Polynômes et fractions rationnelles

Didier Piau et Bernard Ycart

Tout le monde connaît les fonctions polynomiales : ce sont simplement les fonctions comme $t \mapsto 4 + 5t^2 + 7t^3 + t^5$. Les *polynômes* en sont une version plus algébrique, dont les avantages peuvent paraître assez subtils la première fois qu'on les découvre ; soyez cependant assurés qu'ils existent, y compris si on en reste à un point de vue purement pratique. Un bagage minimum suffit pour aborder ce chapitre : un peu d'arithmétique des entiers et quelques notions sur les espaces vectoriels, sans même que ce soit vraiment indispensable.

Table des matières

1 Cours

1.1 Anneau des polynômes

L'idée de la construction sera peut-être compréhensible si on se demande comment stocker une fonction polynomiale de $\mathbb{R}$ dans $\mathbb{R}$ dans une mémoire de machine : stocker *toutes* les valeurs de la fonction étant impossible, un bon procédé pour représenter la fonction $t \mapsto 4 + 5t^2 + 7t^3 + t^5$, par exemple, sera de stocker la suite de ses coefficients ; on entrera donc dans la machine la suite 405701, ce qui indique que le coefficient de t^0 est 4, celui de t est 0, celui de t^2 est 5, etc.

Ce procédé de stockage sera tout bonnement la définition même des polynômes. Simplement, comme un polynôme peut en théorie être de degré gigantesque, bien plus grand que les capacités de stockage de toute machine, il faudra se résigner à stocker une infinité de coefficients, dont seuls les N premiers seront non nuls (la métaphore technologique s'écroule alors) : ainsi notre polynôme-exemple sera stocké comme $4057010000\ldots$ (puis encore une infinité de 0), occupant inutilement une infinité de cases-mémoire.

Définition 1. *Soit $(A, +)$ un groupe de neutre 0. Une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A est dite* à support fini*, ou bien* nulle à partir d'un certain rang*, si le nombre d'indices n pour lesquels $a_n \neq 0$ est fini. En d'autres termes, il existe un indice N fini tel que $a_n \neq 0$ implique $n \leqslant N$.*

Définition 2. *Soit $(A, +, \cdot)$ un anneau commutatif. Notons provisoirement B l'ensemble des suites d'éléments de A, à support fini. On définit sur B une addition et une multiplication par les formules*

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}},$$

et

$$(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}} \qquad \text{où} \quad c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

Proposition 1. *L'ensemble B muni des deux lois définies ci-dessus est un anneau commutatif.*

Démonstration : Il est facile de vérifier que $(B, +)$ est un sous-groupe du groupe abélien (additif) de toutes les suites d'éléments de A. En effet, le neutre de A est la suite identiquement nulle, qui appartient à B ; la somme de deux suites à supports finis est à support fini : si $a_n = 0$ pour tout $n > N$ et si $b_n = 0$ pour tout $n > M$, alors $a_n + b_n = 0$ pour tout $n > \max\{N, M\}$ (et peut-être pour d'autres indices n également mais ce n'est pas important) ; enfin si $-a$ désigne l'opposé d'un élément a de A, alors l'opposé d'un élément $(a_n)_{n\in\mathbb{N}}$ de B est la suite $(-a_n)_{n\in\mathbb{N}}$, qui est effectivement à support fini.

Pour ce qui concerne la deuxième loi, on doit tout d'abord vérifier que $(c_n)_{n\in\mathbb{N}}$ est bien une suite de B. Avec les mêmes notations que pour l'addition, pour tout indice $n > M + N$, dans le calcul de

$$c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{N} a_k b_{n-k} + \sum_{k=N+1}^{n} a_k b_{n-k},$$

tous les termes de la première somme sont nuls, car les indices utilisés sont tels que $n - k > M + N - k \geqslant M$ donc $b_{n-k} = 0$. Tous les termes de la deuxième somme sont nuls aussi car $k > N$ donc $a_k = 0$. Tous les coefficients c_n pour $n > M + N$ sont donc nuls et $(c_n)_{n\in\mathbb{N}}$ est bien un élément de B.

On va ensuite vérifier que pour ces formules, B est un anneau commutatif. C'est peu engageant et il n'y a guère d'astuces. Il faut calculer brutalement.

Commutativité

Soient $(a_i)_{i\in\mathbb{N}}$ et $(b_j)_{j\in\mathbb{N}}$ deux éléments de B ; notons $(c_k)_{k\in\mathbb{N}}$ le produit de $(a_i)_{i\in\mathbb{N}}$ par $(b_j)_{j\in\mathbb{N}}$. Alors pour tout $k \geqslant 0$, $c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{j=0}^{k} a_{k-j} b_j$ (en posant $j = k - i$) ; cette expression est bien celle qu'on trouverait en faisant le produit dans l'autre sens (en utilisant la commutativité de A).

Associativité

Soient $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ et $(c_n)_{n\in\mathbb{N}}$ trois éléments de B ; notons $(d_n)_{n\in\mathbb{N}}$ le produit de $(b_n)_{n\in\mathbb{N}}$ par $(c_n)_{n\in\mathbb{N}}$. Notons $(e_n)_{n\in\mathbb{N}}$ le produit de $(a_n)_{n\in\mathbb{N}}$ par $(d_n)_{n\in\mathbb{N}}$. Pour $n \geqslant 0$, calculons

$$e_n = \sum_{i=0}^{n} a_i d_{n-i} = \sum_{i=0}^{n} a_i \sum_{j=0}^{n-i} c_j b_{n-i-j} = \sum_{(i,j)} a_i b_{n-i-j} c_j,$$

où la dernière somme porte sur tous les couples $(i, j) \in \mathbb{N}^2$ tels que $i + j \leqslant n$.

On trouverait la même chose en calculant de la même façon le produit de $(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}}$ par $(c_n)_{n\in\mathbb{N}}$.

Existence d'un élément neutre

La suite $(1, 0, 0, 0, \ldots)$ est neutre pour cette multiplication.

Distributivité

Encore une vérification ennuyeuse, celle-là on va l'omettre.

On a bien vérifié que B est un anneau commutatif. □

Notation 1. *On note* 0 *la suite nulle. On appelle* indéterminée *l'élément*

$$(0, 1, 0, 0, \ldots)$$

de B dont tous les termes sont nuls sauf le terme de numéro 1 *qui vaut* 1. *On note souvent (mais pas toujours) X l'indéterminée.*

Proposition 2. *Pour tout élément P de B tel que $P \neq 0$, il existe un unique entier $d \geqslant 0$ et un unique $(d+1)$-uplet $(a_i)_{0 \leqslant i \leqslant d}$ d'éléments de A tels que $a_d \neq 0$ et*

$$P = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0.$$

Démonstration : Il suffit de remarquer que, pour tout $n \geqslant 1$, X^n est la suite dont tous les termes sont nuls sauf le terme de numéro n qui vaut 1. Ensuite, on réécrit les définitions. □

Notation 2. *Si X est l'indéterminée de B, on note $B = A[X]$ et on appelle $A[X]$ l'anneau des polynômes sur A.*

Profitons-en pour faire quelques calculs.

Exemple 1. *Soient $P = X^3 - 3X^2 + 2$ et $Q = X^2 - X + 2$. Il s'agit de calculer le polynôme PQ.*

On pourra décomposer un des deux polynômes, par exemple Q, en somme de monômes, donc X^2, $-X$ et 2, puis effectuer chacune des multiplications de P par ces monômes, et enfin tout regrouper. Une présentation claire, en alignant les monômes de mêmes degrés, est une condition nécessaire de calcul sans erreurs.

$$\begin{array}{rcccccccc}
X^2 \times P & = & X^5 & -3X^4 & & +2X^2 & & \\
-X \times P & = & & -X^4 & +3X^3 & & -2X & \\
2 \times P & = & & & 2X^3 & -6X^2 & & +4 \\
\hline
Q \times P & = & X^5 & -4X^4 & +5X^3 & -4X^2 & -2X & +4
\end{array}$$

Définition 3. *Pour tout élément P non nul de $A[X]$, l'unique entier $d \geqslant 0$ intervenant dans l'écriture de P en fonction de l'indéterminée dans la proposition 2 est appelé le* degré *de P. Par convention, le degré du polynôme nul est le symbole $-\infty$.*

Notation 3. *Le degré d'un polynôme P est noté* $\deg P$.

Définition 4. *Pour P élément non nul de $A[X]$, le* coefficient dominant *de P est le coefficient a_d du terme de plus haut degré dans l'écriture de P en fonction de l'indéterminée. Par convention, le coefficient dominant du polynôme nul est* 0. *Enfin, un polynôme est dit* unitaire *lorsque son coefficient dominant est égal à* 1.

Proposition 3. *Soient P et Q deux polynômes de $A[X]$. Alors :*

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

Démonstration : Si P ou Q est nul, le résultat est évident. Sinon, notons d le degré de P et e le degré de Q puis $P = a_d X^d + \cdots + a_0$ et $Q = b_e X^e + \cdots + b_0$ pour des a_i et b_i dans A. Si $d > e$, on peut alors écrire :

$$P + Q = a_d X^d + \cdots + a_{e+1} X^{e+1} + (a_e + b_e) X^e + \cdots + (a_0 + b_0).$$

Il apparaît alors que $\deg(P+Q) = d = \max(\deg P, \deg Q)$. Le cas où $d < e$ est similaire. Enfin, lorsque $d = e$, on a un regroupement :

$$P + Q = (a_d + b_d)X^d + \cdots + (a_0 + b_0).$$

Ou bien tous les coefficients y sont nuls, et $\deg(P + Q) = -\infty$ rendant l'inégalité évidente, ou bien un au moins est non nul et le coefficient non nul de plus fort indice est le degré de $P + Q$ qui est bien inférieur ou égal à d. □

Proposition 4. *Soit A est un anneau commutatif* intègre *(sans diviseur de zéro). Soient P et Q deux polynômes de $A[X]$. Alors :*

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

Remarque : Pour un anneau non intègre, on a encore une inégalité, mais cela ne semble pas indispensable à mémoriser (d'autant que la preuve en est très facile).

Démonstration : Essentiellement déjà faite.

Si P ou Q est nul, c'est évident ; sinon notons d le degré de P et e le degré de Q puis $P = a_dX^d + \cdots + a_0$ et $Q = b_eX^e + \cdots + b_0$ pour des a_i et b_i dans A. On a alors

$$PQ = a_db_eX^{d+e} + (a_db_{e-1} + a_{d-1}b_e)X^{d+e-1} + \cdots + a_0b_0.$$

Si on n'est pas convaincu par les points de suspension, on écrira plus précisément :

$$PQ = \sum_{k=0}^{d+e} \left(\sum_{i=0}^{k} a_ib_{k-i} \right) X^k,$$

en ayant préalablement convenu que $a_i = 0$ pour $i > d$ et $b_i = 0$ pour $i > e$.

Comme l'anneau a été supposé intègre, le produit a_db_e n'est pas nul, donc le degré de PQ est exactement égal à $d + e$. □

Définition 5. *Pour un polynôme $P = a_dX^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$ non nul dans $A[X]$, le* polynôme dérivé *de P est le polynôme :*

$$da_dX^{d-1} + (d-1)a_{d-1}X^{d-2} + \cdots + a_1.$$

Si $P = 0$, le polynôme dérivé de P est le polynôme nul.

Notation 4. *Le polynôme dérivé de P est noté P'. Par analogie avec les fonctions, on notera ensuite P'' la dérivée de P', puis $P^{(n)}$ la dérivée n-ième.*

Proposition 5. *Soient P et Q deux polynômes de $A[X]$. Alors :*

$$(P + Q)' = P' + Q' \qquad \text{et} \qquad (PQ)' = P'Q + PQ'.$$

Démonstration : Simple vérification évidente pour l'addition et ennuyeuse pour la multiplication. □

Définition 6. *Soit*

$$P = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0$$

un polynôme de $A[X]$ et x un élément de A. La valeur de P en x, *notée $P(x)$, est l'élément de A égal à*

$$a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

Proposition 6. *Soient P et Q deux polynômes de $A[X]$ et x un élément de A. Alors*

$$(P+Q)(x) = P(x) + Q(x) \quad et \quad (PQ)(x) = P(x)Q(x)$$

Démonstration : Simple vérification ; on pourrait aussi énoncer $1(x) = 1$ qui est évident et complète la collection d'évidences. □

La notation $P(x)$ n'a pas que des avantages : elle incite hélas à confondre le polynôme P avec la fonction qu'il n'est pas. Bien que la notation soit la même, cette définition ne se confond pas avec celle de valeur d'une application en un point.

La définition qui suit cherche à reproduire la notion de composition des fonctions (encore une fois, insistons sur le fait que les polynômes ne sont pas des fonctions). Elle est utilisée une seule fois plus loin, pour écrire la formule de Taylor relative aux polynômes.

Définition 7. *Soient P et Q deux polynômes de $A[X]$, avec $P = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0$. On appelle* composé *de P par Q le polynôme*

$$a_d Q^d + a_{d-1} Q^{d-1} + \cdots + a_1 Q + a_0$$

Notation 5. *Ce composé est noté, selon le contexte $P \circ Q$ ou $P(Q)$. Typiquement, pour $Q = X^n$, la notation $P(X^n)$ s'impose et est d'ailleurs d'interprétation évidente.*

Nous terminons cette section par quelques remarques d'algèbre linéaire, valables uniquement dans le cas où l'anneau commutatif des coefficients est un corps $\mathbb{K}$. Tout d'abord, $\mathbb{K}[X]$ est un espace vectoriel sur $\mathbb{K}$. Le plus simple est encore de vérifier à la main la définition des espaces vectoriels, ce que l'on va se garder de faire explicitement ici d'autant que la démonstration sera faite dans le chapitre *Espaces vectoriels*.

En fait, la définition de l'anneau des polynômes devrait évoquer le concept de **base**, avec son existence et unicité d'écriture comme une sorte de combinaison linéaire. La seule différence avec les vraies combinaisons linéaires est qu'on va chercher les vecteurs de « base » dans une famille infinie.

Proposition 7. *Soit $\mathbb{K}$ un corps commutatif. La suite $(X^i)_{i\in\mathbb{N}}$ est une « base » de $\mathbb{K}[X]$ au sens suivant. Pour tout élément P de $\mathbb{K}[X]$, il existe une suite unique $(a_n)_{n\geqslant 0}$ d'éléments de $\mathbb{K}$, à support fini, telle que*

$$P = \sum_{n\in\mathbb{N}} a_n X^n,$$

au sens où, si N est tel que $a_n = 0$ pour tout $n > N$, on a

$$P = \sum_{n=0}^{N} a_n X^n.$$

La démonstration étant quasiment tautologique, on l'omettra, se bornant à remarquer que seule la deuxième somme, comportant un nombre fini de termes, est bien définie.

Quoi qu'il en soit, $\mathbb{K}[X]$ est votre premier exemple raisonnablement simple d'espace vectoriel ayant une base infinie. Toutefois, on est toujours plus à l'aise dans les espaces de dimension finie. Il est donc intéressant d'introduire la

Notation 6. *Soit $\mathbb{K}$ un corps commutatif et $n \geqslant 0$ un entier. On note $\mathbb{K}_n[X]$ l'ensemble des polynômes sur $\mathbb{K}$ de degré inférieur ou égal à n.*

Proposition 8. *Pour tout entier $n \geqslant 0$, $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$. Une base de $\mathbb{K}_n[X]$ est $(1, X, \ldots, X^n)$. La dimension de $\mathbb{K}_n[X]$ est $n+1$.*

Démonstration : On remarque que $\mathbb{K}_n[X]$ est l'ensemble engendré par $(1, X, \ldots, X^n)$: c'est donc un sous-espace vectoriel. De plus cette famille génératrice est libre (soit par une vérification directe, soit d'après l'unicité de la décomposition de la proposition 7), c'est donc une base de $\mathbb{K}_n[X]$. □

Définition 8. *La base $(X^i)_{i\in\mathbb{N}}$ de $\mathbb{K}[X]$ est appelée sa* base canonique.
La base $(1, X, \ldots, X^n)$ de $\mathbb{K}_n[X]$ est aussi appelée sa base canonique.

Remarque : Le lecteur pourra avoir l'impression qu'on passe son temps à définir de partout des « bases canoniques » : on en a vu pour $\mathbb{K}^n$, puis pour les espaces de matrices, et maintenant pour les polynômes. C'est fini pourtant. Insistons bien sur le fait qu'un espace « abstrait » n'a *pas* de base canonique : le mot est réservé à certaines bases, remarquables par leur simplicité, d'espaces très particuliers.

Le lemme qui suit servira pour prouver la formule de Taylor et est une redite du chapitre *Espaces vectoriels*. Un énoncé séparé n'était donc peut-être pas nécessaire mais, même si ce n'est pas indispensable, cela ne peut faire de mal de le connaître ; le plus important étant de comprendre et savoir refaire sa brève démonstration.

Lemme 1. *Soit $\mathbb{K}$ un corps commutatif et $(P_0, P_1, \ldots, P_n)$ une famille de polynômes de $\mathbb{K}[X]$ tels que $0 \leqslant \deg P_0 < \deg P_1 < \cdots < \deg P_n$. Alors $(P_0, P_1, \ldots, P_n)$ est une famille libre.*

Démonstration : La famille (P_0) est libre, car il résulte de l'hypothèse $0 \leqslant \deg P_0$ que P_0 n'est pas nul. Puis le système (P_0, P_1) est libre puisque P_1, de degré strictement plus grand que P_0, ne peut lui être proportionnel. Puis (P_0, P_1, P_2) est libre, puisque toute combinaison linéaire de (P_0, P_1) est de degré inférieur ou égal à $\deg P_1$ donc P_2 ne peut en être une. Et ainsi de suite (ou plus proprement on fait une récurrence sur n). □

1.2 Arithmétique des polynômes

Il s'agit de répéter pour les polynômes des résultats similaires à ceux qui ont été énoncés pour les entiers.

Premier point à observer : l'arithmétique sur les polynômes est tout à fait analogue à celle sur les entiers à condition de travailler sur des polynômes sur un corps commutatif. Sur un anneau commutatif quelconque (même intègre) se glissent quelques bizarreries.

Second point à observer : les énoncés donnés sur les entiers l'ont été sur des entiers positifs. Ils se modifient sans trop de mal pour des entiers de $\mathbb{Z}$ mais parfois en s'alourdissant un peu ; ainsi dans $\mathbb{Z}$ on ne peut plus affirmer l'existence d'un entier d unique tel que n divise 10 et 6 si et seulement si n divise d (le pgcd de 10 et 6) : il en existe toujours un, mais il n'est plus unique, on peut prendre $d = 2$ mais aussi $d = -2$. Les polynômes unitaires joueront un rôle analogue aux entiers positifs mais ils sont légèrement moins confortables, dans la mesure où la somme de deux entiers positifs est positive alors que la somme de deux polynômes unitaires n'est pas nécessairement unitaire. Attention à ces petits détails donc, en apprenant les énoncés.

Commençons par donner une définition, à partir de laquelle on ne montrera guère de théorèmes que dans $\mathbb{K}[X]$ mais que ça ne coûte pas plus cher de donner sur un anneau commutatif quelconque.

Définition 9. *Soit A un anneau commutatif. On dit qu'un polynôme P dans $A[X]$ est un* multiple *d'un polynôme S dans $A[X]$, ou, de manière équivalente, que S est un* diviseur *de P, lorsqu'il existe un polynôme T dans $A[X]$ tel que $P = ST$.*

Comme pour les entiers, tout repose sur la division euclidienne.

Théorème 1. *Soit $\mathbb{K}$ un corps commutatif, A un polynôme de $\mathbb{K}[X]$ et B un polynôme non nul de $\mathbb{K}[X]$. Il existe un couple (Q, R) unique de polynômes vérifiant la double condition :*

$$A = QB + R \qquad \text{et} \qquad \deg R < \deg B.$$

Démonstration : On prouvera successivement l'existence et l'unicité de (Q, R).

Existence de (Q, R)

La preuve est significativement différente de celle utilisée pour les entiers. Elle est toujours basée sur une maximisation/minimisation, mais les polynômes n'étant pas totalement ordonnés, cette maximisation est un peu plus technique.

Dans le cas stupide où B divise A, prenons $R = 0$ et Q tel que $A = BQ$. Sinon, considérons l'ensemble

$$\mathcal{R} = \{A - QB \mid Q \in \mathbb{K}[X]\},$$

qui est donc un ensemble non vide de polynômes non nuls ; puis l'ensemble

$$E = \{\deg R \mid R \in \mathcal{R}\},$$

qui est un ensemble d'entiers positifs non vide. Cet ensemble E possède donc un plus petit élément d ; prenons un R dans $\mathcal{R}$ dont le degré soit d et enfin un Q tel que $A - QB = R$.

Nous devons vérifier que ces choix conviennent ; l'identité entre A, B, Q et R est claire, reste l'inégalité concernant les degrés. Vérifions-la par l'absurde, en supposant que $\deg B \leqslant \deg R$; notons e le degré de B et

$$B = b_e X^e + b_{e-1}X^{e-1} + \cdots + b_0, \quad R = r_d X^d + r_{d-1}X^{d-1} + \cdots + r_0.$$

Posons

$$Q_1 = Q + \frac{r_d}{b_e}X^{d-e}.$$

Remarquons qu'en écrivant cette définition, on utilise l'hypothèse $\deg B \leqslant \deg R$, qui justifie que X^{d-e} ait un sens, et simultanément le fait qu'on travaille dans un corps, qui justifie la possibilité de diviser par b_e.

Considérons alors

$$R_1 = A - Q_1 B = A - QB - \left(\frac{r_d}{b_e}X^{d-e}\right)B,$$

donc

$$R_1 = R - \left(b_e X^e + b_{e-1}X^{e-1} + \cdots + b_0\right)\left(\frac{r_d}{b_e}X^{d-e}\right).$$

Dans cette dernière écriture, on voit se simplifier les termes en X^d de R et du produit qu'on lui a soustrait, et on constate donc avoir obtenu un polynôme R_1 de degré strictement plus petit que celui de R. Mais alors le degré de R_1 est dans E et contredit l'hypothèse de minimisation qui a fait choisir d. Contradiction !

Unicité de (Q, R)

Soient (Q_1, R_1) et (Q_2, R_2) deux couples vérifiant les deux conditions exigées dans l'énoncé du théorème.

On déduit de $A = Q_1B + R_1 = Q_2B + R_2$ que $(Q_2 - Q_1)B = R_1 - R_2$. Ainsi, $R_1 - R_2$ est un multiple de B. Des conditions $\deg R_1 < \deg B$ et $\deg R_2 < \deg B$, on déduit que $\deg(R_1 - R_2) < \deg B$.

Ainsi $R_1 - R_2$ est un multiple de B de degré strictement plus petit. La seule possibilité est que $R_1 - R_2$ soit nul. On en déduit $R_1 = R_2$, puis, en allant reprendre l'égalité $(Q_2 - Q_1)B = R_1 - R_2$, que $Q_1 = Q_2$. □

Remarque : On a choisi d'énoncer ce théorème sur un corps commutatif pour faciliter sa mémorisation et parce que l'on n'aura presque jamais besoin d'un énoncé plus général. On aura toutefois besoin une fois de l'utiliser pour des polynômes sur un anneau ; remarquons donc que la démonstration montre que le résultat reste vrai sur un anneau commutatif quelconque à condition de supposer non seulement que B est non nul, mais même que son coefficient dominant est inversible : le seul endroit où on a utilisé qu'on s'était placé dans un corps commutatif a en effet été une division par ce coefficient dominant.

Exemple 2. *Concrètement, on disposera les divisions euclidiennes de polynômes comme les divisions de nombres entiers. Par exemple, pour diviser* $P = X^2 + X + 1$ *par* $Q = X - 1$*, on écrit :*

$$\begin{array}{r|l} X^2+X+1 & X-1 \\ \cline{2-2} X^2-X & X+2 \\ \cline{1-1} \quad 2X+1 & \\ \quad 2X-2 & \\ \cline{1-1} \quad -1 & \end{array}$$

Ce qui fournit la division euclidienne :

$$P = (X+2)Q - 1.$$

Nous définissons ensuite le pgcd. On ne donnera pas ici d'énoncés concernant le ppcm, non qu'il n'y en ait pas (ce sont là aussi les mêmes qu'en arithmétique des entiers) mais parce qu'ils ne semblent pas très importants. Les étudiants curieux les reconstitueront eux-mêmes.

Théorème 2. *Soit* $\mathbb{K}$ *un corps commutatif. Soient* A *et* B *deux polynômes de* $\mathbb{K}[X]$*. Il existe un unique polynôme* unitaire D *de* $\mathbb{K}[X]$ *tel que pour tout polynôme* P *de* $\mathbb{K}[X]$*,* P *divise* A *et* B *si et seulement si* P *divise* D*.*

De plus il existe deux polynômes S *et* T *de* $\mathbb{K}[X]$ *tels que* $D = SA + TB$ *(identité de Bézout).*

Et tant qu'on y est avant de passer aux démonstrations :

Définition 10. *Le* plus grand commun diviseur *de deux polynômes* A *et* B *est le polynôme unitaire* D *apparaissant dans l'énoncé du théorème précédent.*

Notation 7. *Le plus grand commun diviseur de* A *et* B *sera noté* $\mathrm{pgcd}(A, B)$*.*

Comme pour les entiers, plusieurs démonstrations sont possibles ; on ne donne que celle basée sur l'algorithme d'Euclide.

Démonstration : La démonstration est une récurrence sur le degré de B.

Merveilles du copier-coller, voici de nouveau un « résumé de la preuve » sous forme de programme informatique récursif (le même que pour l'arithmétique des entiers) :

```
Début du programme
   * Pour B = 0, pgcd(A, 0) = A/coefficient dominant de A.
   * Soit R le reste de la division euclidienne de A par B.
   Les diviseurs communs de A et B sont ceux de B et R.
   D'où : pgcd(A, B) = pgcd(B, R).
Fin du programme
```

Et voici, toujours par les vertus du copier-coller, la preuve récurrente formelle. On va démontrer par « récurrence forte » sur le degré d de B l'hypothèse (H_d) suivante :

> (H_d) Pour tout polynôme A et tout polynôme B de degré d, il existe deux polynômes S et T tels que, pour tout polynôme P, P divise A et B si et seulement si P divise $SA+TB$.

Vérifions $(H_{-\infty})$.

Il s'agit donc de traiter le cas où $B = 0$. Soit A un polynôme ; tout polynôme P qui divise A divise aussi $B = 0$ puisque $0P = 0$. Pour tout P, P divise A et 0 si et seulement si P divise A. Prenons alors $S = 1$ et $T = 0$: on a donc bien pour tout P : P divise A et 0 si et seulement si P divise $SA + T \times 0$.

Soit d un entier fixé. Supposons la propriété (H_c) vraie pour tout c strictement inférieur à d et montrons (H_d).

Soient A un polynôme et B un polynôme de degré d. Notons $A = BQ+R$ la division euclidienne de A par B (qu'on peut réaliser puisque $B \neq 0$).

Vérifions l'affirmation intermédiaire suivante : pour tout P, P est un diviseur commun de A et B si et seulement si P est un diviseur commun de B et R. (Avec des mots peut-être plus lisibles : « les diviseurs communs de A et B sont les mêmes que ceux de B et R »).

Soit P un diviseur commun de A et B, alors P divise aussi $R = A - BQ$; réciproquement soit P un diviseur commun de B et R, alors P divise aussi $A = BQ + R$.

L'affirmation intermédiaire est donc démontrée.

On peut alors appliquer l'hypothèse de récurrence $(H_{\deg R})$ (puisque précisément $\deg R < \deg B$) en l'appliquant au polynôme B.

On en déduit qu'il existe deux polynômes S_1 et T_1 tels que pour tout P, P divise B et R si et seulement si P divise $S_1B + T_1R$.

Remarquons enfin que $S_1B + T_1R = S_1B + T_1(A - BQ) = T_AA + (S_1 - Q)B$, et qu'ainsi, si on pose $S = T_A$ et $T = S_1 - Q$ on a bien prouvé que, pour tout P, P divise Q et B si et seulement si P divise $SA + TB$.

(H_d) est donc démontrée.

On a donc bien prouvé (H_d) pour tout $d \in \mathbb{N} \cup \{-\infty\}$.

Une fois qu'on en est arrivé là, il ne reste donc plus qu'à montrer que pour *un* polynôme P (le polynôme $SA+TB$) il existe un unique D unitaire tel que Q divise P si et seulement si Q divise D. L'existence est claire : comme le résumé le suggère, on

divise P par son coefficient dominant et on obtient un polynôme D unitaire ayant les mêmes diviseurs que P. Pour ce qui est de l'unicité, elle est évidente pour P nul ; on supposera P non nul. Soit maintenant D_1 un polynôme unitaire ayant exactement les mêmes diviseurs que P. Alors comme P divise P, P divise D_1, et comme D_1 divise D_1, D_1 divise P. Les polynômes P et D_1 se divisent donc mutuellement ; soit Q_1 et Q_2 les quotients respectifs de P par D_1 et de D_1 par P. En utilisant la formule calculant le degré d'un produit, on voit que forcément, P a même degré que D_1 et que les polynômes Q_1 et Q_2 sont de degré nul, donc des constantes λ_1 et λ_2. Soit a_d le coefficient dominant de P ; le coefficient dominant de $Q_1 D_1 = P$ vaut $\lambda_1 \cdot 1$ donc $\lambda_1 = a_d$ et D_1 est égal à $P/$(coefficient dominant de P), donc à D, ce qui prouve l'unicité. □

Nous allons ensuite définir le pgcd d'un nombre fini de polynômes. En arithmétique des entiers, cette notion n'est pas primordiale ; en revanche dans les applications des raisonnements arithmétiques à des polynômes, on est souvent dans des cas où on s'intéresse à des pgcds de plus de deux polynômes à la fois.

L'énoncé donné ci-dessus pour deux polynômes se généralise à un nombre fini, par récurrence sur ce nombre.

Proposition 9. *Soit $\mathbb{K}$ un corps commutatif, $n \geqslant 1$ un entier et A_1, A_2, …, A_n des polynômes de $\mathbb{K}[X]$. Il existe un unique polynôme unitaire D de $\mathbb{K}[X]$ tel que pour tout P dans $\mathbb{K}[X]$, P divise tous les A_i de $i = 1$ à $i = n$ si et seulement si P divise D.*

De plus il existe n polynômes $S_1, \ldots, S_n$ tels que

$$D = S_1 A_1 + S_2 A_2 + \cdots + S_n A_n$$

(identité de Bézout).

Démonstration : C'est une récurrence facile sur n. Le cas $n = 2$ est l'objet du théorème précédent (et le cas $n = 1$ a été traité dans sa démonstration, ou on peut le ramener fictivement à $n = 2$ en disant que les diviseurs de A_1 sont les diviseurs communs de A_1 et de 0).

Soit $n \geqslant 2$ fixé, supposons la proposition vraie pour tout ensemble de n polynômes. Prenons $n+1$ polynômes $A_1, A_2, \ldots, A_{n+1}$. Notons B le pgcd des n premiers, qui existe par l'hypothèse de récurrence. Alors les diviseurs communs de A_1, A_2, …, A_{n+1} sont les diviseurs communs de B et de A_{n+1} ; donc prendre $D = \mathrm{pgcd}(B, A_{n+1})$ répond à la question. L'unicité est claire : si D_1 répondait aussi à la question, les diviseurs de D_1 seraient exactement les mêmes que ceux de D avec D et D_1 tous deux unitaires, et comme dans la preuve du théorème précédent (ou en appliquant le théorème précédent à D et 0), on conclut que $D = D_1$. La relation de Bézout est aussi le résultat d'une récurrence immédiate : il existe $S_1, S_2, \ldots, S_n$ tels que $B = S_1 A_1 + S_2 A_2 + \cdots + S_n A_n$ et T_1 et T_2 tels que $D = T_1 B + T_2 A_{n+1}$ donc

$$D = (T_1 S_1) A_1 + (T_1 S_2) A_2 + \cdots + (T_1 S_n) A_n + T_2 A_{n+1}.$$

□

Définition 11. *Soit* $\mathbb{K}$ *un corps commutatif et* $n \geqslant 1$ *un entier. On dira que* n *polynômes de* $\mathbb{K}[X]$ *sont* premiers entre eux *lorsque leurs seuls diviseurs communs sont constants (en d'autres termes, quand leur* pgcd *est* 1*).*

On prendra garde à ne pas confondre « premiers entre eux » (on dit parfois « premiers entre eux dans leur ensemble ») et « deux à deux premiers entre eux » : dans $\mathbb{R}[X]$, les polynômes

$$(X-1)(X-2)\,, \quad (X-1)(X-3)\,, \quad (X-2)(X-3)$$

sont premiers entre eux (dans leur ensemble) mais ils ne sont pas deux à deux premiers entre eux.

Les polynômes irréductibles sont les analogues des nombres premiers. Toutefois les usages étant ce qu'ils sont, il y a une petite nuance de vocabulaire un peu désagréable : alors que le mot « nombre premier » est réservé à des entiers positifs, le mot « polynôme irréductible » n'est pas réservé à des polynômes unitaires. On se méfiera de cette peu perceptible nuance qui crée de légères discordances entre énoncés analogues portant les uns sur les polynômes et les autres sur les entiers.

Définition 12. *Soit* $\mathbb{K}$ *un corps commutatif. On dira qu'un polynôme* P *dans* $\mathbb{K}[X]$ *est* **irréductible** *lorsqu'il possède exactement deux diviseurs unitaires.*

On remarquera tout de suite que ces deux diviseurs unitaires sont alors forcément les polynômes 1 et $P/$(coefficient dominant de P).

La proposition suivante est évidente, mais donne un exemple fondamental de polynômes irréductibles :

Proposition 10. *Soit* $\mathbb{K}$ *un corps commutatif. Dans* $\mathbb{K}[X]$*, les polynômes du premier degré sont irréductibles.*

Démonstration : Soit $P = aX+b$ avec $a \neq 0$ un polynôme du premier degré dans $\mathbb{K}[X]$. Cherchons ses diviseurs unitaires. Un diviseur de P doit avoir un degré inférieur ou égal à celui de P. Le seul diviseur unitaire constant de P est le seul polynôme constant unitaire : la constante 1. Cherchons les diviseurs unitaires de la forme $X + c$ de P. Si $X + c$ divise P, il existe un polynôme Q tel que $P = (X + c)Q$ et en comparant les degrés, Q est nécessairement constant. En comparant les coefficients dominants, nécessairement $Q = a$ donc $c = \dfrac{b}{a}$. Ainsi P possède exactement un diviseur unitaire du premier degré, le polynôme $X + \dfrac{b}{a}$. Le polynôme P est donc irréductible. □

Sur un corps quelconque, déterminer quels polynômes sont irréductibles et lesquels ne le sont pas est un problème très sérieux ; dans quelques pages, nous verrons que ce problème a une solution simple dans les cas particuliers des polynômes à coefficients complexes ou réels.

Le résultat fondamental est, comme en arithmétique entière, l'existence et unicité de la décomposition en facteurs irréductibles. Elle repose là encore sur le « lemme de Gauss ». On ne réécrit pas les démonstrations pour deux raisons totalement contradictoires : d'abord parce que ce sont exactement les mêmes, et ensuite parce que ce ne sont pas exactement les mêmes –une petite difficulté se pose pour énoncer l'unicité de la décomposition en facteurs irréductibles d'un polynôme. Pour des entiers, on a convenu de classer les facteurs dans l'ordre croissant : ainsi 6 se décompose en $2 \cdot 3$ et non en $3 \cdot 2$. Une telle convention ne peut être appliquée pour décomposer des polynômes, aucun ordre « raisonnable » n'étant à notre disposition sur l'ensemble des polynômes irréductibles ; ainsi dans $\mathbb{C}[X]$ peut-on écrire selon la fantaisie du moment $X^2+1 = (X-\mathrm{i})(X+\mathrm{i})$ ou $X^2+1 = (X+\mathrm{i})(X-\mathrm{i})$. Quand on énonce ci-dessous que la décomposition est « unique » on sous-entend donc qu'on considère les deux exemples qui précèdent comme la même décomposition, ce qui peut s'énoncer rigoureusement mais lourdement. Voulant glisser sur ce détail, on se condamne à rester un peu vaseux.

Voici donc le lemme de Gauss.

Lemme 2. *Soit $\mathbb{K}$ un corps commutatif. Soient A, B et C trois polynômes de $\mathbb{K}[X]$. Si A divise BC et est premier avec C, alors A divise B.*

Démonstration : La même que pour les entiers, avec des majuscules. □

Et voici le théorème de décomposition en facteurs irréductibles.

Théorème 3 (Énoncé moyennement précis)**.** *Soit $\mathbb{K}$ un corps commutatif.*
Tout polynôme P non nul de $\mathbb{K}[X]$ peut s'écrire de façon « unique » en produit :

$$P = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_k^{\alpha_k},$$

dans lequel λ est le coefficient dominant de P, les P_i pour $1 \leqslant i \leqslant k$ sont des polynômes irréductibles unitaires deux à deux distincts, et les α_i sont des entiers strictement positifs.

Démonstration : À peu près la même que pour les entiers, avec un peu plus de soin pour l'unicité. □

1.3 Racines des polynômes

Définition 13. *Soit A un anneau commutatif, P un polynôme de $A[X]$ et a un élément de A. On dit que a est une* racine *(ou un* zéro*) de P lorsque $P(a) = 0$.*

Le résultat qui suit est fondamental, bien que très facile.

Proposition 11. *Soit A un anneau commmutatif, P un polynôme de $A[X]$ et a un élément de A. L'élément a est une racine de P si et seulement si $X - a$ divise P.*

Démonstration : Supposons que $X-a$ divise P, soit $P=(X-a)Q$. On obtient aussitôt $P(a)=(a-a)Q(a)=0$.

Réciproquement, supposons que $P(a)=0$. La remarque qui suit l'énoncé du théorème de division euclidienne montre que, même dans un anneau quelconque, on peut faire la division euclidienne de P par $X-a$; écrivons donc $P=Q(X-a)+R$, où le degré de R est strictement inférieur à $1=\deg(X-a)$ donc R est une constante c.

En appliquant cette relation à a, on obtient $0=P(a)=c$. Ainsi, $P=(X-a)Q$ et donc $X-a$ divise P. □

Corollaire 1. *Soit A un anneau commutatif intègre. Un polynôme non nul de degré n possède au plus n racines.*

Démonstration : Par récurrence sur n. Pour $n=0$, un polynôme constant non nul possède évidemment zéro racine.

Soit n fixé, supposons le résultat vrai pour les polynômes de degré n ; soit maintenant P un polynôme de degré $n+1$. Si P n'a aucune racine, le résultat est vrai pour P ; sinon soit a une racine de P ; par la proposition précédente on peut écrire $P=(X-a)Q$ pour un polynôme Q, qui est clairement de degré n. Maintenant, si b est une racine de P, alors $0=P(b)=(b-a)Q(b)$ donc $b=a$ ou b est une racine de Q (c'est ici qu'on utilise l'hypothèse d'intégrité) ; or Q a au plus n racines, donc P en a au plus $n+1$. □

On va ensuite définir un concept de « racine multiple ».

Définition 14. *Soit A un anneau commutatif, P un polynôme de $A[X]$ et a un élément de A. On dit que a est racine* au moins k-ième *de P lorsque $(X-a)^k$ divise P et que a est* racine k-ième *lorsque a est racine au moins k-ième sans être racine au moins $k+1$-ième. Dans ce dernier cas, on dit que k est la* multiplicité *(ou l'*ordre*) de a comme racine de P.*

La dérivation des polynômes est un outil qui permet d'étudier les racines multiples. Voilà tout d'abord un énoncé concernant les racines doubles (l'énoncé concernant les racines d'ordre supérieur cache une petite subtilité et est reporté plus loin).

Proposition 12. *Soit A un anneau commutatif, P un polynôme de $A[X]$ et a un élément de A. L'élément a est racine au moins double de P si et seulement s'il est simultanément racine de P et de son dérivé P'.*

Démonstration : Supposons a racine au moins double de P et posons $P=(X-a)^2Q$, alors $P'=2(X-a)Q+(X-a)^2Q'$ et il est clair que a est également racine de P'.

Réciproquement, supposons a racine de P et de P'. Comme a est racine de P, on peut écrire $P=(X-a)Q_1$, donc $P'=(X-a)Q_1'+Q_1$. En appliquant cette identité à a, on obtient $Q_1(a)=0$. Donc Q_1 admet lui-même $X-a$ en facteur et peut s'écrire $Q_1=(X-a)Q$ pour un polynôme Q. Donc $P=(X-a)^2Q$. □

1.4 Polynômes versus fonctions polynomiales

Nous avons commencé en insistant sur la différence entre polynômes et fonctions polynomiales ; il est temps de voir le rapport entre ces deux concepts.

Définition 15. *Soit A un anneau commutatif. Une application $f\colon A \to A$ est* polynomiale *lorsqu'il existe un entier $n \geqslant 0$ et un $(n+1)$-uplet $(a_0, \ldots, a_n)$ d'éléments de A tel que pour tout $x \in A$, $f(x) = a_0 + a_1 x + \cdots + a_n x^n$.*

On peut associer à chaque polynôme une fonction polynomiale, mais il n'est pas du tout évident d'associer un polynôme à une fonction polynomiale.

Définition 16. *Soit A un anneau commutatif et P un polynôme de $A[X]$. La* **fonction polynomiale associée à** *P est l'application $f\colon A \to A$ définie de la façon suivante : si P s'écrit $a_0 + a_1 X + \cdots + a_n X^n$, f est l'application définie par :*

$$f\colon A \to A, \quad x \mapsto f(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

Les morceaux « évidents » de la proposition suivante resteraient vrais sur des anneaux, mais on l'énonce sur des corps pour pouvoir prononcer des termes d'algèbre linéaire.

Proposition 13. *Soit $\mathbb{K}$ un corps commutatif et soit $U\colon \mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$ l'application définie par : $U(P)$ est la fonction polynomiale associée à P.*

Alors U est une application linéaire. De plus, $U(PQ) = U(P)U(Q)$ pour tous P et Q et $U(1) = 1$, où le deuxième 1 désigne la fonction constante prenant la valeur 1.

L'image de U est le sous-espace vectoriel de $\mathbb{K}^{\mathbb{K}}$ formé des fonctions polynomiales.

Si $\mathbb{K}$ est infini*, l'application U est injective, donc induit une bijection entre l'espace des polynômes et celui des fonctions polynomiales.*

Démonstration : Les deux premiers paragraphes sont totalement évidents : il faut juste déplier successivement la définition de U, celle de fonction polynomiale associée à un polynôme et celle de valeur d'un polynôme en un point.

Le paragraphe intéressant est le dernier. Puisqu'il s'agit d'une application linéaire, on peut attaquer l'injectivité par l'étude du noyau. Soit P un élément de $\ker(U)$. Cela signifie que l'application polynomiale associée à P est la fonction nulle, c'est-à-dire que pour tout a de A, $P(a) = 0$. Ainsi tous les éléments de $\mathbb{K}$ sont des racines de P. Comme on a supposé $\mathbb{K}$ infini, ceci entraîne que P a une infinité de racines. Mais on sait qu'un polynôme non nul n'a qu'un nombre fini de racines (leur nombre vaut au plus son degré). Donc $P = 0$ ce qui prouve que $\ker(U)$ est réduit à $\{0\}$ donc l'injectivité de U. □

Remarque : Ce que dit en gros cette proposition, pour ceux qui la trouveraient trop abstraite, c'est que si on ne comprend pas la différence entre les polynômes et les fonctions polynomiales et qu'on travaille sur un corps infini, on ne s'expose pas à des

déboires sérieux. Mais cette possibilité de relâchement ne doit pas être exploitée : une telle confusion sur un corps fini serait irrémédiable. Pour voir un exemple simple, contemplez le bête polynôme $X + X^2$ de $\mathbb{Z}/2\mathbb{Z}[X]$; si on le code en machine comme indiqué au début de ce chapitre, c'est la suite de bits 011, qui n'est manifestement pas 0. Pourtant si on regarde non le polynôme mais la fonction polynomiale $x \mapsto x + x^2$, sa valeur en $\mathfrak{cl}(0)$ est $\mathfrak{cl}(0) + \mathfrak{cl}(0)^2 = \mathfrak{cl}(0)$ et sa valeur en $\mathfrak{cl}(1)$ est $\mathfrak{cl}(1) + \mathfrak{cl}(1)^2 = \mathfrak{cl}(0)$ donc c'est bien la fonction polynomiale nulle. Ce n'est donc pas du tout de celle-ci que l'on parle quand on évoque le polynôme $X + X^2$.

Pour vérifier qu'on a compris cet exemple, on résoudra les exercices (très simples) suivants.

Exercice 1. Énumérer **toutes** les applications de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}$.

Exercice 2. Soit $\mathbb{K}$ un corps fini. Exhiber un polynôme P non nul de $\mathbb{K}[X]$ tel que $P(x) = 0$ pour tout x dans $\mathbb{K}$.

1.5 Formule de Taylor pour les polynômes

Alors que pour des fonctions d'une variable réelle en général, la formule de Taylor ne peut tomber juste puisqu'elle consiste à approcher la fonction par une fonction polynomiale et que la fonction quelconque n'est précisément en général pas polynomiale, pour des polynômes, la formule analogue ne contient pas de reste.

Une petite subtilité apparaît dans les divisions par des factorielles qui enjolivent la formule. En effet dans un anneau commutatif quelconque, mais même dans un corps commutatif, on ne peut pas toujours diviser par une factorielle : dans le corps $\mathbb{Z}/3\mathbb{Z}$, la factorielle 3! qui vaut 6 vaut tout simplement 0 puisque 6 est divisible par 3. C'est pourquoi ce théorème nécessite une restriction technique : j'ai choisi de l'énoncer pour des polynômes à coefficients complexes. Les lecteurs qui souhaiteraient utiliser ce cours comme référence (soyons fous) et le relire dans quelques années (idem) noteront que la « bonne » hypothèse est plutôt d'être en caractéristique nulle (quand ils sauront ce que signifie cette hypothèse, ce qui n'est pas encore notre cas).

Théorème 4. *Soit P un polynôme de $\mathbb{C}[X]$ de degré inférieur ou égal à n, et soit a un élément de $\mathbb{C}$. Alors :*

$$P = P(a) + P'(a)(X-a) + \frac{P''(a)}{2!}(X-a)^2 + \cdots + \frac{P^{(n)}(a)}{n!}(X-a)^n \ .$$

Démonstration : On va travailler dans l'espace vectoriel $\mathbb{C}_n[X]$ et considérer dans cet espace le système $(1, X-a, (X-a)^2, \ldots, (X-a)^n)$. Ces polynômes sont de degrés successifs $0 < 1 < \cdots < n$ donc on peut appliquer le lemme mis là tout exprès dans les observations d'algèbre linéaire et conclure que c'est un système libre dans $\mathbb{C}_n[X]$.

Voilà une famille de $n+1$ vecteurs dans un espace de dimension $n+1$, c'en est donc une base, et en particulier un système générateur.

Il existe donc des coefficients c_0, c_1, ..., c_n tels que

$$(*) \qquad P = c_0 + c_1(X-a) + c_2(X-a)^2 + \cdots + c_n(X-a)^n.$$

Il reste à identifier les coefficients c_k. Pour cela, appliquons tout d'abord $(*)$ au point a : on obtient $P(a) = c_0$.

Ensuite, dérivons $(*)$; on obtient :

$$(**) \qquad P' = c_1 + 2c_2(X-a) + 3c_3(X-a)^2 \cdots + nc_n(X-a)^{n-1}.$$

Appliquons $(**)$ au point a : on obtient $P'(a) = c_1$.

Dérivons $(**)$; on obtient :

$$(***) \qquad P'' = c_2 + 6c_3(X-a) + (4\times 3)c_3(X-a)^2 \cdots + n(n-1)c_n(X-a)^{n-2}.$$

Appliquons $(***)$ au point a : on obtient $P''(a) = 2c_2$.

En écrivant formellement une récurrence on montre ainsi que pour tout k avec $1 \leqslant k \leqslant n$, $P^{(k)}(a) = k!\, c_k$.

Comme on est dans $\mathbb{C}$, on peut diviser par $k!$ et obtenir les relations $c_k = \dfrac{P^{(k)}(a)}{k!}$ donc la formule annoncée. □

Remarque : On a énoncé ce théorème pour des polynômes à coefficients complexes. Mais si on a par exemple affaire à un polynôme réel, c'est en particulier un polynôme complexe et la formule est donc parfaitement vraie pour ce polynôme aussi.

De cette formule, on peut tirer un énoncé un peu technique sur les racines multiples.

Proposition 14. *Soit P un polynôme de $\mathbb{C}[X]$, a un nombre complexe et k un entier supérieur ou égal à 1. Alors a est une racine au moins $k+1$-ième de P si et seulement si $P(a) = P'(a) = \ldots = P^{(k)}(a) = 0$.*

Démonstration : Si P est nul, c'est évident, sinon notons n le degré de P et λ son coefficient dominant.

Considérons les indices $i \geqslant 0$ tels que $P^{(i)}(a) \neq 0$, en convenant que $P^{(0)} = P$. Il existe de tels indices, car le polynôme $P^{(n)}$ est égal à la constante $n!\lambda$, donc n'est pas nul en a. Cet ensemble non vide d'entiers positifs a donc un plus petit élément m, qui vérifie $0 \leqslant m \leqslant n$. Écrivons la formule de Taylor en mettant en relief cet entier m :

$$P = \frac{P^{(m)}(a)}{m!}(X-a)^m + \frac{P^{(m+1)}(a)}{(m+1)!}(X-a)^{m+1} + \cdots + \frac{P^{(n)}(a)}{n!}(X-a)^n.$$

On constate qu'on peut mettre $(X-a)^m$ en facteur, mais que le facteur obtenu, qui est le polynôme

$$Q = \frac{P^{(m)}(a)}{m!} + \frac{P^{(m+1)}(a)}{(m+1)!}(X-a) + \cdots + \frac{P^{(n)}(a)}{n!}(X-a)^{n-m},$$

ne s'annule pas en a : la multiplicité de a comme racine de P est donc exactement m.

Dès lors, a est racine au moins $k+1$-ième de P si et seulement si $k < m$, et par définition de m ceci arrive bien si et seulement si $P(a) = P'(a) = \ldots = P^{(k)}(a) = 0$. □

1.6 Polynômes sur $\mathbb{C}$ versus polynômes sur $\mathbb{R}$

Toute cette section repose sur un théorème qu'il n'est pas possible de démontrer dans un cours de notre niveau.

Théorème de d'Alembert-Gauss *Tout polynôme de $\mathbb{C}[X]$ non constant admet au moins une racine complexe.*

Démonstration : Elle repose sur un peu d'analyse, mais d'analyse complexe, qui n'est pas traitée avant l'année de L3. □

Par contre, en admettant le théorème de d'Alembert-Gauss, on peut caractériser les polynômes irréductibles de $\mathbb{C}[X]$.

Corollaire 2. *Dans $\mathbb{C}[X]$, les polynômes irréductibles sont exactement les polynômes du premier degré.*

Démonstration : On sait déjà que dans n'importe quel corps commutatif les polynômes du premier degré sont irréductibles ; il est très facile de voir que les constantes (non nulles) ne possèdent que 1 comme diviseur unitaire et que 0 en possède une infinité : les constantes ne sont donc irréductibles sur aucun corps.

Soit maintenant un P de degré supérieur ou égal à 2 dans $\mathbb{C}[X]$. Par le théorème précédent, P possède au moins une racine a. Mais on sait alors expliciter trois diviseurs unitaires de P : la constante 1, le polynôme du premier degré $X - a$ et le polynôme $P/$ (coefficient dominant de P), qui est de degré supérieur ou égal à deux. Ainsi P n'est pas irréductible. □

Définition 17. *On dit qu'un polynôme est* scindé *lorsqu'il peut s'écrire sous forme de produit de facteurs du premier degré.*

Corollaire 3. *Dans $\mathbb{C}[X]$, tout polynôme non nul est scindé.*

Démonstration : Sa décomposition en facteurs irréductibles est une décomposition en produit de facteurs du premier degré. □

Dans $\mathbb{R}[X]$, les choses sont légèrement plus compliquées, mais pas tant que ça.

Proposition 15. *Dans $\mathbb{R}[X]$ les polynômes irréductibles sont exactement les polynômes du premier degré et les polynômes du deuxième degré à discriminant strictement négatif.*

Avant de donner la preuve, rappelons que le discriminant du polynôme $P = aX^2+bX+c$ vaut

$$\mathrm{disc}(P) = b^2 - 4ac.$$

Démonstration : On sait déjà que les polynômes du premier degré sont irréductibles. Soit maintenant P du deuxième degré ; s'il a un diviseur unitaire autre que les deux évidents, celui-ci est du premier degré, donc P a une racine et son discriminant est positif ou nul. Les polynômes du deuxième degré à discriminant strictement négatif sont donc irréductibles.

Réciproquement, il est clair que les polynômes du deuxième degré à discriminant positif ou nul sont factorisables, donc pas irréductibles. Soit enfin un polynôme P de degré supérieur ou égal à 3. Si P admet une racine réelle a, P n'est pas irréductible de façon quasi évidente. Sinon, considérons pendant quelques lignes P comme un polynôme à coefficients complexes. Par le théorème de d'Alembert-Gauss, il admet au moins une racine complexe a, qui n'est pas réelle puisqu'on a supposé P sans racine réelle. En profitant de ce que le conjugué de la somme est la somme des conjugués, que le conjugué du produit est le produit des conjugués et que chaque coefficient de P est invariant par conjugaison, on voit qu'on a aussi $P(\overline{a}) = 0$. Les polynômes $X - a$ et $X - \overline{a}$ étant deux irréductibles distincts dans $\mathbb{C}[X]$, le fait qu'ils divisent tous deux P entraîne que leur produit divise P dans $\mathbb{C}[X]$. Mais ce produit vaut $(X-a)(X-\overline{a}) = X^2-2\mathrm{Re}(a)X+|a|^2$ et est donc un polynôme B du deuxième degré à coefficients réels.

Si on est distrait, on pourra croire qu'on a ainsi trouvé en B un diviseur unitaire non évident de P dans $\mathbb{R}[X]$ et conclure que P n'est pas irréductible. En réalité, on glisserait sur un détail en affirmant ceci : on sait en effet que B divise P dans $\mathbb{C}[X]$ mais il nous faut encore vérifier qu'il le divise dans $\mathbb{R}[X]$. Pour ce faire, effectuons la division euclidienne de P par B dans $\mathbb{R}[X]$: elle fournit des polynômes Q et R, avec $\deg R < 2$, tels que $P = BQ + R$. Ces polynômes de $\mathbb{R}[X]$ peuvent aussi être vus comme des polynômes à coefficients complexes, donc $P = BQ + R$ est aussi la division euclidienne de P par B dans $\mathbb{C}[X]$. Mais on sait que B divise P dans $\mathbb{C}[X]$ et que la division euclidienne est unique ; donc $R = 0$, donc $P = BQ$ pour un Q à coefficients réels, et on a bien montré que B divise P dans $\mathbb{R}[X]$ aussi.

Une fois cet obstacle franchi, on conclut comme dit au début du paragraphe précédent : on a trouvé un diviseur unitaire non évident de P et celui-ci ne peut donc pas être irréductible. □

1.7 Corps des fractions rationnelles

Le concept est très simple : les fractions rationnelles sont les expressions de la forme $\dfrac{P}{Q}$ où P et Q sont des polynômes. Une mise en forme totalement rigoureuse demande un effort un peu disproportionné par rapport au caractère intuitif de l'objet à construire.

La première idée qui peut venir à l'esprit est de tenter de modéliser la fraction

$\frac{P}{Q}$ par le couple (P,Q) qui contient à première vue la même information : ainsi la fraction $\frac{X}{X+1}$ correspondra au couple $(X, X+1)$. Une telle idée nous met sur la bonne piste, mais elle se heurte à un problème : le couple (X^2, X^2+X) représentera la fraction $\frac{X^2}{X^2+X} = \frac{X}{X+1}$; la même fraction correspond donc à plusieurs couples, et l'ensemble de tous les couples (P,Q) est donc trop gros.

On pourrait penser à n'utiliser que des couples (P,Q) avec P et Q premiers entre eux ; c'est vraisemblablement faisable, mais la preuve risque d'être extrêmement lourde, avec des pgcd à simplifier de partout.

Non, décidément, on ne fera rien de simple si on n'a pas compris ce qu'est un ensemble-quotient, alors que si on maîtrise cette notion, la preuve est longue à écrire, mais sans obstacles.

Dans tout le chapitre, $\mathbb{K}$ désigne un corps commutatif. Notons $A = \mathbb{K}[X]$. La construction utilise simplement le fait que A est un anneau intègre, et nullement en réalité que A est l'anneau des polynômes.

Définition 18. *Soit A un anneau intègre, 0 son neutre pour l'addition, et C l'ensemble*

$$C = A \times (A \setminus \{0\}).$$

Sur C on introduit deux opérations $+$ et $\times$ définies comme suit : pour tous (P_1,Q_1) et (P_2,Q_2) de C, on pose

$$(P_1,Q_1)\times(P_2,Q_2) = (P_1P_2, Q_1Q_2) \qquad (P_1,Q_1)+(P_2,Q_2) = (P_1Q_2+P_2Q_1, Q_1Q_2).$$

On notera qu'on utilise très discrètement l'intégrité de A pour justifier que le produit Q_1Q_2 qui intervient dans les formules n'est pas nul, donc que la somme et le produit d'éléments de C appartiennent effectivement à C.

Signalons une fois encore que les deux formules de la définition précédente se comprennent aisément si on a en tête qu'un couple (P,Q) a vocation à décrire la fraction $\frac{P}{Q}$ (qui n'aura un sens propre qu'une fois la construction terminée) : elles sont les reproductions des formules qu'on sait bien utiliser pour multiplier ou additionner des fractions.

L'ensemble C a une bonne tête vu de loin, mais de près il est trop gros. Pour le faire maigrir, introduisons une relation d'équivalence $\mathcal{R}$ sur C.

Définition 19. *Pour tous (P_1,Q_1) et (P_2,Q_2) de C,*

$$(P_1,Q_1)\mathcal{R}(P_2,Q_2) \qquad \text{lorsque} \qquad P_1Q_2 = P_2Q_1.$$

Si nous savions déjà donner un sens aux barres de fractions, nous aurions écrit la condition sous la forme $\frac{P_1}{Q_1} = \frac{P_2}{Q_2}$, la rendant ainsi compréhensible, mais comme ce

symbole ne nous sera disponible qu'une fois finie la construction, on a dû donner une forme moins limpide.

Proposition 16. *La relation $\mathcal{R}$ est une relation d'équivalence sur C.*

Démonstration : En effet, $P_1Q_2 = P_2Q_1$ et $P_2Q_3 = P_3Q_2$ impliquent $P_1Q_3 = P_3Q_1$, voyez-vous. (Indication : comme $Q_2 \neq 0$, on calcule $P_1Q_3Q_2$.) □

Notation 8. *On note B l'ensemble-quotient $C/\mathcal{R}$ et $\mathfrak{cl}(P,Q)$ la classe d'un élément (P,Q) de C.*

On va alors définir des opérations + et × sur B ; le principe est le même que celui qui nous a permis de définir addition et multiplication sur $\mathbb{Z}/n\mathbb{Z}$: on définit simplement ces opérations sur des représentants des classes d'équivalence, et on vérifie méthodiquement que le résultat obtenu ne dépend pas de la classe utilisée.

Définition 20. *Pour $\mathfrak{cl}(P_1,Q_1)$ et $\mathfrak{cl}(P_2,Q_2)$ éléments de B, on note*

$$\mathfrak{cl}(P_1,Q_1) + \mathfrak{cl}(P_2,Q_2) = \mathfrak{cl}\left((P_1,Q_1) + (P_2,Q_2)\right).$$

et

$$\mathfrak{cl}(P_1,Q_1) \times \mathfrak{cl}(P_2,Q_2) = \mathfrak{cl}\left((P_1,Q_1) \times (P_2,Q_2)\right),$$

Cette « définition » n'en sera une qu'une fois vérifiée la proposition suivante.

Proposition 17. *Le résultat des opérations + et × définies sur C ne dépend pas des représentants choisis.*

Démonstration : On fait la vérification soigneusement pour l'addition, avec « renvoi au lecteur » pour la multiplication.

Soit (P_3,Q_3) un représentant quelconque de la classe de (P_1,Q_1) et (P_4,Q_4) un représentant quelconque de la classe de (P_2,Q_2). Il faut vérifier que

$$(P_1,Q_1) + (P_2,Q_2) = (P_1Q_2 + P_2Q_1, Q_1Q_2)$$

et

$$(P_3,Q_3) + (P_4,Q_4) = (P_3Q_4 + P_4Q_3, Q_3Q_4),$$

sont bien dans la même classe.

Cela revient à comparer les produits P_5 et P_6 définis par :

$$P_5 = (P_1Q_2 + P_2Q_1)Q_3Q_4, \qquad P_6 = (P_3Q_4 + P_4Q_3)Q_1Q_2.$$

On dispose pour ce faire des égalités $P_1Q_3 = P_3Q_1$ et $P_2Q_4 = P_4Q_2$, issues respectivement des relations $(P_1,Q_1)\mathcal{R}(P_3,Q_3)$ et $(P_2,Q_2)\mathcal{R}(P_4,Q_4)$. La vérification est alors directe :

$$P_5 = P_1Q_3Q_2Q_4 + P_2Q_4Q_1Q_3 = P_3Q_1Q_2Q_4 + P_4Q_2Q_1Q_3 = P_6.$$

□

Notation 9. *Quand $A = \mathbb{K}[X]$, on note $\mathbb{K}(X)$ l'ensemble $B = C/\mathcal{R}$ ainsi construit.*

On a donc bien construit un ensemble $\mathbb{K}(X)$ puis une addition et une multiplication sur cet ensemble.

Théorème 5. *L'ensemble $\mathbb{K}(X)$ muni des lois $+$ et $\times$ est un corps commutatif.*

Démonstration : La vérification de toutes les propriétés de la définition d'un corps commutatif est simple, méthodique et lourde. On se bornera ici à justifier l'existence de l'inverse.

Si une classe $\mathfrak{cl}(P_1, Q_1)$ n'est pas nulle, on remarque d'abord que $P_1 \neq 0$, puisque $\mathfrak{cl}(P_1, Q_1) \neq \mathfrak{cl}(0, 1)$. La classe $\mathfrak{cl}(Q_1, P_1)$ existe donc ; ce sera l'inverse de $\mathfrak{cl}(P_1, Q_1)$: en effet le produit des deux est $\mathfrak{cl}(Q_1P_1, P_1Q_1)$ qui est égal à la classe de $(1, 1)$ qui est le neutre pour la multiplication. □

Proposition 18. *L'anneau $\mathbb{K}[X]$ est inclus dans $\mathbb{K}(X)$; plus précisément, il existe un morphisme d'anneaux $j : \mathbb{K}[X] \to \mathbb{K}(X)$ qui est injectif. Tout élément de $\mathbb{K}(X)$ peut s'écrire comme $j(P)j(Q)^{-1}$ pour P et Q dans $\mathbb{K}[X]$ et $Q \neq 0$.*

Démonstration : Soit j l'application définie par $j(P) = \mathfrak{cl}(P, 1)$. Il est très facile de vérifier que j transforme addition en addition et multiplication en multiplication ; son injectivité peut seule interpeller. Mais puisque cette transformation est un morphisme de groupes additifs, l'injectivité se laisse montrer à coups de noyaux ; et effectivement si un polynôme P est envoyé sur le neutre additif de $\mathbb{K}(X)$ qui est la classe de $(0, 1)$, c'est que $(P, 1)\mathcal{R}(0, 1)$ et donc que $P = 0$: le noyau est bien réduit au seul polynôme nul. Enfin,

$$\mathfrak{cl}(P, Q) = \mathfrak{cl}(P, 1)\mathfrak{cl}(1, Q) = \mathfrak{cl}(P, 1)\left[\mathfrak{cl}(Q, 1)\right]^{-1} = j(P)j(Q)^{-1}.$$

□

Notation 10. *On note P/Q ou $\dfrac{P}{Q}$ l'élément $\mathfrak{cl}(P, Q)$ de $\mathbb{K}(X)$.*

1.8 Décomposition en éléments simples

L'objectif principal de cette section est le théorème de décomposition en éléments simples, utilisé notamment pour le calcul des primitives de fractions rationnelles, et qui est un peu indigeste.

Théorème 6. *On se donne une fraction rationnelle P/Q élément de $\mathbb{K}(X)$ et on considère la décomposition de Q en produits de polynômes unitaires irréductibles :*

$$Q = \lambda Q_1^{\alpha_1} Q_2^{\alpha_2} \cdots Q_k^{\alpha_k}.$$

Alors il existe une et une seule écriture :

$$\frac{P}{Q} = R + \frac{A_{1,1}}{Q_1} + \cdots + \frac{A_{1,\alpha_1}}{Q_1^{\alpha_1}} + \frac{A_{2,1}}{Q_2} + \cdots + \frac{A_{2,\alpha_2}}{Q_2^{\alpha_2}} + \cdots + \frac{A_{k,1}}{Q_k} + \cdots \frac{A_{k,\alpha_k}}{Q_k^{\alpha_k}},$$

dans laquelle R et les $A_{i,j}$ sont tous des polynômes de $\mathbb{K}[X]$ qui vérifient en outre la condition suivante, portant sur les degrés : pour tout couple d'indices (i,j) tel que $1 \leqslant i \leqslant k$ et $1 \leqslant j \leqslant \alpha_i$,

$$\deg A_{i,j} < \deg Q_i.$$

Démonstration : **Preuve de l'existence**

Dans un premier temps, on va considérer les polynômes :

$$T_1 = Q_2^{\alpha_2} Q_3^{\alpha_3} \cdots Q_k^{\alpha_k}, \quad T_2 = Q_1^{\alpha_2} Q_3^{\alpha_3} \cdots Q_k^{\alpha_k}, \quad \ldots \quad T_k = Q_1^{\alpha_1} Q_2^{\alpha_2} \cdots Q_{k-1}^{\alpha_{k-1}}.$$

Chaque T_i reprend les facteurs de la décomposition de Q à l'exception de λ et $Q_i^{\alpha_i}$.

Un éventuel diviseur irréductible unitaire commun à tous ces polynômes doit diviser T_k ; ce doit donc être un des polynômes Q_i avec $i < k$. Mais Q_1 ne divise pas T_1, Q_2 ne divise pas T_2, et ce jusqu'à Q_{k-1} qui ne divise pas T_{k-1}. Les polynômes $T_1, \ldots, T_k$ ne possèdent donc aucun diviseur irréductible unitaire commun ; cela entraîne qu'ils sont premiers entre eux.

On peut donc écrire une identité de Bézout : il existe des polynômes $S_1, \ldots, S_k$ de $\mathbb{K}[X]$, tels que

$$1 = S_1 T_1 + S_2 T_2 + \cdots + S_k T_k.$$

Multiplions cette identité par $\dfrac{P}{Q} = \dfrac{P}{\lambda Q_1^{\alpha_1} Q_2^{\alpha_2} \cdots Q_k^{\alpha_k}}$; on obtient :

$$\frac{P}{Q} = PS_1 \frac{T_1}{Q} + PS_2 \frac{T_2}{Q} + \cdots + PS_k \frac{T_k}{Q} = \frac{PS_1}{\lambda} \frac{\lambda T_1}{Q} + \frac{PS_2}{\lambda} \frac{\lambda T_2}{Q} + \cdots + \frac{PS_k}{\lambda} \frac{\lambda T_k}{Q},$$

donc

$$\frac{P}{Q} = \frac{PS_1}{\lambda} \frac{1}{Q_1^{\alpha_1}} + \frac{PS_2}{\lambda} \frac{1}{Q_2^{\alpha_2}} + \cdots + \frac{PS_k}{\lambda} \frac{1}{Q_k^{\alpha_k}}.$$

En notant $B_1, \ldots, B_k$ les divers numérateurs qui interviennent dans la dernière formule, on a donc réussi à écrire :

$$\frac{P}{Q} = \frac{B_1}{Q_1^{\alpha_1}} + \frac{B_2}{Q_2^{\alpha_2}} + \cdots + \frac{B_k}{Q_k^{\alpha_k}}.$$

On va alors manipuler successivement chacun des termes de cette addition. Fixons un i avec $1 \leqslant i \leqslant k$ et travaillons l'expression $\dfrac{B_i}{Q_i^{\alpha_i}}$.

On commence par faire la division euclidienne de B_i par Q_i, en notant judicieusement le quotient et le reste :

$$B_i = B_{i,\alpha_i} Q_i + A_{i,\alpha_i} \text{ avec } \deg A_{i,\alpha_i} < \deg Q_i.$$

En reportant cette division euclidienne en lieu et place de B_i on a réécrit :

$$\frac{B_i}{Q_i^{\alpha_i}} = \frac{B_{i,\alpha_i}}{Q_i^{\alpha_i-1}} + \frac{A_{i,\alpha_i}}{Q_i^{\alpha_i}}.$$

On recommence une division euclidienne, cette fois-ci de B_{i,α_i} par Q_i, en notant toujours opportunément quotient et reste :

$$B_{i,\alpha_i} = B_{i,\alpha_i-1}Q_i + A_{i,\alpha_i-1} \text{ avec } \deg A_{i,\alpha_i-1} < \deg Q_i$$

et on reporte de nouveau dans l'expression la plus fraîche de $\dfrac{B_i}{Q_i^{\alpha_i}}$; on obtient :

$$\frac{B_i}{Q_i^{\alpha_i}} = \frac{B_{i,\alpha_i-1}}{Q_i^{\alpha_i-2}} + \frac{A_{i,\alpha_i-1}}{Q_i^{\alpha_i-1}} + \frac{A_{i,\alpha_i}}{Q_i^{\alpha_i}}.$$

On recommence jusqu'à ne plus pouvoir recommencer, ce qui donne finalement une expression :

$$\frac{B_i}{Q_i^{\alpha_i}} = B_{i,1} + \frac{A_{i,1}}{Q_i} + \cdots + \frac{A_{i,\alpha_i-1}}{Q_i^{\alpha_i-1}} + \frac{A_{i,\alpha_i}}{Q_i^{\alpha_i}}.$$

Il n'y a plus qu'à regrouper toutes ces expressions et à noter

$$R = B_{1,1} + B_{2,1} + \cdots + B_{k,1}$$

pour avoir terminé la preuve d'existence.

Preuve de l'unicité

On l'écrira (peut-être) une prochaine fois, elle n'est pas spécialement amusante. Contrairement à la preuve d'existence, il n'y a guère d'idées, seulement des décomptes de degrés. □

Pour comprendre cette décomposition, le mieux est d'examiner sa forme sur un cas particulier, rassemblant les différentes situations. Voici deux polynômes P et Q dans $\mathbb{R}[X]$ avec Q non nul, qui définissent donc une fraction rationnelle P/Q dans $\mathbb{R}(X)$, et la décomposition de P/Q dans $\mathbb{R}(X)$. On choisit

$$P = X^{13}, \quad Q = (X-1)^3(X-2)^2(X-3)(X^2+1)^2(X^2+X+1).$$

Alors,

$$\begin{aligned}\frac{P}{Q} \;=\; & A + BX + \frac{C}{X-1} + \frac{D}{(X-1)^2} + \frac{E}{(X-1)^3} + \frac{F}{X-2} + \frac{G}{(X-2)^2} + \\ & + \frac{H}{X-3} + \frac{IX+J}{X^2+1} + \frac{KX+L}{(X^2+1)^2} + \frac{MX+N}{X^2+X+1},\end{aligned}$$

où les lettres de A jusqu'à M désignent des réels à déterminer. La théorie assure que ces réels existent et sont uniques. Il suffirait donc de réduire tous les éléments simples

au même dénominateur, et d'identifier les numérateurs pour obtenir autant d'équations que d'inconnues (14 dans notre cas). Ce n'est pas ainsi qu'on procède en pratique. On utilise plusieurs techniques de manière à déterminer le plus de coefficients possibles par des équations simples. Voici ces techniques.

Pour la partie polynomiale

Celle-ci est non nulle seulement dans le cas où le degré du numérateur est supérieur ou égal au degré du dénominateur. Dans ce cas le polynôme cherché, que l'on appelle la partie entière, est le quotient D de la division euclidienne de P par Q :

$$P = DQ + R\ ,$$

où le reste R est de degré strictement inférieur au degré de Q. Dans notre exemple, $D = X + 9$. Il faut s'assurer auparavant que la fraction est bien irréductible, et la simplifier éventuellement si elle ne l'était pas.

Pour les termes en $(X - a)^\alpha$

Si on multiplie les deux membres de la décomposition par $(X-a)^\alpha$, la racine a disparaît. On peut donc remplacer X par a, ce qui annule tous les termes de la décomposition sauf un. Il reste à gauche une certaine valeur, que l'on calcule en général facilement. Dans notre exemple, si on multiplie les deux membres par $(X-1)^3$, et qu'on remplace X par 1, on trouve :

$$\frac{1^{13}}{(1-2)^2(1-3)(1^2+1)^2(1^2+1+1)} = E\ ,$$

soit $E = -\frac{1}{24}$.

Pour les termes en $(aX^2 + bX + c)^\beta$

On procède de même, en remplaçant X par une des racines complexes du trinôme. Dans notre cas, on multiplie les deux membres par $(X^2+1)^2$, et on remplace X par i. On trouve :

$$\frac{\mathrm{i}^{13}}{(\mathrm{i}-1)^3(i-2)^2(\mathrm{i}-3)(\mathrm{i}^2+\mathrm{i}+1)} = K\mathrm{i} + L\ .$$

On identifie alors la partie réelle et la partie imaginaire : $K = -\frac{1}{100}$ et $L = -\frac{1}{50}$.

Pour les autres termes

Il faut chercher les équations les plus simples possibles, en prenant des valeurs particulières pour X, qui ne soient pas des racines du dénominateur ($X = 0$, $X = \pm 1$, etc...). On peut aussi penser à faire tendre X vers l'infini. On n'a recours à une réduction au même dénominateur avec identification des coefficients qu'en dernier ressort.

Voici un exemple plus simple, sur lequel nous allons détailler tous les calculs. Il s'agit de décomposer en éléments simples la fraction rationnelle

$$\frac{P}{Q} = \frac{X^6+1}{(X-1)(X^2+X+1)^2}\ .$$

Le numérateur et le dénominateur sont premiers entre eux, la fraction est bien irréductible. Sa décomposition en éléments simples dans $\mathbb{R}(X)$ a la forme suivante.

$$\frac{P}{Q} = A + BX + \frac{C}{(X-1)} + \frac{DX+E}{(X^2+X+1)} + \frac{FX+G}{(X^2+X+1)^2} \ ,$$

où les lettres de A jusqu'à G désignent des réels à déterminer. La division euclidienne du numérateur par le dénominateur donne :

$$X^6+1 = (X-1)\Big((X-1)(X^2+X+1)^2\Big) + 2X^3 \ .$$

Donc $A=1$, $B=-1$, et :

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

On peut désormais ne travailler que sur la partie restante, à savoir :

$$\frac{2X^3}{(X-1)(X^2+X+1)^2} = \frac{C}{(X-1)} + \frac{DX+E}{(X^2+X+1)} + \frac{FX+G}{(X^2+X+1)^2} \ .$$

On multiplie les deux membres par $(X-1)$, et on remplace X par 1. On trouve $C=\frac{2}{9}$.
On multiplie ensuite les deux membres par $(X^2+X+1)^2$, et on remplace X par $j=-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}$. On trouve $Fj+G=-1-\mathrm{i}\frac{\sqrt{3}}{3}$. En identifiant les parties réelles et imaginaires, on trouve $-\frac{1}{2}F+G=-1$ et $\frac{\sqrt{3}}{2}F=-\frac{\sqrt{3}}{3}$. La solution de ce système de deux équations à deux inconnues est $F=-\frac{2}{3}$ et $G=-\frac{4}{3}$.
On peut ensuite remplacer X par i, et identifier partie réelle et partie imaginaire. On trouve $D=-\frac{2}{9}$ et $E=\frac{14}{9}$.

Une fois tout cela fait, il est bon de vérifier les calculs, en utilisant une ou plusieurs valeurs particulières. Ainsi,

- pour $X=0$, $0=-C+E+G$,
- pour $X=-1$, $-1=-A+B+\frac{C}{-2}+\frac{-D+E}{1}+\frac{-F+G}{1}$,
- après avoir enlevé la partie entière, si on multiplie les deux membres par X et qu'on fait tendre X vers $+\infty$: $0=C+D$.

Voici donc la décomposition dans $\mathbb{R}(X)$.

$$\frac{P}{Q} = X - 1 + \frac{\frac{2}{9}}{(X-1)} + \frac{-\frac{2}{9}X+\frac{14}{9}}{(X^2+X+1)} + \frac{-\frac{2}{3}X-\frac{4}{3}}{(X^2+X+1)^2}$$

La décomposition dans $\mathbb{C}(X)$ a une forme différente. Nous notons encore $j=-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}$, de sorte que j et $\overline{j}$ sont les deux racines de X^2+X+1.

$$\frac{P}{Q} = AX + B + \frac{C}{X-1} + \frac{D}{X-j} + \frac{E}{(X-j)^2} + \frac{F}{X-\overline{j}} + \frac{G}{(X-\overline{j})^2} \ ,$$

A priori, les lettres de A jusqu'à G désignent des nombres complexes, mais le fait que la fraction initiale ait tous ses coefficients réels simplifie quelque peu le problème : la décomposition ne doit pas changer si on prend le conjugué des deux membres. L'unicité de cette décomposition entraîne :

$$A = \overline{A}\,, \quad B = \overline{B}\,, \quad C = \overline{C}\,, \quad D = \overline{F}\,, \quad E = \overline{G}\,,$$

Les techniques de décomposition utilisées dans $\mathbb{R}(X)$ restent valables. On trouve donc encore :

$$A = 1\,, \quad B = -1\,, \quad C = \frac{2}{9}\,.$$

Nous laissons au lecteur le plaisir de calculer les autres coefficients. La décomposition dans $\mathbb{C}(X)$ est la suivante :

$$\frac{P}{Q} = X - 1 + \frac{\frac{2}{9}}{X-1} + \frac{-\frac{1}{9} - \mathrm{i}\frac{\sqrt{3}}{3}}{X-j} + \frac{\frac{1}{3} + \mathrm{i}\frac{\sqrt{3}}{9}}{(X-j)^2} + \frac{-\frac{1}{9} + \mathrm{i}\frac{\sqrt{3}}{3}}{X-\overline{j}} + \frac{\frac{1}{3} - \mathrm{i}\frac{\sqrt{3}}{9}}{(X-\overline{j})^2}\,.$$

2 Entraînement

2.1 Vrai ou Faux

Vrai-Faux 1. Soit $P \in \mathbb{R}[X]$ un polynôme non nul à coefficients réels, et d un entier. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses, et pourquoi ?

1. ☐ Si le degré de P est d, alors le degré de P' est $d-1$.
2. ☒ Si le degré de P est d, alors celui de $P(X^2)$ est $2d$.
3. ☒ Si le degré de P est d, alors celui de $X^2P(X+2)$ est $d+2$.
4. ☐ Si le degré de P est 2, alors celui de X^2+P est 2.
5. ☒ Si le degré de P est 4, alors celui de X^2+P est 4.

Vrai-Faux 2. Soient $P, Q \in \mathbb{R}[X]$ deux polynômes non nuls à coefficients réels. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses, et pourquoi ?

1. ☐ Le degré de $P+Q$ est toujorus la somme des degrés de P et de Q
2. ☐ Le degré de $P+Q$ est toujours égal soit au degré de P soit au degré de Q
3. ☒ Le degré de PQ est la somme des degrés de P et de Q.
4. ☐ Le degré de PQ' est toujours égal au degré de QP'
5. ☒ Le degré de $P(X^2)Q(X^2)$ est le double de la somme des degrés de P et de Q.

Vrai-Faux 3. Soit $P \in \mathbb{R}[X]$ un polynôme à coefficients réels. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses, et pourquoi ?

1. ☒ Si P est divisible par X^2-X alors $P(1)=0$.
2. ☐ Si P est divisible par X^2-X alors $P'(0)=0$.
3. ☒ Si P est divisible par $(X-1)^2$ alors $P'(1)=0$.
4. ☒ Si $P(1)=P'(1)=0$ alors P est divisible par $(X-1)^2$.
5. ☐ Si $P'(1)=0$ alors P est divisible par $(X-1)$.
6. ☐ Si P est irréductible alors P ne s'annule pas sur $\mathbb{R}$.
7. ☒ Si P est irréductible alors P' est de degré 0 ou 1.
8. ☐ Si P ne s'annule pas sur $\mathbb{R}$, alors P est irréductible.

Vrai-Faux 4. Soient P et Q deux polynômes non nuls à coefficients réels. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses, et pourquoi ?

1. ☒ Si P est premier avec Q, alors P est premier avec $P+Q$.
2. ☐ Si P ne divise pas Q, alors P ne divise pas Q^2.
3. ☐ Si P ne divise pas Q^2, alors P est premier avec Q.
4. ☒ Si P est premier avec Q, alors P^2 est premier avec Q^2.

5. ☒ Si $P^2 - Q^2 = 1$, alors P est premier avec Q.

Vrai-Faux 5. Soit $P \in \mathbb{R}[X]$ un polynôme à coefficients réels. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses, et pourquoi ?

1. ☒ Le reste de la division euclidienne de P par $X - 1$ est $P(1)$.
2. ☐ Le reste de la division euclidienne de P par $(X - 1)^2$ est $P'(1)$.
3. ☒ Le reste de la division euclidienne de P par $(X - 1)^2$ est $P'(1)(X - 1) + P(1)$.
4. ☒ Si les restes des divisions euclidiennes de P par X et $X - 1$ sont nuls, alors P est divisible par $X^2 - X$.
5. ☐ Si les restes des divisions euclidiennes de P par X^2 et $(X - 1)^2$ sont égaux, alors P est divisible par $X^2 - X$.
6. ☒ Si les restes des divisions euclidiennes de P par X^2 et $(X - 1)^2$ sont égaux à R, alors $P - R$ est divisible par $(X^2 - X)^2$.

Vrai-Faux 6. Soit $P \in \mathbb{R}[X]$ un polynôme à coefficients réels. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses, et pourquoi ?

1. ☒ Si le degré de P est impair, alors P possède au moins une racine réelle.
2. ☐ Si le degré de P est pair, alors P ne possède aucune racine réelle.
3. ☐ Si P est de degré d, alors P a d racines complexes distinctes.
4. ☒ Si P n'est pas constant et divise $X^{24} - 1$ alors toutes les racines de P sont distinctes.
5. ☐ Si P n'est pas premier avec $X^{24} - 1$ alors toutes les racines de P sont distinctes.
6. ☒ Si P n'est pas premier avec $X^{24} - 1$ alors au moins une racine de P est de module 1.
7. ☒ Si P et P' sont premiers entre eux, alors les racines de P sont distinctes.

Vrai-Faux 7. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses, et pourquoi ?

1. ☒ $X^2 + 4$ est irréductible dans $\mathbb{R}[X]$
2. ☐ $X^2 + 4$ est irréductible dans $\mathbb{C}[X]$
3. ☐ $X^2 - 4$ est irréductible dans $\mathbb{Q}[X]$
4. ☒ $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$
5. ☐ $X^2 - 2$ est irréductible dans $\mathbb{R}[X]$
6. ☒ $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$
7. ☐ $X^2 + 1$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$

Vrai-Faux 8. On considère la fraction rationnelle suivante.

$$\frac{P}{Q} = \frac{X^4}{X^4 - 1} \, .$$

Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses, et pourquoi ?

1. ☐ Les décompositions en éléments simples de P/Q dans $\mathbb{R}(X)$ et $\mathbb{C}(X)$ sont identiques.
2. ☒ La partie entière de la décomposition en éléments simples de P/Q dans $\mathbb{C}(X)$ est 1.
3. ☐ Une décomposition en éléments simples de P/Q dans $\mathbb{R}(X)$ est

$$\frac{P}{Q} = \frac{1}{2} \frac{X^2}{X^2 - 1} + \frac{1}{2} \frac{X^2}{X^2 - 1} \, .$$

4. ☒ Dans la décomposition en éléments simples de P/Q dans $\mathbb{R}(x)$, on trouve un élément simple du type $a/(X^2 + 1)$, où a est un réel.
5. ☒ Les décompositions en éléments simples de P/Q dans $\mathbb{C}(x)$ et dans $\mathbb{R}(X)$ contiennent l'élément $(1/4)/(X - 1)$.
6. ☐ Dans la décomposition en éléments simples de P/Q dans $\mathbb{C}(x)$, on trouve un élément simple du type $a/(X - \mathrm{i})$, où a est un réel.
7. ☒ Dans la décomposition en éléments simples de P/Q dans $\mathbb{C}(x)$, on trouve deux éléments simples du type $a/(X - \mathrm{i})$ et $b/(X + \mathrm{i})$, où a et b sont deux complexes conjugués.

2.2 Exercices

Exercice 3. On considère les couples de polynômes (P, Q) suivants dans $\mathbb{R}[X]$.

- $P = X$, $Q = X - 1$
- $P = X$, $Q = X^2 - 1$
- $P = X^2$, $Q = X^2 - 1$
- $P = X^2 - 1$, $Q = X^2 + X + 1$
- $P = X^2 - 2X + 1$, $Q = X^2 + X + 1$
- $P = X^2 - 1$, $Q = X^3 - 1$
- $P = X^3 - X^2 + 2X - 2$, $Q = X^3 - 1$

Pour chacun de ces couples :

1. Écrire les polynômes P' et Q'.
2. Calculer le polynôme PQ.
3. Calculer les polynômes $P'Q$ et PQ'.
4. Vérifier la formule $(PQ)' = P'Q + PQ'$

5. Calculer les polynômes $P \circ Q$ et $Q \circ P$.
6. Vérifier les formules

$$(P \circ Q)' = Q'(P' \circ Q) \quad \text{et} \quad (Q \circ P)' = P'(Q' \circ P)$$

Exercice 4.

1. Déterminer l'ensemble des polynômes P de $\mathbb{R}[X]$, de degrés au plus 2, tels que

$$P(X+1)P(X) = -P(X^2)$$

2. Déterminer l'ensemble des polynômes P de $\mathbb{R}[X]$ tels que

$$P(2X) = P'P''$$

3. Déterminer l'ensemble des polynômes P de $\mathbb{R}[X]$ tels que

$$P(X^2) = (X^2+1)P(X)$$

4. Déterminer l'ensemble des polynômes P de $\mathbb{R}[X]$ tels que

$$X(X+1)P'' + (X+2)P' - P = 0$$

5. Déterminer l'ensemble des polynômes P de $\mathbb{C}[X]$ tels que

$$18P = P'P''$$

6. Montrer que pour tout $n \in \mathbb{N}$, il existe un polynôme unique P_n de $\mathbb{R}[X]$ tel que

$$P_n - P_n' = X^n$$

et calculer P_n.

Exercice 5. On pose $C_0 = 1$, $C_1 = X$ et pour $n \geqslant 2$, on définit le n-ième polynôme de Chebyshev C_n par la relation de récurrence :

$$C_n = 2XC_{n-1} - C_{n-2}.$$

1. Calculer C_2, C_3 et C_4.
2. Montrer que pour tout $n \in \mathbb{N}$, le polynôme C_n est de degré n et calculer son coefficient dominant.
3. Montrer que pour tout $n \in \mathbb{N}$, et pour tout $\theta \in \mathbb{R}$, $\cos(n\theta) = C_n(\cos(\theta))$.
4. En déduire les racines de C_n.
5. Montrer que pour tout $n \in \mathbb{N}$,

$$(1-X^2)C_n'' - XC_n' + n^2C_n = 0\ .$$

Exercice 6. Soit n un entier strictement positif.

1. Montrer que pour tout polynôme P de $\mathbb{R}_n[X]$, il existe un unique polynôme Q de $\mathbb{R}_n[X]$ tel que
$$P(X)P(-X) = Q(X^2)$$
Dans toute la suite, on note ϕ l'application de $\mathbb{R}_n[X]$ dans lui-même qui à un polynôme P associe le polynôme Q tel que $P(X)P(-X) = Q(X^2)$.
2. Calculer $\phi(1)$, $\phi(X)$, $\phi(X+1)$, $\phi(X-1)$, $\phi(X^2-1)$, $\phi(X^2+2X+1)$.
3. Démontrer que
$$\forall P_1, P_2 \in \mathbb{R}_n[X]\ , \quad \phi(P_1P_2) = \phi(P_1)\phi(P_2)$$
4. Trouver deux polynômes P_1 et P_2 tels que $\phi(P_1+P_2) \neq \phi(P_1)+\phi(P_2)$.

Exercice 7. Soit n un entier strictement positif. On se place dans l'anneau des polynômes à coefficients réels $\mathbb{R}[X]$.

1. Montrer que $X-1$ divise X^n-1.
2. Montrer X^2+2X divise $(X+1)^{2n}-1$.
3. Montrer que X^2 divise $(X+1)^n - nX - 1$.
4. Montrer que $(X-1)^2$ divise $X^n - nX + n - 1$.
5. Montrer que $(X-1)^2$ divise $nX^{n+1} - (n+1)X^n + 1$.
6. Montrer que $(X-1)^2$ divise
$$\left(\sum_{k=0}^{n-1} X^k\right)^2 - n^2X^{n-1}$$
7. Montrer que $(X-1)^3$ divise $nX^{n+2} - (n+2)X^{n+1}(n+2)X - n$
8. Soit P un polynôme quelconque. Montrer que si $X-1$ divise $P(X^n)$ alors
$$\sum_{k=0}^{2n-1} X^k \text{ divise } P(X^{2n})$$

Exercice 8. On se place dans l'anneau de polynômes $\mathbb{Z}/2\mathbb{Z}[X]$.

1. Ecrire tous les polynômes de degrés inférieurs ou égaux à 2.
2. Parmi tous les polynômes de degrés inférieurs ou égaux à 2, lesquels sont irréductibles ?
3. Pour chacun des polynômes de degrés inférieurs ou égaux à 2, écrire sa valeur en $\mathfrak{cl}(0)$ et $\mathfrak{cl}(1)$.
4. Soit P un polynôme de $\mathbb{Z}/2\mathbb{Z}[X]$. Montrer que l'application associée à P est l'application nulle, si et seulement si P est divisible par X^2+X.

5. Montrer que l'application associée à P est l'application identique, si et seulement si la division euclidienne de P par X^2+X a pour reste X.
6. Si P est de degré au moins 2 et irréductible, montrer que l'application associée à P est l'application constante égale à $\mathfrak{cl}(1)$.

Exercice 9. Dans $\mathbb{R}[X]$, effectuer la division euclidienne de P par Q pour les couples (P,Q) suivants.

1. $P=X^2-1$, $Q=X-1$
2. $P=X^3-1$, $Q=X^2+1$
3. $P=X^4-1$, $Q=X^2+1$
4. $P=X^4-2X^2+1$, $Q=X^2-2X+1$
5. $P=X^4-X^3+X-2$, $Q=X^2-2X+4$
6. $P=X^4+2X^3-X+6$, $Q=X^3-6X^2+X+4$
7. $P=3X^5+4X^2+1$, $Q=X^2+2X+3$
8. $P=3X^5+2X^4-X^2+1$, $Q=X^3+X+2$
9. $P=X^5-X^4+2X^3+X^2+4$, $Q=X^2-1$
10. $P=X^6-3X^4+3X^2-1$, $Q=X^2-X$
11. $P=X^6-X^5+X^2-1$, $Q=X^3-X$
12. $P=X^6-2X^4+X^3+1$, $Q=X^3+X^2+1$

Exercice 10. On considère les couples de polynômes (P,Q) suivants dans $\mathbb{R}[X]$.

- $P=X-1$, $Q=X$
- $P=X-1$, $Q=X-2$
- $P=X^3-2$, $Q=X^2-1$
- $P=X^3-1$, $Q=X^2+1$
- $P=X^3+1$, $Q=X^2+X+1$
- $P=X^4-1$, $Q=X^2-4$

Pour chacun de ces couples :

1. Effectuer la division euclidienne de P par Q.
2. Vérifier, en utilisant l'algorithme d'Euclide, que P et Q sont premiers entre eux.
3. Déterminer l'ensemble des couples de polynômes (S,T) tels que $SP+TQ=1$.

Exercice 11. Soient A et B deux polynômes de $\mathbb{R}[X]$, Q et R le quotient et le reste de la division euclidienne de A par B. Soit P un polynôme de degré au moins égal à 1. Démontrer que le quotient de la division euclidienne de $A\circ P$ par $B\circ P$ est $Q\circ P$ et que le reste est $R\circ P$.

Exercice 12. Soit $(P_n)_{n\in\mathbb{N}}$ la suite de polynômes définie par $P_0=1$, $P_1=X$ et pour tout $n\in\mathbb{N}$:

$$P_{n+2}=XP_{n+1}-P_n.$$

1. Calculer P_2 et P_3.
2. Montrer que pour tout $n \in \mathbb{N}$, P_n est de degré n.
3. Montrer que P_n est un polynôme pair si n est pair, impair si n est impair.
4. Montrer que pour tout $n \in \mathbb{N}$:
$$P_{n+1}^2 - P_n P_{n+2} = 1.$$
5. En déduire que pour tout $n \in \mathbb{N}$, les polynômes P_n et P_{n+1} sont premiers entre eux.

Exercice 13. On considère les couples de polynômes (P, Q) suivants dans $\mathbb{R}[X]$.
- $P = X^4 - 1$, $Q = X^2 - 1$
- $P = X^6 - 1$, $Q = X^4 - 1$
- $P = X^3 + 1$, $Q = X^2 - 1$
- $P = X^3 - 2X^2 - X + 2$, $Q = X^3 - 6X^2 + 11X - 6$
- $P = X^3 - X^2 - X - 2$, $Q = X^3 - 1$
- $P = X^4 + X^3 - 2X + 1$, $Q = X^3 + X + 1$
- $P = X^4 + X^3 - 3X^2 - 4X - 1$, $Q = X^3 + X^2 - X - 1$
- $P = X^4 + X^3 + 2X^2 + X + 1$, $Q = X^4 - 1$
- $P = X^3 - X^2 - X - 2$, $Q = X^5 - 2X^4 + X^2 - X - 2$
- $P = X^5 + 5X^4 + 9X^3 + 7X^2 + 5X + 3$, $Q = X^4 - 2X^3 + 2X^2 + X + 1$

Pour chacun de ces couples :
1. Utiliser l'algorithme d'Euclide pour calculer $\text{pgcd}(P, Q)$.
2. Decomposer P et Q en facteurs irréductibles.
3. En déduire la décomposition en facteurs irréductibles de $\text{pgcd}(P, Q)$ et retrouver le résultat de la première question.

Exercice 14. On considère les triplets de polynômes de $\mathbb{R}[X]$ suivants.
- $A = X^2 - X$, $B = X^2 - X$, $C = X^2 - 1$
- $A = (X+3)^2(X+1)(X^2+1)^3$, $B = (X+3)^2(X+2)^2(X^2+1)$, $C = (X+3)(X+2)(X^2+1)^2$
- $A = X^2 + 3X + 2$, $B = X^3 + 2X^2 + X + 2$, $C = X^5 + 4X^4 + 6X^3 + 6X^2 + 5X + 2$

Pour chacun de ces triplets :
1. Calculer $\text{pgcd}(A, B)$, $\text{pgcd}(A, C)$ et $\text{pgcd}(B, C)$.
2. Calculer $\text{pgcd}(A, B, C)$.

Exercice 15. Soient a et b deux nombres complexes distincts. Soit $P \in \mathbb{C}[X]$ un polynôme.

1. Montrer que si P est divisible par $X - a$ et par $X - b$, alors P est divisible par $(X - a)(X - b)$.

2. On suppose que les restes des divisions euclidiennes de P par $X-a$ et par $X-b$ sont tous les deux égaux à 1. Montrer que le reste de la division euclidienne de P par $(X-a)(X-b)$ est 1.
3. On suppose que les restes des divisions euclidiennes de P par $X-1$ et $X+5$ sont respectivement 7 et 3. Quel est le reste de la division euclidienne de P par X^2+4X-5 ?

Exercice 16. Ecrire la décomposition en facteurs irréductibles des polynômes suivants, dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.

1. X^4-1
2. X^6+1
3. X^8+X^4+1
4. $(X^2+X+1)^2-1$
5. X^3-5X^2+3X+9
6. $(X^2-X+2)^2+(X-2)^2$
7. $6X^5+15X^4+20X^3+15X^2+6X+1$
8. $X^5-7X^3-2X^2+12X+8$

Exercice 17. Soit $P\in\mathbb{C}[X]$ un polynôme à coefficients complexes et a un complexe. En utilisant la formule de Taylor, calculer le quotient et le reste de la division euclidienne de P par $X-a$, puis par $(X-a)^2$.

Exercice 18. Ecrire la formule de Taylor pour les polynômes suivants, en $a=1$, puis $a=-1$.

1. X^4-1
2. X^6+1
3. X^8+X^4+1
4. $(X^2+X+1)^2+1$
5. X^3-5X^2+3X+9
6. $(X^2-X+2)^2+(X-2)^2$
7. $6X^5+15X^4+20X^3+15X^2+6X+1$
8. $X^5-7X^3-2X^2+12X+8$

Exercice 19. Décomposer les fractions rationnelles suivantes, dans $\mathbb{R}(X)$:

$$\frac{1}{X(X-1)} \quad ; \quad \frac{X}{X^2-1} \quad ; \quad \frac{X^3-2X+1}{X^2-1} \quad ;$$

$$\frac{X(X^2+1)^2}{(X^2-1)^2} \quad ; \quad \frac{X^3+1}{(X-2)^4} \quad ; \quad \frac{X^5+1}{(X^2+1)^3} \quad ;$$

$$\frac{X^2+1}{(X-2)(X-1)} \quad ; \quad \frac{X^3-2}{X^2-4} \quad ; \quad \frac{X^3-2X+1}{X^3-X} \quad ;$$
$$\frac{X}{(X^2-1)(X-2)} \quad ; \quad \frac{X}{(X-1)^2(X-2)} \quad ; \quad \frac{X^4}{(X-1)^2(X-2)} \quad ;$$
$$\frac{2X^2+5}{(X^2-1)^3} \quad ; \quad \frac{X^5+1}{X^3(X-2)} \quad ; \quad \frac{X^8-X^4+2}{(X^2+X+1)^3} \quad ;$$
$$\frac{X^3+X}{(X-1)(X^6+1)} \quad ; \quad \frac{X^6-X^5+2X^4+X^2+1}{X^3(X^2+1)^2} \quad ;$$
$$\frac{X^5+6X^4+17X^3+25X^2+19X+7}{(X+1)^2(X^2+X+1)^2}.$$

Exercice 20. Décomposer les fractions rationnelles suivantes, dans $\mathbb{C}(X)$ puis dans $\mathbb{R}(X)$:

$$\frac{1}{X^3+X} \quad ; \quad \frac{X^4+1}{X^3+X} \quad ; \quad \frac{X}{(X^2+1)(X^2+4)} \quad ;$$
$$\frac{X^3+1}{X^2+1} \quad ; \quad \frac{X^5-1}{X^4-1} \quad ; \quad \frac{X^2+1}{X^4+1} \quad ;$$
$$\frac{X-1}{X^3-1} \quad ; \quad \frac{X-1}{X^3+X} \quad ; \quad \frac{X^2-1}{(X^2+1)^2} \quad ;$$
$$\frac{X}{X^4+1} \quad ; \quad \frac{X^2+1}{X^4+1} \quad ; \quad \frac{X^2+X+1}{X^4-1} \quad ;$$
$$\frac{X^3}{X^4+1} \quad ; \quad \frac{X}{(X-1)^2(X^2+1)^2} \quad ; \quad \frac{X^2-1}{X^6-1}.$$

2.3 QCM

Donnez-vous une heure pour répondre à ce questionnaire. Les 10 questions sont indépendantes. Pour chaque question 5 affirmations sont proposées, parmi lesquelles 2 sont vraies et 3 sont fausses. Pour chaque question, cochez les 2 affirmations que vous pensez vraies. Chaque question pour laquelle les 2 affirmations vraies sont cochées rapporte 2 points.

Question 1. Soit $P \in \mathbb{R}[X]$ un polynôme à coefficients réels, et d un entier naturel non nul.

A Si le degré de P est d, alors le degré de $P - X^d$ est strictement inférieur à d.
B Si le degré de P est d, alors le degré de P' est $d-1$.
C Si le degré de P est d, alors le degré de $P(X-1)$ est $d-1$.
D Si le degré de P est d, alors le degré de $P'(X-1)$ est $d-1$.
E Si le degré de P est d, alors le degré de $(X+2)P(X+2)$ est $d+2$.

Question 2. Soient P un polynôme non nul à coefficients réels.

A Le degré de $P((X+2)^2)$ est le double du degré de P.

B Le degré de $(X+2)P((X+2)^2)$ est toujours supérieur ou égal à 2.

C Le degré de $P'((X+2)^2)$ est soit un entier pair, soit $-\infty$.

D Le degré de $(X+2)^2P'((X+2)^2)$ est toujours supérieur ou égal à 2.

E Le degré de $(X+2)^2P'((X+2)^2)$ est toujours le double du degré de P.

Question 3. Soient P et Q deux polynômes non nuls, à coefficients réels.

A Les polynômes $P(Q)$ et $Q(P)$ ont toujours le même degré.

B Les polynômes PQ et $P(Q)$ ont toujours le même degré.

C Si le polynôme Q est constant, alors les polynômes PQ et $P(Q)$ ont le même degré.

D Si les polynômes $P+Q$ et PQ ont le même degré, alors au moins un des deux polynômes P et Q est constant.

E Si les polynômes PQ et $P(Q)$ ont le même degré, alors les deux polynômes P et Q sont constants.

Question 4. Soit $P \in \mathbb{R}[X]$ un polynôme non nul à coefficients réels.

A Si 2 est racine de P, alors 0 est racine de $P(X)-2$.

B Si 2 est racine double de P, alors P' est divisible par $(X-2)$.

C Si P' est divisible par $(X-2)$ alors 2 est racine double de P.

D Si 2 est racine double de P', alors P est divisible par $(X-2)^3$.

E Si 2 est racine double de P et de P', alors P est divisible par $(X-2)^3$.

Question 5. Soient P et Q deux polynômes non nuls à coefficients réels.

A Si P divise Q alors $P+Q$ divise Q^2.

B Si P divise Q, alors P' divise Q'.

C Si P divise Q, alors P^2 divise Q^2.

D Si P divise Q, alors $P(X^2)$ divise $Q(X^2)$.

E Si P divise Q, alors P divise $Q(P)$.

Question 6. Soit P un polynôme non nul à coefficients réels.

A Le reste de la division euclidienne de P par $(X-2)$ est $P(2)$.

B Si $P(2)=P'(2)$, alors les restes des divisions euclidiennes de P et P' par $(X-2)$ sont égaux.

C Le reste de la division euclidienne de P par $(X-2)^2$ est $P'(2)(X-2)$.

D Si le reste de la division euclidienne de P' par $(X-2)$ est nul, alors 2 est racine double de P.

E Si le reste de la division euclidienne de P par $(X-2)^2$ est $(X-2)$, alors 2 est racine double de P'.

Question 7. Soient P et Q deux polynômes non nuls à coefficients réels.

A Si P est premier avec Q, alors le reste de la division euclidienne de P par Q est 1.
B Si P est premier avec Q, alors P est premier avec $(X+2)P+2Q$.
C Si P est premier avec Q, alors P' est premier avec Q'.
D Si P est premier avec Q, alors $P+Q$ est premier avec P^2-Q^2.
E Si P est premier avec Q, alors P est premier avec P^2+2Q^2.

Question 8. Soit $P \in \mathbb{R}[X]$ un polynôme à coefficients réels.
A Si le degré de P est pair, alors P' possède au moins une racine réelle.
B Si P est de degré 3, alors P' est irréductible dans $\mathbb{R}[X]$.
C Si P divise (X^5-1), alors P' admet au moins une racine réelle.
D Si un nombre complexe z de partie imaginaire non nulle est racine de P, alors P est divisible par le polynôme $(X^2-2\mathrm{Re}(z)X+|z|^2)$.
E Si P divise $(X^5-1)^2$, alors P' est premier avec P.

Question 9.
A Le polynôme (X^4+4) est réductible dans $\mathbb{Q}[X]$
B Le polynôme (X^4+4) est irréductible dans $\mathbb{R}[X]$
C Le polynôme (X^4+4) est irréductible dans $\mathbb{Z}/5\mathbb{Z}[X]$.
D Le polynôme (X^4+4) est scindé dans $\mathbb{R}[X]$.
E Le polynôme (X^4+4) est scindé dans $\mathbb{C}[X]$

Question 10. On considère la fraction rationnelle :

$$\frac{P}{Q} = \frac{2X^2}{X^4-1}$$

A La décomposition de P/Q dans $\mathbb{R}(X)$ a un seul élément simple.
B La décomposition de P/Q dans $\mathbb{C}(X)$ admet 2 pour partie entière.
C La décomposition de P/Q dans $\mathbb{R}(X)$ admet un élément simple proportionnel à $1/(X+1)$
D La décomposition de P/Q dans $\mathbb{R}(X)$ contient les deux éléments simples $1/(X^2-1)$ et $1/(X^2+1)$.
E La décomposition de P/Q dans $\mathbb{C}(X)$ contient quatre éléments simples.

Réponses : 1–BD 2–AC 3–AD 4–BE 5–CD 6–AB 7–BE 8–AD 9–AE 10–CE

2.4 Devoir

Essayez de bien rédiger vos réponses, sans vous reporter ni au cours, ni au corrigé. Si vous souhaitez vous évaluer, donnez-vous deux heures ; puis comparez vos réponses avec le corrigé et comptez un point pour chaque question à laquelle vous aurez correctement répondu.

Questions de cours :

1. Étant donné un polynôme $P \in \mathbb{R}[X]$, rappeler la définition du polynôme dérivé P'. Démontrer que l'application de $\mathbb{R}[X]$ dans lui-même, qui à un polynôme P associe son polynôme dérivé P' est linéaire, c'est-à-dire :
$$\forall P, Q \in \mathbb{R}[X]\,,\ \forall \lambda, \mu \in \mathbb{R}\,, \quad (\lambda P + \mu Q)' = \lambda P' + \mu Q'\,.$$
2. Soit $P \in \mathbb{R}[X]$ un polynôme à coefficients réels, et $n \in \mathbb{N}^*$ un entier strictement positif. Montrer que :
$$(X^n P)' = nX^{n-1}P + X^n P'\,.$$
3. En déduire que pour tout couple de polynômes (P, Q) à coefficients réels,
$$(PQ)' = P'Q + PQ'\,.$$
4. Soit $P \in \mathbb{R}[X]$ un polynôme à coefficients réels, et $n \in \mathbb{N}^*$ un entier strictement positif. Montrer que :
$$(P^n)' = nP'P^{n-1}\,.$$
5. Montrer que pour tout couple de polynômes (P, Q) à coefficients réels,
$$(Q(P))' = P'Q'(P)\,.$$

Exercice 1 : Soit n un entier. On considère le polynôme $W_n = (X^2-1)^n$. Le n-ième polynôme de Legendre L_n est proportionnel à la dérivée n-ième de W_n :
$$L_n = \frac{1}{2^n n!} W_n^{(n)}\,.$$

NB : On admettra la formule de Leibniz, qui généralise la formule donnant la dérivée d'un produit. Soient P et Q deux polynômes et n un entier, alors :
$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}\,.$$

1. Calculer L_1, L_2 et L_3.
2. Quel est le degré de W_n ? Quel est son coefficient dominant ? Quel est le degré de L_n ? Quel est son coefficient dominant ?
3. Pour tout $n \in \mathbb{N}$, démontrer que $(X^2-1)W_n' = 2nXW_n$. En prenant la dérivée $(n+1)$-ième des deux membres, en déduire que :
$$(X^2-1)L_n'' + 2XL_n' - n(n+1)L_n = 0\,.$$
4. En prenant la dérivée $(n+1)$-ième du produit $(X^2-1)(X^2-1)^{n-1}$, montrer que pour tout $n \geqslant 1$,
$$W_n^{(n+1)} = (X^2-1)W_{n-1}^{(n+1)} + 2X(n+1)W_{n-1}^{(n)} + n(n+1)W_{n-1}^{(n-1)}\,.$$

5. En utilisant les deux questions précédentes, montrer que pour tout $n \geqslant 1$:

$$L'_n = XL'_{n-1} + nL_{n-1} \ .$$

Exercice 2 :

1. En utilisant l'identité $(X^3 - 1) = (X - 1)(X^2 + X + 1)$, démontrer que les polynômes $X^3 + 1$ et $X^2 + X + 1$ sont premiers entre eux.
2. Effectuer la division euclidienne de $X^3 + 1$ par $X^2 + X + 1$.
3. Déterminer l'ensemble des couples de polynômes (U, V) tels que :

$$(X^3 + 1)U + (X^2 + X + 1)V = 1 \ .$$

4. Déterminer une décomposition en facteurs irréductibles dans $\mathbb{R}[X]$ des polynômes $X^5 - X^3 + X^2 - 1$ et $X^3 - 1$. En déduire leur pgcd et leur ppcm.
5. Retrouver le pgcd de $X^5 - X^3 + X^2 - 1$ et $X^3 - 1$ en utilisant l'algorithme d'Euclide.

Exercice 3 : Le but de l'exercice est de calculer la décomposition en éléments simples dans $\mathbb{R}(X)$ de la fraction rationnelle : $(4X^4)/(X^4 - 1)^2$.

1. Décomposer en éléments simples dans $\mathbb{R}(X)$, la fraction rationnelle $(2X)/(X^2 - 1)$. En déduire que :

$$\frac{4X^4}{(X^4-1)^2} = \frac{1}{(X^2+1)^2} + \frac{1}{(X^2-1)^2} + \frac{2}{X^4-1} \ .$$

2. Décomposer en éléments simples la fraction rationnelle $1/(X^2 - 1)$. En déduire la décomposition en éléments simples de la fraction rationnelle $1/(X^2 - 1)^2$.
3. Utiliser la décomposition en éléments simples de la fraction rationnelle $1/(X^2-1)$ pour donner la décomposition en éléments simples dans $\mathbb{R}(X)$ de la fraction rationnelle $1/(X^4 - 1)$.
4. Déduire des questions précédentes la décomposition en éléments simples de la fraction rationnelle $(4X^4)/(X^4 - 1)^2$.
5. Retrouver le résultat de la question précédente en utilisant la méthode présentée dans le cours.

2.5 Corrigé du devoir

Questions de cours :

1. Pour un polynôme $P = a_d X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0$ non nul dans $\mathbb{R}[X]$, le *polynôme dérivé* de P est le polynôme noté P' :

$$P' = da_d X^{d-1} + (d-1)a_{d-1}X^{d-2} + \cdots + a_1.$$

Si $P = 0$, le polynôme dérivé de P est le polynôme nul.

Soient

$$P = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0 \quad \text{et} \quad Q = b_h X^h + b_{h-1} X^{h-1} + \cdots + b_1 X + b_0$$

deux polynômes à coefficients réels. Soient λ et μ deux réels. Sans perte de généralité, supposons $h \leqslant d$. Quitte à poser $b_{h+1} = \cdots = b_d = 0$, nous pouvons écrire :

$$\lambda P + \mu Q = (\lambda a^d + \mu b^d) X^d + \cdots + (\lambda a_0 + \mu b_0) \; .$$

Le polynôme dérivé est :

$$(\lambda P + \mu Q)' = (\lambda a^d + \mu b^d) d X^{d-1} + \cdots + (\lambda a_1 + \mu b_1) \; .$$

Il est bien égal à :

$$\lambda P' + \mu Q' = \lambda (a^d d X^{d-1} + \cdots + a_1) + \mu (b^d d X^{d-1} + \cdots + b_1) \; .$$

2. Posons $P = a_d X^d + \cdots + a_0$: alors $X^n P = a_d X^{n+d} + \cdots + a_0 X^n$. Par définition, le polynôme dérivé de $X^n P$ est :

$$(X^n P)' = a_d (n+d) X^{n+d-1} + \cdots + a_0 n X^{n-1} = \sum_{k=0}^{d} a_k (n+k) X^{n+k-1} \; .$$

Or :

$$\begin{aligned} n X^{n-1} P + X^n P' &= n X^{n-1} \left(\sum_{k=0}^{d} a_k X^k \right) + X^n \left(\sum_{h=1}^{d} h a_h X^{h-1} \right) \\ &= \sum_{k=0}^{d} (n+k) a_k X^{n+k-1} \; . \end{aligned}$$

3. Nous allons démontrer la formule par récurrence sur le degré de Q. Elle est vraie si Q est nul ou de degré 0, puisque dans ce cas $Q' = 0$ et la dérivation est linéaire d'après la question 2. Supposons que la formule est vraie pour tout polynôme de degré inférieur ou égal à $n-1$ et soit Q un polynôme de degré n. Nous pouvons écrire $Q = b_n X^n + Q_1$, où Q_1 est un polynôme de degré inférieur ou égal à $n-1$. Écrivons :

$$\begin{aligned} (PQ)' &= \Big((b_n X^n + Q_1) P \Big)' \\ &= (b_n X^n P + P Q_1)' \\ &= b_n (X^n P)' + (P Q_1)' && \text{(question 1)} \\ &= b_n (n X^{n-1} P + X_n P') + (P Q_1)' && \text{(question 2)} \\ &= b_n (n X^{n-1} P + X_n P') + P Q_1' + P' Q_1 && \text{(hypothèse de récurrence)} \\ &= P Q' + Q P' \; . \end{aligned}$$

4. C'est une autre démonstration par récurrence. La formule est vraie pour $n = 0$, puisque P^0 est le polynôme constant égal à 1, dont la dérivée est nulle. Supposons-la vraie pour $n \geqslant 1$.

$$\begin{aligned}(P^{n+1})' &= (PP^n)' \\ &= P(P^n)' + P'P^n \qquad \text{(question 3)} \\ &= P(nP'P^{n-1}) + P'P^n \quad \text{(hypothèse de récurrence)} \\ &= (n+1)P'P^n \ .\end{aligned}$$

   La formule est vraie pour $n+1$, donc pour tout n.

5. Posons $Q = b_n X^n + \cdots + b_0$. Le polynôme composé $Q(P)$ est :

$$Q(P) = \sum_{k=0}^{n} b_k P^k \ .$$

   D'après la linéarité de la dérivation (question 1) :

$$(Q(P))' = \sum_{k=0}^{n} b_k (P^k)' \ .$$

   En utilisant le résultat de la question précédente :

$$(Q(P))' = \sum_{k=0}^{n} b_k k P'(P^{k-1}) = P' \sum_{k=0}^{n} k b_k P^{k-1} = P'Q'(P) \ .$$

Exercice 1 :

1. On trouve :

$$L_1 = X \quad ; \quad L_2 = \frac{3}{2}X^2 - \frac{1}{2} \quad ; \quad L_3 = \frac{5}{2}X^3 - \frac{3}{2}X \ .$$

2. Le degré de W_n est $2n$, son coefficient dominant est 1. Le degré de L_n est n, son coefficient dominant est :

$$\frac{(2n)(2n-1)\dots(n+1)}{2^n n!} = \frac{1}{2^n}\binom{2n}{n} \ .$$

3. En utilisant la formule donnant la dérivée d'un polynôme composé, on obtient $W_n' = 2nX(X^2-1)^{n-1}$, donc $(X^2-1)W_n' = 2nXW_n$.
   Prenons la dérivée $(n+1)$-ième des deux membres, en utilisant la formule de Leibniz. Pour le membre de gauche, on obtient :

$$(X^2-1)W_n^{(n+2)} + 2X(n+1)W_n^{(n+1)} + n(n+1)W_n^{(n)} \ .$$

   Pour le membre de droite, la formule de Leibniz donne :

$$2nXW_n^{(n+1)} + 2n(n+1)W_n^{(n)} \ .$$

En égalant les deux, et en regroupant les termes, on obtient :

$$(X^2-1)W_n^{(n+2)} + 2XW_n^{(n+1)} - n(n+1)W_n^{(n)} = 0 \ .$$

En divisant par $2^n n!$:

$$(X^2-1)L_n'' + 2XL_n' - n(n+1)L_n = 0 \ .$$

4. En prenant la dérivée $(n+1)$-ième du produit $(X^2-1)(X^2-1)^{n-1}$, on obtient comme dans la question précédente :

$$W_n^{(n+1)} = (X^2-1)W_{n-1}^{(n+1)} + 2X(n+1)W_{n-1}^{(n)} + n(n+1)W_{n-1}^{(n-1)} \ .$$

5. En divisant les deux membres par $2^n n!$:

$$L_n' = (X^2-1)\frac{1}{2n}L_{n-1}'' + 2X\frac{(n+1)}{2n}L_{n-1}' + \frac{n(n+1)}{2n}L_{n-1} \ .$$

Or d'après la question 3,

$$(X^2-1)L_{n-1}'' + 2XL_{n-1}' = n(n-1)L_{n-1} \ .$$

En reportant ceci dans l'expression précédente :

$$\begin{aligned} L_n' &= \frac{n(n-1)}{2n}L_{n-1} + XL_{n-1}' + \frac{n(n+1)}{2n}L_{n-1} \\ &= XL_{n-1}' + nL_{n-1} \ . \end{aligned}$$

Exercice 2 :

1. Puisque $(X^3-1) = (X-1)(X^2+X+1)$, on peut aussi écrire : $(X^3+1) - (X-1)(X^2+X+1) = 2$. Ceci est une identité de Bézout pour les polynômes X^3+1 et X^2+X+1 : ils sont donc premiers entre eux.

2.
$$\begin{array}{r|l} X^3 + 1 & X^2+X+1 \\ \cline{2-2} X^3+X^2+X & X-1 \\ \cline{1-1} -X^2-X+1 & \\ -X^2-X-1 & \\ \cline{1-1} 2 & \end{array}$$

On retrouve l'identité de la question précédente : $(X^3+1) = (X-1)(X^2+X+1)+2$.

3. Soient U et V deux polynômes tels que $(X^3+1)U + (X^2+X+1)V = 1$. Puisque $(X^3+1)/2 - (X-1)(X^2+X+1)/2 = 1$, on a nécessairement :

$$(X^3+1)(U-1/2) + (X^2+X+1)(V+X/2-1/2) = 0 \ .$$

Or (X^3+1) et (X^2+X+1) sont premiers entre eux. En utilisant le lemme de Gauss, on déduit que (X^2+X+1) divise $(U-1/2)$ et que (X^2+1) divise $(V+X/2-1/2)$: il existe un polynôme K tel que :

$$U = \frac{1}{2} + K(X^2+X+1) \quad \text{et} \quad V = \frac{1}{2}(-X+1) - K(X^3+1) \; .$$

Réciproquement, si U et V s'écrivent comme ci-dessus, alors :

$$(X^3+1)(U-1/2) = (X^2+X+1)(V+X/2-1/2) = K(X^3+1)(X^2+X+1) \; .$$

Donc :

$$(X^2+1)U + (X^2+X+1)V = \frac{1}{2}(X^3+1) - \frac{1}{2}(X-1)(X^2+X+1) = 1 \; .$$

L'ensemble des couples (U,V) tels que $(X^3+1)U + (X^2+X+1)V = 1$ est :

$$\left\{ \left(\frac{1}{2} + K(X^2+X+1) \; , \; \frac{1}{2}(-X+1) - K(X^3+1) \right) \; , \quad K \in \mathbb{R}[X] \right\} \; .$$

4. On trouve :

$$X^5 - X^3 + X^2 - 1 = (X^2-1)(X^3+1) = (X+1)^2(X-1)(X^2-X+1) \; ,$$

et

$$X^3 - 1 = (X-1)(X^2+X+1) \; .$$

Le pgcd des deux polynômes est $(X-1)$, leur ppcm est $(X+1)^2(X-1)(X^2-X+1)(X^2+X+1)$.

5. La division euclidienne des deux polynômes donne :

$$X^5 - X^3 + X^2 - 1 = (X^2-1)(X^3-1) + 2X^2 - 2 \; .$$

La division euclidienne de X^3-1 par X^2-1 donne :

$$X^3 - 1 = X(X^2-1) + (X-1) \; .$$

L'algorithme d'Euclide se termine sur : $X^2-1 = (X+1)(X-1)+0$. On retrouve donc bien le fait que $(X-1)$ est le pgcd des deux polynômes (toujours défini à une constante près).

Exercice 3 :

1. On trouve :

$$\frac{2X}{X^2-1} = \frac{1}{X+1} + \frac{1}{X-1} \; .$$

En remplaçant X par X^2, on obtient :

$$\frac{2X^2}{X^4-1} = \frac{1}{X^2+1} + \frac{1}{X^2-1} .$$

Il reste à élever les deux membres au carré :

$$\frac{4X^4}{(X^4-1)^2} = \frac{1}{(X^2+1)^2} + \frac{1}{(X^2-1)^2} + \frac{2}{X^4-1} .$$

Observons que les deux dernières identités *ne sont pas* des décompositions en éléments simples.

2.
$$\frac{1}{X^2-1} = \frac{\frac{1}{2}}{X-1} - \frac{\frac{1}{2}}{X+1} .$$

En élevant au carré, on obtient :

$$\frac{1}{(X^2-1)^2} = \frac{\frac{1}{4}}{(X-1)^2} + \frac{\frac{1}{4}}{(X+1)^2} - \frac{\frac{1}{2}}{X^2-1} .$$

Il reste à réinjecter la décomposition de $1/(X^2-1)$:

$$\frac{1}{(X^2-1)^2} = \frac{\frac{1}{4}}{(X-1)^2} + \frac{\frac{1}{4}}{(X+1)^2} + \frac{\frac{1}{4}}{X+1} - \frac{\frac{1}{4}}{X-1} .$$

3. En remplaçant X par X^2 dans la décomposition de $1/(X^2-1)$, on obtient :

$$\frac{1}{X^4-1} = \frac{\frac{1}{2}}{X^2-1} - \frac{\frac{1}{2}}{X^2+1} .$$

En utilisant à nouveau la décomposition de $1/(X^2-1)$, on trouve :

$$\frac{1}{X^4-1} = \frac{\frac{1}{4}}{X-1} - \frac{\frac{1}{4}}{X+1} - \frac{\frac{1}{2}}{X^2+1} .$$

4. Dans l'expression de la question 1, le terme $1/(X^2+1)^2$ est un élément simple. La décomposition en éléments simples de $1/(X^2-1)^2$ est donnée à la question 2, celle de $1/(X^4-1)$ à la question 3. En rassemblant le tout on obtient :

$$\frac{4X^4}{(X^4-1)^2} = \frac{1}{(X^2+1)^2} - \frac{1}{X^2+1} + \frac{\frac{1}{4}}{(X-1)^2} + \frac{\frac{1}{4}}{X-1} + \frac{\frac{1}{4}}{(X+1)^2} - \frac{\frac{1}{4}}{X+1} .$$

5. Par la méthode du cours, on écrit la décomposition cherchée sous la forme :

$$\frac{4X^4}{(X^4-1)^2} = \frac{AX+B}{(X^2+1)^2} + \frac{CX+D}{X^2+1} + \frac{E}{(X-1)^2} + \frac{F}{X-1} + \frac{G}{(X+1)^2} + \frac{H}{X+1} .$$

On simplifie notablement le calcul en observant que la fraction est invariante par le changement $X \mapsto -X$, et donc sa décomposition vérifie la même propriété. Ceci entraîne :

$$A = 0\,,\ C = 0\,,\ G = E\,,\ H = -F\ .$$

Multiplier par $(X-1)^2$ et remplacer X par 1 donne $E = 1/4$. Multiplier par $(X^2{+}1)^2$ et remplacer X par i donne $B = 1$. Il reste deux coefficients à déterminer, par exemple en prenant deux valeurs particulières. Pour $X = 0$:

$$0 = 1 + D + \frac{1}{4} - F + \frac{1}{4} - F\ .$$

Pour $X = 2$,

$$\frac{64}{15^2} = \frac{1}{25} + \frac{D}{5} + \frac{1}{4} + F + \frac{1}{36} - \frac{F}{3}\ .$$

La résolution du système de deux équations en D et F donne $D = -1$, $F = 1/4$.

3 Compléments

3.1 Algorithme de Horner

Au temps jadis, les physiciens et les astronomes devaient faire tous leurs calculs à la main, et ces calculs pouvaient être très compliqués. Il fallait souvent évaluer des quantités polynomiales, par exemple $5x^4-4x^3+3x^2-2x+1$ pour $x = 8$. La façon naïve d'arriver au résultat est de calculer x, x^2, x^3 et x^4 pour la valeur choisie $x = 8$, ce qui représente 3 multiplications, puis $5x^4$, $4x^3$, $3x^2$ et $2x$, ce qui représente 4 multiplications supplémentaires. En ajoutant les sommes à la liste des opérations nécessaires, on obtient en tout 7 multiplications et 4 additions. La tradition attribue au mathématicien anglais William George Horner (1786-1837) la description en 1819 d'une méthode efficace pour économiser des opérations, méthode encore utilisée de nos jours par les ordinateurs. Remplaçons en effet $5x^4 - 4x^3 + 3x^2 - 2x + 1$ par l'expression équivalente

$$x(x(x(x \times 5 - 4) + 3) - 2) + 1,$$

puis calculons successivement $a = 5$, $b = xa - 4$, $c = xb + 3$, $d = xc - 2$, et enfin $e = xd+1$. Alors e est le résultat cherché, obtenu après 4 multiplications et 4 additions. On économise donc des multiplications, qui sont des opérations longues à réaliser. De plus, on n'a été obligé de stocker en mémoire (ou dans son cerveau, si on n'est pas en silicium) que deux valeurs : x et a, puis x et b, puis x et c, etc.

La tradition a retenu cette méthode sous le nom d'algorithme de Horner à cause de l'article de 1819 cité plus haut. Il se trouve que cet article ne contient pas ladite méthode ! Horner la décrit bien, mais dans un autre article, publié en 1830 seulement. Et entre temps, en 1820, un fabricant de montres londonien nommé Theophilus Holdred avait, lui, effectivement publié la méthode.

Alors, Horner plagiaire ? Quoi qu'il en soit, on sait maintenant que la méthode de Horner était en fait déjà connue d'Isaac Newton en 1669, et avant lui, du mathématicien chinois Ch'in Chiu-Shao (ou Chu Shih-Chieh, ou Zhu Shijie, on s'y perd !) au XIII$^{\text{e}}$ siècle. Elle peut être vue comme un cas particulier d'une règle due au mathématicien italien Paolo Ruffini (1765-1822), règle qui permet de calculer le quotient et le reste de la division euclidienne d'un polynôme P par un monôme $X - a$. Signalons enfin que des versions de cet algorithme permettent aussi d'évaluer des polynômes de matrices, situation où le gain de temps de calcul réalisé est encore plus important.

3.2 Règle des signes de Descartes

Il s'agit d'une méthode pour estimer le nombre de racines réelles positives d'un polynôme : on compte le nombre c de changements de signe dans la suite des coefficients, en ne tenant pas compte des coefficients nuls (voir les exemples plus bas). René Descartes (1596-1650) énonce dans *La Géométrie*, traité publié en 1637, que le nombre de racines positives vaut au plus c. Carl Friedrich Gauss (1777-1855) montrera plus

tard, en 1828, que si l'on compte les racines avec leur multiplicité, alors le nombre de racines positives a la même parité que c, donc que ce nombre vaut c ou $c-2$ ou $c-4$, etc.

Donnons un premier exemple : pour $P = X^7+2X^6-3X^5-X^2+7X-8$, on obtient $c = 3$ (remarquer les coefficients nuls), donc P possède 1 ou 3 racines positives.

Donnons un autre exemple, qui montre qu'on peut même souvent déterminer le nombre exact de racines positives et de racines négatives en utilisant la règle des signes et quelques remarques de bon sens. Soit Q le polynôme $Q = X^3+3X^2-X-2$. Puisque $c = 1$, on sait que Q possède exactement 1 racine positive. Les racines négatives de Q sont les racines positives du polynôme R obtenu en remplaçant X par $-X$ dans Q, soit $R = -X^3+3X^2+X-2$. Pour R, on trouve $c = 2$ donc Q possède 2 racines négatives ou bien aucune. On remarque ensuite que $Q(-1) = 1$ (le calcul de tête est facile en utilisant l'algorithme de Horner), donc $Q(-1)$ est positif, et que le monôme de plus haut degré de Q est X^3 donc $Q(x) < 0$ pour tout x négatif tel que $|x|$ est suffisamment grand. Ainsi Q possède au moins une racine inférieure à -1, ce qui montre que Q possède 2 racines négatives. Enfin $Q(0) = -2$ et $Q(-1) = 1$ sont de signes contraires donc Q possède une racine entre -1 et 0. On a localisé les $1+2 = 3$ racines de Q, en montrant que chacun des intervalles $]-\infty,-1[$, $]-1,0[$ et $]0,+\infty[$ en contient exactement une.

On peut encore préciser les choses en remarquant que $Q(1) = -2$, donc $Q(1)$ est négatif, et, grâce à deux derniers petits coups de Horner, que $Q(-2) = -2$ et $Q(2) = 42$. Donc les racines de Q sont en fait dans les intervalles $]-2,-1[$, $]-1,0[$ et $]1,2[$ et chacun de ces intervalles en contient exactement une.

3.3 Suites de Sturm

Soit P un polynôme à coefficients réels n'ayant que des racines simples. La suite de Sturm de ce polynôme est une suite de polynômes qui permet de déterminer le nombre de racines de P dans un intervalle donné. Elle est définie de la façon suivante : on pose $P_0 = P$ et $P_1 = P'$, où P' désigne le polynôme dérivé de P. Ensuite, pour calculer P_2, on effectue la division euclidienne de P_0 par P_1. Le résultat peut s'écrire comme

$$P_0 = P_1Q_1 - P_2,$$

où le degré de P_2 est strictement inférieur à celui de P_1. En d'autres termes, P_2 est l'opposé du reste dans la division euclidienne de P_0 par P_1. Puis on recommence pour calculer P_3, donc

$$P_1 = P_2Q_2 - P_3,$$

et le degré de P_3 est strictement inférieur à celui de P_2, etc. On s'arrête lorsqu'on obtient un polynôme constant P_n, ce qui arrive forcément puisque le degré des polynômes obtenus diminue à chaque division. La suite de Sturm du polynôme P est alors

$$S = (P_0, P_1, \ldots, P_n).$$

Ensuite, pour chaque nombre réel x, on note $V(x)$ le nombre de changements de signes dans la suite $S(x) = (P_0(x), P_1(x), \ldots, P_n(x))$.

Le théorème de Sturm, démontré par Charles Sturm (1803-1855) en 1829, affirme que le nombre de racines de P dans l'intervalle $[a, b]$ est égal à la différence $V(a) - V(b)$.

Un exemple, un exemple ! Soit $P = X^3 + 6X^2 - 16$. Sa suite de Sturm est

$$S = (X^3 + 6X^2 - 16, 3X^2 + 12X, 8X + 16, 12).$$

En particulier, $S(-7) = (-65, 63, -40, 12)$ et il y a 3 changements de signe dans cette suite, donc $V(-7) = 3$. De même, $S(2) = (16, 36, 32, 12)$ et cette fois, il n'y a pas de changement de signe, donc $V(2) = 0$. Par conséquent, $V(-7) - V(2) = 3$ donc les 3 racines de P sont dans l'intervalle $[-7, 2]$. Étonnant, non ?

3.4 Division suivant les puissances croissantes

Beaucoup moins fondamentale que la division euclidienne, c'est une technique utile pour produire des algorithmes dans des cadres assez variés.

Proposition 19. *Soit $\mathbb{K}$ un corps commutatif, A et B deux polynômes de $\mathbb{K}[X]$ et $n \geq 0$ un entier fixé. On suppose que $B(0) \neq 0$.*

Alors il existe un couple (Q_n, S_n) unique (de polynômes) vérifiant la double condition :

$$A = BQ_n + X^{n+1}S_n \qquad \text{et} \qquad \deg Q_n \leq n.$$

Démonstration : La démonstration d'existence n'est pas passionnante (simple description abstraite de l'algorithme de calcul) ; la démonstration d'unicité est plus agréable.

Preuve de l'existence

C'est une récurrence sur l'entier $n \geq 0$.

• Pour $n = 0$, on note $a_0 = A(0)$ et $b_0 = B(0)$, puis on pose $Q_0 = a_0/b_0$ (qui existe puisque $B(0) \neq 0$). On constate alors que $A - BQ_0$ est par construction un polynôme sans terme constant, donc dans lequel X se factorise ; on peut donc mettre $A - BQ_0$ sous la forme XS_0.

• Soit n fixé et supposons le théorème vrai pour tous polynômes et tout $i \leq n$; montrons le pour les polynômes A et B de l'énoncé et pour l'entier $n+1$. Commençons par effectuer la division suivant les puissances croissantes de A par B à l'ordre n, et écrivons donc $A = BQ_n + X^{n+1}S_n$ (avec $\deg Q_n \leq n$), puis effectuons la division suivant les puissances croissantes de S_n par B à l'ordre 0 : on obtient une constante k et un polynôme T tels que $S_n = kB + XT$. On conclut que $A = BQ_n + kBX^{n+1} + X^{n+2}T$ et donc qu'on peut prendre $Q_{n+1} = Q_n + kX^{n+1}$ et $S_{n+1} = T$ pour répondre à la question.

Preuve de l'unicité

Supposons qu'on ait deux écritures $A = BQ_n^{(1)} + X^{n+1}S_n^{(1)}$ et $A = BQ_n^{(2)} + X^{n+1}S_n^{(2)}$ remplissant les conditions $\deg Q_n^{(1)} \leq n$ et $\deg Q_n^{(2)} \leq n$.

Posons alors $Q_n = Q_n^{(1)} - Q_n^{(2)}$ et $S_n = S_n^{(1)} - S_n^{(2)}$ de telle sorte que $0 = BQ_n + X^{n+1}S_n$ (obtenue en soustrayant les deux écritures de A) avec en outre la condition $\deg Q_n \leq n$. Comme on a supposé $B(0) \neq 0$, X ne figure pas parmi les facteurs irréductibles de B, donc X^{n+1} est premier avec B. Mais d'après l'identité $BQ_n = -X^{n+1}S_n$, X^{n+1} divise BQ_n : on en déduit donc que X^{n+1} divise Q_n (lemme de Gauss) ; vu la condition sur le degré de Q_n, ceci entraîne que $Q_n = 0$. Dès lors $0 = X^{n+1}S_n$ donc $S_n = 0$. Les deux écritures fournies de A étaient donc la même. □

La division selon les puissances croissantes s'effectue comme la division euclidienne, mais à l'envers : on fait disparaître un par un les termes de plus bas degré du dividende, en multipliant le diviseur par la quantité appropriée. Contrairement à la division euclidienne, on peut la continuer indéfiniment : on ne s'arrête que quand l'ordre désiré est atteint. Par exemple, pour diviser $A = X + 1$ par $B = X^2 + 1$, on écrit :

$$\begin{array}{rrrrr|l}
1 & +X & & & & 1+X^2 \\
\cline{6-6}
1 & & +X^2 & & & \\
\cline{1-3}
 & X & -X^2 & & & \\
 & X & & +X^3 & & \\
\cline{2-4}
 & & -X^2 & -X^3 & & \\
 & & -X^2 & & -X^4 & \\
\cline{3-5}
 & & & -X^3 & +X^4 &
\end{array}$$

Ce qui fournit la division suivant les puissances croissantes jusqu'à l'ordre $n = 2$:

$$(1 + X) = (1 + X^2)(1 + X - X^2) + X^3(X - 1)$$

À quoi cela peut-il bien servir ? Eh bien entre autres, à décomposer en éléments simples...

$$\frac{1+X}{X^3(1+X^2)} = \frac{(1+X^2)(1+X-X^2)+X^3(X-1)}{X^3(1+X^2)} = \frac{1}{X^3} + \frac{1}{X^2} - \frac{1}{X} + \frac{X-1}{X^2+1}$$

3.5 Formule de Cardan

Il s'agit d'une formule qui permet de résoudre l'équation générale du troisième degré $ax^3 + bx^2 + cx + d = 0$. Par une réduction facile (saurez-vous effectuer cette réduction ? Indication : poser $x = y + e$ pour une constante e bien choisie et considérer l'équation en y), on peut se ramener au cas de l'équation $x^3 + 3px + 2q = 0$ avec p et q réels. Le discriminant du polynôme $X^3 + 3pX + 2q$ vaut par définition

$$D = q^2 + p^3.$$

La formule de Cardan affirme qu'une racine réelle de l'équation vaut

$$x = \sqrt[3]{\sqrt{D} - q} - \sqrt[3]{\sqrt{D} + q}.$$

Considérons par exemple l'équation $x^3 = 51x + 104$. Alors $p = -17$, $q = -52$ et $D = 52^2 - 17^3 = -2209$. En étudiant les variations de la fonction $x \mapsto x^3 - 51x - 104$, notamment ses limites en plus ou moins l'infini, il est clair que cette équation admet au moins une racine réelle, c'est d'ailleurs le cas de tous les polynômes de degré 3. Pourtant, la formule de Cardan donne :

$$x = \sqrt[3]{52 + \sqrt{-2209}} + \sqrt[3]{52 - \sqrt{-2209}},$$

qui semble être un nombre complexe pas spécialement réel. En fait, $(47\mathrm{i})^2 = -2209$ donc la formule de Cardan devient

$$x = \sqrt[3]{52 + 47\mathrm{i}} + \sqrt[3]{52 - 47\mathrm{i}}.$$

De plus, $(4+\mathrm{i})^3 = 52+47\mathrm{i}$ et $(4-\mathrm{i})^3 = 52-47\mathrm{i}$, donc en reportant cela dans la formule de Cardan, on obtient $x = 8$, qui est effectivement une solution réelle, assez simple de surcroît !

Terminons-en avec les racines de $x^3 - 51x - 104$; maintenant qu'on dispose de la racine $x = 8$, on sait que $x - 8$ est un diviseur donc on va pouvoir calculer le quotient par une division euclidienne puis factoriser le quotient puisqu'il est de degré 2. Dans le détail,

$$x^3 - 51x - 104 = (x - 8)(x^2 + bx + c).$$

Il faut annuler le coefficient en x^2 donc $b = 8$, et le coefficient constant vaut $-104 = -8c$ donc $c = 13$. Pour terminer dans l'esprit des contemporains de Cardan, on complète le carré dans $x^2 + 8x + 13$, donc on utilise la relation $x^2 + 8x + 13 = (x + 4)^2 - 3$ pour obtenir finalement la factorisation

$$x^3 - 51x - 104 = (x - 8)(x + 4 + \sqrt{3})(x + 4 - \sqrt{3}),$$

et les racines $x = 8$, $x = -4 - \sqrt{3}$ et $x = -4 + \sqrt{3}$.

Le schéma général que nous avons utilisé ci-dessus pour trouver une (première) racine de l'équation $x^3 = 51x+104$ a été inventé par une succession de mathématiciens italiens au cours du XVI$^{\mathrm{e}}$ siècle. L'histoire de cette découverte est animée et sordide, pleine de ressentiment, de bruit, de fureur, de mesquineries et de traits de génie. Avant de la raconter, mentionnons que c'est bien à travers l'étude des équations du troisième degré que ces algébristes italiens sont conduits à introduire les nombres complexes. Ils les appelleront au début nombres « impossibles » et les utiliseront comme de simples artifices de calcul, non rigoureux et même un peu mystérieux, mais ayant le bon goût de toujours fournir la solution. Cette résolution des équations cubiques et quartiques peut être considérée comme une des plus grandes contributions à l'algèbre depuis les apports des Babyloniens qui, 4000 ans plus tôt, avaient appris à compléter le carré comme nous l'avons fait pour $x^2 + 8x + 13$ ci-dessus, pour résoudre les équations quadratiques. Rappelons pour finir que seules les équations de degré au plus 4 sont résolubles par

radicaux, c'est-à-dire que seules ces équations peuvent être résolues par des méthodes générales donnant les solutions en fonction des coefficients du polynôme.

L'histoire qui nous intéresse, même si elle comprend de nombreux personnages, est principalement celle de l'affrontement entre Niccolò Fontana, dit Tartaglia, et Girolamo Cardano, que les Français appellent Jérôme Cardan. On peut choisir de la faire commencer un peu plus tôt, à la toute fin du XV^{e} siècle, avec un moine franciscain nommé Luca Paccioli (1445-1517).

En 1494, Paccioli rédige un traité d'algèbre, qu'il intitule la *Summa*. Il y reprend tous les travaux des mathématiciens Arabes connus de lui, notablement ceux du mathématicien, astronome et géographe Al Khwarizmi (780-850), considéré par de nombreux historiens comme l'un des plus grands mathématiciens de tous les temps. On trouve en particulier dans la *Summa* de Paccioli la résolution complète des équations du premier et deuxième degré et l'affirmation (fausse) selon laquelle les équations du troisième degré sont insolubles par des méthodes algébriques.

En 1501 et 1502, Paccioli enseigne les mathématiques à l'université de Bologne. Il y rencontre Scipione del Ferro (1465-1526), lui aussi professeur de mathématiques, et lui fait part de sa conviction sur l'insolubilité des équations du troisième degré. Del Ferro commence à s'intéresser au problème.

En 1515, del Ferro découvre une méthode algébrique de résolution des équations cubiques $x^3 = px + q$ et $x^3 + q = px$ (à l'époque, les deux formes sont vraiment différentes car on ne sait travailler qu'avec des nombres positifs). Plutôt que la publier, il la note sur un carnet et la tient secrète.

En 1526, à la mort de del Ferro, son gendre Hannibal Nave, lui aussi professeur de mathématiques (encore un), hérite du carnet. Toujours sur son lit de mort, del Ferro confie également ses méthodes de résolution à son élève Antonio Maria Fior, peu talentueux semble-t-il. Fior commence à se vanter d'être capable de résoudre toutes les équations du troisième degré et, comme c'est l'usage à l'époque, il lance des défis (en italien, *disfide*) sur ce thème.

Entre alors en scène Niccolò Fontana, dit Tartaglia (1505-1557), un des principaux personnages de notre histoire. Tartaglia est né à Brescia. Son surnom provient de *tartagliare* qui signifie bégayer en italien. Tartaglia avait en effet un défaut de parole, séquelle d'une très grave blessure. Lorsque les Français saccagent la ville de Brescia en 1512, le petit Niccolò et son père se réfugient dans une cathédrale. Les soldats de Louis XII les y découvent, ils tuent le père de Niccolò, fracturent le crâne de celui-ci et lui ouvrent la mâchoire d'un coup de sabre. Toutefois, sa mère réussit à le sauver de la mort.

De famille modeste, Niccolò ne peut aller à l'école mais sa mère (encore elle) économise et elle parvient à lui payer l'école pendant deux semaines. Niccolò profite de ce court laps de temps pour voler des livres et il continue à apprendre en autodidacte. Adulte, il gagnera sa vie en enseignant les mathématiques dans toute l'Italie et en participant, on y revient, à des *disfide* mathématiques.

Tartaglia se consacre donc, lui aussi, à la recherche d'une méthode de résolution des équations cubiques, et il arrive bientôt à résoudre certaines classes. En 1535, il relève le défi de Fior et le duel s'engage entre les deux hommes. Chacun dépose une liste de problèmes chez un notaire ainsi qu'une somme d'argent. Celui qui, sous quarante jours, aura résolu le plus de problèmes proposés par l'autre sera désigné vainqueur et remportera la somme. Juste avant la date limite, Tartaglia découvre une méthode qui lui permet de résoudre tous les problèmes posés par Fior. Fior, lui, ne sait résoudre que $x^3 + px = q$ mais les équations proposées par Tartaglia sont du type $x^3 + px^2 = q$. Fior n'en résoud aucune ou, selon les sources, il n'en résoud qu'une seule, en tous les cas il a perdu la *disfida*.

Tartaglia garde secrète sa méthode de résolution et ne la publie pas. Entre en scène le deuxième protagoniste de notre histoire, Girolamo Cardano (1501-1576), dit aussi Jérôme Cardan, à l'époque conférencier de mathématique à la fondation Piatti de Milan. Cardano connaît le problème des équations cubiques et, avant le défi entre Fior et Tartaglia, il est d'accord avec le verdict de Paccioli selon lequel leur résolution algébrique est impossible. Cette victoire éclatante de Tartaglia intrigue tout de même Cardano, qui tente de découvrir seul une méthode, mais en vain. Cardano contacte alors Tartaglia et lui demande de lui confier sa méthode, en promettant de garder le secret. Tartaglia refuse.

Cardano, qui sait que Tartaglia est pauvre, lui écrit de nouveau pour lui proposer de le présenter au marquis del Vasto, un des plus puissants mécènes du temps — si du moins Tartaglia accepte de lui révéler son secret. Tartaglia réalise qu'un tel appui peut être une aide non négligeable à son ascension sociale. Il propose à Cardano d'organiser une entrevue avec le marquis lors de sa prochaine visite à Milan.

En 1539, Tartaglia quitte donc Venise pour Milan. Mais à son grand désespoir, l'empereur ainsi que le marquis sont absents de Milan. Tartaglia donne alors son accord pour révéler son secret à Cardano à condition que Cardano jure de ne jamais le divulguer. Cardano jure et Tartaglia lui révèle enfin sa méthode, sous la forme d'un poème. En contre-partie et comme promis, Tartaglia obtient de Cardano une lettre de recommandation auprès du marquis. Mais n'osant pas se présenter seul devant le marquis et Cardano refusant de l'accompagner, Tartaglia retourne frustré à Venise sans même avoir vu le fameux marquis et se demandant s'il n'a pas eu tort de dévoiler son secret.

En 1540, Cardano est amené à chercher à résoudre l'équation du quatrième degré $x^4 + 6x^3 + 36 = 60x$. Cardano n'y arrive pas et demande de l'aide à son secrétaire Ludovico Ferrari (1522-1565), auquel on pense devoir en fait un grand nombre des résultats publiés par Cardano. Ferrari parvient à ramener l'équation à une équation du troisième degré que Cardano et lui savent résoudre. Ferrari généralise alors la méthode consistant à ramener une équation du quatrième degré à une équation du troisième degré, procédure qui paraîtra dans un futur livre de Cardano.

En 1543, Cardano et Ferrari se rendent à Bologne et apprennent de Nave que del Ferro avait résolu bien avant Tartaglia certaines équations cubiques. Pour le leur

prouver, Nave leur confie le bloc-notes de feu del Ferro. Cardano décide que, bien qu'il ait juré de ne jamais révéler la méthode de Tartaglia, rien ne l'empêche maintenant de publier celle de del Ferro !

En 1545, Cardano publie enfin son livre *Ars Magna*, instantanément célèbre et bien connu pour contenir la démonstration d'une méthode algébrique permettant de résoudre les équations des troisième et quatrième degrés. Aujourd'hui, on appelle souvent ces formules les formules de Tartaglia-Cardan.

Tartaglia est furieux car il considère que Cardano a transgressé sa promesse. S'ensuivent des échanges de lettres d'insultes entre Tartaglia d'une part et Ferrari agissant pour le compte de Cardano d'autre part, à l'issue desquels Ferrari défie Tartaglia. Tartaglia, dont la vraie cible est Cardano, refuse. En 1546, il publie son propre livre, *Nouveaux problèmes et inventions*, dans lequel il révèle sa version de l'histoire et le parjure de Cardano. Mais grâce à *Ars Magna*, Cardano est devenu intouchable.

En 1548, Tartaglia, toujours pauvre, reçoît une importante proposition d'un poste de conférencier à Brescia, sa ville natale. Mais pour l'obtenir, il doit répondre au défi de Ferrari. Tartaglia se résoud donc enfin au face-à-face avec Ferrari, son concurrent et la créature de Cardano. Le 10 août, le défi a lieu à Milan dans l'église des frères Zoccolanti sous les yeux de toutes les célébrités milanaises de l'époque, dont Don Ferrante di Gonzaga, gouverneur de la ville et arbitre du duel. Ferrari fait une meilleure prestation que Tartaglia, qui va jusqu'à déclarer forfait à l'issue du premier jour, laissant Ferrari vainqueur. Tartaglia, déconsidéré, perdra même son poste à Venise un an plus tard.

Le dernier personnage de notre histoire est Rafaele Bombelli (1526-1573) et avec lui les choses s'apaisent. En 1572, il couronne l'œuvre des savants italiens en réalisant dans son traité *Algebra* la première étude véritable des nombres imaginaires. Dans *Ars Magna*, Cardano manipulait les deux nombres $5+\sqrt{-15}$ et $5-\sqrt{-15}$ et constatait que leur produit et leur somme sont tous deux des nombres positifs ordinaires : 40 et 10. Mais Cardano qualifiait lui-même ces considérations de « subtiles et inutiles ».

En 1560, donc du vivant de Cardano, et en s'inspirant parfois lourdement d'un manuscrit de Diophante tout juste retrouvé, l'*Arithmetica*, Bombelli reprend l'étude du problème. Il remarque que lorsque la formule de Cardan aboutit à un discriminant négatif, la méthode géométrique donne une solution réelle positive. Il retrouve ainsi la racine réelle (connue avant lui) $x=4$ de l'équation $x^3=15x+4$. Bombelli arrive à la conclusion que toute équation du troisième degré posséde au moins une solution réelle. Mais surtout, il est le premier à utiliser dans ses calculs des racines carrées imaginaires de nombres négatifs pour obtenir finalement la solution réelle tant recherchée, et à poser de manière systématique des règles de calcul pour ces nombres.

Voici, pour terminer cette très libre évocation historique, le texte du poème de Tartaglia qui décrit sa méthode de résolution.

> Quando chel cubo con le cose appresso
> Se agguaglia à qualche numero discreto
> Trouan dui altri differenti in esso.

Dapoi terrai questo per consueto
Che'llor produtto sempre sia eguale
Alterzo cubo delle cose neto,
El residuo poi suo generale
Delli lor lati cubi ben sottratti
Varra la tua cosa principale.
In el secondo de cotestiatti
Quando che'l cubo restasse lui solo
Tu osseruarai quest'altri contratti,
Del numer farai due tal part'à uolo
Che l'una in l'altra si produca schietto
El terzo cubo delle cose in stolo
Delle qual poi, per communprecetto
Torrai li lati cubi insieme gionti
Et cotal somma sara il tuo concetto.
El terzo poi de questi nostri conti
Se solue col secondo se ben guardi
Che per natura son quasi congionti.
Questi trouai, e non con passi tardi
Nel mille cinquecentè, quatro e trenta
Con fondamenti ben sald'è gagliardi
Nella Citta dal mar'intorno centa.

Et pour ceux qui ne lisent pas l'italien, voici une traduction de la première partie avec, entre crochets, les étapes de la méthode de résolution décrite par le texte.

Quand le cube avec les choses
Est égalé à un certain nombre [Cas $x^3 + px = q$]
Trouves-en deux autres qui diffèrent de ce dernier [Trouver u et v]
Ensuite tu tiendras ceci pour habituel [tels que $u - v = q$]
Que leur produit soit égal
Au tiers du cube, des choses exactement [et tels que $uv = (p/3)^3$]
Ensuite son reste général,
De leurs racines cubiques bien soustraites,
Vaudra ta chose principale. [Alors $x = \sqrt[3]{u} - \sqrt[3]{v}$.]