Les polynômes : guide de survie en milieu hostile

Marc Chevalier
DI ENS

2019-2020

Table des matières

On va voir ici les différents aspects des polynômes en commençant par leur définitions suivies des propriétés utiles. Les définitions sont là pour mettre les choses au clair. Comme il s'agit d'objets assez particuliers, on ne peut se contenter de les interpréter que comme des fonctions polynomiales. Toutefois, le parallèle est saisissant.

On se donne un corps $\mathbb{K}$. Pour la première partie, il peut être quelconque mais est typiquement $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. Pour la suite, on se restreindra à $\mathbb{R}$ et $\mathbb{C}$ avec une pérégrination dans $\mathbb{Q}$.

La partie 1 est là pour des raisons administratives. Vous devez surtout savoir ce qu'est un polynôme (pas avec la définition formelle), un monôme, le degré, le coefficient dominant, les polynômes unitaires et comment additionner et multiplier des polynômes. Normalement, vous savez déjà presque tout.

La partie 2 par contre est importante.

1 Définition

Nous connaissons déjà les polynômes sous leur forme de fonctions polynomiales, une fonction de la forme $x \mapsto a_n x^n + ... + a_1 x + a_0$. Toutefois, les polynômes ont d'autres utilités que d'être des fonctions et des propriétés qui leurs sont propres. Ils ont ainsi gagné une définition à part qui permet de les étudier sans la charge de toute l'analyse.

Définition 1 – Suite presque nulle

On dit qu'une suite $u \in \mathbb{K}^{\mathbb{N}}$ (suite à valeurs dans $\mathbb{K}$) est presque nulle si elle ne contient qu'un nombre fini de termes non nuls.

On déduit immédiatement qu'une telle suite est nulle à partir d'un certain rang. Mathématiquement, cela s'écrit :

$$\exists N \in \mathbb{N} : \forall n \geqslant N, u_n = 0$$

Exemple 1

La suite nulle $(0, 0, \ldots)$ est presque nulle.
Pour tout $n \in \mathbb{N}$, la suite $(0, \ldots, 0, 1, 0, 0, \ldots)$ où le 1 est en $n^{\text{ème}}$ position est presque nulle.

Notation 1

Par habitude, convention tacite, des points de suspensions suivant 2 '0' indique qu'à partir de là, la suite est nulle.

Définition 2 – Polynôme

On appelle polynôme à coefficients dans $\mathbb{K}$ toute suite presque nulle à valeur dans $\mathbb{K}$.

On peut dès lors intuiter que la suite correspondant à $x \mapsto 1 + 2x + 7x^2 - 5x^4$ sera $(1, 2, 7, 0, -5, 0, 0, \ldots)$ (on remarque le 0 correspondant au coefficient de x^3). Les définitions qui suivent sont faites pour coller à cette intuition.

Définition 3 – Degré

On appelle degré d'un polynôme P, et on note $\deg(P)$, le plus grand entier i tel que $P_i \neq 0$. Si le polynôme est nul, le degré est $-\infty$. En effet on peut écrire :

$$\deg(P) = \max \{i \mid P_i \neq 0\}$$

et on rappelle que $\max \emptyset = -\infty$.

Exemple 2

Le premier terme d'une suite $(u_i)_{i\in\mathbb{N}}$ est u_0. Donc un polynôme qui n'aurait que son premier terme de non nul est de degré 0. Par exemple :

$$\deg(7, 0, 0, \ldots) = 0$$

Comme le premier rang est 0, le cinquième élément est de rang 4. Donc

$$\deg(1, 2, 7, 0, -5, 0, 0, \ldots) = 4$$

Ici, $u_4 = -5$.

Notation 2

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$. On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré au plus n.

1.1 Opérations

Certaines opérations sont directement induites par la définition sous forme de suite presque nulle. Par exemple, deux polynômes sont égaux si et seulement si tous leurs coefficients sont égaux. C'est également le cas de la somme. Mais certaines opérations sont spécifiques aux polynômes, comme le produit.

Définition 4 – Addition

Soit $P = (P_0, P_1, \ldots)$ et $Q = (Q_0, Q_1, \ldots)$ deux polynômes. On appelle somme de P et Q et on note $P + Q$ le polynôme $(P_0 + Q_0, P_1 + Q_1, \ldots)$.

Il convient de faire remarquer qu'en toute rigueur il faudrait prouver que la somme de deux polynômes est un polynôme. En effet, sachant que les deux suites sont nulles, la somme l'est également.

On peut s'intéresser au degré d'une somme. Si tous les termes de P et Q sont nuls au delà du rang r, les termes de $P + Q$ sont également nuls à partir du rang r. Donc le degré d'une somme de polynôme ne peut pas être plus grand que les degrés des termes de la somme.

Proposition 1

$$\deg(P + Q) \leqslant \max(\deg(P), \deg(Q))$$

Notez bien que je ne prends pas de risques avec un $\leqslant$ et non, on n'a pas d'égalité. On peut expliquer sur des exemples.

Exemple 3

$(1, 2, 3, 0, 0, \ldots)$ est de degré 2 et $(1, 2, 3, 4, 0, 0, \ldots)$ est de degré 3. La somme est $(2, 4, 6, 4, 0, 0 \ldots)$ et est de degré 3.
Par contre, l'égalité n'est pas toujours atteinte, en particulier quand les coefficients dominants s'annulent. $(1, 2, 3, 0, 0, \ldots) + (1, 0, -3, 0, 0, \ldots) = (2, 2, 0, 0, 0, \ldots)$ qui est seulement de degré 1.

Définition 5 – Multiplication par un scalaire

Soit $P = (P_0, P_1, \ldots)$ un polynôme et λ un scalaire. On note λP le polynôme $(\lambda P_0, \lambda P_1, \ldots)$.

Encore des considérations de degré. Si tous les termes à partir du rang r sont nuls, on ne va pas créer de nouveaux termes non nuls en les multipliant par λ. Mais cette fois, on peut être plus précis. Si λ est non nul, en multipliant un terme non nul par λ. Donc λP a le même degré que P.

Proposition 2

Si $\lambda \neq 0$,

$$\deg(\lambda P) = \deg(P)$$

Si $\lambda = 0$, $\lambda P = 0$ et $\deg(0) = -\infty$.

On va maintenant s'intéresser à la multiplication de polynômes. Elle est intrinsèquement liée à la relation entre les polynômes et fonctions polynomiales. En effet, on veut que $P(x)Q(x) = (PQ)(x)$. Seulement, quand on pose un tel produit, on se retrouve avec une multiplication de deux grosses sommes qui se distribuent en plein de termes qu'on groupe par degré. Le produit de Cauchy correspond exactement à ce calcul.

Définition 6 – Produit de Cauchy

Soit $(u_i)_{i\in\mathbb{N}}$ et $(v_i)_{i\in\mathbb{N}}$ deux suites à valeur dans $\mathbb{K}$. Le produit de Cauchy de u et v est la suite w définie par

$$w_i = \sum_{k=0}^{i} u_k v_{i-k}$$

On peut remarquer un parallèle entre cette formule et le binôme de Newton.

Définition 7 – Multiplication de polynômes

Soit P et Q deux polynômes. On appelle produit de P et Q et on note PQ le polynôme défini par le produit de Cauchy de P et Q.

La définition semble barbare, mais c'est exactement celle qu'on pratique tous les jours. Le principe est de sommer les produits des termes dont la somme des rangs est la même.

Proposition 3

$$\deg(PQ) = \deg(P) + \deg(Q)$$

Il serait de bon goût d'avoir des meilleures notations pour travailler que des suites... Commençons par une constatation. Prenons un polynôme : $P = (2, 3, 5, 0, 0\ldots)$, par exemple. On peut le réécrire en isolant les coefficients :

$$\begin{aligned} P &= (2, 3, 5, 0, 0\ldots) \\ &= (2, 0, 0, 0, 0\ldots) + (0, 3, 0, 0, 0\ldots) + (0, 0, 5, 0, 0\ldots) \\ &= 2(1, 0, 0, 0, 0\ldots) + 3(0, 1, 0, 0, 0\ldots) + 5(0, 0, 1, 0, 0\ldots) \end{aligned}$$

On se rend ainsi compte qu'on peut tout écrire comme une **combinaison linéaire** des polynômes de la forme $(0, \ldots, 0, 1, 0, 0\ldots)$. Prenons ici un moment pour remarquer que cela signifie que la famille des $(0, \ldots, 0, 1, 0, 0\ldots)$ est **génératrice**.

Notation 3

Notons X le polynôme $(0, 1, 0, 0\ldots)$.

Calculons $X \cdot X = X^2$ avec la définition ci-dessus. Avec une surprise modérée, en posant le calcul, on trouve $(0, 0, 1, 0, 0\ldots)$. Calculons $X^3 = X^2 \cdot X$. On trouve $(0, 0, 0, 1, 0, 0, 0\ldots)$. Et X^4 ? Vous me voyez venir avec mes gros sabots : $(0, 0, 0, 0, 1, 0, 0, 0\ldots)$. On généralise : X^n a un seul 1, au rang n. Bon, et X^0 ? Il s'agit du produit de 0 termes, donc l'élément neutre du produit de Cauchy. En calculant un peu, on peut remarquer que c'est $(1, 0, 0\ldots)$. En effet pour tout polynôme P, on a $(1, 0, 0\ldots)P = P$.

Reprenons

$$\begin{aligned} P &= (2, 3, 5, 0, 0\ldots) \\ &= 2X^0 + 3X + 5X^2 \end{aligned}$$

Voilà qui est plus familier ! X est appelée l'**indéterminée**. Curieux nom, alors que le symbole est parfaitement déterminé, puisque c'est $(0, 1, 0, 0, \ldots)$.

Un peu de vocabulaire.

Définition 8 – Monôme

Un monôme est une polynôme de la forme kX^i. On dit que k est le coefficient de ce monôme.

Définition 9 – Coefficient dominant

Le coefficient dominant d'un polynôme est le coefficient de son monôme de plus haut degré.

Exemple 4

Le coefficient dominant de $1 + 5X^2 + 6X^5$ est 6.

Définition 10 – Polynôme unitaire

Un polynôme est dit unitaire si son coefficient dominant est 1.

Exemple 5

Les polynômes suivants sont unitaires :

- 1
- X
- $X + 2$
- $X^{10} + 42X^9 + 57X^8 - \pi X^2 + 2.7X$

Mais ceux-ci ne sont pas unitaires :

- 0
- 2
- $5X$
- $10X^3 + 1$

Avec cette notation, on peut exprimer le produit. Si on a $P = \sum_{i=0}^{n} a_i X^i$ et $Q = \sum_{i=0}^{n} b_i X^i$, alors $PQ = \sum_{i=0}^{2n} X^i \sum_{j=0}^{n} a_j b_{i-j}$, quitte à compléter par des 0 si P et Q ne sont pas de même degré.

On peut s'amuser à exprimer d'autres choses avec ces notations. Par exemple la dérivée.

Définition 11 – Dérivée

Soit $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ un polynôme. On appelle dérivée de P et on note P' le polynôme $a_1 + 2a_2 X + ... + n a_n X^{n-1}$.

Notons bien que c'est une définition dans le monde des polynômes, pas la dérivée de l'analyse usuelle. Mais évidemment, c'est fait pour que ça coïncide !

FIGURE 1 – Augustin Louis CAUCHY — 1789 – 1857

Proposition 4

Si P est de degré au moins 1 :

$$\deg(P') = \deg(P) - 1$$

Si P est constant $P' = 0$.

1.2 Fonction polynomiale

Définition 12 – Fonction polynomiale

Une fonction polynomiale est une fonction de la forme $x \mapsto a_0 + a_1 x + \cdots + a_n x^n$.

On voit immédiatement qu'il y a un lien avec la notation à base de X^i des polynômes. En effet, il y a une correspondance parfaite.

Proposition 5

L'ensemble des fonctions polynomiales et $\mathbb{K}[X]$ sont en bijection.

On peut même être beaucoup plus précis que ça.

Notation 4

Soit $P = a_0 + a_1 X \cdots + a_n X^n$ et $x \in \mathbb{K}$. On note $P(x)$, $a_0 + a_1 x + \cdots + a_n x^n$.

Proposition 6

La fonction

$$\psi : \mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$$
$$P \mapsto \begin{cases} \mathbb{K} \to \mathbb{K} \\ x \mapsto P(x) \end{cases}$$

est est un morphisme injectif (monomorphisme). ψ est appelé « morphisme d'évaluation ».

Cet objet peut être un peu déroutant. C'est une fonction qui prend en paramètre un polynôme et renvoie la fonction polynomiale associée. Comme cette fonction est à valeur dans les fonctions, on peut parler de fonction d'ordre supérieur.

2 Racines et factorisation

On rentre ici dans le vif du sujet. Je rappelle que le but est de factoriser les polynômes en produits de polynômes plus simples. Les plus simples possibles. Nous commencerons par étudier les racines, car elles fournissent des factorisations simples.

2.1 Racines

Définition 13 – Racine

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. a est une racine de P si $P(a) = 0$.

Pour une fonction qui n'est pas *a priori* un polynôme, on parle simplement de « zéro de la fonction ».

Proposition 7 – Division euclidienne

Soit A et B des polynômes. Il existe une unique paire (Q, R) de polynômes tels que

$$A = QB + R$$

avec $\deg R < \deg B$. On appelle Q le quotient de la division euclidienne de A par B et R le reste.

Démonstration. On prouve l'existence en appliquant l'algorithme de division euclidienne.

Démontrons l'unicité. Supposons qu'on ait Q, Q', R et R' tels que $A = QB + R = Q'B + R'$ avec $\deg R < \deg B$ et $\deg R' < \deg B$. On peut écrire $(Q - Q')B = R' - R$. Donc $\deg((Q - Q')B) = \deg(R' - R)$ et $\deg(R' - R) < \deg B$. Or $\deg((Q-Q')B) = \deg(Q-Q')+\deg B$. Si $\deg(Q-Q') \geqslant 0$, on a une contradiction. Donc $\deg(Q - Q') < 0$. Or, le seul polynôme de degré négatif est le polynôme nul. Donc $Q = Q'$ puis il vient que $R = R'$. □

Proposition 8 – Factorisation par $X - a$

Soit $P \in \mathbb{K}[X]$ et a une racine de P. Il existe un polynôme Q tel que $P = (X - a)Q$.

Démonstration. Divisons P par $(X - a)$. Il existe alors Q et R tels que $P = (X - a)Q + R$ avec $\deg R < \deg(X - a)$. Or, $\deg(X - a) = 1$, donc R est de degré 0 ou $-\infty$. R est donc une constante. $R = r$.

D'autre part, on sait que $P(a) = 0$. Donc $((X - a)Q + R)(a) = 0$. Or $((X - a)Q + R)(a) = (a - a)Q(a) + R(a) = R(a) = r$, d'où $r = 0$. Donc P est bien de la forme $P = (X - a)Q$. □

Ici, rien ne dit que a n'est pas racine de Q. Par exemple, pour $P = X^3 - 4X^2 + 5X - 2$, on peut constater que 1 est une racine. On a alors $P = (X - 1)Q$ avec $Q = X^2 - 3X + 2$. Mais 1 est encore racine de Q. En effet, $Q = (X - 1)R$ avec $R = X - 2$.

On peut faire de ce désagrément un avantage : une fois qu'on a mis la main sur une racine, on veut factoriser le plus possible par $(X - a)$, tant qu'on y est.

Définition 14 – Multiplicité

Soit $P \in \mathbb{K}[X]$ et a une racine de P. On appelle multiplicité de a le plus grand entier k tel qu'il existe Q tel que $P = (X - a)^k Q$.

On a alors $Q(a) \neq 0$. En effet, si a était une racine de Q, on pourrait factoriser une fois de plus (cf. proposition 8).

Définition 15

On dit qu'une racine est simple si son ordre de multiplicité est 1. On dit qu'elle est double si son ordre est 2. Etc.. On dit qu'une racine est multiple si elle n'est pas simple.

Dans l'exemple précédent, 1 est de multiplicité 2.

2.2 Factorisation

On va détailler ici la factorisation de polynômes, c'est à dire écrire un polynôme sous forme d'un produit d'autres polynômes. C'est une chose assez intéressante, car si chaque terme est plus simple à étudier, on peut sans doute trouver plus facilement des propriétés sur le polynôme entier. On a vu que trouver les racines aide à factoriser, mais ce n'est pas forcément le seul moyen !

2.2.1 Dans $\mathbb{R}$ et $\mathbb{C}$

Itérons le processus de factorisation par $X - a$ où a est une racine. Prenons un polynôme P, si on a une racine λ_1, on peut le factoriser par $X - \lambda_1$, et on obtient $P = (X - \lambda_1)Q_1$. Recommençons avec Q_1 qui a une racine λ_2, on trouve alors $P = (X - \lambda_1)(X - \lambda_2)Q_2$. On peut continuer ainsi jusqu'à trouver un Q_i qui n'ait pas de racine. On a alors $P = (X - \lambda_1) \cdots (X - \lambda_n)Q_n$. On remarque ici que les λ_k ne sont pas forcément distincts. On dit que la famille $\lambda_1, \ldots, \lambda_i$ forme la famille des racines avec ordre de multiplicité.

On peut aussi écrire P sous une autre forme : $P = (X - \lambda_1)^{\mu_1} \cdots (X - \lambda_j)^{\mu_j} Q_j$. μ_k est l'ordre de multiplicité de λ_k et les λ_k sont deux à deux distincts. On dit que que la famille des $\lambda_1, \ldots, \lambda_j$ sont les racines distinctes.

Exemple 6

On prend $P = -8 + 20X - 10X^2 - 13X^3 + 17X^4 - 7X^5 + X^6$. On remarque que $P = (X + 1)(X - 1)^2(X - 2)^3$. La famille des racines de P avec ordre de multiplicité est $(-1, 1, 1, 2, 2, 2)$ et la familles des racines distinctes est $(-1, 1, 2)$ avec multiplicité respective $(1, 2, 3)$.

L'une ou l'autre des deux formes peut être la plus pratique selon les cas. Quand on veut factoriser par une racine sans se poser de question, la première est bien. Si on veut décomposer entièrement le polynôme, la seconde forme est avantageuse.

On peut d'ores et déjà majorer le nombre de racines. Puisque $P = (X - \lambda_1) \cdots (X - \lambda_n)Q_n$, on a $\deg P = \deg(X - \lambda_1) + \cdots + \deg(X - \lambda_n) + \deg Q_n$. Or, $\deg(X - a) = 1$, donc si P est de degré n, il ne peut pas avoir plus que n racines. Mais peut-il en avoir moins ?

Une question se pose quand on en arrive là : quels sont les polynômes sans racines, qui vont tenir rôle de Q ? Tout d'abord, on remarque que les polynômes constants n'ont pas de racine, mais ce n'est pas très intéressant, puisqu'en multipliant un polynôme par une constante non nulle, on ne change pas ses racines.

2.2.1.1 Polynômes réels sans racines

Dans $\mathbb{R}$, on sait que les polynômes de la forme $P = aX^2 + bX + c$ avec $a \neq 0$ n'ont pas de racine quand $\Delta = b^2 - 4ac < 0$. Mais dans ce cas, il a deux racines complexes. On remarque que si $\Delta = 0$, il existe une racine double λ telle que $P = (X - \lambda)^2$ et si $\Delta > 0$ il y a exactement deux simples doubles distinctes. Si on admet les racines complexes, il y a bien deux racines (avec ordre de multiplicité) à chaque fois.

Toujours dans $\mathbb{R}$, on peut remarquer que le polynôme $P = a_n X^n + \cdots + a_0$ se comporte à l'infini comme $a_n X^n$. Il vient que si n est impair (et sans perte de généralité $a_n > 0$, quitte à prendre $-P$), on a $\lim\limits_{-\infty} P = -\infty$ et $\lim\limits_{+\infty} P = +\infty$. Par le théorème des valeurs intermédiaires, il existe au moins une racine. À l'inverse, si le degré est pair (toujours avec $a_n > 0$), on trouve $\lim\limits_{-\infty} P = \lim\limits_{+\infty} P = +\infty$. Il existe donc un minimum m atteint en x_0. On va construire un polynôme à partir de P sans racine réelle. Comme on a $P(x_0) = m$ et $\forall x \in \mathbb{R}, P(x) \geqslant m$, si on prend $S = P - m + 1$, on a $S(x_0) = 1$ et $\forall x \in \mathbb{R}, S(x) \geqslant S(x_0) = 1$. S peut être de n'importe quel degré et ne pas avoir de racine !

Exemple 7

Pour tout n naturel, $X^2 n + 1$ n'a pas de racine réelle. Il y a donc des polynômes de degré aussi grand qu'on veut sans racine réelle.

Tout est-il perdu ? Pas forcément. Ce qui nous intéresse, tout compte fait, c'est moins de trouver des racines que de factoriser P. Nous y reviendrons. Nous avons vu que le cas de $\mathbb{C}$ était plus sympathique, au moins pour le degré 2. Regardons cela. C'est toujours ça de gagné.

2.2.1.2 La factorisation dans $\mathbb{C}$

Dans $\mathbb{C}$, tous les polynômes de degré 2 ont exactement deux racines avec ordre de multiplicité. Cela serait trop beau si ça marchait pour tous les degrés. Mais les maths sont belles ! Il s'agit d'ailleurs du théorème qui suit, aussi appelé théorème de D'Alembert-Gauss.

Théorème 1 – Théorème fondamental de l'algèbre

Tout polynôme non constant à coefficients complexes admet au moins une racine complexe.

$$\underbrace{\forall P \in \mathbb{C}[X],}_{\text{pour tout polynôme à coef. complexes}} \quad \underbrace{\deg P \geqslant 1 \Rightarrow}_{\text{s'il est non constant, alors}} \quad \underbrace{\exists z \in \mathbb{C} : P(z) = 0}_{\text{il existe une racine}}$$

FIGURE 2 – Jean Le Rond D'ALEMBERT — 1717 – 1783

FIGURE 3 – Carl Friedrich GAUSS — 1777 – 1855

Il a une importance capitale dans les maths modernes, comme l'indique l'adjectif « fondamental », mais aussi dans l'histoire des maths. Plusieurs grands noms se sont acharnés à le prouver, avec plus ou moins de succès. La preuve de D'Alembert supposait l'existence de n racines pour un polynôme de degré n. Il disait qu'il y a des racines réelles ou complexes (qui existent) et les autres (qui sont complètement abstraites), et prouvait que ces dernières sont au nombre de 0. Toutefois, il est bizarre de raisonner sur des objets qui sont en dehors de tout ensemble. C'est le problème que Gauss a réglé. Nous ne le démontrerons pas ici.

La puissance de ce théorème se voit mieux en itérant. Reprenons notre factorisation. Nous en étions à $P = (X-\lambda_1)\cdots(X-\lambda_n)Q_n$ et avions supposé qu'on avait factorisé le plus possible, donc que Q_n n'avait plus de racines. D'après le théorème, Q_n devrait avoir une racine s'il n'était pas constant. Donc Q_n est constant. On peut donc mettre tout polynôme complexe sous la forme $P = k(X-\lambda_1)\cdots(X-\lambda_n)$ où k est le coefficient dominant de P. Pour des raisons pratiques, on peut parfois se restreindre à travailler avec des polynômes unitaires, de façon à ce que $k = 1$ et l'oublier discrètement.

Le fait de pouvoir écrire les polynômes sous cette forme est un outil puissant. Tellement que ça a un nom.

Définition 16

On dit qu'un polynôme P est scindé s'il est le produit de polynômes de degré 1 ou 0 (pour le coefficient dominant).

Ainsi, on peut reformuler le théorème fondamental de l'algèbre :

Corollaire 1 – Reformulation du théorème fondamental de l'algèbre.

Dans $\mathbb{C}$, tout polynôme est scindé.

C'est plus concis.

On dit que $\mathbb{C}$ est algébriquement clos. On peut voir $\mathbb{C}$ comme ce qu'on obtient si on prend $\mathbb{R}$ et qu'on ajoute les racines des polynômes à coefficients dans $\mathbb{R}$. C'est d'ailleurs la motivation première de $\mathbb{C}$. Aparté historique. Dans les formules de Cardan, dont je parle plus loin, pour résoudre des équations de degré 3, il arrivait qu'on trouvait sur des choses « absurdes » comme $\sqrt{-1}$. Mais si au lieu de paniquer, on se disait « Bah, c'est pas grave, on va bien voir ce que ça donne », on pouvait trouver que des racines réelles et ces quantités problématiques se simplifiaient ou étaient mises au carré. Beaucoup de mathématiciens ont trouvé ça curieux mais ont laissé faire car *in fine*, ça faisait l'affaire. Avec l'algèbre moderne, on s'est dit que dans ce genre de calculs, il fallait ajouter ces nombres bizarres qui apparaissaient pour former la clôture algébrique de $\mathbb{R}$. D'où la notion moderne de $\mathbb{C}$.

2.2.1.3 La factorisation dans $\mathbb{R}$

Nous avions également laissé de côté le cas des polynômes réels, où on autorise que des racines réelles. Nous avions vu que ça ne peut pas se passer aussi bien, puisqu'il existe des polynômes de n'importe quel degré pair sans racine et nous étions resté sur cette note pessimiste. Mais je me répète : la factorisation ne consiste pas uniquement à trouver des racines ! Et en matière de factorisation, tout n'est pas perdu. On peut prouver à partir du théorème de D'Alembert une variante pour les réels, en terme de factorisation, et non de racines.

Théorème 2 – Théorème de D'Alembert-Gauss dans $\mathbb{R}$

Soit $P \in \mathbb{R}[X]$. On peut écrire P sous la forme

$$P = C(X - \lambda_1) \cdots (X - \lambda_i) \cdot (X^2 + a_1 X + b_1) \cdots (X^2 + a_j X + b_j)$$

Où $\lambda_1, \ldots, \lambda_i \in \mathbb{R}$ sont les racines de P avec ordre de multiplicité, C le coefficient dominant de P et $\forall k \in [\![1, j]\!], a_k^2 - 4b_k < 0$.

En d'autres termes, tout polynôme sans racine dans $\mathbb{R}$ est le produit de trinômes du second degré à discriminant négatif (sans racine réelle).

Étonnant, non ? Prenons un exemple. $P = X^4 + 1$ est clairement sans racine réelle. Un petit peu d'analyse complexe permet de montrer que pour avoir une racine complexe, il faut que $X^2 = i$ ou $X^2 = -i$, donc $X = \frac{1}{\sqrt{2}}(\pm 1 \pm i)$. Donc $P = \left(X - \frac{1}{\sqrt{2}}(1+i)\right)\left(X - \frac{1}{\sqrt{2}}(1-i)\right)\left(X - \frac{1}{\sqrt{2}}(-1+i)\right)\left(X - \frac{1}{\sqrt{2}}(-1-i)\right)$. On remarque que ça forme deux paires de complexes conjugués, on peut les grouper et on trouve $P = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$ qui est bien un produit de deux polynômes réels de degré 2 à discriminant strictement négatif (vérification laissée au lecteur).

Il existe du vocabulaire propre à la factorisation pour dire ça plus facilement

Définition 17

Un polynôme P est dit irréductible s'il n'existe pas de polynômes non constants Q et R tels que $P = QR$.

On peut reformuler le théorème 2 en disant que les seuls polynômes irréductibles dans $\mathbb{R}$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.

Dans $\mathbb{C}$, les seuls polynômes irréductibles sont les polynômes de degré 1.

Eh bien ! Il suffit de trouver les racines d'un polynôme et on connaît tous ses mystères. Oui... mais c'est pas si simple. Vous savez comment trouver les racines des polynômes de degré 1 et 2. Il existe des formules pour les degrés 3 et 4, dites formules de Cardan (qui ont une histoire chaotique), inspirées du degré 2, mais

FIGURE 4 – Évariste GALOIS — 1811 – 1832

nettement plus compliquées. Et c'est tout. Il existe une branche des maths, la théorie de GALOIS, qui prouve qu'on peut pas faire mieux.

Théorème 3 – Théorie de GALOIS

Il n'existe pas de formule générale pour trouver les racines d'un polynôme de degré au moins 5.

Il faut alors parier sur des cas particuliers, de la chance ou des méthodes numériques (mais alors, on n'a qu'une approximation). La conséquence, c'est que si dans vos calculs, vous devez trouver les racines d'un polynôme de degré au moins 5, c'est qu'il y a une erreur ou une autre méthode qui rend ça possible car les polynômes sont particuliers.

Remarque 1

Les polynômes qu'on étudie proviennent des matrices. Or, en physique, ces matrices sont souvent de tailles 2, 3 ou 4 (en mécanique quantique typiquement). Donc trouver les racines n'est pas une tâche herculéenne. Et quand les matrices viennent des maths, elles sont suffisamment particulières pour qu'il existe une méthode.

Vous voilà armés en guerre pour affronter les polynômes caractéristiques que nous verrons une autre fois.

2.2.2 Dans $\mathbb{Q}$

Ce passage est une ouverture pour signaler que malgré les enseignements de Pangloss, tout n'est pas au mieux dans le meilleur des mondes possibles. Ou alors,

FIGURE 5 – Gottfried Wilhelm LEIBNIZ — 1646 – 1716

FIGURE 6 – Ferdinand Gotthold Max EISENSTEIN — 1823 – 1852

notre monde n'est pas le meilleur possible. Je vous laisse en tête à tête avec LEIBNIZ si vous tenez à trancher la question.

Faisons un petit détour par $\mathbb{Q}$. Sous quelles conditions un polynôme rationnel admet des racines rationnelles ? Examinons un exemple : X^2-2. Il a comme racines réelles $\sqrt{2}$ et $-\sqrt{2}$. Mais ces nombres ne sont pas rationnels. Et quid de $X^{2n}-2$? On a $\sqrt[2n]{2}$ et $-\sqrt[2n]{2}$. Même problème. Ça part très mal !

En fait, les polynômes à coefficients dans $\mathbb{Q}$ sont fréquemment rencontrés, mais se comportent très mal et sont souvent étudiés dans $\mathbb{R}$ ou $\mathbb{C}$. En particulier, il existe des polynômes irréductibles de n'importe quel degré. Les plus curieux d'entre vous pourront voir les polynômes cyclotomiques (ainsi que le critère de Gotthold EISENTEIN).

Il existe toutefois un cadre pour travailler avec de tels polynômes. On peut faire

comme avec $\mathbb{R}$! Il manque des nombres dans $\mathbb{R}$ pour exprimer toutes les racines des polynômes, on les ajoute, ça construit la clôture algébrique, c'est $\mathbb{C}$. Faisons pareil avec $\mathbb{Q}$. On prend les polynômes à coefficient dans $\mathbb{Q}$, et on saisi toutes les racines. On obtient alors un ensemble qui contient les rationnel, et certains irrationnels. Ces nombres sont appelés les nombres algébriques. Un nombre qui n'est pas algébrique est dit transcendant.

L'ensemble des algébriques a une structure bâtarde qu'on n'étudiera pas. Mais on trouve des incongruités, $\cos\left(\frac{\pi}{9}\right)$ est algébrique, mais π ou e sont transcendants. On peut également prouver que les nombres algébriques sont dénombrables, c'est à dire en bijection avec $\mathbb{N}$, donc très peu nombreux par rapport à $\mathbb{R}$.

2.3 Lien entre coefficients et racines

On se place ici dans $\mathbb{C}$ où tout polynôme est scindé.

Il est évident qu'il y a un lien entre les racines et les coefficients d'un polynôme. Malheureusement on sait par le théorème 3 (Théorie de Galois) que trouver les racines depuis les coefficients est impossible en général, mais qu'en est-il de l'inverse ?

Prenons un polynôme $P \in \mathbb{C}[X]$ dont les racines avec ordre de multiplicité (donc non nécessairement distinctes) sont $\lambda_1, \ldots, \lambda_n$. Donc $P = k(X-\lambda_1)\cdots(X-\lambda_n)$. Pour ne pas s'embêter avec ça, prenons P unitaire et donc $k = 1$.

$$P = (X-\lambda_1)\cdots(X-\lambda_n) = \prod_{i=1}^{n}(X-\lambda_i)$$

On peut développer le produit et on obtiendra les coefficients. Commençons avec des petits degrés :

$$\begin{aligned} P &= (X-\lambda_1)(X-\lambda_2) \\ &= X^2 - (\lambda_1+\lambda_2)X + \lambda_1\lambda_2 \end{aligned}$$

C'est un résultat connu, la somme et le produit des racines. Mais qu'est ce que ça donne aux degrés supérieurs ?

$$\begin{aligned} P &= (X-\lambda_1)(X-\lambda_2)(X-\lambda_3) \\ &= X^3 - (\lambda_1+\lambda_2+\lambda_3)X^2 + (\lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_2\lambda_3)X - \lambda_1\lambda_2\lambda_3 \end{aligned}$$

Que voit-on émerger ? Pas grand chose encore. Essayons avec 4.

$$\begin{aligned} P &= (X-\lambda_1)(X-\lambda_2)(X-\lambda_3)(X-\lambda_4) \\ &= X^4 - (\lambda_1+\lambda_2+\lambda_3+\lambda_4)X^3 + (\lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_1\lambda_4+\lambda_2\lambda_3+\lambda_2\lambda_4+\lambda_3\lambda_4)X^2 \\ &- (\lambda_1\lambda_2\lambda_3+\lambda_1\lambda_2\lambda_4+\lambda_1\lambda_3\lambda_4+\lambda_2\lambda_3\lambda_4)X + \lambda_1\lambda_2\lambda_3\lambda_4 \end{aligned}$$

Deux observations. En notant n le degré de P, le signe devant le coefficient X^i est $(-1)^{n-i}$. On part de $+$ pour X^n, puis on alterne.

D'autre part, examinons les coefficients. Chacun est constitué d'une somme de produits de racines. Le coefficient de X^4, ce sont tous les produits de 0 racines donc 1 (cas un peu particulier). X^3, la somme de tous les produits de 1 racines, donc simplement la somme des racines. X^2, c'est la somme des produits de 2 racines. X, la somme des produits de 3 racines. Et enfin, la constante est simplement le produit de toutes les racines (le seul produit de n racines).

On peut voir les coefficients comme des polynômes à plusieurs indéterminées en fonction des racines. On appelle ces polynômes, les polynômes symétriques élémentaires.

On peut les exprimer ainsi :

$$\sigma_k(T_1, \ldots, T_n) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} T_{i_1} \cdots T_{i_k}$$

$\sigma_k(T_1, \ldots, T_n)$ est bien la somme de tous les produits de k termes.

À quoi ça sert ? Deux choses. La première utilité est de pouvoir donner des résultats sur les racines alors qu'on est incapable de les trouver. Parfois n'a pas besoin de les déterminer pour prouver ce qu'on veut, et il arrive que les polynômes symétriques élémentaires nous y aident. Le second bienfait, c'est que ça permet de trouver rapidement les racines sans avoir à factoriser. Il ne nous en manque qu'une ? On peut se souvenir que le coefficient de X^0 est le produit des racines et de X^{n-1}, la somme des racines (toujours au signe près), ce qui permet parfois de s'en tirer facilement !