Dialogue Polynomial

Socrate aimait à dire que les hommes sont mortels. Pourtant, Platon l'a rendu immortel, lui et ses interlocuteurs.
Il arrive quelquefois que les amis de Socrate quittent leur jardin éternel pour venir faire un tour chez les mortels; ils s'intéressent alors particulièrement aux développements de la philosophie et des sciences chez les humains. Ils affectent particulièrement les mathématiques, et ils ont été passionnés (et un peu jaloux) par la découverte de l'algèbre chez les arabes et les développements qui ont suivi.
Ils ont été scandalisés par Evariste Galois (on a même dit que c'était l'un de leur dieux qui avait fait mourir Galois si jeune, mais cette thèse n'est plus aujourd'hui prise au sérieux). Il a fallut toute la persuasion de Socrate pour que nos amis étudient les idées de Galois sans préjugé et admettent, par exemple, l'impossibilité de la trisection de l'angle.
L'extrait ci-dessous provient d'un dialogue entre Théétète et Hermocrate, il date de l'une de leur dernières visites chez nous vers 1930. Ici et là, ce dialogue est incomplet, mais on peut tout de même en suivre le fil.

Marc Troyanov [1]

THÉÉTÈTE Comme je te le disais donc, très cher Hermocrate, l'algèbre est une science qui avance encore en ce jour. Mais ce dont je voudrais le plus t'entretenir, c'est de la réflexion contemporaine sur les fondements de cette science.

HERMOCRATE Parle donc, très estimé Théétète, et ne me fais pas attendre davantage.

THÉÉTÈTE Eh bien, sous le nom d'"Algèbre Moderne", les gens de cette époque ont opéré une grande réorganisation de toutes les notions algébriques. La caractéristique qui frappe le plus dans cette algèbre moderne est son caractère très abstrait. Te souviens-tu par exemple de la notion de groupe ?

HERMOCRATE Certainement, les groupes sont ces familles de transformations qui préservent une structur. Par exemple une équation algébrique, chez notre ami Evariste Galois, ou une équation différentielle, chez Sophus Lie.

THÉÉTÈTE Tu appelles Galois ton ami, toi qui étais le plus hostile à ses idées !

HERMOCRATE J'avoue qu'il m'a été très difficile de le comprendre. Cette notion de groupe, précisément, ne me semblait pas assez claire. Pouvait-on admettre ces groupes dans le monde des Idées mathématiques, éternelles et immuables ? Je ne te cacherai pas qu'il m'arrive encore d'avoir quelques soupçons. Mais quel lien y a-t-il avec cette algèbre que tu appelles moderne ?

[1] petit dialogue socratique pour étudiants, rédigé en 1992 en marge d'un cours d'algèbre donné à l'Université du Québec Montréal

THÉÉTÈTE Vois-tu, très cher Hermocrate, cette nouvelle algèbre nous permet justement de donner plus de chair à ces groupes qui sont si importants dans les mathématiques d'aujourd'hui. On donne ainsi une existence autonomes aux groupes et aux autres objets de l'algèbre.

HERMOCRATE Tu veux dire les corps...

THÉÉTÈTE ...oui, les corps, les anneaux, ... les idéaux, les modules...

HERMOCRATE ...apprends-moi donc sans plus tarder, cher Théétète, cette algèbre moderne...

THÉÉTÈTE ...l'approche est axiomatique, je veux dire en cela que si tu veux définir un groupe abstrait, tu dois y penser comme un ensemble abstrait sur lequel est définie une loi de multiplication. Tu demanderas que soit satisfaites les propriétés usu...

Les dernières paroles de ce fragment-ci sont illisibles et la suite du dialogue est manquante. Nous disposons d'un autre dialogue qui à manifestement lieu le lendemain, c'est une suite du précédent.

HERMOCRATE Je te remercie, distingué Théétète, de ton enseignement sur cette nouvelle algèbre et je vois maintenant que les groupes et les anneaux sont aussi nobles que les nombres ou les figures géométriques. Mais il y a une question qui me tracasse encore.

THÉÉTÈTE Je t'écoute, excellent Hermocrate.

HERMOCRATE Ce que je n'arrive pas bien à comprendre dans l'algèbre moderne, c'est l'interprétation que l'on doit faire de l'algèbre classique.

THÉÉTÈTE Par exemple ?

HERMOCRATE L'algèbre classique s'est développée autour de la notion d'équation et non celle de corps et d'anneau. Comment discutes-tu des équations dans cette nouvelle algèbre ?

THÉÉTÈTE Il faut, pour examiner cette question, que tu me précises ce que tu entend par "équation".

HERMOCRATE C'est pourtant clair, chacun entend ce qu'est une équation.

THÉÉTÈTE Il y en a pourtant de différentes sortes. Certaines appartiennent à l'algèbre et d'autres non.

HERMOCRATE Expliques donc ta pensée.

THÉÉTÈTE Je te le demande encore une fois, définis-moi ce qu'est une équation !

HERMOCRATE Bien, si tu n'as pas d'objection, je te définirai l'équation comme un problème du type : "trouver les valeurs de la variable t pour lesquelles $f(t) = g(t)$ " où f et g sont des fonctions.

THÉÉTÈTE Cette définition me convient, tu peux même écrire l'équation sous la forme "$f(t) = 0$" sans perdre de généralité.

HERMOCRATE Certainement. Il n'y a donc pas de problème à définir ce qu'est une équation et nous nous accordons sur ce point.

THÉÉTÈTE Il nous faut pourtant être plus précis.

HERMOCRATE En quoi donc ?

THÉÉTÈTE Tu n'as pas dit ce qu'il fallait entendre par "fonction" et "variable".

HERMOCRATE Je conçois une fonction comme une suite de règles qui, appliquées à une variable, nous en produit une nouvelle.

THÉÉTÈTE Voilà une définition imparfaite, mais nous pourrons, je pense, nous en contenter. Tu vois maintenant je pense, la raison pour laquelle je disais qu'il y a plusieurs sortes d'équations.

HERMOCRATE Sans doute. Je serais néanmoins bien aise d'entendre ton explication.

THÉÉTÈTE La distinction qu'il nous faut introduire provient du fait qu'il existe deux sortes de fonctions, les algébriques et les transcendantes.

HERMOCRATE Certainement, la fonction $sin(t)$ n'est par exemple pas algébrique.

THÉÉTÈTE Nous considérerons donc que l'équation $sin(2t-5)+cos(1-t)=0$ ne relève pas vraiment de notre sujet d'aujourd'hui qui est l'algèbre.

HERMOCRATE Mais nous conserverons les équations du type $\sqrt{t+1}=t$.

THÉÉTÈTE Parfaitement. Tu me suivras, je n'en doute pas, si je te dis que toutes les équations algébriques peuvent être mises sous la forme $f(t)=0$ où f est un polynôme.

HERMOCRATE Aucun doute, l'équation dont je parlais plus haut peut s'écrire $t^2-t-1=0$.

THÉÉTÈTE Et nous voilà obligés, cher Hermocrate, de définir ce qu'est un polynôme.

HERMOCRATE Laisse moi essayer de donner cette définition, il faut bien sûr le faire dans le contexte de l'algèbre moderne.

THÉÉTÈTE Assurément.

HERMOCRATE Je dirai donc qu'un polynôme en une variable sur un anneau A est une fonction f sur A pouvant s'écrire sous la forme $f(t)=a_0+a_1t+a_2t^2+...+a_nt^n$.

THÉÉTÈTE Il te reste à préciser ce qu'il faut entendre par variable.

HERMOCRATE La variable est simplement un élément quelconque t de l'anneau A.

THÉÉTÈTE Il s'agit me semble-t-il d'une convention trop restrictive.

HERMOCRATE Et en quoi donc ?

THÉÉTÈTE Si nous reprenons le polynôme $f(t)=t^2-t-1$, il s'agit alors d'un polynôme sur l'anneau $\mathbb{Z}$ des entiers. L'équation $f(t)=0$ ne possède alors pas de solution. Si tu admet cependant d'être plus large et de permettre à la variable t de prendre des valeurs réelles alors l'équation a deux solutions qui sont le nombre d'or $\frac{1}{2}\left(1+\sqrt{5}\right)$ et son conjugué $\frac{1}{2}\left(1-\sqrt{5}\right)$.

HERMOCRATE Tu as raison, mais ton exemple montre simplement que je dois conserver une certaine liberté et permettre à la variable d'appartenir à un anneau ou à l'une de ses extensions.

THÉÉTÈTE Sans doute, mais la définition que tu donnes d'un polynôme peut encore nous poser des problèmes.

HERMOCRATE Et quel genre de problèmes, je te prie.

THÉÉTÈTE Eh bien regardons à nouveau le polynôme$f(t)=t^2-t-1$, mais cette fois sur le corps à deux éléments $\mathbb{F}_2=\{0,1\}$. On voit que pour tout t dans $\mathbb{F}_2$, on a $f(t)=1$. Selon ta définition, ce polynôme n'est pas distinct du polynôme $g(t)\equiv 1$, en particulier, il n'a pas de racine, ce qui signifie, tu t'en souviens, que l'équation $f(t)=0$ n'a pas de solution.

HERMOCRATE Tout cela me paraît fort clair, où vois-tu donc une difficulté ?

THÉÉTÈTE La difficulté, très cher Hermocrate, est que nous avons convenu que la variable t pouvait prendre ses valeurs dans une extension de l'anneau et non seulement dans l'anneau lui-même.

HERMOCRATE J'ai peur de ne pas comprendre.

THÉÉTÈTE Regardons notre exemple de plus près. Nous pouvons regarder $\mathbb{F}_2$ comme sous corps du corps à quatre éléments $\mathbb{F}_4$. Te souviens-tu de ce corps ?

HERMOCRATE Mais oui, et il est fort simple à décrire. Il contient $\{0,1\} = \mathbb{F}_2$ et deux élément supplémentaire a et a^2. Ce corps est de caractéristique 2, donc $a + a = 0$ et $a^2 + a^2 = 0$. On a aussi $a^3 = 1$, l'inverse de a est donc a^2 et comme $\mathbb{F}_4$ est un corps, il est impossible que (a+1) = 0,1 ou a , d'où a+1 = a2. De là, il est facile d'écrire les tables d'addition et multiplication pour $\mathbb{F}_4$.

Les tables ont été rendues illisibles. On espère que les experts pourront les reconstituer...

THÉÉTÈTE Je te félicite, très bonHermocrate, tu vois maintenant clairement je pense la difficulté posée par ta définition du polynôme.

HERMOCRATE Certainement, mais il me ferait plaisir de l'entendre de ta bouche.

THÉÉTÈTE Observe donc! Les polynômes étaient définis comme fonctions sur l'anneau de base. Dans notre cas, $f(t) = t^2 - t - 1$ et $g(t) = 1$ sont donc deux polynômes identiques. Mais lorsqu'on les regarde sur $\mathbb{F}_4$, on a $f(a) = 0$ et $g(a) = 1$. Il faut donc distinguer ces polynômes et considérer que f possède une racine dans $\mathbb{F}_4$.

HERMOCRATE Je te comprends à présent. Au fond il n'y a pas assez d'éléments dans $\mathbb{F}_2$ pour distinguer les deux polynômes. Mais je ne vois plus du tout comment définir la notion de polynôme et mon esprit devient obscur.

THÉÉTÈTE Il y a pourtant une solution.

HERMOCRATE Sois charitable et dis-la moi vite !

THÉÉTÈTE La solution s'appuie sur l'idée qu'il ne faut pas regarder un polynôme comme une fonction. Mais si A est un anneau, disons unitaire et commutatif, alors on peut regarder les polynômes comme des éléments d'une certaine extension $A^{\#}$ de l'anneau A. Plusieurs approches sont possibles pour définir $A^{\#}$, l'une des plus simples est la suivante : $A^{\#}$ est défini comme étant l'ensemble des suites infinies

$$f = (a_0, a_1, a_2, ..., a_n, ...)$$

d'éléments de A qui sont presque tous nuls. Il faut définir sur cet ensemble une structure d'anneau, les éléments 0 et 1 sont donnés par les suites
$0 = (0, 0, 0, ...0, ...), 1 = (1, 0, 0, ...0, ...)$.
La somme de $f = (a_0, a_1, a_2, ..., a_n, ...)$ et $g = (b_0, b_1, b_2, ..., b_n, ...)$ est donnée par

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b^0, ...).$$

et le produit par

$$f \cdot g = (c_0, c_1, c_2, ..., c_n, ...)$$

où

$$c_k = a_0 b_k + a_1 b_k - 1 + ... + a_k b_0 -$$

$A^{\#}$ est donc un anneau et A est isomorphe au sous anneau formé par les suites

$$(a, 0, 0, ..., 0, ...)$$

avec $a \in A$.

HERMOCRATE Cela ne ressemble guère aux polynômes dont j'ai l'habitude !

THÉÉTÈTE Si c'est plus commode pour toi, tu peux introduire un symbole t et écrire le polynôme $f = (a_0, a_1, a_2, ..., a_n, ...)$ sous la forme $f(t) = a_0 + a_1 t + a_2 t^2 + ... + a_n t^n$. Ce qui est important, c'est de ne pas considérer t comme une variable parcourant l'anneau A , mais comme un élément de l'extension $A^{\#}$ de A, on a en effet $t = (0, 1, 0, 0, ...)$. En fait, une fois toutes ces précautions prises, rien ne nous empêche d'utiliser les notations usuelles, d'appeler t l'*indéterminée*, de noter $A[t]$ l'anneau $A^{\#}$ et d'appeler *constantes* les éléments de A vu comme sous-anneau de $A[t]$.

HERMOCRATE Si je te comprends clairement, la notion de fonction a été évacuée au profit d'une notion abstraite de polynôme. Mais quel est à présent le lien entre cette notion de polynôme et les équations ?

THÉÉTÈTE Tu as raison de dire que les fonctions ont disparu, mais seulement de la définition des polynômes. On peut faire resurgir les fonctions d'une manière naturelle.

HERMOCRATE Et comment donc ?

THÉÉTÈTE Tu conviendras sans doute que l'ensemble de toutes les fonctions $A \to A$ forme, lui aussi, un anneau.

HERMOCRATE Certainement, je puis additionner et multiplier deux fonctions.

THÉÉTÈTE Fort bien, je noterai donc A^A cet anneau. Il existe un homomorphisme canonique entre $A[t]$ et A^A, cet homomorphisme associe à toute constante a la fonction constante $f(x) = a$ et à l'indéterminée t , la fonction identité $I(x) = x$. On peut donc penser à un polynôme comme à une fonction $A \to A$, mais il faut se souvenir que l'homomorphisme $A[t] \to A^A$ n'est pas toujours injectif.

HERMOCRATE A présent je te suis parfaitement. L'extension du domaine de définition de la variable de l'anneau A à un anneau $B \supseteq A$ correspond simplement à étudier l'homomorphisme analogue $A[t] \to B^B$. Par exemple les deux polynômes $f(t) = t^2 - t - 1$ et $g(t) = 1$ ont la même image dans $\mathbb{F}_2^{\mathbb{F}_2}$ mais ils ont des images distinctes dans $\mathbb{F}_4^{\mathbb{F}_4}$.

THÉÉTÈTE Je vois que tu as fort bien compris, excellent Hermocrate. Je crois qu'il ne te reste qu'une chose à apprendre sur cette question.

HERMOCRATE Laquelle donc ?

THÉÉTÈTE C'est que le problème que nous venons de discuter et résoudre ne se pose que dans le cas des anneaux finis. En effet si A est un anneau intègre commutatif et unitaire infini, alors l'homomorphisme $A[t] \to A^A$ est injectif. En d'autres termes, le polynôme est entièrement caractérisé par sa fonction polynomiale.

HERMOCRATE Je vois, ainsi l'origine du problème est bien dans le fait qu'il y a trop peu d'éléments dans un anneau fini pour distinguer tous les polynômes. C'est au fond évident puisqu'il n'y a qu'un nombre fini de fonctions et un nombre infini de polynômes. Mais dis-moi, d'où vient que dans un anneau intègre commutatif et unitaire infini, l'homomorphisme $A[t] \to A^A$ est injectif ?

THÉÉTÈTE C'est une conséquence fort simple du théorème bien connu disant que dans un anneau intègre commutatif, unitaire, tout polynôme de degré d a au plus d racines. Mais dis-moi, cher Hermocrate, qu'as tu appris de ton côté en fréquentant les mortels d'aujourd'hui.

HERMOCRATE J'ai appris de fort belles choses sur une nouvelle science dont les très belles vérités exercent leur pouvoir en géométrie et en analyse.

THÉÉTÈTE Et comment s'appelle cette nouvelle science ?

HERMOCRATE La topologie, mais nous en parlerons une autre fois si tu le veux bien.