]. Dans leur méthode, ils relient la logique booléenne à des opérateurs de projection issus initialement du groupe Heisenberg-Weyl. Ils associent la dimension du projecteur considéré au poids de Hamming (nombre de 1 dans la table de vérité) de la fonction booléenne correspondante. Les opérateurs logiques qu'ils obtiennent sont des projecteurs qui commutent, comme dans le travail présenté ici.

L'idée de lier logique et algèbre linéaire devient également naturelle du fait de l'effort de recherche dû à la promesse que la théorie quantique peut apporter à des domaines extérieurs à la physique, principalement à l'informatique. Bien sûr, il faut considérer la quête de l'ordinateur quantique, mais aussi les développements plus récents dans d'autres domaines de recherche tels que la recherche d'informations sur le web sémantique [34, 35] et l'apprentissage automatique [36].

Toutes ces méthodes reposent sur des méthodes d'algèbre linéaire utilisant des vecteurs et des opérateurs dans l'espace de Hilbert.

Récemment le concept de *prédicat quantique* introduit par E. d'Hondt et P. Panangaden [37] propose une interprétation similaire à celle présentée ici. Comme l'a déclaré Mingsheng Ying dans [38] : "Dans la logique classique, les prédicats sont utilisés pour décrire les propriétés des individus ou des systèmes... alors qu'est-ce qu'un prédicat quantique ? ; ... un prédicat quantique est défini comme une observable physique représentée par un opérateur hermitien avec des valeurs propres dans l'intervalle unitaire".

8. Conclusion et perspectives

Dans la formulation donnée ici, une méthode plus générale est proposée, permettant la construction de projecteurs logiques à partir d'un seul opérateur de projection semis utilisant le produit de Kronecker. La formulation est aussi plus simple car l'interprétation élective de la logique de George Boole montre que la propriété d'idempotence (3) et (4) en association avec la distributivité (1) et la commutativité (2) permet d'identifier directement les opérateurs de projection qui commutent avec les fonctions logiques.

La formulation de la logique présentée ici est appelée logique propre (eigenlogic), elle utilise des opérateurs en algèbre linéaire comme propositions et elle est liée à la formulation de l'algèbre symbolique élective de George Boole dans [1]. Cette similitude est frappante et c'est plus qu'une simple analogie, comme justifié ci-dessus, car au cœur de la formalisation se trouve la propriété d'idempotence. Les opérateurs logiques appartiennent à des familles d'opérateurs de projection qui commutent. La caractéristique intéressante est que les valeurs propres de ces opérateurs sont les valeurs de vérité des connecteurs logiques, leurs vecteurs propres associés correspondant à l'une des combinaisons fixes des entrées (interprétations). Le résultat d'une "mesure" ou d'une "observation" sur une observable logique donnera la valeur de vérité de la proposition logique qui lui est associée, et elle devient "interprétable" lorsqu'elle est appliquée à son espace propre, ce qui conduit à une

analogie naturelle avec le postulat de mesure en mécanique quantique. Le schéma suivant résume ce point de vue :

opérateurs de projection $\longrightarrow$ connecteurs logiques

valeurs propres $\longrightarrow$ valeurs de vérité

vecteurs propres $\longrightarrow$ interprétations (cas propositionnels atomiques)

Quelques précisions doivent être apportées concernant la dernière ligne du schéma, le mot interprétation s'entend au sens logique : une interprétation est une affectation de valeurs de vérité pour chaque proposition atomique qui apparaît dans une *formule bien formée*. Une *formule bien formée* étant une formule complexe contenant exclusivement des connecteurs logiques. Cela signifie que l'ensemble des propositions atomiques peut avoir différentes interprétations, celles conduisant à la *satisfaction* d'une proposition logique (une proposition est satisfaite lorsqu'elle est vraie) sont appelées les *modèles* (n.b. parfois le mot modèle est utilisé plus généralement comme synonyme du mot interprétation).

Une justification théorique et un lien avec la mécanique quantique peuvent également être trouvés chez Pierre Cartier [39], relatant le lien entre l'algèbre des propositions logiques et l'ensemble de toutes les valuations sur celle-ci, il écrit : "... dans la *théorie des modèles* en logique, un modèle d'un ensemble de propositions a pour effet de valider certaines propositions. A chaque proposition logique on peut associer par dualité l'ensemble de toutes ses vraies valuations représentées par le nombre 1. Cette correspondance permet d'interpréter l'algèbre des propositions comme une classe de sous-ensembles, la conjonction et la disjonction devenant respectivement l'intersection et l'union des ensembles. Cela correspond à la *dualité de Stone* prouvée par le théorème de représentation de Stone et est l'un des succès spectaculaires des mathématiques du XX$^{\text{e}}$ siècle. Le développement de la théorie quantique a conduit au concept d'état quantique, qui peut être compris comme une nouvelle incarnation de la notion d'évaluation". L'idée n'est pas nouvelle, comme cela a été discuté auparavant et dans [27], et découle de la proposition de John Von Neumann de "projections as propositions" dans [26] qui a ensuite été formalisée en logique quantique par Garret Birkhoff dans [25].

Concernant la première ligne du schéma, on peut généraliser aux valeurs propres différentes du couple $\{0, 1\}$ associé aux opérateurs de projection, par exemple en utilisant le couple $\{+1, -1\}$ associé aux opérateurs unitaires auto-inverses, ceci a été fait dans [11], en général on peut associer un opérateur logique binaire à n'importe quel couple de valeurs propres $\{\lambda_1, \lambda_2\}$ dont la famille d'opérateurs logiques correspondants peut être trouvée par les méthodes d'interpolation matricielle proposées dans [40].

En logique propositionnelle, les arguments d'une proposition logique composée sont les propositions atomiques, en logique propre (eigenlogic), ce sont ce que nous avons nommé les *opérateurs logiques projecteurs* (aussi parfois nommés *dictateurs* en logique [11, 32]). Des exemples sont le projecteur logique à un argument $\boldsymbol{A}$ dans l'équation (32) ; les deux projecteurs logiques à deux arguments $\boldsymbol{A}^{[2]}$ et $\boldsymbol{B}^{[2]}$ dans les équations (37,38) ; les trois projecteurs logiques à trois arguments $\boldsymbol{A}^{[3]}$, $\boldsymbol{B}^{[3]}$

et $\boldsymbol{C}^{[3]}$ dans l'équation (48) et ainsi de suite pour une arité plus élevée.

C'est une différence fondamentale avec ce qui est habituellement considéré en logique quantique (pour une définition des propositions atomiques en logique quantique voir par exemple [27] p. 98) où les propositions atomiques sont associées à des rayons c'est-à-dire des matrices quantiques de densité d'états purs. En logique propre (eigenlogic) la conjonction connective logique (AND $\wedge$), non atomique, est représentée par un rayon (opérateur de projection de rang 1), voir équations (39) et (49), les autres $n-1$ rayons s'obtiennent simplement en complémentant sélectivement les arguments de la conjonction. En général, ici, les rayons correspondent à des produits de Kronecker d'opérateurs de projection générateurs (opérateur de projection semis), voir les équations (34) et (47) et sont non atomiques (sauf dans le cas d'un argument : $n = 1$). Du point de vue de la logique, les propositions atomiques doivent être des propositions indépendantes et cela ne peut être réalisé qu'avec la formulation donnée par (37) et (38) et non par des opérateurs de projection mutuellement exclusifs, tels que les opérateurs de projection de rang 1 qui ne sont donc pas indépendants. Ainsi en logique propre (eigenlogic), les propositions atomiques ne sont pas des rayons lorsque l'on considère des connecteurs à plus d'un argument ($n \geq 2$).

Dans ce travail, des familles logiques complètes d'opérateurs de projection qui commutent correspondent à des propositions compatibles, c'est aussi une différence avec la logique quantique. Comme mentionné par David W. Cohen (p. 37 [33]) "Une logique quantique est une logique avec au moins deux propositions qui ne sont pas compatibles". Dans les recherches futures, l'interaction des observables logiques qui n'appartiennent pas à la même famille logique compatible d'observables qui commutent sera considérée, cela pourrait apporter des informations pour la logique quantique et le calcul quantique et permettre d'aborder le sujet important de la non-contextualité quantique.

Une approche algorithmique pour les connecteurs logiques avec un grand nombre d'arguments pourrait être intéressante à développer en utilisant les observables de la logique propre (eigenlogic) dans des espaces vectoriels de grande dimension. Mais comme l'espace grandit très rapidement, il peut ne pas être particulièrement utile pour une mise en œuvre pratique sans réduction logique. Il serait intéressant de développer des méthodes spécifiques de réduction algébrique d'observables logiques inspirées de la recherche actuelle dans le domaine. Pour une bonne synthèse de l'état de l'art, voir par exemple [18].

Des applications dans le domaine de la recherche d'information pour des applications en web sémantique semblent possibles. La communauté Quantum Interaction à travers des conférences annuelles promeut les liens entre la mécanique quantique et des domaines extérieurs à la physique avec de nombreuses applications en sciences sociales [41]. Les méthodes sont basées sur l'exploitation du formalisme mathématique, fondamentalement l'algèbre linéaire dans l'espace de Hilbert, de la mécanique quantique [34] combiné avec les aspects particuliers des postulats quantiques. Des applications se trouvent dans les théories sémantiques modernes telles que la sémantique distributionnelle ou dans les modèles connexionnistes de la cognition [42].

Plus généralement, nous pensons que cette vision de la logique pourrait apporter un éclairage sur des questions plus fondamentales. Les fonctions booléennes sont aujourd'hui considérées comme une "boîte à outils" pour résoudre de nombreux problèmes en informatique théorique, en théorie de

l'information et même en mathématiques fondamentales. De même, la logique propre (eigenlogic) peut être considérée comme une nouvelle "boîte à outils".

9. Remerciements

Je tiens à remercier mon collègue et ami François Dubois, mathématicien du CNAM Paris (FR), avec qui j'ai une collaboration continue sur la modélisation quantique et à qui est due l'idée d'utiliser les méthodes d'interpolation classique pour les développements logiques, qui ont été appliqués pour les logiques multivaluées dans [11]. Je suis également très reconnaissant à Francesco Galofaro, Sémioticien du Politecnico di Milano (IT) et de l'Université libre de Bolzano (IT) pour ses conseils pertinents sur la sémantique et la logique des idées qui sont introduites reliant l'informatique quantique, la récupération d'information et la sémantique. Je veux aussi associer mon collègue Bich-Lien Doyen de Centrale-Supélec et du LRI (Laboratoire de Recherche en Informatique) pour être à l'origine de certaines de ces recherches pluridisciplinaires.

J'ai beaucoup apprécié les retours de la communauté Quantum Interaction pour le travail de ces dernières années ([11,35]), les aspects historiques du travail présenté ici ont été exposés lors de la conférence QI-2016 à San Francisco et je tiens à remercier les organisateurs et le personnel du comité technique en particulier José Acacio da Barros de l'Université d'État de San Francisco (CA, USA) et Ehtibar Dzhafarov de l'Université Purdue (IN, USA). Dans cette communauté, j'ai apprécié les discussions fructueuses avec Peter Bruza de QUT (Brisbane, AUS), Emmanuel Haven et Sandro Sozzo de l'Université de Leicester (Royaume-Uni), Andrei Khrennikov de l'Université Linnaeus (SWE), Dominic Widdows de Microsoft Bing Bellevue (WA, USA), Trevor Cohen de l'Université du Texas à Houston (TX, USA), Peter Wittek de l'ICFO de Barcelone (ESP) et enfin Keith van Rijsbergen de l'Université de Glasgow (Royaume-Uni) qui fut peut-être à l'origine de cette recherche à cause de son commentaire à l'issue de la conférence QI-2012 à Paris sur le fait que George Boole avait déjà des idées géométriques sur la représentation des fonctions logiques, en particulier la négation, dans un espace vectoriel...

Je tiens à remercier l'examinateur du premier article que j'ai soumis dans un journal pour son analyse approfondie de ce travail et pour avoir apporté des critiques très constructives à l'œuvre originale de George Boole, plusieurs de ses remarques ont été introduites dans cette version. Et enfin je tiens à remercier Stanley Burris de l'Université de Waterloo (CAN) avec qui j'ai eu une correspondance et qui a souligné la contribution de Theodore Hailperin, beaucoup de ses remarques ont été incluses ici.

Références

[1] George Boole, "The Mathematical Analysis of Logic. Being an Essay To a Calculus of Deductive Reasoning", (1847), (réédité Ed. Forgotten Books ISBN 978-1444006642-9).

[2] George Boole, "An Investigation of the Laws of Thought on Which are Founded the Mathematical Theories of Logic and Probabilities", Macmillan (1854) (réédité par Cambridge University Press, 2009 ; ISBN 978-1-108-00153-3).

[3] Maria Panteki, "The Mathematical Background of George Boole's Mathematical Analysis of Logic (1847)", J. Gasser (ed.), A Boole Anthology, 167-212, Kluwer Academic Publishers, (2000).

[4] Theodore Hailperin, "Boole's Logic and Probability, a Critical Exposition from the Standpoint of Contemporary Logic and Probability Theory", North Holland, (1976) II ed. (1986).

[5] Theodore Hailperin, "Boole's Algebra isn't Boolean Algebra. A Description Using Modern Algebra, of What Boole Really Did Create", Mathematics Magazine 54(4) : 172-184 (1981). Réimprimé dans A Boole Anthology ed. James Gasser. Volume de synthèse 291, Spring-Verlag. (2000).

[6] Charles Sanders Peirce, "On the Algebra of Logic : A Contribution to the Philosophy of Notation", American Journal of Mathematics, Volume 7, (1885).

[7] Emil Post, "Introduction to a General theory of Elementary Propositions", American Journal of Mathematics 43 : 163-185, (1921).

[8] Ludwig Wittgenstein, "Logisch-Philosophische Abhandlung", Annalen der Naturphilosophie, Ed. Wilhelm Ostwald, Wien (1921), "Tractatus Logico-Philosophicus", traduit et publié en édition bilingue, Routledge & Kegan Paul, London, (1922).

[9] Karl Menger, "Reminiscences of the Vienna Circle and the Mathemathical Colloquium" (1942), éditeurs : L. Golland, B.F. McGuinness, Sklar, Ap.be - Springer (1994).

[10] John Corcoran, "Aristotle's Prior Analytics and Boole's Laws of Thought", History and Philosophy of Logic, 24, pp. 261-288. (2003).

[11] François Dubois, Zeno Toffano, "Eigenlogic : a Quantum View for Multiple-Valued and Fuzzy Systems", Quantum Interaction. QI 2016. Lecture Notes in Computer Science, vol 10106. Springer, pp. 239-251, 2017, https://arxiv.org/pdf/1607.03509.pdf.

[12] Donald E. Knuth, "The Art of Computer Programming", Volume 4, Fascicle 0 : Introduction to Combinatorial Algorithms and Boolean Functions, Ed. Addison-Wesley Professional, (2009).(1847)

[13] Stanley Burris, (2000). "The Laws of Boole's Thought". Mdictatoranuscript (https://www.math.uwaterloo.ca/ snburris/htdocs/LT$_1$5$_C$*HAPS.pdf*) (2000), and private correspondence.

[14] Edward V. Huntington, "Sets of independent postulates for the algebra of logic". Trans. AMS 5:288-309 (1904).

[15] John Venn, "Symbolic Logic", London : Macmillan and Company, ISBE. D'Hondt and P. Panangaden 1-4212-6044-1. (1881).

[16] Schroder, E., "Vorlesungen über die Algebra der Logik", Vol. I, Anh. 6, B.G. Teubner, Leipzig. (1890)

[17] Hassler Whitney, "Characteristic functions and the algebra of logic" in Annals of Mathematics 34 (1933), pp. 40-414.

[18] Svetlana N. Yanushkevich, Shmerko, V.P. : "Introduction to Logic Design". CRC Press (2008).

[19] Howard H. Aiken, "Synthesis of electronic computing and control circuits" Ann. Computation Laboratory of Harvard University, XXVII, Harvard University, Cambridge, MA, (1951).

[20] Shannon, C. E. "A Symbolic Analysis of Relay and Switching Circuits". Trans. AIEE. 57 (12) : 713-723. (1938).

[21] Marshall H. Stone, "Linear Transformations in Hilbert Space and Their Applications to Analysis", p. 70 : "Projections". (1932)

[22] Marshall H. Stone. "The theory of representation for Boolean algebras". Transactions of the American Mathematical Sdictatorociety, 40(1):37-111, Jul. (1936)

[23] Marshall H. Stone. "Applications of the theory of Boolean rings to general topology". Transactions of the American Mathematical Society, 41(3):375-481, May (1937)

[24] Dirk Schlimm, "Bridging Theories with Axioms : Boole, Stone, and Tarski", New Perspectives on Mathematical Practices, World Scientific pp. 222-235, (2009)

[25] Garret Birkhoff, John von Neumann : "The Logic of Quantum Mechanics". The Annals of Mathematics, 2nd Ser., 37 (4), 823-843 (1936)

[26] John von Neumann, "Mathematische Grundlagen der Quantenmechanik. Grundlehren der mathematischen Wissenschaften", volume Bd. 38. (Springer, Berlin, 1932) 106. "Mathematical Foundations of Quantum Mechanics". Investigations in Physics, vol. 2. (Princeton University Press, Princeton, 1955)

[27] François David, "The Formalisms of Quantum Mechanics, An Introduction", Springer Lecture Notes in Physics, ISBN 978-3-319-10538-3, (2015)

[28] Nielsen, M.A., Chuang, I.L. : Quantum Computation and Quantum Information. Cambridge University Press (2000)

[29] August Stern, "Matrix logic", North-Holland, (1988).

[30] Eduardo Mizraji, "Vector logics : the matrix-vector representation of logical calculus". Fuzzy Sets and Systems, 50, 179-185, (1992).

[31] Vaneet Aggarwal and Robert Calderbank, "Boolean functions, projection operators, and quantum error correcting codes," in Proc. Int. Symp. Inf. Theory, Nice, France, pp. 2091-2095, (2007).

[32] Ryan O'Donnell, "Analysis of Boolean Functions", Cambridge University Press, 2014.

[33] David W. Cohen, "An introduction to Hilbert space and quantum logic," Springer-Verlag, (1989).

[34] Keith van Rijsbergen, "The Geometry of Information Retrieval", Cambridge University Press, Cambridge (2004).

[35] Barros, J., Toffano, Z., Meguebli, Y., Doan, B.-L., "Contextual query using bell tests", In : Atmanspacher, H., Haven, E., Kitto, K., Raine, D. (eds.) QI 2013. LNCS, vol. 8369, pp. 110-121. Springer, Heidelberg (2014). doi:10.1007/ 978-3-642-54943-4 10

[36] Peter Wittek, "Quantum Machine Learning. What Quantum Computing Means to Data Mining", Academic Press Elsevier, Amsterdam, 2014

[37] E. D'Hondt and P. Panangaden, "Quantum weakest preconditions". Mathematical Structures in Computer Science, 16, pp. 429-451,(2006).

[38] Ying, M.S., "Foundations of Quantum Programming", Morgan Kaufmann, (2016).

[39] Pierre Cartier, "A mad day's work : from Grothendieck to Connes and Kontsevich The evolution of concepts of space and symmetry", Journal : Bull. Amer. Math. Soc. 38 (2001), 389-408.

[40] Zeno Toffano and François Dubois : "Interpolation Methods for Binary and Multivalued Logical Quantum Gate Synthesis", presented at TQC2017, Paris, France, June 14-16, 2017, https://arxiv.org/pdf/1703.10788.pdf

[41] Emmanuel Haven, Andrei Khrennikov, "Quantum Social Science", Cambridge University Press, (2013).

[42] Busemeyer, J.R., Bruza, P.D., "Quantum models of cognition and decision", Cambridge University Press (2012)