Les polynômes tordus

Xavier Caruso

5 novembre 2018

Résumé

Nous expliquons comment l'introduction d'une multiplication non commutative sur l'ensemble des polynômes à coefficients complexes permet de résoudre certains exercices de géométrie plane.

1 Les équations algébriques

La question de la résolution des équations algébriques est un problème très ancien qui a façonné (et continue de façonner) de nombreux travaux mathématiques. Après les équations de degré 1, celles de la forme $ax = b$, viennent rapidement les équations de degré 2 :

$$ax^2 + bx + c = 0$$

dont la résolution rémonte aux Babyloniens et est enseignée en classe de 1ère S (dans le cursus actuel). Les équations de degré 3 et 4 ont donné plus de fil à retordre aux mathématiciens. Elles ont néanmoins été résolues au 16ème siècle par l'école italienne. Pour les degrés supérieurs (5 et au-delà), la situation est toute autre puisque, suivant des idées de Lagrange, Abel puis Galois ont démontré que ces équations n'étaient généralement pas *résolubles par radicaux*, c'est-à-dire qu'il n'est pas possible d'exprimer leurs solutions en utilisant uniquement les opérations algébriques usuelles et l'extraction de racines. Derrière ces résultats, il y a toute une série de découvertes qui débute avec deux notions fondamentales : celle de nombres complexes et celle de polynôme.

Les nombres complexes. Les nombres complexes, on le sait, sont ceux qui s'obtiennent en ajoutant formellement aux nombres réels une racine carrée de -1, quantité qui ne saurait exister *a priori* étant donné qu'un carré est toujours positif. Traditionnellement, on désigne cette racine carrée imaginaire par la lettre i. Le lien entre les nombres complexes et la résolution d'équations algébriques a été observé en premier par Cardan lorsqu'il travaillait sur l'équation de degré 3. Il avait remarqué, en effet, qu'en appliquant la formule de résolution générale avec l'équation $x^3 - 3x - 1 = 0$, il aboutissait à la solution [1] :

$$\sqrt[3]{\frac{1+\sqrt{-81}}{2}} + \sqrt[3]{\frac{1-\sqrt{-81}}{2}}.$$

Par ailleurs, une étude de fonctions montre que l'équation $x^3 - 3x - 1 = 0$ a ses trois racines réelles. Cependant l'expression obtenue par Cardan n'a *a priori* pas de sens et ne saurait donc définir un nombre réel. Sauf, bien sûr, à accepter l'existence de la racine carrée d'un nombre négatif ! Après cela, il a fallu encore beaucoup de temps pour que la notion de nombre complexe émerge complètement, mais la nécessité de les définir est apparue de manière flagrante dès lors.

Il s'est avéré par la suite que les nombres complexes fournissent un cadre théorique parfait pour la compréhension des équations algébriques puisque ils forment un ensemble « clos » dans lequel toute équation algébrique a toutes ses solutions. Les travaux de Lagrange, Abel et Galois sur les équations de degré 5 trouvent naturellement leur place dans ce cadre.

1. Bien entendu, tout ceci est retranscrit dans notre langage moderne ; Cardan n'utilisait évidemment pas les mêmes notations.

Les polynômes. Une autre notion qui a été façonnée par le problème de la résolution des équations algébriques est celle de polynôme. Un *polynôme* est une expression de la forme :

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

où les a_j sont des quantités connues, appelées les *coefficients* et où X est ce que l'on appelle une *variable*. Le *degré* de $P(X)$ est, par définition, l'entier n qui apparaît dans l'écriture précédente, en supposant $a_n \neq 0$. À l'instar des nombres entiers, les polynômes possèdent d'intéressantes propriétés de nature arithmétique qui servent de point d'appui aux démonstrations de nombreux résultats sur les équations algébriques.

Un premier exemple est l'existence d'une *division euclidienne* qui stipule que, si $A(X)$ et $B(X)$ sont deux polynômes avec $B(X) \neq 0$, il existe deux polynômes uniquement déterminés $Q(X)$ et $R(X)$ tels que $A(X) = B(X)Q(X) + R(X)$ et $\deg R(X) < \deg B(X)$. L'une des premières conséquences de cela est la propriété bien connue suivante : un polynôme $P(X)$ s'annule en a, si et seulement si $P(X) = (X-a) \cdot Q(X)$ où $Q(X)$ est un certain autre polynôme. En effet, la division euclidienne de $P(X)$ par $X-a$ s'écrit :

$$P(X) = (X-a) \cdot Q(X) + R(X)$$

où $R(X)$ est un polynôme constant (c'est-à-dire ne dépendant pas de X). L'équivalence annoncée s'obtient alors en évaluant en $X = a$. Une seconde conséquence importante de la division euclidienne est l'existence de PGCD que l'on peut calculer grâce à l'algorithme d'Euclide.

Une autre propriété arithmétique des polynômes est la décomposition *unique* de tout polynôme en produit de facteurs irréductibles, qui est le pendant du théorème de factorisation des entiers en produit de nombres premiers. Lorsque les coefficients a_j sont des nombres complexes, les seuls polynômes irréductibles sont de degré 1 et le théorème précédent revient à dire que tout polynôme $P(X)$ se factorise comme un produit :

$$P(X) = a \cdot (X - \lambda_1)\,(X - \lambda_2) \cdots (X - \lambda_n)$$

pour des nombres complexes $a, \lambda_1, \lambda_2, \ldots, \lambda_n$. Pour des polynômes à coefficients réels, des facteurs irréductibles de degré 2 peuvent apparaître. Typiquement le polynôme $X^2 + 1$ s'écrit $(X+i)(X-i)$ si on s'autorise à introduire des nombres complexes mais est irréductible dans le cas contraire.

2 Nombres complexes et géométrie

Non contents de fournir le cadre théorique adéquat à l'étude des équations algébriques, les nombres complexes jouent aussi un rôle prépondérant dans de nombreux autres domaines des mathématiques et, en particulier, en géométrie. Le lien est transparent : à un nombre complexe $a+ib$, on fait correspondre le point du plan de coordonnées (a, b). *Via* ce dictionnaire, de nombreuses notions de nature géométrique possèdent des réinterprétations algébriques intéressantes. Par exemple, la notion de distance est en lien direct avec la notion de module d'un nombre complexe. Les transformations du plan possèdent, elles aussi, une réinterprétation plaisante dans le langage des nombres complexes.

Intéressons-nous particulièrement aux similitudes. Rappelons pour commencer qu'une *similitude* est une transformation du plan qui préserve les rapports de distances. Parmi celles-ci, on distingue les similitudes *directes* qui conservent l'orientation et les similitudes *indirectes* qui inversent l'orientation.

Cas des similitudes directes. On dispose dans cette situation d'un théorème classique qui s'énonce comme suit.

Théorème 1. *Les simitudes directes du plan correspondent exactement aux fonctions complexes de la forme $z \mapsto az + b$ où a et b sont des nombres complexes avec $a \neq 0$.*

Certains invariants de la similitude se lisent en outre sur a et b ; par exemple, le module de a est égal au rapport de similitude, c'est-à-dire au nombre par lequel la similitude multiplie les distances. Pareillement, l'argument de a est égal à l'angle de la similitude. Les translations (qui sont des

similitudes particulières) correspondent au cas où $a = 1$. Lorsque $a \neq 1$, le centre de la similitude correspond à l'unique point fixe de $z \mapsto az + b$, c'est-à-dire $\frac{b}{1-a}$. En particulier, la similitude a pour centre l'origine si et seulement si $b = 0$.

La discussion précédente permet, dans certains cas, d'aborder la résolution d'« équations » portant sur les similitudes par le biais des équations algébriques. Le cas le plus simple est celui où seules des similitudes directes de centre l'origine apparaissent. En guise d'illustration de ce principe, regardons un instant l'exercice suivant.

Exercice 1. *Soient O et M deux points du plan. Soit f la similitude directe de centre O, de rapport $\sqrt{2}$ et d'angle $\frac{\pi}{4}$. Trouver toutes les similitudes directes s de centre O pour lesquelles O, $f(M)$, $s(s(M))$ et $s^{-1}(M)$ sont les sommets (ordonnés) d'un parallélogramme.*

Pour résoudre cet exercice, choisissons le repère orthonormé direct dans lequel les points O et M ont pour coordonnées respectives $(0, 0)$ et $(1, 0)$. Passant aux nombres complexes, la similitude s s'écrit sous la forme $z \mapsto xz$ pour une inconnue complexe x. La condition de l'énoncé s'écrit alors :

$$x^2 = (1 + i) + x^{-1}.$$

En multipliant par x des deux côtés, on aboutit à l'équation $x^3 - (1 + i)x - 1 = 0$ que l'on peut maintenant résoudre par des méthodes purement algébriques.

Cas des similitudes indirectes. Une méthode pour traiter le cas des similitudes indirectes est de le ramener à celui des similitudes directes grâce à une transformation simple. Précisément, soit σ la symétrie par rapport à l'axe des abscisses. Dans le monde complexe, elle correspond à l'application de conjugaison $z \mapsto \bar{z}$. Remarquons maintenant que si s est une similitude indirecte, la composée $s \circ \sigma$ devient une similitude directe. Il resulte de cela que les similitudes indirectes correspondent exactement aux fonctions de la forme $z \mapsto a\bar{z} + b$ (pour certains nombres complexes a et b avec $a \neq 0$).

À nouveau, pour simplifier l'exposition, nous nous restreignons à partir de maintenant aux similitudes indirectes fixant l'origine, c'est-à-dire à celles pour lesquelles $b = 0$. Reprenons à présent l'exercice 1 mais cherchons à présent s parmi les similitudes indirectes (de centre O). Dans le monde complexe, une telle similitude s'écrit $z \mapsto x\bar{z}$ et la condition de l'énoncé se traduit par l'équation :

$$|x|^2 = (1 + i) + \bar{x}^{-1}$$

qui fait à présent intervenir des modules et des conjugués et ne relève donc plus de la théorie des équations algébriques. Tentons néanmoins de la résoudre. Pour ce faire, cherchons x sous la forme $u + iv$. En posant $T = |x|^2 = u^2 + v^2$ et en séparant partie réelle et partie imaginaire, on aboutit aux deux équations $T = 1 + \frac{u}{T}$ et $0 = 1 - \frac{v}{T}$, soit encore $u = T^2 - T$ et $v = T$. La condition $u^2 + v^2 = T$ conduit alors à :

$$T^3 - 2T^2 + 2T - 1 = 0. \tag{1}$$

Nous retrouvons de cette manière une équation *algébrique* de degré 3 que l'on peut donc *a priori* résoudre par la méthode générale. Dans le cas présent, la situation est encore plus favorable car l'on s'aperçoit que 1 est racine évidente. L'équation que l'on cherche à résoudre se factorise donc sous la forme $(T - 1)(T^2 - T + 1) = 0$. Le discriminant du trinôme $T^2 - T + 1$ étant strictement négatif, la valeur 1 est l'unique solution acceptable à notre problème. Autrement dit, il existe une unique similitude indirecte de centre O satisfaisant à la condition requise : c'est celle qui correspond à la fonction $z \mapsto i\bar{z}$. Géométriquement, il s'agit de la symétrie d'axe (OM) suivie de la rotation de centre O et d'angle $\frac{\pi}{2}$.

3 Les polynômes tordus

Précédemment, nous avons constaté qu'aussi bien dans le cas des similitudes directes que dans celui des similitudes indirectes, la question de l'exercice 1 se reformulait en une équation algébrique de degré 3. Toutefois, si cette réduction était purement mécanique pour les simitudes directes, elle demandait un raisonnement plus sophistiqué dans le cas des similitudes indirectes. La raison en est

que la conjugaison complexe « perturbe » les calculs. Précisément, lorsqu'on transpose la condition de l'équation, on aboutit à une équation faisant intervenir à la fois x et son conjugué $\bar{x}$.

Le cadre théorique adéquat pour traiter ce type d'équations est la notion de polynôme tordu. Par définition, un *polynôme tordu* en la variable X est une expression de la forme :

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

pour des nombres complexes $a_1, \ldots, a_n$... c'est-à-dire en fait un polynôme. La différence entre polynômes tordus et polynômes usuels se manifeste au niveau de la loi de multiplication. Par définition, la multiplication sur les polynômes tordus n'est pas *commutative* mais est régie par la règle suivante :

$$X \cdot a = \bar{a}\, X$$

pour tout nombre complexe a. Il se trouve que cette règle simple suffit à définir de manière unique, grâce à l'associativé et à la distributivité, le produit de deux polynômes tordus quelconques. À titre d'exemple, le calcul suivant montre comment effectuer la multiplication de deux polynômes tordus de degré 2 :

$$\begin{aligned}
&\big(a_0 + a_1 X + a_2 X^2\big) \cdot \big(b_0 + b_1 X + b_2 X^2\big) \\
&= a_0 b_0 + a_0 b_1 X + a_0 b_2 X^2 + a_1 X b_0 + a_1 X b_1 X + a_1 X b_2 X^2 + a_2 X^2 b_0 + a_2 X^2 b_1 X + a_2 X^2 b_2 X^2 \\
&= a_0 b_0 + a_0 b_1 X + a_0 b_2 X^2 + a_1 \bar{b}_0 X + a_1 \bar{b}_1 X^2 + a_1 \bar{b}_2 X^3 + a_2 b_0 X^2 + a_2 b_1 X^3 + a_2 b_2 X^4 \\
&= a_0 b_0 + (a_0 b_1 + a_1 \bar{b}_0) X + (a_0 b_2 + a_1 \bar{b}_1 + a_2 b_0) X^2 + (a_1 \bar{b}_2 + a_2 b_1) X^3 + a_2 b_2 X^4.
\end{aligned}$$

la relation $X^2 b_j = b_j X^2$ (pour $j = 0, 1, 2$) provenant de la suite d'égalités $X^2 b_j = X \bar{b}_j X = \bar{\bar{b}}_j X^2 = b_j X^2$. Les identités remarquables tordues s'écrivent, quant à elles, de la manière suivante :

$$\begin{aligned}
(X + a)^2 &= X^2 + 2\,\mathrm{Re}(a)\, X + a^2 \\
(X + a)(X - a) &= X^2 + 2\,\mathrm{Im}(a)\, X - a^2 \\
(X + a)(X + \bar{a}) &= X^2 + 2aX + |a|^2 \\
(X + a)(X - \bar{a}) &= X^2 - |a|^2.
\end{aligned}$$

Il résulte en particulier de ces égalités que le polynôme tordu $X^2 - 1$ possède une infinité de factorisations : il s'écrit $(X + a)(X - \bar{a})$ pour tout nombre complexe a de module 1.

Division euclidienne et conséquences

De façon remarquable, les polynômes tordus possèdent de nombreux points communs avec les polynômes classiques sur le plan arithmétique. En particulier, on dispose de la proposition suivante.

Proposition 2 (Division euclidienne à droite)**.** *Soient $A(X)$ et $B(X)$ deux polynômes tordus avec $B(X) \neq 0$. Alors il existe des polynômes tordus $Q(X)$ et $R(X)$ uniquement déterminés tels que $A(X) = Q(X)B(X) + R(X)$ et $\deg R(X) < \deg B(X)$.*

Nous omettons la démonstration de cette proposition, laissant le soin au lecteur ou à la lectrice de compléter ce point. Notons cependant qu'on parle de division euclidienne *à droite* car le diviseur $B(X)$ apparaît à droite dans le produit. De la même manière, il existe une division à gauche où l'on demande à ce que la relation $A(X) = B(X)Q(X) + R(X)$ soit satisfaite. Il est important de prendre garde au fait que les polynômes tordus $Q(X)$ et $R(X)$ sont modifiés lorsque l'on effectue la division euclidienne à gauche ou à droite. Par exemple, très simplement, on a :

$$aX = a(X - c) + ac = (X - c)\bar{a} + \bar{a}c.$$

Dans la suite de ce texte, nous ne considèrerons que des divisions euclidiennes à droite.

PGCD de polynômes tordus. De même que dans le cas classique, l'existence d'une division euclidienne permet de mettre en place l'algorithme d'Euclide et, ce faisant, d'aboutir à la notion de PGCD. Plus précisément, partons de deux polynômes tordus $A(X)$ et $B(X)$ et définissons la suite d'Euclide par $R_1(X) = A(X)$, $R_2(X) = B(X)$ puis, tant que $R_j(X) \neq 0$ pour $j \geqslant 2$, définissons $R_{j+1}(X)$ comme le reste de la division euclidienne (à droite) de $R_{j-1}(X)$ par $R_j(X)$. Le dernier reste non nul $D(X)$ de cette suite vérifie alors la propriété suivante : un polynôme tordu $P(X)$ est un diviseur commun à droite de $A(X)$ et $B(X)$ si et seulement $P(X)$ est un diviseur à droite de $D(X)$. On dit que $D(X)$ est le PGCD à droite de $A(X)$ et $B(X)$. Remarquons que, quitte à multiplier $D(X)$ à gauche par un nombre complexe non nul, on peut le normaliser de manière à ce qu'il soit unitaire sans perdre ses propriétés de divisibilité. Lorsqu'il est normalisé de cette manière, on le notera $\mathrm{RGCD}(A(X), B(X))$.

Division par un polynôme de degré 1**.** Un calcul intéressant à mener (que nous avons déjà esquissé précédemment) est la division euclidienne d'un polynôme tordu quelconque $P(X)$ par un polynôme de la forme $X-c$. Lorsque $P(X) = X^n$ est un monôme, on vérifie que celle-ci s'écrit :

$$X^n = \left(X^{n-1} + N_1(c)X^{n-2} + N_2(c)X^{n-3} + \cdots + N_{n-1}(c)\right)(X - c) \; + \; N_n(c)$$

où on a posé $N_j(c) = |c|^{j/2}$ si j est pair et $N_j(c) = |c|^{(j-1)/2}\, c$ sinon. En particulier, le reste de la division de X^n par $X-c$ est $N_n(c)$. À partir de là, on déduit, plus généralement, que si $P(X)$ s'écrit :

$$P(X) = a_0 + a_1X + \cdots + a_nX^n$$

alors le reste de la division de $P(X)$ par $X-c$ est :

$$a_0 + a_1N_1(c) + a_2N_2(c) + \cdots + a_nN_n(c).$$

Cette dernière valeur est parfois considérée comme l'*évaluation* du polynôme tordu $P(X)$ en c et sera notée simplement $P(c)$ dans la suite de cet article. On prendra garde toutefois à ce que la fonction d'évaluation $P(X) \mapsto P(c)$ n'est *pas* multiplicative.

Lien avec les similitudes indirectes

L'introduction des polynômes tordus est pertinente pour l'étude des similitudes indirectes car il se trouve que la manière dont se composent les similitudes indirectes est parfaitement reflétée par la multiplication tordue que nous avons introduite précédemment. Précisément, supposons donnée une similitude indirecte s fixant l'origine. Si $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ est un polynôme tordu, on peut former la transformation du plan :

$$P(s) = s_0 + s_1 \circ s + s_2 \circ s^2 + \cdots + s_n \circ s^n$$

où s_j est, par définition, la similitude *directe* donnée par la fonction complexe $z \mapsto a_jz$ et où le signe $\ll + \gg$ fait référence à la somme vectorielle dans le plan. Le fait remarquable (qui se vérifie à la main par un calcul) est que, pour deux polynômes tordus $P(X)$ et $Q(X)$, on a :

$$P(s) \circ Q(s) = (PQ)(s)$$

où la multiplication dans le membre de droite est celle des polynômes tordus.

De manière similaire, on vérifie que si s correspond à la fonction complexe $z \mapsto c\bar{z}$ (pour un certain c), alors l'application $P(s)$ envoie le point d'affixe 1 sur le point d'affixe $P(c)$ où $P(c)$ désigne l'évaluation du polynôme tordu $P(X)$ au point c telle que nous l'avons définie précédemment. Ces propriétés amènent un nouveau regard sur l'exercice 1 dans le cas des similitudes indirectes. En effet, la condition de l'énoncé s'écrit $s^2(M) = f(M) + s^{-1}(M)$ soit encore, en appliquant s :

$$s^3(M) = s \circ f(M) + M$$

Ainsi, en écrivant $z \mapsto x\bar{z}$ pour la transformation complexe associée à s, on s'aperçoit que l'exercice revient à résoudre l'équation algébrique tordue $P(x) = 0$ où $P(X)$ est le polynôme tordu :

$$P(X) = X^3 - X(1+i) + 1 = X^3 + (i-1)X + 1. \tag{2}$$

Résolution des équations algébriques tordues

La résolution générale des équations algébriques tordues pourrait sembler difficile au premier abord. En réalité, elle se ramène relativement simplement à la résolution d'équations algébriques classiques grâce à un outil fondamental : la norme réduite.

La norme réduite. Soit $P(X) = a_0 + a_1X + \cdots + a_nX^n$ un polynôme tordu. En séparant les exposants pairs des exposants impairs, on peut écrire $P(X)$ sous la forme :

$$P(X) = P_0(X^2) + P_1(X^2)\, X.$$

De manière très concrète, $P_0(X^2)$ et $P_1(X^2)$ sont simplement définis par :

$$P_0(T) = a_0 + a_2T + a_4T^2 + \cdots \quad \text{et} \quad P_1(T) = a_1 + a_3T + a_5T^2 + \cdots$$

pour une nouvelle variable T. Dans la suite, on considèrera les polynômes $P_0(T)$ et $P_1(T)$ comme des polynômes classiques, donc soumis à la loi de multiplication usuelle. Cela est légitime car il est facile de vérifier que les polynômes tordus $P_0(X^2)$ et $P_1(X^2)$ commutent entre eux. Nous posons également :

$$\bar{P}_0(T) = \bar{a}_0 + \bar{a}_2T + \bar{a}_4T^2 + \cdots \quad \text{et} \quad \bar{P}_1(T) = \bar{a}_1 + \bar{a}_3T + \bar{a}_5T^2 + \cdots$$

Ce sont les polynômes obtenus à partir de $P_0(T)$ et $P_1(T)$ en conjuguant tous les coefficients. Avec ces notations, la norme réduite de $P(X)$ est le polynôme en T, noté $\mathcal{N}_{P(X)}(T)$, défini par la formule :

$$\mathcal{N}_{P(X)}(T) = P_0(T)\bar{P}_0(T) - TP_1(T)\bar{P}_1(T).$$

Clairement $\mathcal{N}_{P(X)}(T)$ est stable par la conjugaison complexe et est donc un polynôme à coefficients réels.

Pour se familiariser avec cette notion, examinons deux exemples qui, qui plus est, nous seront utiles dans la suite. Le premier d'entre eux est celui des polynômes tordus de degré 1 de la forme $P(X) = X - c$ (pour un nombre complexe c). Dans ce cas, on a $P_0(T) = -c$ et $P_1(T) = 1$, d'où il résulte :

$$\mathcal{N}_{X-c}(T) = |c|^2 - T.$$

Le second exemple est celui du polynôme tordu $P(X)$ donnée par la formule (2) correspondant à la situation de l'exercice 1. On trouve $P_0(T) = 1$, $P_1(T) = (i-1) + T$ et donc :

$$\mathcal{N}_{P(X)}(T) = 1 \, - \, T(i - 1 + T)(-i - 1 + T) = -T^3 + 2T^2 - 2T + 1$$

qui, remarquons-le, est égal, au signe près, au polynôme de l'équation (1) sur lequel nous étions déjà tombé tantôt.

La norme réduite possède d'agréables propriétés vis-à-vis de la divisibilité qui en font un outil efficace dans de nombreuses situations. La proposition suivante en donne une première saveur.

Proposition 3. *1. La norme réduite est une application multiplicative dans le sens où :*

$$\mathcal{N}_{P(X)\cdot Q(X)}(T) = \mathcal{N}_{P(X)}(T) \cdot \mathcal{N}_{Q(X)}(T)$$

pour tous polynômes tordus $P(X)$ et $Q(X)$.

2. *Pour tout polynôme tordu $P(X)$, le polynôme $\mathcal{N}_{P(X)}(X^2)$ (vu comme un polynôme tordu) est un multiple à gauche et à droite de $P(X)$.*
3. *Soit $P(X)$ un polynôme tordu et soit $N(T)$ un diviseur de degré strictement positif de $\mathcal{N}_{P(X)}(T)$. Alors* RGCD$(N(X^2), P(X))$ *est également de degré strictement positif.*

Démonstration. Pour ce qui concerne la première assertion, on considère deux polynômes tordus $P(X)$ et $Q(X)$ écrits sous la forme $P(X) = P_0(X^2) + P_1(X^2)X$ et $Q(X) = Q_0(X^2) + Q_1(X^2)X$.

On remarque, par ailleurs, que la loi de multiplication entraîne que $XQ_j(X^2) = \bar{Q}_j(X^2)X$ lorsque j vaut 0 ou 1. Ainsi :

$$\begin{aligned} P(X)Q(X) &= \big(P_0(X^2) + P_1(X^2)X\big) \cdot \big(Q_0(X^2) + Q_1(X^2)X\big) \\ &= \big(P_0(X^2)Q_0(X^2) + P_1(X^2)\bar{Q}_1(X^2)X^2\big) + \big(P_1(X^2)\bar{Q}_0(X^2) + P_0(X^2)Q_1(X^2)\big)X \end{aligned}$$

d'où, en suivant la définition, on déduit que la norme réduite du produit $P(X)Q(X)$ est égale à :

$$\begin{aligned} &\big(P_0(T)Q_0(T) + TP_1(T)\bar{Q}_1(T)\big) \cdot \big(\bar{P}_0(T)\bar{Q}_0(T) + T\bar{P}_1(T)Q_1(T)\big) \\ -\ &T \cdot \big(P_1(T)\bar{Q}_0(T) + P_0(T)Q_1(T)\big) \cdot \big(\bar{P}_1(T)Q_0(T) + \bar{P}_0(T)\bar{Q}_1(T)\big). \end{aligned}$$

En développant l'expression ci-dessus, d'une part, et le produit $\mathcal{N}_{P(X)}(T)\,\mathcal{N}_{Q(X)}(T)$, d'une part, on vérifie l'égalité annoncée.

Pour le second énoncé, partant d'un polynôme tordu $P(X) = P_0(X^2) + P_1(X^2)X$, on forme le polynôme tordu $Q(X) = \bar{P}_0(X^2) - P_1(X^2)X$. Un calcul similaire à ce que l'on a fait précédemment montre alors que $P(X)Q(X) = Q(X)P(X) = \mathcal{N}_{P(X)}(X^2)$. Les propriétés de divisibilité annoncées en résultent.

Enfin, le troisième point est plus délicat. Pour ne pas alourdir ce texte, nous l'admettons. □

Des racines de la norme réduite à celles du polynôme tordu. En guise d'application de la proposition 3, voyons comment celle-ci permet de ramener la résolution des équations algébriques tordues à celle des équations algébriques classiques.

Considérons donc $P(X)$ un polynôme tordu et, comme précédemment, notons $\mathcal{N}_{P(X)}(T)$ sa norme réduite. Soit c une racine de P, c'est-à-dire un nombre complexe tel que $P(c) = 0$. Par définition, cela signifie que le reste de la division de $P(X)$ par $X-c$ s'annule, ce qui revient encore à dire que $X-c$ est un diviseur à droite de $P(X)$, *i.e.* $P(X) = Q(X)\cdot(X-c)$ pour un certain polynôme tordu $Q(X)$. D'après le premier point de la proposition 3, cette dernière égalité implique, en prenant les normes réduites :

$$\mathcal{N}_{P(X)}(T) = \mathcal{N}_{Q(X)}(T) \cdot \mathcal{N}_{X-c}(T) = \mathcal{N}_{Q(X)}(T) \cdot \big(|c|^2 - T\big).$$

On en déduit que $|c|^2$ est une racine du polynôme $\mathcal{N}_{P(X)}(T)$.

Concentrons-nous à présent sur la réciproque. Pour cela, supposons donné un nombre positif ou nul, noté r^2 (pour un certain nombre réel $r \geqslant 0$), qui est une racine de $\mathcal{N}_{P(X)}(T)$. Autrement dit, le polynôme $N(T) = r^2-T$ apparaît comme un diviseur de $\mathcal{N}_{P(X)}(T)$. Posons $D(X) = \text{RGCD}(N(X^2), P(X))$. D'après la dernière assertion de la proposition 3, le polynôme $D(X)$ est de degré strictement positif. Comme c'est en outre un diviseur de $N(X^2) = r^2-X^2$, il est de degré au plus 2. Il ne reste donc plus que deux possibilités : soit $\deg D(X) = 1$, soit $\deg D(X) = 2$.

Dans le premier cas, on peut écrire $D(X) = X-c$ pour un certain nombre complexe c. Du fait que $D(X)$ divise $P(X)$, on déduit que $P(c) = 0$, c'est-à-dire que c est une racine de $P(X)$. Par ailleurs, on sait que $D(X)$ divise $N(X^2) = r^2-X^2$, ce qui implique de même que précédemment que $|c|^2 = r^2$ et, par suite, $|c| = r$. Autrement dit, nous avons construit une racine de $P(X)$ de norme r, à savoir c. Remarquons en outre qu'une racine ayant cette propriété supplémentaire est unique. En effet, si c' était une autre racine de $P(X)$ de norme r, le polynôme $X-c'$ diviserait à la fois $P(X)$ et $N(X^2)$. Il serait donc également un diviseur de $D(X)$, ce qui n'est pas possible dès lors que $c \neq c'$.

Examinons maintenant le cas où $D(X)$ est de degré 2. On a alors $D(X) = -N(X^2)$. D'autre part, étant donné un nombre complexe c de module r, on dispose de la factorisation :

$$(X + \bar{c})(X - c) = X^2 - r^2 = D(X).$$

Du fait que $D(X)$ divise $P(X)$, on déduit que $X-c$ divise également $P(X)$ ou, autrement dit, que c est une racine de P. Dans ce cas, nous avons donc démontré que *tout* nombre complexe de module r est racine de $P(X)$.

La proposition suivante résume les propriétés que nous venons d'établir.

Proposition 4. *Soit $P(X)$ un polynôme tordu.*

1. *Si c est une racine de $P(X)$, alors $|c|^2$ est une racine de $\mathcal{N}_{P(X)}(T)$.*
2. *Si r^2 est une racine de $\mathcal{N}_{P(X)}(T)$, on pose $D(X) = \text{RGCD}(P(X), X^2 - r^2)$ et on a alors l'alternative suivante :*
   i) soit $\deg D(X) = 1$ auquel cas $D(X) = X - c$ et c est l'unique racine de $P(X)$ de norme r,
   ii) soit $\deg D(X) = 2$ auquel cas tout nombre complexe de module r est racine de $P(X)$.

La proposition précédente fournit une méthode systématique pour résoudre les équations algébriques tordues. Pour résoudre l'équation $P(x) = 0$ (où $P(X)$ est un polynôme tordu), on calcule tout d'abord la norme réduite $\mathcal{N}_{P(X)}(T)$. Dans un deuxième temps, on résout l'équation algébrique $\mathcal{N}_{P(X)}(t) = 0$ puis, pour chaque racine positive ou nulle $t = r^2$ de cette équation, on calcule $D_r(X) = \text{RGCD}(P(X), X^2 - r^2)$ par l'algorithme d'Euclide. Si $\deg D_r(X) = 1$, on écrit $D_r(X) = X - c$ et le nombre complexe c que l'on obtient ainsi est une racine de $P(X)$. C'est, en outre, l'unique racine de $P(X)$ de norme r. Si, au contraire, $\deg D_r(X) = 2$, on déduit que tout nombre complexe de module r est racine de $P(X)$.

Pour conclure, appliquons cette méthode avec le polynôme tordu :

$$P(X) = X^3 + (i-1)X + 1$$

(*cf* Eq. (2)). Nous avons déjà calculé sa norme réduite qui vaut :

$$\mathcal{N}_{P(X)}(T) = -T^3 + 2T^2 - 2T + 1.$$

L'unique racine réelle positive de ce dernier polynôme est $t = 1$. Nous en déduisons déjà que tout racine de $P(X)$ est de module 1. Pour aller plus loin, il nous faut calculer le PGCD à droite de $P(X)$ et $X^2 - 1$. L'algorithme d'Euclide montre qu'il vaut $X - i$, d'où on déduit que i est l'unique racine de $P(X)$. Nous retrouvons de cette manière le résultat que nous avions déjà obtenu par un calcul *ad hoc* à la fin de la partie 2.

Conclusion

Dans cet article, sous le prétexte de vouloir résoudre un exercice de géométrie plane portant sur les similitudes indirectes, nous avons introduit la notion d'équation algébrique tordue afférente, elle-même, à la notion de polynôme tordu. Il faut comprendre, évidemment, que de même que les polynômes usuels sont devenus un objet omniprésent en mathématiques, l'utilisation des polynômes tordus ne se limite pas à l'application « jouet » que nous avons présentée. Ils apparaissent, en fait, comme un outil particulièrement adapté en algèbre semi-linéaire, une variante de l'algèbre linéaire qui autorise des twists par des automorphismes de corps tels que la conjugaison complexe. Une variante des polynômes tordus sert également à mieux comprendre la structure interne des équations différentielles linéaires d'ordre arbitraire. Les propriétés de factorisation de ces polynômes — et, en particulier, le calcul de leurs racines en correspondance avec les facteurs de degré 1 — fournissent des renseignements précieux sur la réduction des applications semi-linéaires ou sur la manière d'aborder la résolution de certaines équations différentielles.