

L'aventure des nombres

Gilles Godefroy

Leçon de Mathématiques d'aujourd'hui (mai 99-Bordeaux)

Je vais parler essentiellement de deux choses ici, à savoir, d'une part, de l'histoire des mathématiques et d'autre part de certains aspects de l'arithmétique. Mais je voulais, par avance, m'excuser de la chose suivante : je ne suis spécialiste ni de l'histoire des mathématiques ni de l'arithmétique donc toutes les critiques constructives comme on dit seront les bienvenues. De plus, il s'agit certes de leçons de mathématiques d'aujourd'hui mais je vais commencer par parler de mathématiques d'hier et même d'avant-hier. Ensuite, progressivement, on arrivera, j'espère, à des mathématiques un peu plus contemporaines.

1 Que nul n'entre ici s'il n'est géomètre

En fait, je vais commencer mon histoire aux environs de l'an 530 avant J.C. Je vous parlais d'avant-hier, vous voyez que je n'avais pas menti ! Alors, dans le sud de l'Italie, dans ce qu'on appelait la Grande Grèce (la ville de Crotona, par exemple), l'école pythagoricienne est très active. On possède extrêmement peu de documents, naturellement, sur cette école et en particulier aucun document contemporain n'existe. On n'a que des commentaires beaucoup plus tardifs. Il est donc très difficile de savoir vraiment ce qui se faisait et comment cette école travaillait. On n'est même pas tout à fait certain de l'existence historique de Pythagore. Il se peut que ce soit une sorte d'analogue antique de Bourbaki. Vous savez tous que Bourbaki n'existe pas en tant que personne physique. Mais, dans 3000 ans, ce sera peut-être un peu plus difficile de savoir que Bourbaki n'a jamais existé physiquement, même si nous, on le sait ! Le même phénomène peut jouer sur Pythagore ou sur Euclide car on ne sait rien de leur biographie. C'était peut-être un groupe de personnes. Quoiqu'il en soit, il y a une activité qu'on peut en partie qualifier de scientifique et une théorie qu'on peut essayer de reconstituer un petit peu.....

Leurs mathématiques étaient de la pure mathématique discrète et disons géométrique. On peut penser qu'ils étaient en particulier influencés par l'astronomie de l'époque, qui était déjà développée, et par l'idée qu'on constate tous en levant les yeux au ciel la nuit, à savoir que les constellations sont formées

d'étoiles qu'on peut, disons, identifier à des points. Entre ces étoiles, on peut créer des alignements. C'est ce que les astronomes font, ou faisaient autrefois, pour identifier les constellations. Donc, ça peut amener à des mathématiques discrètes ou géométriques. D'autre part, on pense que l'école pythagoricienne avait déjà une théorie de l'harmonie. En particulier, ils pouvaient avoir constaté que lorsqu'on fait vibrer simultanément des cordes, par exemple les cordes d'une lyre, le son produit est harmonieux quand les rapports des longueurs sont des rationnels de petit numérateur et dénominateur, en utilisant notre terminologie. De nos jours, on connaît la transformée de Fourier, donc on comprend un petit peu mieux, mais on peut dire qu'on fait de l'analyse harmonique précisément depuis le temps des pythagoriciens. À leur époque, ils n'avaient pas tous ces outils d'analyse et assez naturellement, ils pouvaient être amenés à tirer des conclusions un peu métaphysiques de ces considérations. Par exemple, ils pouvaient être amenés à percevoir l'idée d'une longueur unité. Il est clair que si l'espace est indivisible, c'est-à-dire si on ne peut pas diviser indéfiniment une longueur donnée, et s'il existe en quelque sorte une longueur minimale, eh bien, toute longueur est un multiple entier de cette longueur minimale et par conséquent, tous les rapports de longueur seront des rationnels dans notre terminologie. On peut donc penser que c'était une partie de leur théorie. D'autre part, ils devaient connaître au moins dans les cas particuliers et peut-être de façon expérimentale, ce qu'on appelle aujourd'hui le théorème de Pythagore. Au niveau expérimental, il n'y a guère de doute qu'ils en avaient connaissance. Il y a des tablettes mésopotamiennes du 16^{ième} siècle avant J.C. où on a déjà une valeur de $\sqrt{2}$ avec 4 chiffres sexagésimaux significatifs après la virgule. Donc 1000 ans avant les pythagoriciens, on connaissait déjà $\sqrt{2}$ avec une précision supérieure à 10^{-6} , ce qui ne peut pas venir d'un simple calcul sur une figure. On peut penser que les pythagoriciens, qui sont venus bien après, avaient des connaissances de ce type. Essayons de parler d'un cas particulier simple et important qui est rapporté dans le dialogue du Ménon de Platon où on voit Socrate amener un esclave question après question à la découverte de ce cas particulier du théorème de Pythagore. D'abord on juxtapose 4 carrés de côté 1. On trace les diagonales correspondantes (voir Fig. 1). On constate que la surface du carré central de cette figure est formée de 4 demi-carrés et comme $4 \times \frac{1}{2} = 2$, ce carré central a pour surface 2 et par conséquent, on en déduit aisément, comme Socrate le fait faire à son esclave, que le côté du carré correspondant a une longueur dont le carré est égal à 2.

Je ne prétends pas vous apprendre grand chose avec ce résultat. Je vous rappelle seulement l'usage pédagogique que Socrate avait pu en faire. Bien entendu, ce type de considération ne pouvait qu'amener les pythagoriciens ou leurs contemporains à la découverte de ce qu'on appelle aujourd'hui les irrationnels et à une remise en question de la nature discrète de la géométrie. Cette découverte est très difficile à dater. On ne peut pas donner en tous cas, dans l'état actuel des connaissances ni l'auteur ni la date exacte de la découverte et il n'est pas clair du tout que cela ait représenté une catastrophe pour les pythagoriciens. C'est

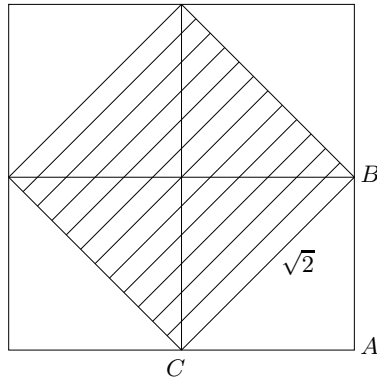


FIG. 1 – $\frac{BC}{AB} = \sqrt{2}$

une interprétation un peu tardive que cela avait provoqué mort d'hommes et on ne sait quoi.....En fait, on n'en sait strictement rien. C'est une interprétation romantique de la chose. Ce qui est certain, c'est qu'ils sont arrivés à la notion et d'une façon que je vais essayer de décrire. Dans les textes d'Aristote qui sont nettement plus tardifs, celui-ci parle plusieurs fois de la question et il parle de "l'irrationalité du rapport de la diagonale sur le côté". Ça c'est une phrase qui était probablement déjà connue telle quelle au temps de Platon. Simplement, Aristote ne précise jamais de quelle figure il s'agit, à savoir la diagonale de quelle figure et le côté de quelle figure..... Alors, bien évidemment, il semble assez naturel de penser au carré qui est le plus simple mais il y a une autre hypothèse que je vais essayer de développer maintenant puisque ça va m'amener à la suite de mon exposé ; une hypothèse, certes invérifiable, mais qui est assez séduisante, à savoir que les pythagoriciens ont pu découvrir cette irrationalité à l'aide du pentagone régulier. Le pentagone était l'un de leurs symboles mystiques d'après ce qu'on peut savoir. Voilà un pentagone régulier.

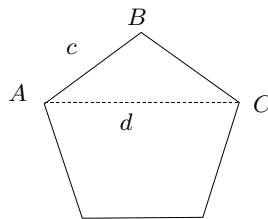


FIG. 2 – Un pentagone régulier.

Je prétends établir que le rapport de la diagonale sur le côté (égal dans la Figure 2 à $\frac{d}{c}$) est un nombre irrationnel. Comme je suis un Grec de l'époque classique, bien entendu, je ne connais pas les équations du second degré, je ne sais pas les résoudre, je ne dispose pas des notations algébriques. Je suis simplement

un géomètre un petit peu inventif. On peut commencer par remarquer que dans cette figure, il y a des pentagones réguliers absolument partout, par exemple, je peux tracer cette figure qui se trouve également être un pentagone régulier.

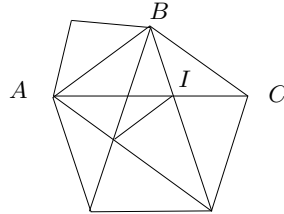


FIG. 3 –

On peut alors en déduire que toutes les diagonales de ce pentagone régulier, que je viens de tracer, ont même longueur, c'est-à-dire que $AB = AI$. D'autre part, si on revient au pentagone originel, tous les côtés ont même longueur, et donc $AB = BC$. Je vais me permettre de tracer une figure de plus et considérer ce pentagone-ci, qui est aussi un pentagone régulier :

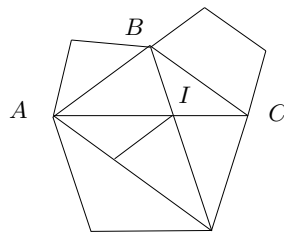


FIG. 4 –

Alors, qu'est-ce que je remarque ? Eh bien, son côté est égal à $IC = AC - AI = d - c$ et sa diagonale est égale à $BC = c$. Essayons maintenant de traduire ce qu'on a démontré. Si je calcule le rapport de la diagonale d'un pentagone régulier sur son côté, bien entendu, par similitude, ce rapport-là ne dépend pas du pentagone régulier considéré. Si on calcule, d'abord dans le grand pentagone originel puis dans le petit pentagone, on démontre, sans calcul, que

$$\frac{AC}{AB} = \frac{BC}{IC},$$

c'est-à-dire

$$(1) \quad \frac{d}{c} = \frac{c}{d - c}.$$

C'est une première chose, mais bon, je ne sais pas plus que tout à l'heure résoudre une équation du second degré. Donc, je voudrais quand même montrer que ce

rapport est irrationnel. Comment est-ce que je peux faire? Comment fait-on pour trouver la commune mesure de deux longueurs? On cherche à savoir si deux longueurs sont commensurables, donc on essaie de trouver leur commune mesure. Si on travaille avec des entiers, la commune mesure de deux entiers c'est simplement le PGCD. Si on veut travailler en langage moderne, on dit qu'on cherche le générateur de l'idéal monogène mais finalement, c'est un peu toujours la même chose! Pour faire ça, on a une méthode qui marche très bien, à savoir l'algorithme d'Euclide; en terme géométrique, c'est ce qu'on peut appeler la méthode du menuisier. On a deux planches et on veut déterminer une mesure commune à ces deux planches. On prend la plus petite et on la met un certain nombre de fois sur la grande. On coupe ce qui dépasse. Puis on prend ce qui reste et on la remet dans la petite un certain nombre de fois. On coupe ce qui dépasse, ainsi de suite... jusqu'au moment où ça tombe juste. En terme de calcul, bien sûr, c'est la chose suivante : je cherche la commune mesure à a, b . Eh bien, je commence à diviser a par b (imaginons que a soit plus grand que b). J'obtiens un quotient q_1 et un reste r_1 :

$$a = bq_1 + r_1 .$$

Si r_1 est nul, j'ai déjà terminé! Ça veut dire que b divise a . Sinon le diviseur b devient le dividende et le reste r_1 devient le diviseur :

$$b = r_1q_2 + r_2 .$$

Si j'obtiens r_2 égal à 0, j'ai déjà terminé, j'obtiens que q_2 est le PGCD ; sinon je continue. J'écris la troisième ligne :

$$r_1 = r_2q_3 + r_3 ,$$

ainsi de suite...

Chacun des chiffres effectue un mouvement diagonal (reste, diviseur, dividende) jusqu'à ce qu'on finisse par tomber sur un reste nul, ce qui bien sûr se produit dans le cas où on a des entiers. Ça permet également d'écrire le développement en fraction continue de $\frac{a}{b}$. Il est très facile de déduire de ça que

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{q_4 + \dots}}} .$$

Il y a une hypothèse selon laquelle les Grecs de l'époque classique connaissaient ce qu'on appelle maintenant le développement en fraction continue. C'est bien décrit dans un livre de D. Fowler, *The Mathematics of Plato's Academy, A New Reconstruction* qui est assez fascinant mais tout cela reste hypothétique. On manque bien entendu de textes contemporains pour soutenir cela. Il ya deux arguments qui plaident en cette faveur. L'un est que l'expression de rationnels comme somme

d'inverses d'entiers est quelque chose que les Egyptiens pratiquaient et qui a pu influencer les Grecs. L'autre est que, dans des textes comme ceux d'Aristote, il y a deux termes distincts qui sont employés pour désigner les irrationnels. Ils utilisent, d'une part, le terme "alogos" et d'autre part, le terme "arhetos". La distinction faite apparemment au temps des Grecs de l'époque classique entre deux formes d'irrationnels peut indiquer qu'ils connaissaient le développement en fraction continue des algébriques de degré 2, qu'ils savaient qu'ils étaient périodiques mais ne savaient pas ce qui se passait pour la racine cubique de 2, qu'ils avaient étudiée dans le problème de la duplication du cube, ou d'autres nombres de ce type. Donc ils pouvaient avoir accès, à la notation près, au développement en fraction continue je viens d'essayer de décrire ici.

Alors qu'est-ce qui se passe dans le cas où on a le rapport des diagonales du pentagone régulier sur le côté? Si je fais cette suite de divisions, c'est-à-dire si j'effectue l'algorithme d'Euclide sur ceci, ça commence par

$$d = c + (d - c).$$

Mon premier quotient est égal à 1, le reste à $d - c$. L'opération suivante, c'est

$$c = (d - c) + (2c - d),$$

et ainsi de suite. Mais je ne vais pas tellement écrire la suite puisque je m'aperçois, à l'aide de l'équation (1), qu'entre la première ligne et la deuxième, je n'ai absolument rien gagné. Donc la méthode "patine". Je peux continuer indéfiniment, je ne tomberai jamais sur un reste nul et par conséquent, ce rapport est effectivement un nombre irrationnel. En termes géométriques, cela signifie que je continue à tracer des pentagones réguliers interminablement, et je ne tombe jamais bien entendu sur le vide. Ça nous donne évidemment tout de suite le développement en fraction continue de ce rapport : c'est un développement où tous les quotients sont égaux à 1. Vous connaissez tous ce nombre-là qui a été appelé au 19^{ème} siècle, le nombre d'or. Je ne sais pas si les Grecs lui donnaient un nom particulier et bien entendu, comme nous avons appris à résoudre les équations du second degré, nous savons tous que ce nombre est égal à $(1 + \sqrt{5})/2$. Mais on n'a pas du tout besoin de ça pour démontrer l'irrationalité du rapport de la diagonale sur le côté d'un pentagone régulier. Le raisonnement ci-dessus marche tout à fait. Les Grecs de l'époque classique devaient être conscients de tout ça et bien entendu, ils n'aurait pas été eux-mêmes s'ils n'avaient pas cherché à théoriser toutes ces questions. En effet, ils ne sont pas restés les bras croisés devant ce défi. La théorisation est due, ou en tous cas, est contemporaine à l'école de Platon et elle est traditionnellement attribuée à Eudoxe qui a dû, à peu près, vivre de -408 à -355 avant J.C. Il fallait une définition de ce qu'on pouvait appeler un nombre. Assez naturellement, dans le contexte de l'époque, les Grecs ont réagi en terme de nature géométrique. Ce qu'Eudoxe va appeler un nombre, c'est un rapport de deux grandeurs de même genre. "Du même genre", voulant dire, dans le contexte qu'on peut comprendre,

deux longueurs, deux surfaces, deux volumes. C'est une définition qui en vaut certainement une autre. Mais se posent immédiatement deux problèmes : d'une part, l'égalité entre deux nombres et d'autre part la comparaison entre deux nombres. Pour formaliser l'égalité, on a des outils géométriques que les Grecs ont développé dans le livre d'Euclide. Si je veux l'égalité entre deux rapports de grandeur, je fais ce qu'on fait encore de nos jours en troisième, j'utilise le théorème de Thalès. Le théorème de Thalès nous dit exactement que $\frac{OB}{OA} = \frac{OB'}{OA'}$.

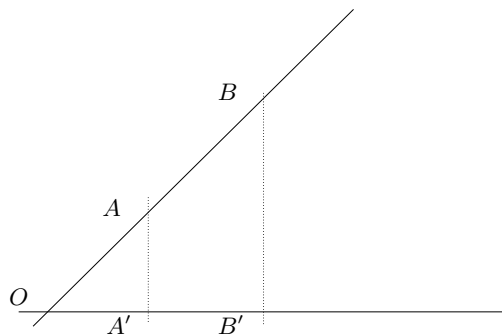


FIG. 5 – Le théorème de Thalès

Thalès théorise très bien l'égalité entre deux nombres. Maintenant vient le problème de la comparaison qui est un problème nettement plus délicat d'un point de vue géométrique. Dans les notations modernes, Eudoxe a simplement réagi comme ça : on va dire que $a \leq b$ si chaque fois que $m/n \leq a$ alors $m/n \leq b$. Bien entendu, ça n'est pas écrit comme cela, a et b étaient eux-mêmes des rapports et au lieu de faire des divisions, on faisait des multiplications mais ça revient exactement au même. Il faut noter que la définition d'Eudoxe a permis de se passer d'une unité puisqu'on définit un nombre comme un rapport. Nous savons tous que cette définition est théoriquement forte puisque c'est essentiellement celle qu'a reprise Dedekind en 1858, après avoir lu Eudoxe d'ailleurs, pour définir les réels par ce qu'on appelle les coupures. Donc c'est une idée en fait très moderne de voir un nombre comme une infinité de nombres rationnels, c'est-à-dire comme l'ensemble des nombres rationnels qui sont plus petits. Les Grecs étaient conscients que ça posait, malgré tout, un problème aigu, à savoir, qu'un nombre se trouvait être identifié à une infinité de nombres plus simples. Cette idée, d'un point de vue moderne, a permis des tas de choses. Un nombre idéal, définition qu'a justement reprise Dedekind, c'est un ensemble de nombres. C'est un peu la même idée. Mais le fait de devoir manipuler l'infini était quelque chose de perçu comme gênant par les Grecs de l'époque classique.

Malgré l'aspect très fort de cette théorie, il y a, en un certain sens, deux points faibles. Le premier, c'est sa nature géométrique, à savoir que ça conduit naturellement à l'absence de 0. Comme on ne peut pas représenter une longueur nulle,

on ne travaille qu'avec des nombres strictement positifs et les Grecs n'avaient pas une algèbre suffisamment développée pour avoir la notion de 0 et à fortiori la notion de nombres négatifs. Le fait qu'ils aient influencé si profondément notre culture scientifique fait que ces nombres sont apparus et ont acquis droit de cité nettement plus tard, en tout cas en Europe. Les négatifs sont apparus pratiquement en même temps que les nombres complexes au moment où les algébristes italiens ont résolu l'équation du troisième degré, environ en l'an 1600. La nature géométrique de leur théorie a donc eu une grande influence historique. Pour la même raison, il n'y a pas d'infinitésimaux. C'est assez piquant de voir que Leibniz, au 17^{ième} siècle, quand il introduit les infinitésimaux, quand il les manipule, précise qu'aucune construction ne peut montrer un tel accroissement. C'était quelque chose de fondamentalement nouveau par rapport à l'approche grecque des nombres. Si j'ai parlé de tout ça, c'était pour essayer de faire un petit parallèle avec un événement scientifique moderne qui, peut-être, peut se comparer avec la découverte des irrationnels par les pythagoriciens. C'est ce que les logiciens ont pu faire au 20^{ième} siècle et que je vais essayer d'expliquer maintenant. Mais avant de passer à l'époque moderne, je voudrais faire une petite récréation, un petit intermède qui va nous permettre d'établir un lien entre l'école pythagoricienne et les travaux modernes des logiciens.

2 La suite de Fibonacci

Je prends des nombres comme cela :

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, \dots$$

Bien entendu, tout le monde reconnaît la suite de Fibonacci qu'on définit par récurrence

$$f_0 = 0, f_1 = 1, \text{ et } f_{n+2} = f_{n+1} + f_n.$$

Cette suite est effectivement apparue sous une forme de récréation mathématique dans un livre de Léonard de Pise qu'on connaît sous le surnom de Fibonacci. Léonard de Pise a vécu de 1180 à 1250. C'était un mathématicien impressionnant à beaucoup d'égards et on lui doit en particulier l'importation des notations arabo-indiennes et des algorithmes de multiplication et de division modernes en Europe. Il a été peut-être le précurseur de la renaissance italienne en Algèbre et il a permis de convertir l'Europe aux méthodes modernes de calcul qui ont été les méthodes dominantes, jusqu'à l'invention des calculettes en tous cas. Il est clair qu'à son époque la science arabe dominait complètement les mathématiques mondiales. Son père commerçait avec l'Afrique du Nord. Léonard de Pise a vécu à Bougie, a reçu un enseignement compétent là bas et il a réimporté tout ça en Europe. Il a aussi certainement contribué de façon originale, bref c'était quelqu'un de très remarquable ! Cette suite est introduite dans un de ses livres pour décrire

la croissance d'une famille de lapins sur une île déserte. C'était un prétexte, car à l'époque, il ne pouvait pas donner des problèmes abstraits. Alors pourquoi s'intéresser à cette suite ? Un grand classique de Mathématiques Spéciales vous dit que

$$f_n = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n .$$

De ça, se déduit immédiatement que $\frac{f_{n+1}}{f_n}$ tend vers le nombre d'or dont il a été question précédemment

$$\lim_{n \rightarrow +\infty} \frac{f_{n+1}}{f_n} = \frac{1 + \sqrt{5}}{2} .$$

Donc, en fait, on a les réduites du développement en fraction continue de $(1 + \sqrt{5})/2$. Cette suite-là peut donc être vue comme une approximation discrète de ce qu'on a fait tout à l'heure avec le pentagone régulier, du rapport de la diagonale sur le côté. On peut voir ça comme une sorte de curiosité mais c'est en fait un peu plus que cela. On effectue l'algorithme d'Euclide sur deux termes consécutifs de la suite de Fibonacci

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1}, \\ f_n &= f_{n-1} + f_{n-2}. \end{aligned}$$

On doit bien sûr opérer jusqu'à tomber sur $f_1 = 1$ pour trouver le PGCD et montrer en particulier que deux termes consécutifs sont premiers entre eux. C'est le nombre maximal d'opérations pour des nombres de cette grandeur-là. Donc la suite de Fibonacci joue un rôle crucial d'exemple pour l'identité de Bezout. Assez naturellement, si on pense que c'est une approximation discrète, arithmétique du problème géométrique soulevé précédemment, on a la formule

$$f_{\text{PGCD}(n,k)} = \text{PGCD}(f_n, f_k) .$$

Cette suite est un ensemble de nombres qui est stable par prise de PGCD. Finalement ça n'a rien d'extraordinaire : si on pense que l'ensemble des puissances du nombre d'or est stable par l'algorithme d'Euclide, il est assez naturel que son approximation arithmétique vérifie cette propriété. Là aussi, ça peut être vu comme une simple curiosité et pourtant, j'ai parlé de cela pour préparer ce qui viendra vers la fin de l'exposé, à savoir l'usage qui a été fait par Robinson et Matijasevic, très récemment en 1970, de la suite de Fibonacci et des identités qu'elle satisfait dans la solution du 10^{ième} problème de Hilbert. Cet objet fait le lien entre les travaux platoniciens ou pythagoriciens et les travaux qui sont vraiment pour nous des travaux contemporains.

3 Du paradis que Cantor a créé pour nous

Je vais maintenant passer aux temps modernes ou presque modernes avec les travaux de Cantor, mais je ne peux pas parler de ce que les logiciens ont pu faire sans rappeler ce que Cantor a introduit, pourquoi il l'a introduit et le type de questions que ça a amené. Alors de quoi va-t-on partir ? Je vais me situer vers le milieu du 19^{ième} siècle et on va revenir à cette très vieille idée pythagoricienne de l'étude des cordes vibrantes. Eux bien sûr le faisaient d'une façon expérimentale, sans doute intuitive. Evidemment, aux alentours de l'an 1800, les choses sont tout à fait différentes. Si on fait vibrer une corde entre deux points, si je calcule l'ordonnée y en fonction de l'abscisse x du temps, j'ai une équation aux dérivées partielles qui va être

$$\frac{\partial^2 y}{\partial t^2} = c^2 \frac{\partial^2 y}{\partial x^2}.$$

C'est l'équation des cordes vibrantes ! Si la corde est homogène, la quantité c est une constante. C'est une quantité qui décrit les propriétés physiques de la corde. Quelle a été l'importance de cette équation dans l'histoire de l'analyse ? On peut résoudre cette équation de la façon suivante :

$$y(x, t) = F(ct + x) + G(ct - x),$$

où F et G sont des fonctions pratiquement arbitraires. Autrement dit, on peut voir la vibration de la corde comme la superposition de deux ondes qui se déplacent dans deux directions opposées, et les fonctions F et G sont essentiellement quelconques, en tout cas dans l'esprit du 19^{ième} où tout était C^∞ et il n'y avait pas de problème de ce genre. Pourquoi est-ce important ? Aux alentours de 1730, D. Bernoulli avait eu cette idée tout à fait remarquable : la vibration d'une corde doit être une superposition de vibrations sinusoïdales, c'est-à-dire de vibrations simples, où on a un nombre fini de noeuds. Comme on a des fonctions essentiellement arbitraires dans l'écriture de la solution y , il faut bien que ces vibrations soient des superpositions de vibrations simples et donc que ces fonctions puissent s'écrire comme des sommes de sinus. Si n'importe quelle vibration est une superposition de vibrations simples, n'importe quelle fonction va être une somme de sinus. Alors 1730, ça fait un petit peu tôt et l'idée n'a pas été reçue à l'époque mais elle est revenue à la surface avec les travaux de Fourier en 1807. Fourier a obtenu le développement en série de Fourier d'une fonction périodique qu'on peut écrire

$$f(x) = \frac{a_0}{2} + \sum_{n=1}^{+\infty} a_n \cos(nx) + \sum_{n=1}^{+\infty} b_n \sin(nx),$$

d'une façon tout à fait non rigoureuse, bien sûr, à l'époque, mais l'idée de base était là et on sait combien cela est devenu important par la suite. Alors, dès le moment où on pose une équation de ce genre, arrivent deux questions. Etant donné f , comment calculer les a_n et les b_n ? Pour les fonctions intégrables, cette

question-là est assez simple, au moins en théorie.....La question inverse se pose aussi. Etant donnés les a_n et les b_n , comment fait-on pour reconstituer f ? Ça, c'est considérablement plus difficile, tellement difficile, que deux siècles après, le sujet n'est pas encore épuisé. Il existe diverses méthodes, par exemple, le théorème de Carleson pour les fonctions L^2 , la totalisation de Denjoy et des choses de ce genre, toutes difficiles et profondes. Mais ce qu'on peut se demander, et ce qu'on se demandait déjà à l'époque de Cantor, c'est la chose suivante : est-ce que du moins, on a injectivité de l'application

$$(a_0, a_n, b_n) \longrightarrow f ?$$

C'est-à-dire, si on a

$$\lim_{N \rightarrow +\infty} \left(\frac{a_0}{2} + \sum_{n=1}^N a_n \cos(nx) + b_n \sin(nx) \right) = 0$$

pour tout x , est-il vrai que $a_0 = a_n = b_n = 0$, pour tout n ? Cette question simple à formuler n'est pas totalement évidente mais Cantor y a répondu positivement en 1871. En fait, sa méthode permet même de démontrer un petit peu mieux. Il montre qu'une série est identiquement nulle dès que sa somme est nulle pour tout $x \in [0, 2\pi] \setminus F$, où F est un ensemble fini arbitraire, puis il montre que cela reste vrai si la somme se trouve être nulle pour tout $x \in [0, 2\pi] \setminus G$, où G est un ensemble avec un nombre fini de points d'accumulations, et puis c'est encore vrai si la limite est nulle en dehors d'un ensemble H dont l'ensemble des points d'accumulations n'a qu'un nombre fini de points d'accumulations et puis on continue comme cela.....oui mais jusqu'où? Je vais essayer d'expliquer comment cela a amené Cantor à faire "démarrer" la théorie des ensembles. Essayons d'introduire une notation qui permette d'expliquer cela un petit peu mieux. Si j'ai un sous-ensemble F d'un segment, par exemple $[0, 2\pi]$, je note F' son *ensemble dérivé*, c'est-à-dire l'ensemble de ses points d'accumulations. Cantor montre donc qu'une somme trigonométrique est identiquement nulle dès qu'elle est nulle pour tout x en dehors d'un ensemble F fini, ou tel que F' soit fini, ou tel que $F'' = (F')'$ soit fini... Le résultat de Cantor va s'appliquer aux ensembles F dont l'un des dérivés $F', F'' \dots F^{(n)}$ est fini (ce qui revient à dire que le dérivé suivant est vide). Mais, en fait, Cantor va aller beaucoup plus loin que ça. Même si à son époque, il n'y avait aucune notation, aucun concept qui permettait d'aller plus loin, Cantor va y parvenir en créant les entiers transfinis et en introduisant son idée centrale qui est *l'idée de la diagonalisation*. Suivons le dans sa découverte et partons de l'ensemble

$$F_1 = \left\{ -\frac{1}{n}, n \geq 1 \right\} \cup \{0\}.$$

Il n'est pas difficile de montrer que

$$F_1' = \{0\}.$$

Si l'on considère maintenant

$$F_2 = F_1 \cup \left\{ -\frac{1}{n} - \frac{1}{2n^2k}, n, k \geq 1 \right\},$$

on voit que $F_2' = F_1$ et donc $F_2'' = \{0\}$. On peut alors utiliser cette technique pour construire un ensemble F_n tel que

$$(F_n)^{(n)} = \{0\}.$$

Comment faire pour en déduire l'existence d'un ensemble F_ω tel que

$$F_\omega^{(n)} \neq \emptyset$$

pour tout n , mais tel que

$$\bigcap_{n \geq 1} F_\omega^{(n)} = \{0\}?$$

La construction de F_ω utilise l'idée de la diagonalisation : on commence donc par construire, pour tout n , un sous ensemble F_n de l'intervalle $[-\frac{1}{2n}, -\frac{1}{2n+1}]$, tel que $(F_n)^{(n)}$ soit réduit à un point. On considère alors l'ensemble

$$F_\omega := \left(\bigcup_{n \geq 1} F_n \right) \cup \{0\}.$$

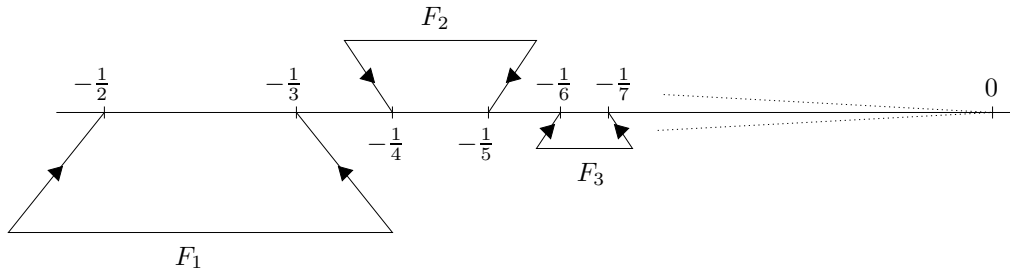


FIG. 6 – La construction de l'ensemble F_ω .

Si on considère les sous-ensembles dérivés, on a

$$F_\omega^{(n)} \neq \emptyset, \quad \forall n \geq 1,$$

et

$$\bigcap_{n \geq 1} F_\omega^{(n)} = \{0\}.$$

L'ensemble réduit à $\{0\}$ est un dérivé d'ordre infini de F_ω . C'est ce qu'on note, depuis Cantor,

$$F_\omega^{(\omega)} := \bigcap_{n \geq 1} F_\omega^{(n)}.$$

Cet ω n'existait pas avant Cantor. Il a été amené à l'introduire en étudiant les sous-ensembles fermés de la droite qu'il a étudiés à cause de ce problème d'analyse harmonique. Bien entendu, je peux continuer. Je peux considérer des copies G_n de l'ensemble F_ω contenues dans $[-\frac{1}{2n}, -\frac{1}{2n+1}]$ et les coller en définissant

$$Z := \left(\bigcup_{n \geq 1} G_n \right) \cup \{0\}.$$

J'obtiens un ensemble Z , où cette fois-ci, le dérivé d'ordre ω sera une suite convergente vers 0. Il faut que je prenne un dérivé de plus pour obtenir un point. Alors, à ce moment-là, le dérivé d'ordre (ce qu'on appelle maintenant) $\omega + 1$, est réduit à un point et le dérivé d'ordre $\omega + 2$ est vide. Il faut continuer comme cela. Je suis en train d'étudier la complexité des sous-ensembles fermés dénombrables de la droite réelle. La question qui s'est alors posée à Cantor, c'est "jusqu'où va-t-on ?" On est sorti du cadre des entiers mais jusqu'où peut-on continuer ? On peut remarquer qu'on manque de notations pour indexer cette construction. J'ai noté $\omega, \omega + 1$ mais en un certain sens, tout est à créer quand on arrive à ce point-là. Cette diagonalisation est certes très utile en analyse mais il faut reconnaître que, en un certain sens, la *réurrence transfinitie*, quand on l'utilise, est la porte ouverte à un certain nombre de problèmes conceptuels ou existentiels. Pour fabriquer le fermé dont le dérivé d'ordre ω est un point, j'ai utilisé la totalité des fermés d'ordre précédents. L'idée de base de la diagonalisation, c'est de construire un objet à partir d'une infinité d'objets préalablement construits. Bien entendu, 130 ans après, on s'est tous donné le droit de faire ça. Il y a très peu de mathématiciens d'aujourd'hui qui considèrent cela comme illicite. A l'époque de Cantor, ça n'était absolument pas clair parce qu'on effectue une opération qui, en un certain sens, est concrètement impossible. C'est ce qu'on appelle en termes philosophiques *l'infini actuel*, que sous-entend l'usage de la diagonalisation. Cantor se pose la question suivante : comment indexer cette construction ? Eh bien, on va l'indexer de la façon suivante : quand on fait une construction finitiste, un objet après l'autre, on l'indexe naturellement avec les entiers naturels \mathbb{N} . Le principe de récurrence repose sur le fait que tout sous-ensemble d'entiers non vide a un plus petit élément. Au lieu de faire une récurrence simple, Cantor veut faire une récurrence au-delà du fini, *une récurrence transfinitie*. Il est amené à transposer ce qui sert de base à la récurrence, à savoir à considérer des ensembles bien ordonnés, c'est-à-dire des ensembles tels que tout sous-ensemble non vide a un plus petit élément. C'est donc un ensemble muni d'une structure d'ordre qu'on appelle *un bon ordre*. Qu'est-ce, alors, qu'un ordinal ? C'est-à-dire qu'est-ce que l'objet dont se sert Cantor pour indexer sa construction ? C'est, en théorie des ensembles très naïve, "un type de bon ordre", c'est-à-dire une classe d'équivalence d'ensembles bien ordonnés pour la relation "il existe une bijection croissante". Alors, bien entendu, c'est en théorie des ensembles très naïve, car ça conduit à parler de l'ensemble de tous les ensembles, d'ensemble d'ensembles bien ordonnés et on va voir que ceci amène à une catas-

trophe. Alors, même si c'est bon pour l'intuition, ça n'est certainement pas très bon, et même assez mauvais, pour la logique. Depuis Cantor, tout ceci a été mieux formulé, en particulier, par Von Neumann qui a trouvé la bonne formulation : *un ordinal est l'ensemble de ses prédécesseurs*. C'est recycler un peu une idée de Shopenhauer qui disait "qu'un entier présuppose tous les précédents". C'est la même chose avec les ordinaux. L'ordinal 0, c'est l'ensemble vide \emptyset . L'ordinal 1, c'est l'ensemble dont l'unique élément est l'ensemble vide : $\{\emptyset\}$. L'ordinal 2, c'est l'ensemble dont les deux éléments sont l'ordinal 0 et 1 : $\{\emptyset, \{\emptyset\}\}$. L'ordinal 3, c'est : $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$On a une échelle d'ensembles sur lesquels l'appartenance coïncide avec l'inclusion : un ensemble appartient à un autre si et seulement si il est inclus dans l'autre. Alors, qu'est-ce que ω_0 , le premier ordinal infini ? Eh bien, c'est l'ensemble de tous ses prédécesseurs, c'est-à-dire

$$\omega_0 := \{0, 1, 2, \dots\},$$

et

$$\omega_0 + 1 := \{0, 1, 2, \dots, \omega_0\}.$$

Cette fois-ci, c'est la bonne formalisation des ordinaux dans la théorie moderne des ensembles. Il se trouve, pour conclure sur ce problème d'analyse harmonique, que Cantor aurait pu, avec ses méthodes, montrer qu'en effet, si la série trigonométrique converge vers zéro en dehors d'un ensemble dont un dérivé d'ordre arbitraire est vide, alors tous ses coefficients sont nuls. Mais, même si Cantor le savait et l'avait peut être démontré, il ne l'a pas formellement énoncé dans ses oeuvres. Rappelons pour les analystes que dans le cas des sous-ensembles de \mathbb{R} , on s'arrête au bout d'un ordinal dénombrable et alors tout marche bien !

Les entiers, ça sert à compter. Cantor étend les entiers et leur ordre en créant ses entiers transfinis ; il est bien naturel qu'il se demande si, avec ses nouveaux nombres, il va pouvoir compter des ensembles infinis. Donc, assez naturellement, il a été amené à considérer ce qu'on appelle aujourd'hui *un cardinal*. Essayons d'expliquer cette idée-là, en commençant par ce qu'on a tous fait dans notre enfance, à savoir compter sur nos doigts. Quand on compte un ensemble fini, par exemple, un ensemble de chaises, eh bien, je l'identifie à un sous-ensemble de l'ensemble de mes doigts ; ça c'est 1, ça c'est 2 et ça c'est 3 et puis je remarque la chose suivante : quel que soit l'ordre dans lequel je compte mes chaises, je finis toujours sur le même doigt. On a tous constaté cela depuis si longtemps qu'on ne s'en rappelle même plus ! Quand on y réfléchit, ce n'est d'ailleurs pas si évident que ça. Si l'homme de la rue nous demandait de démontrer cela formellement, eh bien ce n'est pas si clair ! Mais enfin, c'est vrai et on est tous d'accord que c'est vrai pour les ensembles finis. Cantor généralisait les entiers. C'est tout à fait naturel, dans son contexte, qu'il se soit demandé si ces nouveaux objets, ces ordinaux, lui permettaient de compter des ensembles infinis. Lorsqu'on fait ça, deux problèmes se posent. Cantor veut compter des ensembles infinis en comptant sur ses doigts, mais lui, il a une infinité de doigts. Le premier problème, c'est

que pour compter des ensembles infinis, l'ordre compte. Par exemple, si je veux compter les vrais entiers, je peux les compter

$$1, 2, \dots, 0$$

on compte le 0 à la fin et on trouve $\omega_0 + 1$. Ou bien, on peut les compter

$$1, 3, 5, 7 \dots, 0, 2, 4, 6$$

on compte les impairs puis les pairs et on trouve $\omega_0 + \omega_0 \dots$ et ainsi de suite. On s'aperçoit qu'on va trouver comme ça tous les ordinaux dénombrables. Mais évidemment ce n'est pas la bonne façon de compter. La bonne façon de compter, c'est la plus simple qui consiste à compter

$$0, 1, 2, 3, 4, \dots$$

et là on trouve ω_0 . Parmi toutes les façons qu'on a de compter un ensemble infini, ce qu'on va appeler son cardinal, c'est celui qui est issu de la façon la plus simple de compter, à savoir le plus petit ordinal obtenu lorsque j'ai compté de toutes les façons possibles mon ensemble. Cantor a tout à fait compris et analysé ce premier problème. Mais il y a un deuxième problème : est-ce que je peux faire ça avec n'importe quel ensemble? Autrement dit, est-ce que tout ensemble possède un cardinal? Avec la définition que j'ai prise des cardinaux, qui est bien sûr la bonne définition, à savoir le plus petit ordinal possible qui peut être mis en bijection avec l'ensemble, ça revient exactement à se demander si sur tout ensemble il existe un bon ordre. C'est le deuxième problème : le problème de l'existence d'un bon ordre. Ce problème a fait terriblement souffrir Cantor, au sens littéral du mot souffrir. Il a certainement participé à une dépression qui l'a accompagné pendant les 20 dernières années de sa vie. Il faut savoir que Cantor connaissait l'existence d'ensembles non dénombrables. Il avait en particulier démontré le résultat suivant :

Théorème 3.1 (Cantor) *Soit E un ensemble quelconque. Alors E ne peut pas être mis en bijection avec l'ensemble de ses parties $\mathcal{P}(E)$.*

En effet, imaginons que f soit une surjection de E sur $\mathcal{P}(E)$ et considérons

$$X := \{x \in E : x \notin f(x)\}.$$

Alors c'est immédiat de voir que $X \neq f(t)$, pour t quelconque puisque si $X = f(t)$ alors

$$t \in X \iff t \notin f(t) = X.$$

□

C'est bien sûr une application de la diagonalisation. En fait, c'est la même idée que la diagonalisation mais appliquée à un cadre un peu différent. En particulier,

Cantor savait que l'ensemble des nombres réels ne peut pas être mis en bijection avec l'ensemble des entiers. Donc la théorie des cardinaux était vraiment non triviale. D'autre part, il savait aussi qu'il existait des ensembles bien ordonnés non dénombrables, à savoir justement l'ensemble des ordinaux dénombrables. Si on prend ce qu'on note avec lui

$$\aleph_1 = \omega_1 = \{0, 1, 2, \dots, \omega_0, \omega_0 + 1, \dots, \omega_0 + \omega_0, \dots\},$$

c'est-à-dire l'ensemble de tous les ordinaux dénombrables, alors Cantor savait que cet ensemble là n'est pas dénombrable. S'il l'était, il serait en bijection avec l'un de ses segments propres et ça c'est impossible! Donc, d'une part, il y a des ensembles non dénombrables et d'autre part, il y a des ensembles bien ordonnés non dénombrables. La théorie était donc véritablement ouverte, non triviale et en même temps possible. Bien entendu, le premier exemple naturel d'ensemble non dénombrable, c'est l'ensemble des parties de \mathbb{N} , à savoir les réels. Il y a un ordinal non dénombrable \aleph_1 , qui est clairement le plus petit ordinal non dénombrable. La question était : est-ce que cet ordinal non dénombrable, qui semble être le candidat naturel pour mesurer la cardinalité de la droite réelle, est le bon? Autrement dit, est ce qu'on a

$$2^{\aleph_0} = \aleph_1?$$

Pour élire ce candidat, il faudrait mettre en évidence une bijection entre l'ensemble des ordinaux non dénombrables et l'ensemble des réels. Cette bijection permettrait du même coup d'établir l'existence d'un bon ordre sur l'ensemble des réels. Bien sûr, c'est ce qu'on appelle aujourd'hui *l'hypothèse du continu*. On sait depuis 1963 que ça n'est ni démontrable, ni réfutable. Donc c'est indécidable dans la théorie des ensembles qui a été formalisée depuis. Et donc Cantor ne pouvait pas y arriver, puisque dans l'état actuel de la théorie, on ne sait pas et on ne saura jamais. Mais, bien entendu, à son époque, les choses étaient moins claires et cela a été la source d'une grande souffrance psychologique. Disons quand même sur le côté positif que l'existence d'un bon ordre sur tout ensemble a été démontrée par Zermelo, en 1904, en utilisant, ce qu'on appelle aujourd'hui, l'axiome du choix. Ce qui n'est pas tellement étonnant! On cherche à bien ordonner un ensemble. De façon intuitive, je prends un élément de l'ensemble après l'autre et je dis que celui-là, c'est le premier, celui-là, c'est le deuxième, celui-là le troisième... je dois continuer cela indéfiniment et, en particulier bien sûr, une infinité de fois. Alors, est-ce qu'on a le droit ou pas de faire ça? C'est un vaste sujet! En tant qu'analyste, je suis bien sûr un très fervent croyant en l'axiome du choix. Je ne suis pas monté sur le bûcher pour avoir dit que c'est vrai, mais c'est un fait que cela permet quand même de faire de drôles de choses. Avec l'axiome du choix, disons que la porte est ouverte à l'indescriptible, comme dans le cas des irrationnels, comme chaque fois qu'on se permet de faire une infinité d'opérations. On va voir que l'indescriptible ne va faire que croître et embellir avec les années. Avant de passer à la suite, je voudrais insister sur l'une des choses les plus connues parmi

les travaux de Cantor et qui est peut-être, en un sens, la plus importante. C'est la chose suivante qui motive son étude des cardinaux : dans son article de 1874, où il montrait que l'ensemble des réels n'est pas dénombrable, c'est-à-dire ne peut pas être mis en bijection avec les entiers, on a bien sûr le corollaire suivant

Corollaire 3.2 *Il existe des nombres transcendants.*

En effet, Cantor arrive, dans cet article, à montrer, non seulement que l'ensemble des réels n'est pas dénombrable mais il réussit aussi, avec une numérotation assez simple des polynômes à coefficients entiers, à prouver que l'ensemble des nombres algébriques est dénombrable. Donc, l'ensemble des nombres transcendants, complémentaire de l'ensemble des nombres algébriques, n'est pas vide. \square

On est tous d'accord, mathématiciens de la fin du 20^{ième} siècle, sur le fait que la démonstration de Cantor est tout à fait valable. A son époque, c'était beaucoup moins clair et des mathématiciens de tout premier ordre considéraient cela comme un tour de passe-passe sans aucune valeur probante. Alors essayons de comprendre pourquoi. Cantor utilise une idée qui est tout à fait remarquable, à savoir que $\mathbb{R} \setminus \mathbb{E} \neq \emptyset$, car \mathbb{E} , l'ensemble des nombres algébriques, est petit. Autrement dit, je montre quelque chose sur un ensemble, en travaillant sur son complémentaire. Alors, en un sens, c'est une idée naturelle : un ensemble peut être beaucoup plus simple, beaucoup mieux connu que son complémentaire. Si je connais bien la France, ça n'est absolument pas pour cela que je connais bien le reste du monde ! On peut connaître quelque chose, sans connaître le reste. On travaille sur ce qu'on connaît et on essaie, avec plus ou moins de bonheur, d'en déduire quelque chose sur ce qu'on ne connaît pas. Rappelons que les analystes, les utilisateurs du théorème de Baire, par exemple, utilisent cette idée sans arrêt. On veut démontrer quelque chose sur un ensemble, on montre, par exemple, que son complémentaire est maigre ; donc on sait que l'ensemble est résiduel et donc non vide. Cette idée-là a permis énormément de choses depuis mais elle était, disons neuve, au temps de Cantor : montrer qu'un nombre transcendant existe, en ne travaillant qu'avec des algébriques, n'était pas quelque chose d'a priori évident. Je voudrais insister sur le fait qu'on utilise finalement une idée très simple : il se peut que X soit simple et son complémentaire, disons $U \setminus X$, compliqué. Je vais essayer de revenir là-dessus dans un autre cadre un peu plus loin. Il y a quand même un prédécesseur très ancien à cette idée de Cantor, qui n'a peut-être pas été reconnu comme tel à l'époque, c'est la démonstration qui figure dans Euclide de l'infinitude des nombres premiers. Supposons qu'il n'y ait qu'un nombre fini de nombres premiers, disons $2, 3, 5, \dots, p$. On fait le produit de ces nombres $2 \times 3 \times 5 \times \dots \times p$ et on rajoute 1. Le nombre obtenu $2 \times 3 \times 5 \times \dots \times p + 1$ est divisible par un nombre premier. Mais ce nombre premier ne peut être ni 2, ni 3, \dots , ni p . Donc c'est un nombre premier strictement plus grand. Personne, ni à l'époque d'Euclide, ni à l'époque de Cantor, n'a contesté la validité de cet argument. Cependant, il montre qu'il y a des nombres premiers arbitrairement

grands, sans donner aucun moyen de les exhiber. Beaucoup de gens dans cette salle à Bordeaux savent beaucoup mieux que moi que c'est très difficile d'exhiber des nombres premiers arbitrairement grands. Nous ne disposons à ce jour d'aucun procédé automatique qui permettrait d'en exhiber. C'est par contre évident pour les nombres qui ne sont pas premiers, qu'on appelle les nombres composés. C'est sûrement dur de trouver un nombre premier supérieur à 10^{200} , mais c'est très simple de fabriquer un nombre composé supérieur à 10^{200} , par exemple 10^{201} . Le crible d'Erastothène, qui exhibe les nombres premiers comme étant ceux qui ne sont pas composés, reflète cette dissymétrie. Il arrive qu'on appréhende bien un ensemble, sans comprendre son complémentaire. On a donc un complémentaire simple mais malheureusement, ce qui nous intéresse, dans ce cas-là, c'est plutôt l'ensemble compliqué. En un certain sens, cette idée peut être vue comme un prédécesseur de l'idée de Cantor et, en tous cas, comme un autre aspect où on constate la présence de cette dissymétrie.

Cela nous amène vers la fin du 19^{ième} siècle, c'est l'époque de ce qu'on a appelé *la crise des fondements*. On arrive à tous ces paradoxes de la théorie des ensembles. Cantor, qui sait donc que $\text{Card}(\mathcal{P}(E)) > \text{card}(E)$, s'aperçoit en 1896 que ça rend impossible de parler de l'ensemble de tous les ensembles puisque que l'ensemble de ses parties en serait un sous-ensemble de cardinal strictement plus gros ! Il écrit à D. Hilbert pour lui faire part de cette découverte. L'année d'après, Burali-Forti retrouve exactement le même argument. Lui, bien évidemment, il le publie, puisque ce n'est pas sa théorie qui tombe par terre avec ça, il n'a donc aucune raison de garder cela "sous le manteau". C'est alors la panique générale... Il y a un certain nombre de calembours mathématiques qui apparaissent. Par exemple, Richard parle de l'ensemble des nombres entiers qui ne peuvent pas se définir en moins de 16 mots. C'est un ensemble non vide et donc, par le principe de récurrence, il possède un plus petit élément. Son plus petit élément est "le plus petit entier qui ne peut pas se définir en moins de seize mots". On vient justement de le définir en 15 mots ! Donc il n'est pas dans l'ensemble, donc... Je ne sais pas quelle a été la réaction des auditoires de l'époque à cela, sans doute leurs cheveux se sont-ils dressés sur leur tête ! Ce qui était sûr, c'est qu'il était temps de mettre de l'ordre dans la maison.

4 Le programme de Hilbert

Cette mise au clair des notions a commencé avec Hilbert qui a, dans le même temps, permis de sauver la réputation de Cantor et peut-être d'une partie de son oeuvre. Hilbert était visiblement convaincu de la qualité des travaux de Cantor. Il a dit plus tard "du paradis que Cantor a créé pour nous, nul ne doit pouvoir nous chasser", ce qui indique qu'il était convaincu du fait que c'était le bon fondement pour les mathématiques. Il a exprimé une partie de ses convictions dans un célèbre programme, au Congrès de Paris, en 1900, où il a livré à l'attention

des mathématiciens 23 problèmes qui ont en partie servi de programmes de travail aux mathématiciens du 20^{ième} siècle. L'influence des problèmes de Hilbert a bien sûr été énorme, c'est assez fantastique! Parmi ces 23 problèmes, 3 se rapportent directement à notre sujet. C'est le problème 1, qui est exactement la question de l'hypothèse du continu, à savoir, est-ce que

$$2^{\aleph_0} = \aleph_1?$$

C'était certainement très important pour Cantor que quelqu'un de l'importance de Hilbert présente ce problème comme le premier d'une liste aussi cruciale. Le problème 2, visiblement très utile au moment de cette crise des fondements, était d'établir, à l'aide de procédés finis, la non-contradiction de la théorie des ensembles (qu'on n'appelait pas encore à l'époque ZFC, Zermelo-Fraenkel, plus l'axiome du Choix, mais je vais me permettre ce petit anachronisme). Le problème 10 était d'établir si toute équation diophantienne peut être résolue, c'est-à-dire, si on peut déterminer l'existence ou l'absence de solutions au moyen d'un algorithme. Hilbert a employé le terme "procédés réguliers". On pense interpréter sa pensée correctement en pensant à un algorithme ou un programme, au sens de l'informatique moderne. Il n'avait bien sûr pas employé ces termes-là. Par "procédés finis", là non plus, il n'a pas été très précis sur ce qu'il voulait dire. On peut penser à des calculs effectifs sur des entiers explicites. Il s'agissait de montrer la non-contradiction de l'arithmétique et si on se permet, par exemple, de faire une récurrence, eh bien, on est en train de supposer ce qu'on veut démontrer! Il faut arriver à se ramener à quelque chose de plus faible si on veut établir de façon probante la non-contradiction de quelque chose. Personne ne pouvait quand même contester que $2 + 3 = 5$, donc si on arrivait à montrer la non-contradiction de la théorie des ensembles ou de l'arithmétique, à l'aide de calculs de ce genre, disons que ça aurait certainement valeur probante. Quelle était la motivation de Hilbert? On peut penser à deux motivations. D'une part, il venait d'écrire les "Grundlage der Geometrie", où il essayait de fonder la géométrie sur la théorie des nombres réels, en particulier, et donc finalement en dernier ressort sur la théorie des ensembles et sur la nécessité de considérer des ensembles infinis. Rappelons-nous les coupures de Dedekind.... Pour que la géométrie soit fondée sur un terrain un peu solide, il fallait quand même qu'on puisse parler d'ensembles infinis, donc c'était scientifiquement nécessaire d'arriver à parler à peu près raisonnablement d'ensembles infinis, même pour démontrer le théorème de D'Alembert-Gauss d'ailleurs, dont on ne pouvait quand même pas se passer. Quant au problème 10, on peut voir une influence lointaine de Leibniz, avec cette idée de ramener ou essayer de ramener les mathématiques à un calcul automatique. La question finalement que Hilbert testait sur les équations diophantiennes c'est : est-ce qu'il existe un automate, peut être très compliqué mais enfin au moins concevable, qui lorsque je rentre une feuille avec un problème mathématique dans cet automate, me dise, après un certain temps, c'est vrai ou ce n'est pas vrai? C'était ramener

les mathématiques à un calcul automatique, et, en particulier, on pouvait tester ça sur les équations diophantiennes. Il y avait à l'époque une grosse pression pour la trivialisaiton des mathématiques. Sans vouloir dévoiler "la fin du film", heureusement pour nous, ça n'est pas possible! Ce programme ambitieux de Hilbert ou au moins une partie de ce programme, n'a pas été résolu. On peut établir un certain lien entre le problème 2 et le problème 10. Imaginons qu'on ait un automate qui permette de répondre aux questions qu'on pose dans le langage d'une certaine théorie, pensons, par exemple, à la géométrie élémentaire pour laquelle ça existe effectivement ou la théorie des corps réels du premier ordre; car il y a certaines théories mathématiques pour lesquelles un tel automate existe effectivement. On veut savoir si la théorie est contradictoire ou pas. On rentre dans l'automate un énoncé quelconque du type " P et non P " et puis l'automate, après un certain temps, sort une réponse. Si la réponse est positive, certainement, la théorie est contradictoire. Si la réponse est négative, par contre, je sais déjà que la théorie n'est pas contradictoire car si elle l'était, on pourrait démontrer n'importe quoi et en particulier " P et non P " serait vrai. Dans une théorie contradictoire, tout est vrai, y compris qu'elle ne l'est pas! et en particulier, l'énoncé " P et non P " va être vrai... Donc un seul énoncé de ce genre, avec un automate approprié, me permet de savoir si la théorie, en question, est ou non contradictoire. En particulier, si on avait un automate qui répondait aux questions de la théorie des ensembles ou de l'arithmétique de Peano, le problème de la non-contradiction serait terminé. C'est ce qu'on appelle *le problème de la décision*. La nature a voulu que les théories décidables en ce sens-là, c'est-à-dire les théories pour lesquelles existent effectivement un automate, soient des théories faibles et de toutes petites parties des mathématiques, comme la théorie des corps algébriquement clos, par exemple. Donc, encore une fois, notre travail n'est pas terminé!

5 Le vertige contemporain

Celui qui nous a permis de comprendre la complexité réelle des mathématiques, et en particulier de l'arithmétique, c'est Gödel. En 1930, il a montré que le problème 2 du programme de Hilbert n'admettait pas de réponse positive, mettant ainsi fin aux espoirs de l'école de Hilbert et de Von Neumann. Ce dernier a d'ailleurs immédiatement compris qu'il se passait quelque chose de fondamental. Les autres ont peut-être mis un petit peu plus longtemps.

5.1 Le théorème de Gödel

Alors que dit le premier théorème de Gödel? Eh bien, si j'ai une théorie τ qui contient l'arithmétique de Peano, on ne peut pas montrer la non-contradiction de τ par des procédés finis sauf si τ est contradictoire, auquel cas on peut tout

y démontrer, y compris qu'elle n'est pas contradictoire. Ça c'est vraiment un théorème très important et qui a des conséquences proprement arithmétiques qui sont, sans doute, encore très loin d'être épuisées. Je voudrais maintenant dire quelques mots, non pas sur la démonstration de ce théorème qui est très longue, difficile et très formelle, mais sur de petits éléments d'idées de démonstration. Le théorème de Gödel, comme il l'a présenté lui-même, c'est une métaphore arithmétique du paradoxe du menteur. Si je dis "je mens", est-ce que je mens ou est ce-que je dis la vérité? C'est un peu le même genre d'idées que dans la démonstration de Cantor du fait que E ne peut pas être mis en bijection avec $\mathcal{P}(E)$. Il y a un côté autoréférentiel. Je suis vrai si et seulement si je suis faux! Comment est-ce que ça marche? Un peu plus concrètement, il y a deux idées. La première, c'est ce qu'on peut appeler *la numérotation de Gödel*, qui est un analogue de la méthode pour énumérer les nombres algébriques. Je prends toutes les formules de l'arithmétique à une variable libre. Par exemple, je prends la formule

$$x \times x = x + x + x + x$$

qui est une formule de l'arithmétique à une variable libre. On emploie uniquement les symboles qui sont le langage de la théorie. Ces formules peuvent être listées de façon tout à fait mécanique et explicite. C'est-à-dire qu'on peut les numéroter à l'aide des entiers intuitifs, des entiers explicités. Cette liste, je la note

$$F_1(x), F_2(x), \dots, F_n(x), \dots$$

Il faut comprendre cela comme un dictionnaire infini où on met non seulement tous les mots mais aussi toutes les phrases de l'arithmétique. Ce dictionnaire étant écrit, du moins théoriquement, je vais considérer la formule à une variable libre suivante :

$$"F_n(n) \text{ n'est pas démontrable}."$$

Cette formule est une formule en la variable libre n , donc c'est une des formules de notre dictionnaire. Autrement dit, il existe un entier p tel que $F_p(n)$ exprime la condition " $F_n(n)$ n'est pas démontrable". Je vais maintenant considérer l'énoncé arithmétique suivant

$$G := F_p(p).$$

G est un énoncé de l'arithmétique mais qui a une interprétation métamathématique. En effet, cette idée de numérotation de Gödel permet d'établir une correspondance entre les entiers et les formules sur les entiers. Autrement dit, lorsque j'ai un énoncé sur les entiers, je peux aussi très bien le traduire en un énoncé sur les formules, et réciproquement, si j'ai un énoncé sur les formules, je peux le traduire en un énoncé proprement arithmétique. On a représenté la métamathématique, i.e. la science des formules, dans la mathématique ou la métaarithmétique dans l'arithmétique. C'est l'idée de la numérotation de Gödel. Maintenant revenons à l'énoncé G qui interprète le fait que $F_p(p)$ n'est pas démontrable. Si l'arithmétique

de Peano est non-contradictoire, l'énoncé G est vrai car s'il était faux, $F_p(p)$ serait démontrable et faux, ce qui n'est pas possible. Donc l'énoncé G est vrai et donc $F_p(p)$ n'est pas démontrable. Quant à la négation de $F_p(p)$, elle est également non démontrable, puisque sinon (toujours en supposant l'arithmétique de Peano non-contradictoire) $F_p(p)$ serait fausse, donc démontrable. Nous venons donc de montrer que si l'arithmétique de Peano est non-contradictoire, $F_p(p)$ est vraie mais que, ni elle, ni sa négation ne sont démontrables dans l'arithmétique. C'est donc une proposition de l'arithmétique qui est indécidable, au sens où ni elle ni sa négation n'admettent de démonstration. Cependant, elle est vraie. Mais, comment sait-on que cet énoncé est vrai s'il n'est pas démontré? Eh bien, il est vrai si l'arithmétique, telle que l'ont formalisée Dedekind et Peano, n'est pas contradictoire. Et comme il n'est pas démontrable dans l'arithmétique, nous voici amenés à la conclusion que la non-contradiction de l'arithmétique de Peano ne peut pas se démontrer à l'intérieur de celle-ci. En fait, on peut interpréter l'idée de Gödel comme une idée de point fixe. On a un énoncé arithmétique qui, lorsqu'on l'interprète comme un énoncé sur les formules de l'arithmétique, s'interprète en disant "je ne suis pas démontrable". Et donc l'énoncé G est vrai et non-démontrable! Bien entendu, ceci a provoqué un petit coup de tonnerre dans le monde des mathématiques de l'époque. Ce que je voudrais simplement faire pour conclure sur ce sujet, c'est essayer de vous décrire comment cette idée, cette méthode de Gödel peut avoir des conséquences beaucoup plus concrètes que cette approche un petit peu formelle, un petit peu verbale, que j'ai tentée de vous donner ici. Le théorème de Gödel est un énoncé qui peut avoir un jour de l'importance pour les vrais arithméticiens qui travaillent avec les vrais entiers. Je voudrais dire, avant de passer à la suite, que ce que je viens de faire là n'est absolument pas une démonstration du théorème de Gödel. C'est une esquisse très vague de quelques-unes des idées qu'il y a dans le théorème. Par exemple, lorsque j'ai dit "ceci est une formule en la variable libre n , donc c'est l'un des F_p ", vous comprenez qu'il y a des formalités longues et difficiles qui sont complètement éludées. La contribution de Gödel c'est beaucoup plus que de se dire simplement que cette idée-là pourrait marcher. Il y a des formalités très difficiles dans la démonstration. Je vais essayer de ramener tout ça à quelque chose d'un peu plus concret. Je vais parler d'une part d'ensembles récursivement énumérables et récursifs et puis ensuite d'ensembles diophantiens. On va revoir la suite de Fibonacci et finalement cette étrange analogie entre l'époque pythagoricienne et notre époque. Alors qu'est-ce que ces ensembles-là?

5.2 Ensembles récursivement énumérables et ensembles récursifs

Ils sont parfois appelés ensembles semi-calculables et calculables dans d'autres contextes. Je considère un sous-ensemble E de \mathbb{N} . On dit que E est *récursivement énumérable*, en s'exprimant en termes un peu vagues, s'il existe un programme \mathcal{P} (pensons à un programme informatique) tel que $n \in E$ si et seulement si le programme $\mathcal{P}(n)$, i.e. le programme \mathcal{P} appliqué à n , dit oui après un certain temps. J'ai un programme informatique \mathcal{P} qui agit sur les entiers. Je lui entre un entier n . La machine tourne. Elle finira par dire oui exactement quand n appartient à E . Elle peut ne pas se terminer si $n \notin E$. On dit que E est *récursif* s'il existe un programme \mathcal{P} tel que si $n \in E$ alors $\mathcal{P}(n)$ dit oui au bout d'un certain temps et si $n \notin E$ par contre le programme dit non. Au bout d'un temps fini, le programme \mathcal{P} va me dire si oui ou non n est dans E ou n n'est pas dans E . Si je prends par exemple l'ensemble des carrés, c'est un ensemble récursif. Mon programme consiste, n étant donné, à prendre tous les entiers qui sont plus petits, à calculer leurs carrés et à voir si je suis tombé sur n ou pas. L'ensemble des carrés est récursif, l'ensemble des nombres premiers est récursif. Les ensembles les plus naturels de l'arithmétique sont récursifs. Il y a un fait très simple :

Fait 1 : E est récursif si et seulement si E et son complémentaire $\mathbb{N} \setminus E$ sont tous les deux récursivement énumérables.

Pourquoi est-ce que c'est vrai? Eh bien imaginons que E soit récursif. Il est certainement récursivement énumérable, ça c'est évident. Son complémentaire est aussi récursivement énumérable : si E est défini par le programme \mathcal{P} , je prends le programme \mathcal{P}' qui dit "oui" quand \mathcal{P} dit "non" et qui dit "non" quand \mathcal{P} dit "oui". Certainement, ce programme va montrer que le complémentaire est récursivement énumérable. Inversement, si E est récursivement énumérable, j'ai un certain programme \mathcal{P} qui le définit. Si son complémentaire est aussi récursivement énumérable, j'ai également un programme \mathcal{Q} qui définit $\mathbb{N} \setminus E$. Puis, je fais tourner les deux programmes en simultanément $\mathcal{P}(n)$ et $\mathcal{Q}(n)$. D'après la condition que E et son complémentaire sont tous les deux récursivement énumérables, pour tout $n \geq 1$, l'un des deux va me dire "oui", au bout d'un temps fini. Dès que l'un des deux aura dit "oui", je saurai que n est dans E ou dans son complémentaire. Donc le programme simultané $(\mathcal{P}, \mathcal{Q})$ me montre que E est récursif. Ces deux choses sont donc équivalentes. \square

Un deuxième fait, un tout petit peu plus délicat :

Fait 2 : il existe un ensemble \mathcal{U} qui est récursivement énumérable non récursif. Cet ensemble est construit par une méthode d'universalité assez simple. C'est à nouveau une méthode de diagonalisation du type Cantor. Je ne vais pas vous la donner en détails et, avant d'utiliser cela, je voudrais mentionner pour les analystes l'analogie avec les théorèmes de Souslin qui montre, en 1917, qu'un ensemble est borélien si et seulement si il est analytique et de complémentaire analytique; et de plus, il existe un ensemble analytique non borélien. C'est

complètement analogue mais assez curieusement, l'analogie n'a été découverte qu'après. La théorie des ensembles récursifs a été développée par des gens qui ne connaissaient pas les travaux de Souslin et a posteriori on s'est aperçu qu'ils faisaient deux fois la même chose, en un certain sens. On retrouve ici un phénomène d'assymétrie. Si vous prenez le récursivement énumérable non récursif E , eh bien, il est plus simple que son complémentaire puisque son complémentaire n'est pas récursivement énumérable. Ainsi, il existe un programme \mathcal{P} qui, appliqué à un entier n , répondra "oui" en un temps fini si n est dans E ; par contre, si n n'est pas dans E , le programme \mathcal{P} répondra peut être parfois "non" mais pour certaines valeurs de n , il ne se terminera pas. Autrement dit, si nous faisons tourner le programme pendant dix minutes ou dix heures et que nous n'obtenons pas de réponses, nous ne pouvons rien en conclure. Est-ce qu'on peut comprendre les résultats de Gödel à ce niveau? Je vais essayer brièvement d'expliquer comment on peut les comprendre. Si j'essaie de dessiner l'ensemble des énoncés de l'arithmétique, j'ai des énoncés démontrables, des énoncés réfutables et puis une frontière bien difficile à définir : d'un côté les énoncés vrais et de l'autre les énoncés faux.

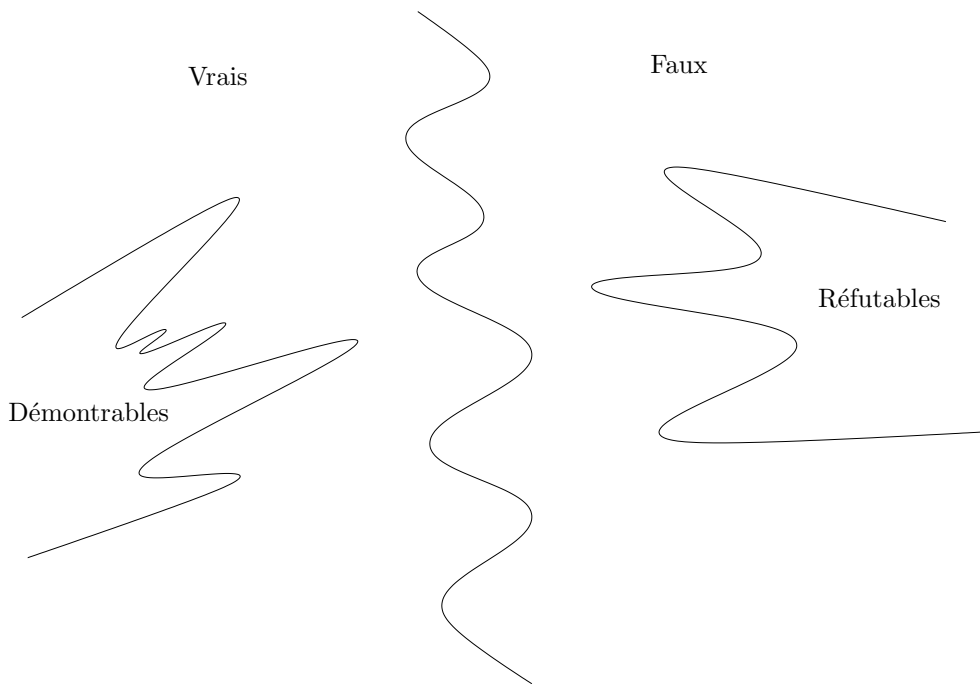


FIG. 7 – La frontière entre les énoncés vrais et les énoncés faux

Bien entendu, tous les énoncés démontrables sont vrais, tous les énoncés réfutables sont faux. Aucun énoncé n'est à la fois vrai ou faux ou alors notre modèle, i.e. le modèle des entiers intuitifs, est complètement inconsistent. Ce qui peut être démontré, c'est que l'ensemble des énoncés démontrables (on peut bien

sûr remettre tout cela dans le cadre de \mathbb{N} puisque parler d'énoncés ou d'entiers, par la numérotation de Gödel c'est la même chose) est récursivement énumérable non récursif. En gros, le programme c'est "je cherche une démonstration" et quand j'y suis arrivé, je sais que mon énoncé est démontrable! C'est ce que chacun d'entre nous fait à longueur de journée, appliquer ce programme à l'ensemble des énoncés démontrables. Bien entendu, l'ensemble des énoncés réfutables est aussi récursivement énumérable non récursif. Précisément, comme ils sont non récursifs, le fait 1 va me dire qu'ils ne peuvent pas être complémentaires l'un de l'autre. Ils sont trop complexes pour être mutuellement complémentaires. Il reste donc de la place à côté pour les vrais et les faux. Il y a une complexité trop grande. En fait, de ce point de vue là on n'est plus en analogie avec les théorèmes de Souslin; Tarski a montré qu'on ne pouvait même pas séparer les énoncés démontrables des réfutables par des récursifs. Donc, en particulier, quel que soit le modèle de l'arithmétique choisi, l'ensemble des énoncés vrais n'est jamais récursif. On ne peut donc pas formaliser la vérité en arithmétique. On peut formaliser la démontrabilité mais pas la vérité. C'est une découverte un peu fascinante de Tarski sur la nature très compliquée de cette frontière entre les énoncés vrais et faux. La frontière, elle, dépend en plus du modèle mais je ne vais pas trop m'étendre là-dessus. Vous avez différents modèles de la géométrie qu'on connaît tous. Vous avez la géométrie Euclidienne avec le postulat d'Euclide, la géométrie hyperbolique, la Riemannienne... Si vous prenez les axiomes de la géométrie moins le postulat d'Euclide, il y a des choses démontrables, des choses réfutables et des choses qui sont en dehors comme justement le postulat. La frontière vrai/faux passe d'un côté ou de l'autre de cet énoncé-là, suivant le modèle de la géométrie qu'on prend au départ. C'est également vrai pour l'arithmétique. Simplement, c'est intuitivement plus dur d'avoir des modèles non standards de l'arithmétique. Pour terminer, je voudrais traduire tout cela, en termes diophantiens, ce qui peut être fait grâce aux travaux de Robinson-Matijasevic.

5.3 Le théorème de Robinson-Matijasevic

Qu'est ce qu'un ensemble diophantien? Eh bien, la définition va presque de soi. L'usage qu'on en fait est certainement moins triviale.....Je vais donc parler là de travaux qui sont dus, d'une part, à Julia Robinson et, d'autre part, à Matijasevic. Il y a, en particulier, un séminaire Bourbaki, en 1970, sur ces travaux-là, et notamment sur les travaux de Matijasevic. Alors qu'est-ce qu'un ensemble diophantien?

Si je prends un sous-ensemble E de \mathbb{N} , on dit, par définition, qu'il est *diophantien* s'il existe un polynôme P à coefficients entiers, $P \in \mathbb{Z}[t, x_1, \dots, x_n]$ tel que

$$t \in E \iff \exists (x_1, \dots, x_n) \in \mathbb{Z}^n \text{ tel que } P(t, x_1, \dots, x_n) = 0.$$

Autrement dit, t est dans E exactement quand l'équation diophantienne corres-

pondante

$$P(t, x_1, \dots, x_n) = 0$$

a une solution (x_1, \dots, x_n) en nombres entiers. Il est à peu près évident que si E est diophantien alors E est récursivement énumérable. Quel est le programme ? Eh bien, je prends un entier t . Je veux savoir s'il est dans E . Alors mon programme va être d'essayer l'un après l'autre toutes les valeurs entières (x_1, \dots, x_n) , en ordonnant \mathbb{Z}^n , de façon propre, ce qui est très facile. Je les essaye stupidement et à la 2000 milliardième fois, je m'aperçois justement que le polynôme est nul et par conséquent j'ai démontré qu'effectivement t est dans E . Ce programme-là finira par me donner une réponse si t appartient à E . Evidemment, si je me dis "je ne vais essayer que 1000 milliards de fois" et qu'au bout de ces 1000 milliards de fois, je n'ai toujours pas trouvé 0, ça ne me dira rien. Il y a une assymétrie. Les grecs pensaient beaucoup à la symétrie parce qu'ils avaient une vision spatiale des mathématiques. Là, on dirait qu'on a une sorte de vision temporelle des mathématiques. On sait quand on commence une chose, on ne sait pas quand on la finit ! Ça c'est vraiment une assymétrie fondamentale, y compris quand on essaie de faire une démonstration. Donc, tout ensemble diophantien est récursivement énumérable. Ce qui est beaucoup moins évident, c'est le théorème de Matijasevic, à savoir que *tout ensemble récursivement énumérable est diophantien*. En fait, je peux toujours trouver un polynôme qui fait usage de programme au sens précédent. La complexité des équations diophantiennes polynomiales est suffisante pour rendre compte de tous les ensembles récursivement énumérables. Bien entendu, je ne vais pas démontrer ça. Je voudrais simplement dire que la démonstration a été faite en deux temps. Il y a d'abord le premier temps qui, je crois, doit dater des années 50 où Davis, Robinson et Putman ont montré que c'était vrai si on autorisait certaines variables à figurer en exposant dans le polynôme. Ils ont démontré que tout ensemble récursivement énumérable était exponentiellement diophantien. Ce qui leur manquait pour terminer, c'était de se ramener à quelque chose d'effectivement diophantien et en particulier d'avoir une relation à croissance exponentielle qui soit diophantienne. Je vais dire qu'une relation $R(u, v)$, entre nombres entiers (u, v) , est diophantienne si et seulement si il existe un polynôme P tel que

$P(u, v, x_1, \dots, x_n) = 0$ a une solution $(x_1, \dots, x_n) \in \mathbb{Z}^n \iff R(u, v)$ est satisfaite.

Ce que Matijasevic a démontré c'est que la relation $R(u, v)$ définie par

" v est le $(2u)$ -ième nombre de Fibonacci"

est une relation diophantienne et à croissance exponentielle. Il a montré qu'en fait, on pouvait trouver 9 polynômes, qui pouvaient se ramener à un seul, tel que la conjonction de ces équations était équivalente à $R(u, v)$. Autrement dit, on a un objet un peu intermédiaire entre l'algébrique et le transcendant. La suite de

Fibonacci a une croissance exponentielle, cependant elle est presque polynomiale. Il y a tellement de relations arithmétiques comme celle mentionnée tout à l'heure sur le PGCD qu'elles suffisent à avoir le caractère diophantien. Néanmoins, la suite a une croissance exponentielle et ça a permis de se ramener du cas exponentiellement diophantien au cas diophantien et donc de montrer cette équivalence entre récursivement énumérable et diophantien. On déduit assez facilement du théorème de Robinson-Matijasevic qu'on a les 2 résultats intrigants suivants, qui bien sûr étaient la motivation pour tout cela.

Corollaire 5.1 *Le 10-ième problème de Hilbert a une réponse négative : il existe une équation diophantienne sans solution dont aucun programme ne peut montrer qu'elle n'a pas de solutions.*

Autrement dit, si vous avez un automate, vous pouvez toujours fabriquer une équation diophantienne pour laquelle cet automate ne sera pas capable de vous dire si oui ou non elle a des solutions. L'arithmétique n'est pas terminée et elle ne le sera jamais, en un certain sens. La deuxième chose, c'est qu'on peut traduire l'énoncé de Gödel en terme diophantien. L'énoncé "l'arithmétique de Peano est non-contradictoire" peut se traduire effectivement en une équation diophantienne.

Corollaire 5.2 *Quelle que soit l'axiomatisation de l'arithmétique utilisée, il existe un polynôme P , à coefficients entiers, tel que l'équation*

$$P(x_1, \dots, x_n) = 0$$

n'a pas de solutions entières, mais cette absence de solutions ne peut pas se démontrer dans l'axiomatique en question.

Si vous trouvez soit une démonstration, soit une solution alors cette axiomatique est contradictoire. Donc si Peano est non-contradictoire, il y a des polynômes indémontrablement sans solutions. Là, on voit bien la différence, l'asymétrie, si vous vous rappelez de la démonstration triviale du fait qu'être diophantien implique récursivement énumérable. Quand une équation diophantienne a une solution, trouver la solution est formellement triviale. Vous essayez tous les entiers, puis un jour, vous allez la trouver ! Par contre, s'il n'y en a pas, là on est dans le complémentaire d'un récursivement énumérable, on peut être complètement dépourvu de moyens pour démontrer qu'il n'y en a pas. Autrement dit, si on disposait d'un temps infini, si on était capable de faire des démonstrations de longueur infinie, on essaierait, par exemple, tous les entiers mais vraiment tous ; ça ne serait jamais 0 et on y serait arrivé ! Simplement une démonstration, pour nous, c'est une suite finie de symboles. Avec une suite finie de symboles et en utilisant cette méthode, on ne pourra jamais établir qu'un tel polynôme n'a pas de solutions. Je dois préciser que le théorème de Robinson-Matijasevic est effectif, c'est-à-dire qu'on peut effectivement écrire ce polynôme. Dans l'état actuel des choses, je crois, qu'il a 13 variables et est de degré 5. Mais, bien entendu, c'est

juste un théorème d'existence un peu artificiel comme l'énoncé de Gödel. Il se peut très bien, par exemple, qu'il existe un polynôme à 3 variables qui soit tel que l'équation

$$P(x_1, x_2, x_3) = 0$$

n'ait pas de solutions mais de façon indémontrable dans l'axiomatique de Peano. Je voudrais aussi dire que c'est moins contre-intuitif qu'on pourrait le croire. Imaginons qu'on veuille démontrer cela. Ce qui se passe c'est que \mathbb{N} n'est pas compact. Vous ne pouvez pas uniformiser une démonstration. Imaginez que pour $x_1 = 1$, la démonstration ait au moins deux caractères, pour $x_1 = 2$, on travaille juste sur x_2 et x_3 mais il faut 4 caractères, pour $x_1 = 3$ il en faut 8 et ainsi de suite... Il n'y a aucune raison, si je considère x_1 comme paramètre, pour que la démonstration de l'absence de solution puisse être uniformisée en x_1 . Pour chaque valeur donnée de x_1 , on a peut-être une démonstration mais pourquoi pourrait-on uniformiser cela? Il n'y a aucune raison! La complexité croît peut-être arbitrairement. En fait, ce que Robinson et Matijasevic disent c'est que ça n'est pas seulement une idée théorique mais ça croît vraiment arbitrairement. Il y a d'autres aspects intéressants au fait que ça soit explicite. Par exemple, il existe un polynôme explicitement donné à coefficients entiers (24 variables, je crois) tel que les valeurs positives prises par ce polynôme soient exactement l'ensemble des nombres premiers. Donc on a envie de se dire "voilà, on a une formule qui donne tous les nombres premiers". Malheureusement, dans la nature, il y a quelque chose de diabolique, car quand on fait tourner ce polynôme, il prend pratiquement sans arrêt des valeurs négatives et le seul nombre premier qu'on ait pu expliciter avec ça, c'est 2!!!! Peut-être qu'on peut tirer de tout ça qu'il n'y a pas de formules qui donnent tous les nombres premiers? Disons, en tous cas que les espoirs qu'ont pu faire naître le côté constructif du théorème de Matijasevic, semblent buter sur un mur. Pour terminer, je voudrais dire que naturellement ces énoncés sont pour l'instant très artificiels, à peu près comme l'énoncé de Gödel. Ça existe mais c'est très loin de la pratique des arithméticiens. Mais bien entendu, on n'a pas de raisons a priori de penser que cette famille des énoncés indémontrablement vrais ne va pas se propager vers le centre de l'arithmétique. Il n'y a aucune raison que ça reste confiné dans des "trucs" artificiels. Par exemple, regardons un énoncé comme celui-là : il existe une constante C telle que

$$|\pi(x) - Li(x)| \leq C\sqrt{x} \log(x), \quad \forall x > 0,$$

où $\pi(x) := \text{card}(\{n \leq x\} \cap \mathbb{P})$ (\mathbb{P} désigne l'ensemble des nombres premiers) et

$$Li(x) := \int_0^x \frac{1}{\log t} dt.$$

Alors, sans doute, avez-vous reconnu une forme équivalente de *l'hypothèse de Riemann*. Eh bien, il n'y a pas au niveau logique, de raisons a priori pour que cet énoncé ne soit pas indémontrablement vrai. Il se peut très bien, même en prenant

une constante explicite que cette inégalité soit indémontrablement vraie. Alors, si c'est le cas, d'abord comment est-ce qu'on s'en assurera ? Je n'en sais rien ! Et j'ai du mal à l'imaginer parce que la véracité des énoncés non démontrables repose sur le fait que Peano est non-contradictoire. Si un arithméticien arrivait à démontrer cela, en supposant Peano non-contradictoire, tout le monde serait d'accord pour dire que c'est une vraie démonstration de l'hypothèse de Riemann. Si donc c'est effectivement indémontrablement vrai, je n'arrive pas à concevoir comment on le saurait. Simplement, on constatera que dans 5 siècles, l'hypothèse de Riemann n'est toujours pas démontrée et si c'est le cas, on prendra l'habitude d'en parler comme les analystes parlent de l'hypothèse du continu...de dire, si (RH) est vraie alors telle et telle chose se passent et on sera peut-être amené par l'expérience des mathématiciens à considérer cela comme un axiome. On ne peut pas, dans l'état actuel des mathématiques, exclure cette possibilité.

Remerciements : Je tiens à exprimer ma gratitude à Laurent Habsieger, qui a organisé cette conférence de “mathématiques d'aujourd'hui” à l'Université de Bordeaux I, ainsi qu'à Emmanuel Fricain, qui a bien voulu se charger de la rédaction avec beaucoup de gentillesse et de disponibilité.