COURS SUR LES POLYNÔMES À UNE VARIABLE

- Opérations sur les polynômes -

On commence par définir la notion de polynôme et voir quelques propriétés.

Définition 1. Une fonction P de $\mathbb{R}$ dans $\mathbb{R}$ est appelée polynôme à coefficient réels (abrégé en polynôme dans ce qui suit) s'il existe un entier $n \geqslant 0$ et des nombres réels $a_0, \dots, a_n$ tels que pour tout $x \in \mathbb{R}$:

$$P(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

On verra plus tard (Corollaire 9) qu'un polynôme à coefficients réels s'écrit de manière unique sous cette forme. Si $a_n \neq 0$, on dit que le degré de P, noté $\deg P$, vaut n. Dans ce cas, a_n est appelé le coefficient dominant de P. On décrète que le degré du polynôme nul est $-\infty$. Si le coefficient dominant de P vaut 1, on dit que ce polynôme est unitaire. On note $\mathbb{R}[X]$ l'ensemble des polynômes à coefficients réels. De même, on note $\mathbb{Q}[X]$ l'ensemble des polynômes à coefficients rationnels et $\mathbb{Z}[X]$ l'ensemble des polynômes à coefficients entiers.

Dans ce qui suit, nous ne ferons pas de distinction entre polynôme et fonction polynomiale associée. Il faudrait la faire en toute rigueur, mais plutôt que de rendre l'exposition abstraite, nous préférons insister sur les idées sous-jacentes. Voir l'appendice situé à la fin du cours pour plus de détails.

On notera indifféremment $P(x)$ ou $P(X)$ ou encore P.

Exemple 2. La fonction $P(x) = \sqrt{2} - 2x + \pi x^2$ est un polynôme de degré 2 de coefficient dominant π. La fonction $Q(x) = |x|$ n'est pas un polynôme (pourquoi ?).

Remarque 3. Par convention, le degré du polynôme nul est $-\infty$. Ainsi, les polynômes de degré zéro sont exactement les fonctions constantes non nulles.

Proposition 4. Soient P, Q deux polynômes. Alors $P + Q$ et $P \times Q$ sont également deux polynômes.

Démonstration. Pour $P + Q$ il suffit d'utiliser le fait que $\alpha x^i + \beta x^i = (\alpha + \beta) x^i$ pour un nombre réel x, et pour $P(x) \times Q(x)$, il suffit de développer le produit. $\square$

Exemple 5. Pour tout réel a et tout entier positif n, $P(x) = (x - a)^n$ est un polynôme de degré n.

Proposition 6. Soient P, Q deux polynômes. Alors $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$ et $\deg(P \times Q) = \deg P + \deg Q$ (avec la convention $-\infty + \alpha = -\infty$ pour que cet énoncé soit valable si l'un des deux polynômes est nul).

Démonstration. On vérifie aisément que $\deg(P + Q) = \deg P$ si $\deg P > \deg Q$, que $\deg(P + Q) = \deg Q$ si $\deg Q > \deg P$ et que si $\deg P = \deg Q$, alors $\deg(P + Q) \leqslant \deg P$. Il peut cependant ne pas y avoir égalité (prendre par exemple $P(x) = x^2$ et $Q(x) = -x^2$).

La deuxième partie de la proposition découle du fait que si a_n est le coefficient dominant de P et b_m est le coefficient dominant de Q, alors $a_n b_m$ est le coefficient dominant de PQ. $\square$

Exemple 7. Soit E un ensemble fini et $f : E \to \mathbb{N}$ une application. Alors

$$P(x) = \sum_{\alpha \in E} x^{f(\alpha)}$$

est un polynôme à coefficients entiers. Si k_n désigne le nombre nombre d'éléments $\alpha \in E$ tels que $f(\alpha) = n$, alors le coefficient devant x^n est égal à k_n. Le polynôme P est appelé fonction génératrice associée à f. Ce genre de polynômes apparaissent fréquemment en combinatoire, ou il arrive qu'on ne connaisse pas de formule explicite pour k_n, bien que le polynôme P se calcule aisément (voir exercice 42). L'intérêt d'introduire cette fonction génératrice est que la connaissance du polynôme P nous permet alors d'accéder à certaines informations (par exemple des formules de récurrence ou un comportement asymptotique).

Le résultat crucial suivant permet de montrer l'unicité de l'écriture d'un polynôme :

Théorème 8. Soit $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ un polynôme à coefficients réels tel que $P(x) = 0$ pour tout $x \in \mathbb{R}$. Alors $a_0 = a_1 = \cdots = a_n = 0$.

Démonstration. Raisonnons par l'absurde, est supposons que $P(x) = a_k x^k + a_{k+1} x^{k+1} + \cdots + a_n x^n$ avec $k \geqslant 0$ et $a_k \neq 0$. Comme pour tout $x \in \mathbb{R}^*$ on a $P(x) = 0$, en divisant par x^k on en déduit que $a_k + x a_{k+1} + \cdots + a_n x^{n-k} = 0$ pour tout $x \in \mathbb{R}^*$. En faisant tendre x vers 0, on en déduit que $a_k = 0$, ce qui est absurde. □

Corollaire 9. Soient $a_0, a_1, \ldots, a_n$ et $b_0, b_1, \ldots, b_m$ des nombres réels tels que $a_n \neq 0$ et $b_m \neq 0$. On suppose que pour tout nombre réel x :

$$a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n = b_0 + b_1 x + \cdots + b_m x^m.$$

Alors $m = n$ et $a_i = b_i$ pour tout $0 \leqslant i \leqslant m$.

Démonstration. Soit $P(x) = a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n - (b_0 + b_1 x + \cdots + b_m x^m)$, qui est un polynôme à coefficients réels tel que $P(x) = 0$ pour tout $x \in \mathbb{R}$. Le résultat découle alors du théorème précédent. □

- Division euclidienne et racines -

Dans cette partie, notre but est d'expliquer en quoi la connaissance des racines d'un polynôme P, c'est-à-dire des éléments x tels que $P(x) = 0$, donne des informations sur P. On commence par montrer qu'il existe une notion de division euclidienne de polynômes très similaire à celle des entiers.

Division euclidienne de polynômes

Ici, et dans tout ce qui suit, $\mathbb{K}$ désigne $\mathbb{Q}$ ou $\mathbb{R}$.

Théorème 10. Soient $P, U \in \mathbb{K}[X]$ avec $\deg U \geqslant 1$. Alors il existe un unique couple de polynômes $Q, R \in \mathbb{K}[X]$ tels que :

$$P = QU + R \qquad \text{et} \qquad \deg(R) \leqslant \deg(U) - 1.$$

Démonstration. Pour l'existence, on adapte en quelque sorte l'algorithme de division euclidienne pour les nombres entiers aux polynômes. Plus précisément, on pose $P_0 = P$ et $Q_0 = 0$. On commence à l'étape 0 et voici ce qu'on fait à l'étape k : notons d_k le degré de P_k et c_k son coefficient dominant. Notons également n le degré de U et u_n son coefficient dominant. Si $\deg(P_k) \leqslant \deg(U) - 1$, on arrête l'algorithme en prenant $Q = Q_k$ et $R = P_k$. Sinon, on pose :

$$P_{k+1} = P_k - \frac{c_k}{u_n} X^{d_k - n} U \qquad \text{et} \qquad Q_{k+1} = Q_k + \frac{c_k}{u_n} X^{d_k - n}.$$

On passe ensuite à l'étape $k+1$. L'algorithme se termine bien car le degré de P_k est au plus $\deg P - k$, et les polynômes Q et R donnés par l'algorithme vérifient les conditions requises.

Pour l'unicité, supposons par l'absurde qu'il existe deux tels couples Q, R et Q', R'. Alors $QU + R = Q'U + R'$. En particulier, $Q \neq Q'$, car sinon on a aussi $R = R'$. Cela implique également :

$$U(Q - Q') = R' - R.$$

Or, d'après la proposition 6, le degré du terme de gauche et supérieur ou égal à celui de U et celui de droite est inférieur ou égal à $\deg(U) - 1$, ce qui est contradictoire et conclut la démonstration. □

Exemple 11. La division euclidienne de $X^5 - 3X^3 + 2X + 1$ par $X^3 + 3X^2 - 2X - 1$ est :

$$X^5 - 3X^3 + 2X + 1 = (X^2 - 3X + 8)(X^3 + 3X^2 - 2X - 1) + \left(-29X^2 + 15X + 9\right).$$

Remarque 12. La division euclidienne telle quelle est fausse pour des polynômes à coefficients entiers. Par exemple, il n'existe pas de $Q \in \mathbb{Z}[X]$ tel que $3x^2 + 1 = Q(x)(2x+1)$ (comparer les coefficients dominants). En revanche, en reproduisant la démonstration précédente, si $P, U \in \mathbb{Z}[X]$ **et que le coefficient dominant de** U **est** 1, alors si $\deg U \geqslant 1$, il existe il existe un unique couple de polynômes $Q, R \in \mathbb{K}[X]$ tels que :

$$P = QU + R \qquad \text{et} \qquad \deg(R) \leqslant \deg(U) - 1.$$

En effet, dans la preuve précédente, il a fallu diviser par « u_n ». Or, lorsqu'on divise par des éléments de $\mathbb{Z}$, on ne reste pas dans $\mathbb{Z}$. Ceci explique un peu d'ailleurs pourquoi la théorie des polynômes à plusieurs variables est plus compliquée que celle des polynômes à une variable. En effet, on peut par exemple voir les polynômes réels à deux variables comme les polynômes en y à coefficients dans $\mathbb{R}[X]$. Mais, de même que dans $\mathbb{Z}$, tous les éléments de $\mathbb{R}[X]$ ne sont pas inversibles.

Définition 13. Soient $P, Q \in \mathbb{K}[X]$ avec P non nul. On dit que P divise Q s'il existe $R \in \mathbb{K}[X]$ tel que $Q = PR$.

Ainsi, P divise Q si le reste de la division euclidienne de Q par P vaut 0.

Exemple 14. Trouvons le reste de la division euclidienne de $A(x) = x^{2013} + 2013$ par $B(x) = x - 1$. Par division euclidienne, on écrit $A(x) = Q(x)B(x) + R(x)$ avec $R(x)$ un polynôme de degré au plus 0. Ainsi R est un polynôme constant qu'on notera c. Autrement dit, $A(x) = Q(x)B(x) + c$ et il nous reste à trouver la valeur de c. Prenons $x = 1$: $A(1) = Q(1)B(1) + c$. Or $B(1) = 1$. On en déduit que $c = A(1) = 2014$.

Exercice 1 Trouver le reste de la division euclidienne de $x^{100} - 2x^{51} + 1$ par $x^2 - 1$.

Racines et factorisation de polynômes

Nous voyons ici que la connaissance des racines d'un polynôme permet de le factoriser. Rappelons que $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{Q}$.

Définition 15. Un élément $x \in \mathbb{K}$ est appelé *racine* d'un polynôme $P \in \mathbb{K}[X]$ si $P(x) = 0$.

Exemple 16. Le polynôme réel $X^2 - 1$ a deux racines réelles, qui sont 1 et -1. Le polynôme X^2+1 n'a pas de racine réelle. Le polynôme réel X^2-2 a deux racines réelles, mais le polynôme à coefficients rationnels $X^2 - 2$ n'a pas de racines rationnelles car $\sqrt{2}$ est irrationnel. Si $a \in \mathbb{K}$, le polynôme $(X-1)^{2012}$ est de degré 2012 mais n'a qu'une seule racine qui est 1.

Le théorème suivant est très important et doit être connu.

Théorème 17. Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Les deux propositions suivantes sont équivalentes :

1. a est racine de P, autrement dit $P(a) = 0$.
2. Il existe un polynôme $Q \in \mathbb{K}[X]$ tel que :

$$P(x) = Q(x)(x-a).$$

Démonstration. Il est clair que le deuxième point implique le premier. Quant à la réciproque, le point clé est d'utiliser la division euclidienne. En effet, supposons que $P(a) = 0$. Écrivons alors la division euclidienne de P par $X - a$ sous la forme $P(x) = Q(x)(x-a) + R(x)$ avec R un polynôme de degré au plus $1 - 1 = 0$. Ainsi, R est un nombre réel, noté c. Bref, $P(x) = Q(x)(x-a) + c$. Évaluons cette quantité en $x = a$: $0 = P(a) = Q(a)(a-a) + c$. Donc $c = 0$, ce qu'on voulait démontrer. $\square$

Théorème 18. Soit $n \geqslant 0$ un entier. Un polynôme de $\mathbb{K}[X]$ de degré n a au plus n racines différentes dans $\mathbb{K}$.

Démonstration. On raisonne par récurrence sur n. Pour $n = 0$, c'est vrai car par définition un polynôme de degré 0 est une constante non nulle. Soit $n \geqslant 1$ et supposons le résultat acquis pour tous les polynômes de $\mathbb{K}[X]$ degré $n-1$. Soit alors $P \in \mathbb{K}[X]$ de degré n. Si P n'a pas de racines dans $\mathbb{K}$, il n'y a rien à faire. Sinon, soit $a \in K$ une racine de P. D'après le théorème précédent, on peut écrire $P(X) = (X-a)R(X)$ avec $R \in \mathbb{K}[X]$ un polynôme de degré $n-1$, qui par hypothèse de récurrence a au plus $n-1$ racines différentes. On en déduit que P a au plus n racines différentes. $\square$

Remarque 19. Il existe des polynômes qui n'ont pas de racines réelles, par exemple $P(x) = x^4 + 1$. En revanche, un polynôme P à coefficients réels et de degré impair a au moins une racine réelle. En effet, soit c son coeffictient dominant. Alors $P(x) \to +\infty$ quand $x \to \infty$ et $P(x) \to -\infty$ quand $x \to -\infty$ lorsque $c > 0$ et $P(x) \to -\infty$ quand $x \to \infty$ et $P(x) \to +\infty$ quand $x \to -\infty$ lorsque $c < 0$. Le polynôme P doit donc forcément couper quelque part l'axe des abcsisses (en termes rigoureux, c'est une conséquence du théorème des valeurs intermédiaires appliqué à la fonction continue P).

Ce théorème important implique quelques corollaires donnant une information concernant le polynôme sachant quelque chose sur ses racines.

Corollaire 20. Soit $n \geqslant 0$ un entier. Soit $P \in \mathbb{K}[X]$ un polynôme de degré au plus n ayant au moins $n+1$ racines. Alors P est le polynôme nul. En particulier, un polynôme ayant une infinité de racines est forcément le polynôme nul.

Démonstration. Il suffit de dire que si P n'est pas le polynôme nul, alors d'après le théorème précédent il a au plus $\deg(P) \leqslant n$ racines. □

Corollaire 21. Soit $P(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{K}[X]$ un polynôme de degré n. On suppose qu'il a n racines différentes $r_1, \ldots, r_n \in \mathbb{K}$. Alors :

$$P(x) = a_n(x - r_1)\cdots(x - r_n).$$

Démonstration. Soit $Q(X) = P(x) - a_n(x - r_1)\cdots(x - r_n) \in \mathbb{K}[X]$. Ce polynôme admet au moins n racines différentes $(r_1, \ldots, r_n)$, et on voit qu'il est de degré au plus $n-1$ (le terme $a_n x^n$ se simplifie dans la soustraction). D'après le corollaire précédent, Q est le polynôme nul. □

Corollaire 22. Un polynôme de degré n ayant $n+1$ racines est nul. Ainsi, un polynôme ayant une infinité de racines est forcément le polynôme nul.

Exercice 2 En utilisant le corollaire précédent, retrouver le fait que $Q(x) = |x|$ n'est pas un polynôme.

Exemple 23. Soit P un polynôme de degré 2013 vérifiant $P(k) = k$ pour $k = 1, 2, \ldots, 2013$ et $P(0) = 1$. Trouvons $P(-1)$.

Le polynôme $P(x) - x$ est de degré 2013 et admet 2013 racines qui sont $k = 1, 2, \ldots, 2013$. On a donc forcément

$$P(x) - x = c \cdot (x-1)(x-2)\cdots(x-2013)$$

avec c un nombre réel. En évaluant en $x = 0$, il vient $1 = P(0) = -c \cdot 2013!$, de sorte que $c = -1/2013!$. D'où

$$P(-1) = -1 + \frac{2014!}{2013!} = 2013.$$

Pour conclure cette partie, prouvons la propriété utile suivante en identifiant les coefficients.

Proposition 24. Soit P un polynôme tel que $P(x)^2$ soit un polynôme en x^2 (c'est-à-dire qu'il existe un polynôme R tel que $P(x)^2 = R(x^2)$). Alors il en est de même de $P(x)$ ou de $P(x)/x$ (c'est-à-dire qu'il existe un polynôme Q tel que soit $P(x) = Q(x^2)$, soit $P(x) = xQ(x^2)$).

Démonstration. Écrivons $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ avec $a_n \neq 0$. Comme $P(x)^2 = R(x^2)$, le coefficient devant x^{2n-1} dans $P(x)^2$, à savoir $2a_n a_{n-1}$, est nul. On en déduit que $a_{n-1} = 0$. De même, le coefficient devant x^{2n-3} dans $P(x)^2$, à savoir $2a_n a_{n-3}$, est nul. On en déduit que $a_{n-3} = 0$. De même, on obtient que $a_{n-2k-1} = 0$ pour $n - 2k - 1 \geqslant 0$. Le résultat en découle. □

Pour illustrer cette propriété, on pourra chercher l'exercice suivant.

Exercice 3 Trouver tous les polynômes $P \in \mathbb{R}[X]$ tels que $16P(x^2) = P(2x)^2$.

Racines multiples et polynôme dérivé

Doit-on dire que le polynôme $P(x) = (x-1)^n$ a une seule racine, ou bien n racines qui sont les mêmes ? Pour ne pas faire de confusion, nous traitons le cas des racines multiples.

Définition 25. Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et un entier $m \in \mathbb{N}^*$. On dit que α est racine de multiplicité m de P s'il existe $Q \in \mathbb{K}[X]$ tel que $P(x) = (x-\alpha)^m Q(x)$ et $Q(\alpha) \neq 0$.

Il se trouve qu'on dispose d'un critère assez pratique permettant de reconnaître une racine multiple.

Définition 26. Soit $P = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{K}[X]$. On définit le polynôme dérivé P' par $P'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$.

La proposition suivante, réminiscente des propriétés de l'opérateur de dérivation sur les fonctions réelles dérivables, est fondamentale. On laisse sa démonstration au lecteur.

Proposition 27. Pour $P, Q \in \mathbb{K}[X]$, on a :

$$(PQ)' = PQ' + P'Q.$$

Proposition 28. Soient $a \in \mathbb{K}$ et $n \geqslant 1$ un entier. Soit $P(x) = (x-a)^n$. La dérivée de P est $P'(x) = n(x-a)^{n-1}$.

Démonstration. Prouvons cela par récurrence sur n. Pour $n = 1$, le polynôme dérivé de $x - a$ est bien 1. Supposons le résultat acquis au rang n, montrons-le au rang $n+1$. Soit $Q(x) = (x-a)^{n+1}$. En écrivant $(x-a)^{n+1} = (x-a)(x-a)^n$, on obtient

$$Q'(x) = (x-a)^n + (x-a)\left((x-a)^n\right)'.$$

Donc par hypothèse de récurrence, $Q'(x) = (x-a)^n + (x-a) \cdot (n-1)(x-a)^n = n(x-a)^n$. Ceci conclut la récurrence et la preuve de la proposition. □

Théorème 29. Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$. Alors α est une racine multiple de P si, et seulement si, $P'(\alpha) = 0$.

Démonstration. Dans le sens direct, écrivons $P(x) = (x-\alpha)^m Q(x)$ avec $m \geqslant 2$ et $Q \in \mathbb{K}[X]$. En dérivant cette expression, il vient $P'(x) = m(x-\alpha)^{m-1}Q(x) + (x-\alpha)^m Q'(x)$. En prenant $x = \alpha$, on conclut que $P'(\alpha) = 0$.

Pour la réciproque, supposons que $P'(\alpha) = 0$ et raisonnons par l'absurde en supposant que α soit une racine non multiple de P. Alors P s'écrit $P(x) = (x-\alpha)Q(x)$ avec $Q(\alpha) \neq 0$ (si $Q(\alpha) = 0$, d'après le théorème 17, on pourrait écrire $P(x) = (x-\alpha)^2 R(X)$). En dérivant cette expression, il vient $P'(x) = Q(x) + (x-\alpha)Q'(x)$. En prenant $x = \alpha$, il vient $P'(\alpha) = Q(\alpha) \neq 0$, ce qui est absurde. □

Exemple 30. Soit $n \geqslant 1$ un entier et montrons que $(X+1)^2$ divise $P(X) = X^{4n+2} + 2X^{2n+1} + 1$. D'après le théorème 17, il suffit que -1 est racine double de P. Ceci découle aisément du fait que $P(-1) = 0$ et $P'(-1) = 0$.

Remarque 31. Si $P'(\alpha) = 0$, cela n'implique pas que α soit racine multiple (ou racine tout court !) de P. Il faut en effet s'assurer que $P(\alpha) = 0$ pour utiliser le corollaire précédent. Par exemple, si $P(x) = x^2 - 2$, on a $P'(x) = 2x$, mais 0, bien que racine de P', n'est pas racine de P.

Remarque 32. Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Pour un entier $k \geqslant 1$, notons $P^{(k)}$ le polynôme P dérivé k fois. Soit $n \geqslant 1$ un entier. Plus généralement, on peut démontrer par récurrence sur n l'équivalence

$$P(a) = 0, P'(a) = 0, \dots, P^{(n)}(a) = 0 \iff (x-a)^n \text{ divise } P.$$

Exercices d'application

Exercice 4 Trouver les réels a, b tels que $(x-1)^2$ divise $ax^4 + bx^3 + 1$.

Exercice 5 Trouver tous les polynômes $P \in \mathbb{R}[X]$ tels que pour tous réels x, $P(2x) = P'(x)P''(x)$.

Exercice 6 Soit $P(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{R}[X]$ qui possède n racines réelles différentes. Montrer que pour tout x réel, $P(x)P''(x) \leqslant P'(x)^2$. En déduire que pour $1 \leqslant k \leqslant n-1$, $a_{k-1}a_{k+1} \leqslant a_k^2$.

Exercice 7 (Oral ENS 2009) Soit $P \in \mathbb{R}[X]$ de degré $n \geqslant 1$. On suppose que toutes les racines de P sont réelles. Montrer que $(n-1)\left(P'(x)\right)^2 \geqslant nP(x)P''(x)$ et déterminer les cas d'égalité.

Interpolation

Étant donnés un nombre fini de points du plan, existe-t-il un polynôme tel que que sa courbe représentative passe par ces points ? Trouver un tel polynôme, c'est résoudre un problème d'interpolation.

Théorème 33. Soient $a_1, \dots a_n$ et $b_1, \dots, b_n$ des nombres réels (avec les a_i deux à deux distincts). Alors il existe un unique polynôme P de degré $n-1$ tel que pour tout i, $P(a_i) = b_i$.

Démonstration. Montrons d'abord l'unicité en considérant P, Q deux polynômes vérifiant les conditions de l'énoncé du théorème. Alors le polynôme $P - Q$ est de degré au plus $n-1$, qui admet au moins n racines différentes, à savoir $a_1, \dots, a_n$. Il est donc nécessairement nul.

Quant à l'existence, pour $1 \leqslant i \leqslant n$, introduisons les polynômes suivants, appelés polynômes d'interpolation de Lagrange :

$$L_i(x) = \prod_{j=1, j \neq i}^{n} \frac{x - a_j}{a_i - a_j}.$$

L'intérêt est que pour tout j différent de i, $L_i(a_j) = 0$, alors que $L_i(a_i) = 1$. On en déduit aisément que le polynôme :

$$P(x) = \sum_{i=1}^{n} b_i L_i(x)$$

convient. $\square$

Ainsi, un polynôme de degré n est complètement déterminé par les images de $n+1$ points distincts.

Exercice 8 Soient $a_1, \dots a_n$ et $b_1, \dots, b_n$ des éléments de $\mathbb{K}$ (avec les a_i deux à deux distincts). Trouver tous les polynômes $P \in \mathbb{K}[X]$ tels que $P(a_i) = b_i$.

Exercice 9 Trouver tous les polynômes à coefficients complexes P tels que pour tout rationnel q, $P(q)$ est rationnel.

Exercice 10 On définit les polynômes de Hermite comme suit : $H_0 = 1$ et pour $n \geqslant 1$, $H_n(x) = \frac{1}{n!}\prod_{k=0}^{n-1}(X-k)$.

1. Vérifier que pour tout $k \in \mathbb{Z}$, $H_n(k) \in \mathbb{Z}$.
2. Trouver tous les polynômes $P \in \mathbb{C}[X]$ tels que pour tout $k \in \mathbb{N}$, on a $P(k) \in \mathbb{Z}$.
3. (i) Calculer, pour des entiers $j \leqslant k$ la somme :
$$\sum_{i=j}^{k}(-1)^{k-i}\binom{k}{i}\binom{i}{j}.$$
Indication. On pourra écrire $X^k = (X+1-1)^k$.
   (ii) Soit (u_j) une suite de nombres réels. Montrer que les deux conditions suivantes sont équivalentes :
   1. Il existe $P \in \mathbb{R}[X]$ tel que, pour tout $j \in \mathbb{N}$, on a $u_j = P(j)$.
   2. Il existe un entier positif n tel que pour tout entier $i \geqslant n+1$, on a $\sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}u_j = 0$.

Cas des polynômes à petit degré

Nous maintenant quelques applications des résultats précédents, parfois sous la forme d'exercice corrigé.

Proposition 34. Soient b, c deux nombres réels. On souhaite connaître le nombre de réels x tels que $x^2 + bc + c = 0$. Soit $\Delta = b^2 - 4c$, appelé le discriminant. Alors :

1. Si $\Delta < 0$, il n'y a pas de solution.
2. Si $\Delta = 0$, il y a une seule solution qui est $-\frac{b}{2}$.
3. Si $\Delta > 0$, il y a exactement deux solutions, qui sont :
$$\frac{-b+\sqrt{b^2-4c}}{2} \quad \text{et} \quad \frac{-b-\sqrt{b^2-4c}}{2}.$$

Démonstration. L'idée est de se ramener au cas $b = 0$ en écrivant $x^2 + bx + c$ sous la forme suivante, dite forme canonique :
$$x^2 + bx + c = (x + \frac{b}{2})^2 + c - \frac{b^2}{4}.$$
L'intérêt réside dans le fait que x n'intervient qu'une fois dans la nouvelle expression. Cette forme rend très souvent de précieux services et est à retenir. Ainsi, $x^2 + bx + c = 0$ si, et seulement si, $(x + \frac{b}{2})^2 = \frac{b^2}{4} - c$. Ainsi, un carré étant positif, si $\frac{b^2}{4} - c = \Delta/4 < 0$, il n'y a pas de solution, d'ou̧ le premier point. D'un autre côté, si $\Delta \geqslant 0$, alors $(x + \frac{b}{2})^2 = \frac{b^2}{4} - c$ si, et seulement si :
$$x + \frac{b}{2} = \sqrt{\frac{b^2}{4} - c} \quad \text{ou} \quad x + \frac{b}{2} = -\sqrt{\frac{b^2}{4} - c}.$$
On en déduit les points 2. et 3. $\square$

Exemple 35. Le polynôme $P(x) = x^2 + x + 1$ a un discriminant égal à -3, et n'a donc pas de racine réelle.

Exercice 11 Soient $a, b, c \in \mathbb{R}$, avec $a \neq 0$, et considérons le graphe de la fonction $P(x) = ax^2 + bx + c$. Montrer qu'en faisant une homothétie et une translation, on peut obtenir le graphe de la fonction $Q(x) = x^2$.

Remarque 36. Il s'ensuit qu'étant donné un polynôme de degré 2, on peut aisément dire s'il a des racines réelles, et le cas échéant donner leur expression. Ceci est tout à fait remarquable : on peut montrer qu'il existe des polynômes de degré 5 dont les racines réelles ne s'expriment pas en utilisant des racines carrées, cubiques, etc. Cependant, si $P(x)$ est un polynôme de degré 3 et si on trouve une racine évidente a (par exemple $a = 1, 2, -1, -2, ...$), alors on peut effectuer la division euclidienne de P par $x - a$. On en déduit qu'il existe Q, un polynôme de degré 2, tel que $P(x) = Q(x)(x - a)$. Mais Q est de degré 2, et ce qui précède s'applique. La moralité de ceci est que si on trouve une racine évidente d'un polynôme de degré 3, alors on arrivera à connaître toutes ses racines. À titre d'illustration, on pourra chercher l'exercice suivant.

Exercice 12 Trouver tous les nombres réels x, y, z vérifiant :

$$\begin{cases} (x+1)yz = 12 \\ (y+1)zx = 4 \\ (z+1)xy = 4. \end{cases}$$

- Polynômes symétriques élémentaires -

Dans cette partie, nous nous intéressons aux liens unissant les coefficients d'un polynôme à ses racines.

Relations de Viète

Proposition 37 (Relations de Viète)**.** Soit $P(x) = ax^2 + bx + c$ un polynôme réel de degré 2 (avec $a \neq 0$) ayant z_1 et z_2 comme racines réelles. Alors $z_1 z_2 = \frac{c}{a}$ et $z_1 + z_2 = -\frac{b}{a}$.

Démonstration. D'après le corollaire 21, on a $P(x) = a(x - z_1)(x - z_2)$. En développant le terme de droite et en identifiant les coefficients, on trouve les égalités annoncées. □

Ces relations sont utiles car elles expriment les coefficients du polynôme en fonction des racines. À ce titre, on cherchera l'exercice suivant.

Exercice 13 Trouvez toutes les valeurs du paramètre a pour que l'équation

$$ax^2 - (a+3)x + 2 = 0$$

admette deux racines réelles de signes opposés.

Définition 38. Soit $n \geqslant 1$ un entier. Soient $z_1, \dots, z_n \in \mathbb{K}$. Pour $1 \leqslant k \leqslant n$, la k-ième fonction symétrique élémentaire est par définition

$$\sigma_k(z_1, \dots, z_n) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} z_{i_1} \cdots z_{i_k},$$

Lorsque les éléments $z_1, \dots, z_n$ sont sous-entendus, pour simplifier on notera parfois σ_k au lieu de $\sigma_k(z_1, \dots, z_n)$.

Ainsi, par exemple, pour $n = 3$, on a $\sigma_1 = z_1 + z_2 + z_3$, $\sigma_2 = z_1 z_2 + z_1 z_3 + z_2 z_3$ et $\sigma_3 = z_1 z_2 z_3$.

Proposition 39 (Relations de Viète dans le cas général)**.** Soit $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{K}[X]$ avec $a_n \neq 0$. On suppose que P admet n racines $z_1, \dots, z_n \in \mathbb{K}$ comptées avec multiplicité (c'est-à-dire que si z est racine d'ordre k, z apparaît k fois dans la liste $z_1, \dots, z_n$). Alors, pour tout entier $1 \leqslant k \leqslant n$,

$$\sigma_k(z_1, \dots, z_k) = (-1)^k \frac{a_{n-k}}{a_n}.$$

Autrement dit,

$$\sum_{i=1}^{n} z_i = -\frac{a_{n-1}}{a_n}, \sum_{1 \leqslant i < j \leqslant n} z_i z_j = -\frac{a_{n-2}}{a_n}, \dots, \prod_{i=1}^{n} z_i = (-1)^n \frac{a_0}{a_n}.$$

Démonstration. D'après le Corollaire 21, on a $P(x) = a_n(x - z_1) \cdots (x - z_n)$. Or, dans le développement de $a_n(x - z_1) \cdots (x - z_n)$, on voit aisément que le coefficient devant x^{n-k} vaut $(-1)^k a_n \sigma_k(z_1, \dots, z_k)$. Or ce coefficient vaut aussi a_{n-k}. Le résultat en découle. $\square$

Exemple 40. Cherchons tous les nombres réels x, y, z tels que

$$x + y + z = 17, \qquad xy + yz + xz = 94, \qquad xyz = 168.$$

D'après les relations de Viète, x, y, z sont racines de $P(x) = x^3 - 17x^2 + 94x - 168 = 0$. Cherchons des racines "évidentes" de P. Il est naturel de d'abord chercher des racines entières, qui sont forcément des diviseurs de 168 (pour tester si par exemple 2 est racine, on effectue la division euclidienne de P pa $x - 2$ et on regarde si le reste est nul). On remarque que $x = 4$ est racine, et sans difficulté on trouve que $x = 6$ et $x = 7$ sont racines du polynôme $P(x)/(x - 4)$. Ainsi, les solutions (x, y, z) sont les six permutations possibles de $(4, 6, 7)$.

Remarque 41. Les fonctions $\sigma_1(z_1, \dots, z_n), \dots, \sigma_n(z_1, \dots, z_n)$ sont appelés *fonctions symétriques élémentaires des z_i*. *Symétriques*, parce qu'une permutation des z_i laisse les σ_k invariants. *Élémentaires*, parce qu'on peut montrer que toute expression symétrique en n variables peut s'exprimer polynomialement à l'aide de ces fonctions symétriques élémentaires. Plus précisément, si $P(z_1, \dots, z_n)$ est un polynôme à n variables (on laisse le lecteur imaginer ce que c'est) tel que pour toute permutation σ de $\{1, \dots, n\}$ on ait $P(z_1, \dots, z_n) = P(z_{\sigma(1)}, \dots, z_{\sigma(n)})$, alors il existe un polynôme à n variables R tel que $P(z_1, \dots, z_n) = R(\sigma_1(z_1, \dots, z_n), \dots, \sigma_n(z_1, \dots, z_n))$.

Exemple 42. En notant $\sigma_1 = x_1 + x_2 + x_3$, $\sigma_2 = x_1 x_2 + x_1 x_3 + x_2 x_3$ et $\sigma_3 = x_1 x_2 x_3$, on a :

$$x_1^3 + x_2^3 + x_3^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3.$$

Bref, lorsqu'on a affaire à des quantités symétriques, il peut être parfois judicieux de faire intervenir les fonctions symétriques élémentaires associées.

Exercice 14 Soit $P \in \mathbb{R}[X]$ non nul. Montrer que les sommes des racines complexes de $P, P', \dots, P^{(n-1)}$ (où $P^{(n-1)}$ désigne le polynôme P dérivé $n-1$ fois) forment une suite arithmétique.

Exercice 15 Trouver tous les réels x, y vérifiant $x^5 + y^5 = 33$ et $x + y = 3$.

Relations de Newton

Nous allons voir que des sommes symétriques particulières (sommes des puissances k-ièmes) peuvent s'exprimer assez simplement grâce aux fonctions symétriques élémentaires.

Théorème 43 (Relations de Newton)**.** Soit $n \geqslant 1$, et notons $\sigma_1, \dots, \sigma_n$ les fonctions symétriques élémentaires de $(z_1, z_2, \dots, z_n)$. Notons $S_k = \sigma_1^k + \cdots + \sigma_n^k$ pour $k \geqslant 0$. Alors, pour tout entier $k \geqslant 1$,

$$\sum_{r=0}^{k-1} (-1)^r \sigma_r S_{k-r} + (-1)^k k \sigma_k = 0, \tag{1}$$

avec la convention $\sigma_0 = 1$ et $\sigma_r = 0$ quand $r > n$.

Ainsi, à titre d'illustration, pour $r = 1, 2, \dots, n$:

$$\begin{aligned}
S_1 - \sigma_1 &= 0 \\
S_2 - \sigma_1 S_1 + 2\sigma_2 &= 0 \\
S_3 - \sigma_1 S_2 + \sigma_2 S_1 - 3\sigma_3 &= 0 \\
&\vdots \\
S_n - \sigma_1 S_{n-1} + \cdots + (-1)^{n-1}\sigma_{n-1} S_1 + (-1)^n n \sigma_n &= 0
\end{aligned}$$

et pour $r > n$:

$$S_r - \sigma_1 S_{r-1} + \sigma_2 S_{r-2} + \cdots + (-1)^n \sigma_n S_{r-n} = 0.$$

Remarque 44. Si $z_1, \dots, z_n$ sont les racines du polynôme $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, alors pour tout entier $k \geqslant 0$:

$$a_n S_{k+n} + a_{n-1} S_{k+n-1} + a_{n-2} S_{k+n-2} + \cdots + a_0 S_k = 0.$$

En effet, il suffit d'écrire que $z_1^k P(z_1) + \cdots z_n^k P(z_n) = 0$. Les formules de Newton sont donc très facilement établies lorsque $k \geqslant n$.

Par ailleurs, en réécrivant le polynôme P sous la forme $P(x) = x^n + b_1 x^{n-1} + \cdots + b_{n-1} x + b_n$ (attention aux indices !), les relations de Viète donnent $b_j = (-1)^j \sigma_j$, de sorte que les relations de Newton s'écrivent aussi, pour tout entier $k \geqslant 1$,

$$\sum_{r=0}^{k-1} b_r S_{k-r} + k b_k = 0.$$

Preuve des relations de Newton, qui peut être sautée en première lecture. Nous avons déjà traité le cas $k \geqslant n$ plus haut et pouvons donc supposer que $k < n$. La preuve qui suit est due à Doron Zeilberger. Considérons $\mathcal{A} = \mathcal{A}(n, k)$ l'ensemble des couples $(A, j^{(l)})$, où :

(i) A est un sous-ensemble de $\{1, 2, \ldots, n\}$,

(ii) j appartient à $\{1, 2, \ldots, n\}$,

(iii) $|A| + l = k$, où $|A|$ est le nombre d'éléments de A,

(iv) $l \geqslant 0$, et si $l = 0$ alors $j \in A$.

On définit ensuite le poids $w(A, j^{(l)})$ de $(A, j^{(l)})$ par la formule

$$w(A, j^{(l)}) = (-1)^{|A|} \left(\prod_{a \in A} z_a \right) z_j^l.$$

Par exemple, $w(\{1, 3, 5\}, 2^{(3)}) = (-1)^3 z_1 z_3 z_5 \cdot z_2^3 = -z_1 z_2^3 z_3 z_5$. On voit aisément que la somme des poids de tous les éléments de $\mathcal{A}$ est égale au terme de gauche de (1).

Prouvons maintenant que cette somme est nulle. À cet effet, considérons l'application $T : \mathcal{A} \to \mathcal{A}$ définie par :

$$T(A, j^{(l)}) = \begin{cases} (A \backslash \{j\}, j^{(l+1)}), & j \in A, \\ (A \cup \{j\}, j^{(l-1)}), & j \notin A. \end{cases}$$

Cette application vérifie $w(T(A, j^{(l)})) = -w(A, j^{(l)})$ et est une involution (i.e. T composé avec elle-même donne l'identité). On peut donc assembler tous les poids par paires de sorte que chaque paire contienne un poids et son opposé. La somme de tous les poids est donc bien nulle, ce qui conclut la preuve.

Mentionnons qu'il est également possible de procéder par récurrence sur $n - k$ pour prouver les relations de Newton. □

Exemple 45. Soient x, y, z des nombres réels tels que $x + y + z = 1$, $x^2 + y^2 + z^2 = 3$ et $x^3 + y^3 + z^3 = 7$. Trouvons la valeur de $x^5 + y^5 + z^5$.

À cet effet, notons S_k et σ_k respectivement les sommes des puissances k-ièmes et la k-ième fonction symétrique élémentaire de x, y, z. Les relations de Newton donnent

$$S_1 - \sigma_1 = 0, \qquad S_2 - \sigma_1 S_1 + 2\sigma_2 = 0, \qquad S_3 - \sigma_1 S_2 + \sigma_2 S_1 - 3\sigma_3 = 0.$$

On en tire que $\sigma_1 = 1$, $\sigma_2 = -1$ et $\sigma_3 = 1$. D'après les relations de Viète, x, y, z sont donc les solutions de $t^3 - t^2 - t - 1 = 0$. Ainsi, d'après la Remarque 44, nous avons

$$S_{k+3} = S_{k+2} + S_{k+1} + S_k$$

pour $k \geqslant 0$. Il s'ensuit que $S_4 = 1 + 3 + 7 = 11$ puis que $S_5 = 3 + 7 + 11 = 21$.

Exercice 16 Soient x et y deux nombres non nuls tels que $x^2 + xy + y^2 = 0$ (x et y sont des nombres complexes, mais ce n'est pas trop grave). Trouver la valeur de

$$\left(\frac{x}{x+y} \right)^{2013} + \left(\frac{y}{x+y} \right)^{2013}.$$

Exercice 17 Trouver tous les nombres réels x, y, z tels que

$$x + y + z = 3, \qquad x^2 + y^2 + z^2 = 3, \qquad x^3 + y^3 + z^3 = 3.$$

- Polynômes à coefficients entiers -

Nous présentons maintenant quelques spécificités des polynômes à coefficients entiers :

- ⋆ Nous avons déjà vu que si $P, Q \in \mathbb{Z}[X]$ et que $\deg Q \geqslant 1$, on peut toujours effectuer la division euclidienne de P par Q à condition que le coefficient dominant de Q soit égal à 1.
- ⋆ Une propriété extrêmement utile est que si $P \in \mathbb{Z}[X]$, alors pour tous entiers $a \neq b$, $a-b$ divise $P(a)-P(b)$. Ceci est une simple conséquence du fait que $a-b$ divise a^n-b^n pour $n \geqslant 1$.
- ⋆ Si $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$, et si p/q est une racine rationnelle de P sous forme irréductible, alors p divise a_0 et q divise a_n. Ce simple fait permet de restreindre la recherche des racines rationnelles d'un polynôme à coefficients entiers.
- ⋆ Un polynôme $P \in \mathbb{Q}[X]$ vérifie $P(k) \in \mathbb{Z}$ pour tout $k \in \mathbb{Z}$ si et seulement si il existe des entiers $a_0, a_1, \ldots a_n$ tels que

$$P(x) = a_0\binom{x}{0} + a_1\binom{x}{1} + \cdots + a_n\binom{x}{n},$$

où on note $\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}$ si $k \neq 0$ et $\binom{x}{0} = 1$. Cette propriété découle de l'Exercice 10 (2).

Exercice 18 Soient a, b, c des entiers différents. Montrer qu'il n'existe pas de polynôme P à coefficients entiers tel que $P(a) = b$, $P(b) = c$ et $P(c) = a$.

La factorisation par $a-b$ du polynôme $P(a)-P(b)$ peut être utile dans d'autres cas également, voir par exemple l'exercice suivant.

Exercice 19 Soient $P, Q \in \mathbb{R}[X]$ deux polynômes unitaires tels que $P(P(x)) = Q(Q(x)$ pour tout réel x. Prouver que $P(x) = Q(x)$.

- Polynômes à coefficients réels -

Nous considérons dans cette partie des polynômes à coefficients réels et voyons comment des résultats de la théorie de l'analyse réelle s'appliquent dans notre cas. Nous utiliserons la propriété suivante :

Proposition 46. Soit $P \in \mathbb{R}[x]$ un polynôme, et a, α, b, β des réels tels que $a < b$, $P(a) = \alpha$ et $P(b) = \beta$. Alors pour tout réel γ compris entre α et β, il existe un réel c tel que $a \leqslant c \leqslant b$ et $P(c) = \gamma$.

En particulier, si $a < b$ sont tels que $P(a) < 0$ et $P(b) > 0$, alors il existe au moins une racine réelle de P dans l'intervalle $]a, b[$.

La proposition précédent est un cas particulier du théorème des valeurs intermédiaires, valable plus généralement pour toute fonction *continue* à valeurs réelles.

On en déduit le résultat intéressant suivant :

Proposition 47. Soit $P \in \mathbb{R}[X]$ un polynôme de degré impair. Alors P admet au moins une racine réelle.

Démonstration. Écrivons $P(x) = a_n x^n + \cdots + a_1 x + a_0$ avec $a_n \neq 0$ et $n \geqslant 1$. Supposons en premier lieu que $a_n > 0$ et rouvons tout d'abord que $P(x) \to \infty$, lorsque $x \to \infty$, c'est-à-dire que pour tout $M > 0$, il existe x_0 tel que pour tout $x > x_0$ on ait $P(x) > M$. À cet effet, écrivons

$$P(x) = a_n x^n \left(1 + \frac{a_{n-1}}{a_n} \cdot \frac{1}{x} + \cdots + \frac{a_0}{a_n} \cdot \frac{1}{x^n}\right).$$

La somme à l'intérieur de la paranthèse converge vers 1 lorsque $x \to \infty$, et le terme $a_n x^n$ diverge vers $+\infty$ lorque $x \to \infty$. Le résultat en découle. Lorsque $x \to \infty$, on prouve de même que $P(x) \to -\infty$. On en déduit qu'il existe $a < 0 < b$ tels que $P(a) < 0$ et $P(b) > 0$. Le résultat en découle d'aprs la proposition 46.

Si $a_n < 0$, le raisonnement est similaire, mais cette fois-ci $P(x) \to -\infty$ quand $x \to \infty$ et $P(x) \to \infty$ lorsque $x \to -\infty$. □

Exercice 20 Trouver tous les polynômes P à coefficients réels tels que pour tout réel $x > 0$ on ait :

$$\left|P(x)P\left(\frac{1}{x}\right)\right| \leqslant 1.$$

- Polynômes à coefficients complexes -

Nombres complexes

Nous avons vu qu'il existait des polynômes de $\mathbb{R}[X]$ qui ne possédaient pas de racines réelles. Un des intérêts de l'introduction des nombres complexes (et c'est dans cette optique qu'ils ont été introduits au XVIè siècle) est de pallier cette difficulté via le théorème de d'Alembert-Gauss (énoncé par d'Alembert et démontré par Gauss).

Définition 48. Notons $\mathbb{C}$ l'ensemble des couples de nombres réels (a, b) munis :

1. de l'addition suivante : $(a, b) + (c, d) = (a + c, b + d)$,
2. des multiplications suivantes : $(a, b) \times (c, d) = (ac - bd, ad + bc)$ et pour λ réel, $\lambda(a, b) = (\lambda a, \lambda b)$.

Nous voyons l'ensemble des nombres réels plongés dans l'ensemble des nombres complexes : à chaque réel a, on peut associer le nombre complexe $(a, 0)$. Notons enfin i le nombre complexe $(0, 1)$. Ainsi, nous pouvons représenter chaque nombre complexe (a, b) sous la forme $(a, b) = a(1, 0) + b(0, 1) = a + ib$.

Remarque 49. Avec les règles de multiplication précédentes, on voit que $i^2 = -1$, et que $(a + bi)(c + di) = ac - bd + (ad + bc)i$. Ainsi, tout se passe comme si i était un « nombre » tel que $i^2 = -1$ dans toutes les manipulations. En particulier, i est racine du polynôme $X^2 + 1 = 0$.

Remarque 50. Tout élément non nul de $\mathbb{C}$ possédant un inverse, les résultats des sections précédentes sont aussi valables pour $\mathbb{K} = \mathbb{C}$.

Exercice 21 Pour quels entiers $n \geqslant 1$ le polynôme $1 + x^2 + x^2 + \cdots + x^{2n-2}$ est-il divisible par le polynôme $1 + x + x^2 + \cdots + x^{n-1}$?

Théorème de d'Alembert-Gauss

Nous admettons le théorème (qu'on appelle aussi théorème fondamental de l'algèbre) suivant :

Théorème 51. Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine. On dit que $\mathbb{C}$ est algébriquement clos.

Par une récurrence sur le degré, on en déduit :

Corollaire 52. Soit $P \in \mathbb{C}[X]$. Alors P peut s'écrire sous la forme :

$$P(x) = c(x-\alpha_1)^{m_1}\cdots(x-\alpha_k)^{m_k},$$

où $c, \alpha_1, \ldots, \alpha_k$ sont des nombres complexes et $m_1, \ldots, m_k$ sont des entiers strictement positifs.

Nous définissons finalement la conjugaison complexe, qui sera utile lorsque nous voudrons déterminer les polynômes irréductibles de $\mathbb{R}[X]$.

Définition 53. Soit $z = a + bi \in \mathbb{C}$. On définit son *conjugué* $\overline{z}$ par $\overline{z} = a - bi$.

Proposition 54. Pour tous $w, z \in \mathbb{C}$, on a $\overline{wz} = \overline{w} \cdot \overline{z}$.

Démonstration. Exercice. □

- **Arithmétique de** $\mathbb{K}[X]$ -

De même que dans le cas des nombres entiers, la division euclidienne entre polynômes permet de démontrer le théorème de Bézout, et par voie de conséquence de définir la notion de PGCD et d'avoir accès au lemme de Gauss. Les démonstrations étant similaires au cas des entiers, nous ne les reproduisons pas. Dans tout ce qui suit, $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.

Théorème de Bézout dans $\mathbb{K}[X]$

Définition 55. Soient $P, Q \in \mathbb{K}[X]$. Lorsque P est non nul, on rappelle que P divise Q s'il existe $R \in \mathbb{K}[X]$ tel que $Q = PR$. On dit que P et Q sont premiers entre eux s'ils n'ont comme diviseurs communs (dans $\mathbb{K}[X]$) que les constantes non nulles. Nous utilisons aussi ces définitions dans le cas de $\mathbb{Z}[X]$.

Remarque 56. La définition précédente laisse penser que la notion de primalité entre deux polynômes dépend de l'ensemble choisi pour ses coeffecients : ainsi, a priori, rien n'empêche que deux polynômes à coefficients entiers soient premiers entre eux lorsqu'ils sont vus comme éléments de $\mathbb{Q}[X]$, mais qu'ils ne le soient plus lorsqu'on les voit comme éléments de $\mathbb{C}[X]$.

Théorème 57 (Bézout)**.** Soient $P, Q \in \mathbb{K}[X]$. Alors P et Q sont premiers entre eux si, et seulement si, il existe $U, V \in \mathbb{K}[X]$ tels que $PU + QV = 1$.

Exercice 22 Soit $x \in \mathbb{R}$. Les énoncés suivants sont-ils vrais ou faux ?

a. Si x^7 et x^{12} sont rationnels, alors x est rationnel.

b. Si x^9 et x^{12} sont rationnels, alors x est rationnel.

Corollaire 58. Si $P, Q \in \mathbb{Q}[X]$ sont premiers entre eux, alors, vus comme éléments de $\mathbb{R}[X]$, ils sont premiers entre eux.

Démonstration. D'après le théorème de Bézout, il existe $U, V \in \mathbb{Q}[X]$ tels que $PU + QV = 1$. A fortiori, $U, V \in \mathbb{R}[X]$, donc, d'après la réciproque du théorème de Bézout, P et Q sont premiers entre eux vus comme éléments de $\mathbb{R}[X]$. □

Du théorème de Bézout on déduit le théorème de Gauss.

Théorème 59. Si $P, Q, R \in \mathbb{K}[X]$ sont tels que P soit premier avec Q et P divise QR, alors P divise R.

Polynômes irréductibles de $\mathbb{K}[X]$

Les polynômes irréductibles jouent le rôle des nombres premiers : ce sont en quelque sorte les briques de base lorsqu'on souhaite factoriser des polynômes.

Définition 60. Un polynôme $P \in \mathbb{K}[X]$ est dit *irréductible* dans $\mathbb{K}[X]$ si P n'est pas constant et si ses seuls diviseurs dans $\mathbb{K}[X]$ sont les constantes et les polynômes proportionnels à P non nuls, ou, de manière équivalente, s'il n'existe pas $Q, R \in \mathbb{K}[X]$ avec $\deg Q \geqslant 1$ et $\deg R \geqslant 1$.

On en déduit l'équivalent du théorème de factorisation en nombre premiers.

Théorème 61. Tout polynôme de $\mathbb{K}[X]$ se décompose de manière unique, à l'ordre des facteurs près, sous la forme :

$$P = cP_1^{k_1} P_2^{k_2} \cdots P_k^{\alpha_k},$$

ou $c \in \mathbb{K}^*$, $k_i \in \mathbb{N}^*$ et les P_i sont des polynômes distincts unitaires et irréductibles dans $\mathbb{K}[X]$.

À titre d'exercice nous laissons la preuve de ce théorème (très proche de son équivalent pour les nombres entiers).

Le théorème précédent nous invite à chercher les polynômes irréductibles de $\mathbb{C}[X], \mathbb{R}[X], \mathbb{Q}[X]$. Nous commenons par une proposition générale.

Proposition 62. Un polynôme $P \in \mathbb{K}[X]$ de degré 2 ou 3 est irréductible si, et seulement si, il n'a pas de racine.

Démonstration. Exercice. □

Proposition 63. Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de premier degré.

Démonstration. Il est clair que ces polynômes sont bien irréductibles. Réciproquement, si $P \in \mathbb{C}[X]$ de degré au moins 2 est irréductible, d'après le théorème de d'Alembert-Gauss, il peut s'écrire $P(x) = (x - \alpha)Q(x)$, se qui contredit son irréductibilité. □

Passons maintenant à l'étude des polynômes à coefficients réels.

Proposition 64. Tout polynôme $P \in \mathbb{R}[X]$ se décompose sous la forme :

$$P(x) = c \prod_{i=1}^{r} (x - \alpha_i) \prod_{i=1}^{s} (x^2 + a_i x + b_i).$$

En conséquence, les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de premier degré et ceux du second degré à discriminant négatif.

Démonstration. D'après le corollaire 52, on peut écrire $P(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$, ou les α_i sont complexes. En utilisant la proposition 54, on voit que si α est racine de P, alors $\overline{\alpha}$ est également racine de P. En effet, si $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ avec les a_i réels, on a $0 = \overline{P(\alpha)} = \overline{a_0 + a_1 x + \cdots + a_n x^n} = \overline{a_0} + \overline{a_1 x} + \cdots + \overline{a_n x}^n = a_0 + a_1 \overline{x} + \cdots + a_n \overline{x}^n$. Dans l'expression donnant P sous forme factorisée, on regroupe alors par pairs les racines complexes (non réelles) avec leurs conjugués. En remarquant que pour un nombre complexe z, $(x - z)(x - \overline{(}z)) = x^2 + ax + b$, avec $a, b \in \mathbb{R}$ tels que $a^2 - 4b \leqslant 0$, on conclut.

Le raisonnement précédent montre qu'un polynôme irréductible de $\mathbb{R}[X]$ est un polynôme de premier degré ou du second degré à discriminant négatif. Réciproquement, de tels polynômes sont irréductibles en vertu de la proposition 62. □

Exercice 23 Soient $P, Q \in \mathbb{R}[X]$ deux polynômes non nuls tels que pour tout réel x, $P(x^2 + x + 1) = P(x)Q(x)$. Montrer que P est de degré pair. Peut-on trouver de tels polynômes ?

Exercice 24 Soit P un polynôme à coefficients réels tel que $P(x) \geqslant 0$ pour tout réel x. Montrer qu'il existe deux polynômes $Q, R \in \mathbb{R}[X]$ tels que $P = Q^2 + R^2$.

Polynômes irréductibles à coefficients entiers ou rationnels

Dans le cas de $\mathbb{Q}[X]$, il n'y a pas de caractérisation satisfaisante des polynômes irréductibles (essentiellement parce que des propriétés arithmétiques de $\mathbb{Z}$ rentrent en jeu). On peut toutefois donner quelques méthodes de recherche de racines et des critères d'irréductibilité.

Proposition 65. Soit $P(x) \in \mathbb{Q}[X]$ et cherchons ses racines rationnelles. Quitte à multiplier P par le ppcm des dénominateurs de ses coefficients, on peut supposer que $P(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[X]$. Soit p/q une racine rationnelle de P. Alors p divise a_0 et q divise a_n.

Démonstration. Il suffit d'écrire $P(p/q) = 0$, de réduire au même dénominateur et d'utiliser le lemme de Gauss pour les entiers. □

Venons-on à l'irréductibilité.

Remarque 66. En vertu de la remarque 62, on peut en pratique vérifier si un polynôme de degré 2 ou 3 à coefficients entiers ou rationnels est irréductible.

Exemple 67. Le polynôme $x^3 + x^2 - 2x - 1$ est irréductible dans $\mathbb{Q}[X]$ puisqu'il est sans racine dans $\mathbb{Q}$.

On commence par introduire le contenu d'un polynôme afin de montrer que les irréductibles de $\mathbb{Z}[X]$ sont irréductibles dans $\mathbb{Q}[X]$, ce qui n'est pas évident a priori.

Définition 68. Soit $P \in \mathbb{Z}[X]$ non nul. On appelle contenu de P et on note $c(P)$ le pgcd de ses coefficients (au signe près).

Exemple 69. Par exemple, $c(-6x^6 + 3x^5 + 27x - 90) = 3$.

Lemme 70. Pour $P, Q \in \mathbb{Z}[X]$ non nuls, $c(PQ) = c(P)c(Q)$ au signe près.

Démonstration. Montrons d'abord le résultat lorsque $c(P) = c(Q) = 1$. Raisonnons par l'absurde que $c(PQ) \neq 1$ en considérant un nombre premier p divisant $c(PQ)$. Écrivons $P(x) = \sum_i a_i x^i$, $Q(x) = \sum_i b_i x^i$, $P(x)Q(x) = \sum_i c_i x^i$. Comme $c(P) = c(Q) = 1$, il existe $i_0, j_0 \in \mathbb{N}$ tels que :

$$\begin{aligned} \forall i < i_0, &\quad p|a_i \text{ mais } p \not| a_{i_0} \\ \forall j < j_0, &\quad p|b_j \text{ mais } p \not| b_{j_0}. \end{aligned}$$

Par hypothèse, on a :

$$p|c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_i b_i = a_{i_0} b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i<i_0 \text{ ou } j<j_0}} a_i b_j.$$

Mais alors p divise $a_{i_0} b_{j_0}$, ce qui est absurde.

Dans le cas général, notons $P' = P/c(P), Q' = Q/c(Q)$ de sorte que $c(P') = c(Q') = 1$. Ainsi, $c(P'Q') = 1$. Or $c(P'Q') = c(PQ)/c(P)c(Q)$, d'ou̧ le résultat. □

On en déduit également le résultat suivant.

Proposition 71. Soit $P \in \mathbb{Z}[X]$. Alors P est irréductible dans $\mathbb{Z}[X]$ si, et seulement, si P est irréductible dans $\mathbb{Q}[X]$ et $c(P) = 1$.

Démonstration. Si P est irréductible dans $\mathbb{Q}[X]$ et $c(P) = 1$, il est clair qu'il l'est dans $\mathbb{Z}[X]$. Réciproquement, supposons P irréductible dans $\mathbb{Z}[X]$ (ce qui implique $c(P) = 1$) et par l'absurde supposons qu'il n'est pas irréductible dans $\mathbb{Q}[X]$. Écrivons alors $P = QR$ avec $Q, R \in \mathbb{Q}[X]$ unitaires de degré au moins 1. Écrivons $Q(x) = \frac{a}{b} Q'(x)$ avec $Q' \in \mathbb{Z}[X]$, $c(q') = 1$ et a, b entiers premiers entre eux. De même, écrivons $R(x) = \frac{c}{d} R'(x)$ avec $R' \in \mathbb{Z}[X]$, $c(R') = 1$ et c, d entiers premiers entre eux. Alors $bdP(x) = acQ'(x)R'(x)$. Comme $c(P) = 1$, il vient $bd = c(bdP(x)) = c(acQ'R') = ac$ (au signe près). Ainsi, $P = QR = \frac{ac}{bd} Q'R' = Q'R'$ (au signe près) avec $Q', R' \in \mathbb{Z}[X]$. Ceci contredit l'irréductibilité de P dans $\mathbb{Z}[X]$. □

De manière un peu similaire, on démontre la proposition suivante, parfois utile.

Proposition 72. Soit $P, Q \in \mathbb{Q}[X]$ unitaires tels que $R = PQ \in \mathbb{Z}[X]$. Alors P et Q sont à coefficients entiers.

Démonstration. Notons u (resp. v) le ppcm des dénominateurs des coefficients de P (resp. Q). Alors $uvR = uvPQ = (uP)(vQ)$. Donc $c(uvR) = c(uP)c(vQ)$ d'après le lemme précédent. Or, comme P et Q sont unitaires, $c(uP) = c(vQ) = 1$ et $c(uvR) \geqslant uv$. On en déduit que $u = v = 1$ et donc que $P, Q \in \mathbb{Z}[X]$. □

Exercice 25 Soit $P(x) = ax^3 + bx^2 + cx + d \in \mathbb{Z}[X]$ avec ad impair et bc pair. On suppose que P a toutes ses racines réelles. Montrer qu'au moins une racine de P est un nombre réel irrationnel.

Remarque 73. Ainsi, l'étude de l'irréductibilité d'un polynôme à coefficients entiers sur $\mathbb{Q}[X]$ se réduit à l'étude de l'irréductibilité de $\mathbb{Z}[X]$, qui est a priori plus facile.

Voici un exemple (important) d'application de ceci.

Théorème 74. Soit $P(x) = a_n x^n + \cdots + a_1 x + a_0$ un polynôme de $\mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que :

1. p divise $a_0, a_1, \ldots, a_{n-1}$,
2. p ne divise pas a_n,
3. p^2 ne divise pas a_0.

Alors P est irréductible dans $\mathbb{Q}[X]$.

Démonstration. D'après la proposition précédente, il suffit de montrer que P est irréductible dans $\mathbb{Z}[X]$. Supposons donc par l'absurde que $P(x) = Q(x)R(x)$ avec Q, R deux polynômes non constants de $\mathbb{Z}[X]$ avec $Q(x) = q_k x^k + \cdots q_0$ et $R(x) = r_l x^l + \cdots + r_0$. Alors $a_0 = q_0 r_0$. Par suite, d'après le point 3., p divise q_0 ou r_0, mais pas les deux à la fois. Sans perte de généralité, supposons que $p|q_0$ et que $p \not| r_0$. D'autre part, p ne divise pas q_k car sinon il diviserait a_n, ce qui est exclu. Soit donc i_0 le plus petit indice i $(1 \leqslant i \leqslant k)$ tel que p ne divise par q_i. Alors :

$$a_{i_0} = q_{i_0} r_0 + q_{i_0 - 1} r_1 + \cdots + q_o r_{i_0}.$$

Comme $i_0 \leqslant k < n$, p divise a_{i_0} et donc p divise $q_{i_0} r_0$, et donc p divise r_0, ce qui est absurde. □

Exemple 75. Soit p un nombre premier et $P(x) = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[X]$. En appliquant le critère d'Eisenstein au polynôme $Q(x) = P(x+1)$, on voit que P est irréductible dans $\mathbb{Q}[X]$.

Exercice 26 (IMO 93, exercice 1) Soit $n \geqslant 2$ un entier. Montrer que le polynôme $f(x) = x^n + 5x^{n-1} + 3$ est irréductible sur $\mathbb{Z}[X]$.

- Quelques exercices supplémentaires -

Les exercices qui suivent sont plus ou moins rangés par difficulté croissante.

Exercice 27
Soit P un polynôme de degré 4 tel que $P(0) = P(1) = 1$, $P(2) = 4$, $P(3) = 9$ et $P(4) = 16$. Calculer $P(-2)$.

Exercice 28
α, β, γ étant les trois racines de $x^3 - x - 1$, calculer : $\frac{1-\alpha}{1+\alpha} + \frac{1-\beta}{1+\beta} + \frac{1-\gamma}{1+\gamma}$

Exercice 29
Soit $a = \sqrt{4 + \sqrt{5 - a}}$, $b = \sqrt{4 + \sqrt{5 + b}}$, $c = \sqrt{4 - \sqrt{5 - c}}$ et $d = \sqrt{4 - \sqrt{5 + d}}$. Calculer $abcd$.

Exercice 30 (Canada 1970)
Soit P un polynôme à coefficients entiers. On suppose qu'il existe des entiers deux à deux distincts a, b, c, d tels que $P(a) = P(b) = P(c) = P(d) = 5$. Montrer qu'il n'existe pas d'entier k tel que $P(k) = 8$.

Exercice 31
Trouver les polynômes P tels que pour tout réel x :

$$(x - 16)P(2x) = 16(x - 1)P(x)$$

Exercice 32
Soit $x \in \mathbb{R}$ tel que $x^2 - x \in \mathbb{Z}$ et il existe un entier positif $n \geqslant 3$ tel que $x^n - x \in \mathbb{Z}$. Montrer que x est entier.

Exercice 33
Soit P et Q des polynômes unitaires de degré 2014, tels que pour tout réel x, $P(x) \neq Q(x)$. Montrer qu'il existe un réel x tel que $P(x-1) = Q(x+1)$.

Exercice 34 (Benelux 2010)
Trouver tous les polynômes $P \in \mathbb{R}[X]$ tels que pour tous réels a, b, c on ait :

$$P(a+b-2c) + P(b+c-2a) + P(c+a-2b) = 3P(a-b) + 3P(b-c) + 3P(c-a).$$

Exercice 35
Alcina et Bajazet jouent au jeu suivant : on écrit $x^4 + *x^3 + *x^2 + *x + 1$ au tableau. Alcina choisit une étoile et la remplace par un réel, puis c'est à Bajazet, et ainsi de suite jusqu'à épuisement des étoiles. Alcina gagne si le polynôme P obtenu n'a pas de racine réelle. Sinon, c'est Bajazet. Montrer que ce dernier a une stratégie gagnante.

Exercice 36
Soit $a_i \in \mathbb{Z}, i = 1, \dots, n$ des entiers deux à deux distincts, et soit $P := \prod_{i=1}^{n}(X - a_i) - 1$. Montrer que P est irréductible dans $\mathbb{Z}[X]$.

Exercice 37 (IMO 1988, exercice 1)
Montrer que l'ensemble des réels x vérifiant $\sum_{k=1}^{70} \frac{k}{x-k} \geqslant \frac{5}{4}$ est réunion d'intervalles dont la somme des longueurs vaut 1988.

Exercice 38
Trouver tous les polynômes autre que les polynômes constants, à coefficients dans $\mathbb{R}$ et tels que, pour tout $z \in \mathbb{C}$,

$$P(z^2) = P(z)P(z-1).$$

Exercice 39
Soit $P, Q \in \mathbb{R}[X]$ deux polynômes réels non constants ayant les mêmes racines, et tels que $P-1$ et $Q-1$ aussi. Montrer que $P = Q$.

Exercice 40
On se donne $2n$ réels distincts $a_1, a_2, \dots, a_n, b_1, \dots, b_n$. On ramplit une table $n \times n$ en mettant $a_i + b_j$ dans la case (i, j). On suppose qu'il existe une constante c telle que le produit de chaque ligne est c. Montrer qu'il existe une constante d telle que le produit de chaque colonne soit d.

Exercice 41 (IMO 2004, exercice 2)
Trouver tous les polynômes P à coefficients réels qui vérifient, pour tous a, b, c réels tels que $ab + bc + ca = 0$:

$$P(a-b) + P(b-c) + P(c-a) = 2P(a+b+c).$$

Exercice 42 Soit $n \geqslant 1$ un entier. On note $\mathfrak{S}_n$ l'ensemble des permutations de l'ensemble $\{1, 2, \ldots, n\}$. Pour $\sigma \in \mathfrak{S}_n$, on note aussi $\text{cyc}(\sigma)$ le nombre de cycles de σ. Soit $P_n(x)$ le polynôme suivant :

$$P_n(x) = \sum_{\sigma \in \mathfrak{S}_n} x^{\text{cyc}(\sigma)}.$$

Montrer que P_n a toutes ses racines réelles et que ce sont des entiers négatifs.

Exercice 43 (Test de sélection Chine 2008)
Soient m, n des entiers strictement positifs et $P \in \mathbb{Z}[X]$ un polynôme de degré n tel que tous ses coefficients soient impairs. On suppose que $(x-1)^m$ divise P. Montrer que si $m \geqslant 2^k$ (avec $k \geqslant 2$ entier), alors $n \geqslant 2^{k+1} - 1$.

Exercice 44
Si P est un polynôme à coefficients entiers, on note $w(P)$ le nombre de ses coefficients impairs. Soit $Q_i = (1+x)^i$. Montrer que pour tout suite d'entiers $0 \leqslant i_1 < i_2 < \cdots < i_n$, $w(Q_{i_1} + \cdots + Q_{i_n}) \geqslant w(Q_{i_1})$.

Exercice 45 (IMO 2002, exercice 3)
Trouver les couples (n, m) tels que $n > 2$, $m > 2$, et il existe une infinité d'entiers naturels k tels que $k^n + k^2 - 1$ divise $k^m + k - 1$.

- Quelques motivations -

Pourquoi étudie-t-on les polynômes ? Voici quelques éléments de réponse donnés sans démonstration.

Théorème 76. Soit f une fonction réelle infiniment dérivable (si vous ne savez pas ce que ça veut dire, imaginez qu'elle est très gentille). Soit $x_0 \in \mathbb{R}$. Alors pour tout entier n, pour tout $\epsilon > 0$, il existe $\eta > 0$ et des réels $a_0, \ldots, a_n$ tels que pour tout $x \in [x_0 - \eta, x_0 + \eta]$:

$$|f(x - x_0) - a_0 - a_1(x - x_0) - \cdots - a_n(x - x_0)^n| \leqslant \epsilon |(x - x_0)^n|.$$

Ainsi, au voisinage de tout point, la fonction « ressemble » à un polynôme.

Théorème 77. Soit $f : [0, 1] \to \mathbb{R}$ une fonction continue. Alors il existe une suite de polynômes $P_1(x), P_2(x), \cdots$ telle que pour tout $\epsilon > 0$, il existe $N > 0$ tel que pour tout $n \geqslant N$:

$$\text{pour tout } x \in [0, 1] \qquad |f(x) - P_n(x)| \leqslant \epsilon.$$

Ainsi, toute fonction continue sur $[0, 1]$ peut être approchée sur tout $[0, 1]$ par des polynômes.

Signalons finalement que l'étude de l'ensemble des zéros communs de plusieurs polynômes à n variables, appelé variété algébrique, est centrale en géométrie algébrique.

- Distinction entre polynôme et fonction polynomiale -

Ici, nous expliquons pourquoi il est nécessaire de faire cette distinction en commençant par définir d'une autre manière un polynôme. Ici, $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ou bien $\mathbb{Z}/p\mathbb{Z}$ muni des lois d'addition et de multiplication usuelles.

Définition 78. Un polynôme à coefficients dans $\mathbb{K}$ est une suite infinie d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang.

Exemple 79. Par exemple, $(0,1,2,3,0,0,\dots,0,\dots)$ est un polynôme, de même que $(0,0,\dots,0,\dots)$. Par contre, $(1,1,\dots,1,\dots)$ n'en est pas un.

Définition 80. Soit $P = (u_n)_n$ et $Q = (v_n)_n$ deux polynômes. On définit le polynôme $P + Q$ par la suite $w_n = u_n + v_n$ (qui est bien nulle à partir d'un certain rang) et le polynôme $P \times Q$ par la suite (z_n), ou $z_n = \sum_{i+j=n} u_n v_n$ (vérifier que (z_n) est nulle à partir d'un certain rang). On identifie les éléments de $\mathbb{K}$ avec les polynômes constants via l'application qui à un élément $\lambda \in \mathbb{K}$ associe le polynôme $(\lambda, 0, 0, \dots, 0, \dots)$. Remarquons que ceci est cohérent avec la notion de multiplication intuitive d'un polynôme par un élément de $\mathbb{K}$: si (u_n) est un polynôme et $\lambda \in \mathbb{K}$, alors le polynôme $\lambda \times (u_n)$ est le polynôme (λu_n).

Nous introduisons maintenant l'indéterminée X.

Définition 81. Notons X le polynôme $(0,1,0,0,\dots)$.

Proposition 82. Tout polynôme P s'exprime sous la forme $P = \sum_{i=0}^{n} a_n X^n$. On note indifféremment P ou $P(X)$ pour rappeler qu'on note X l'indéterminée (on pourrait très bien la noter Y !).

Démonstration. Si $P = (a_0, a_1, a_2, \dots)$, notons N un entier tel que $i \geqslant N$ implique $a_i = 0$. Alors $P(X) = a_0 + a_1 X + \cdots + a_N x^N$. Ceci est une conséquence immédiate de la définition de X et de la multiplication entre polynômes. □

Voici maintenant le lien entre polynôme et fonction polynomiale associée. Rappelons que, pour l'instant, un polynôme est juste une suite de nombres qui est nulle à partir d'un certain rang et n'est pas vu comme une application.

Proposition 83. Soit $P(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$ un polynôme. On note $\widetilde{P}$ l'application définie par $\widetilde{P}(x) = a_0 + a_1 x + \cdots + a_n x^n$ pour $x \in \mathbb{K}$, qu'on appelle application polynomiale associée à P. L'application $P \mapsto \widetilde{P}$ est injective si $\mathbb{K}$ est infini. Si $\mathbb{K}$ est fini, cette application n'est pas nécessairement injective.

Démonstration. Plaçons nous d'abord dans le cas ou $\mathbb{K}$ est infini. Soient $P, Q \in \mathbb{K}[X]$ tels que $\widetilde{P} = \widetilde{Q}$. Écrivons $P(X) = \sum_i a_i X^i$ et $Q(X) = \sum_i b_i X^i$. Alors le polynôme $P(x) - Q(x)$, au sens des sections précédentes, a une infinité de racines, donc est nul. Donc $a_i = b_i$ pour tout i.

Par contre, dans le cas ou $\mathbb{K}$ est fini, le raisonnement précédent ne s'applique pas. Exhibons d'ailleurs un contre-exemple. Considérons $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ et $P(X) = X^p - X$. D'après le petit théorème de Fermat, pour tout $x \in \mathbb{K}$, on a $P(x) = 0$. Ainsi, P n'est pas le polynôme nul, mais les deux fonctions polynomiales associées sont les mêmes. □

En d'autres termes, lorsque $\mathbb{K}$ est infini (par exemple $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, ce qui explique que nous n'avons pas perdu de généralité dans les premières sections), nous pouvons parler sans distinction de polynôme ou de fonction polynomiale associée. En revanche, dans les autres cas, il faut faire très attention !

- Éléménts de réponse aux exercices -

<u>*Solution de l'exercice 1*</u> On cherche le reste sous la forme $R(X) = aX + b$. On a $R(1) = P(1)$, $R(-1) = P(-1)$, ce qui permet de calculer $R(X) = -2X + 2$.

<u>*Solution de l'exercice 2*</u> Si $Q(x)$ était un polynôme, alors $Q(x) - x$ serait un polynôme avec une infinité de racines, donc serait de degré nul, c'est absurde.

<u>*Solution de l'exercice 3*</u> Comme $P(x)^2 = 16P(x^2/4)$ est un polynôme en x^2, on peut appliquer la proposition 24. Dans le premier cas, s'il existe un polynôme Q tel que $P(x)^2 = Q(x^2)$, on obtient $16Q(x^4) = 16P(x^2) = P(2x)^4 = Q(4x^2)^2$, et donc $16Q(x^2) = Q(4x)^2$. Dans le deuxième cas, s'il existe un polynôme Q tel que $P(x)^2 = xQ(x^2)$, on obtient similairement que $4Q(x^2) = Q(4x)^2$.

On peut donc réappliquer la proposition 24 à Q, et de même on obtien que pour tout entier $k \geqslant 0$, il existe un entier $0 \leqslant i \leqslant 2^k$ et un polynôme R_k tel que $P(x) = x^i R_k(x^{2^k}$.

En choisissant k tel que $2^k > \deg P$, il s'ensuit que R_k est forcément constant et donc que $P(x) = c \cdot x^i$. En réinjectant dans l'équation de départ, on obtient $P(x) = 16(x/4)^i$ pour un certain entier $i \geqslant 0$ (et toutes ces solutions conviennent bien, réciproquement).

<u>*Solution de l'exercice 4*</u> 1 doit être racine double de P. Cela nous donne deux équations : $P(1) = 0$ et $P'(1) = 0$, qui permettent de trouver $a = 3$ et $b = -4$.

<u>*Solution de l'exercice 5*</u> On note n le degré de P. En passant l'équation aux degrés, on obtient $n = (n-1)+(n-2) = 2n-3$, donc $n = 3$. On peut facilement calculer le coefficient dominant, on laisse le soin au lecteur de terminer les calculs.

<u>*Solution de l'exercice 6*</u> On remarque que la dérivée de $\frac{P'}{P}$ est $\frac{P''-P'^2}{P^2}$ qui est du même signe que $P'' - P'^2$. Or on voit facilement que $\frac{P'(x)}{P(x)} = \sum \frac{1}{x-\alpha_i}$ donc $(\frac{P'(x)}{P(x)})' = \sum \frac{-1}{(x-\alpha_i)^2} < 0$ d'où le résultat. Pour obtenir l'inégalité sur les coefficients on procède de la manière suivante. Pour $k = 1$, l'inégalité provient de $P(0)P''(0) \leqslant P'(0)^2$. Ensuite on applique l'inégalité aux polynômes $P^{(k-1)}$: $P^{(k-1)}P^{(k+1)} \leqslant \left(P^{(k)}\right)^2$ d'où $a_{k-1}(k-1)! \times a_{k+1}(k+1)! \leqslant a_k^2 \times k!^2$ or $\frac{k!^2}{(k-1)!(k+1)!} = \frac{k}{k+1} \leqslant 1$ d'où le résultat.

<u>*Solution de l'exercice 7*</u> Notons $\alpha_1, \dots, \alpha_n$ les n racines de P. On écrit :

$$\frac{P''(x)P(x) - P'(x)^2}{P(x)^2} = \left(\frac{P'(x)}{P(x)}\right)' = \sum_{i=1}^{n} \frac{-1}{(x-\alpha_i)^2}.$$

Ainsi,

$$\begin{aligned}(n-1)P'(x)^2 - nP(x)P''(x) &= P(x)^2 \cdot \frac{n(P'(x)^2 - P(x)P''(x)) - P'(x)^2}{P(x)^2} \\ &= P(x)^2 \left(\sum_{i=1}^{n} \frac{n}{(x-\alpha_i)^2} - \left(\sum_{i=1}^{n} \frac{1}{(x-\alpha_i)} \right)^2 \right),\end{aligned}$$

qui est positif d'après l'inégalité de Cauchy–Scwharz. Le cas d'égalité s'obtient lorsque tous les α_i sont égaux, i.e. lorsque $P(x)$ est de la forme $P(x) = c(X-a)^n$.

<u>*Solution de l'exercice 8*</u> On a déja résolu le problème lorsque le degré de P est au plus $n - 1$ grâce aux interpolateurs de Lagrange. Si le degré de P est supérieur ou égal à n, notons L le

polynôme interpolateur associé aux a_i et b_i. Le polynôme $P-L$ s'annule en $a_1, \dots, a_n$. On a donc

$$P(X) = c_1 \sum_{i=1}^{n} b_i \prod_{j=1, j\neq i}^{n} \frac{X-a_j}{a_i-a_j} + c_2(X-a_1)(X-a_2)\cdots(X-a_n).$$

<u>*Solution de l'exercice 9*</u> Un polynôme à coefficients rationnels est clairement solution. Réciproquement, si P est un polynôme de degré n vérifiant cette propriété, alors en interpolant en $n+1$ points rationnels, on remarque que P est à coefficients rationnels.

<u>*Solution de l'exercice 10*</u>

1. Soit $i \geqslant n$. Alors
$$\frac{1}{n!}\prod_{k=0}^{n-1}(i-k) = \binom{i}{n} \in \mathbb{Z}.$$
On traite similairement le cas $i < 0$.
2. On remarque que $H_n(n) = 1$ et $H_n(i) = 0$ pour des entiers $0 \leqslant i \leqslant n-1$. Si $P \in \mathbb{C}[X]$ est tel que $P(k) \in \mathbb{Z}$ pour tout $k \in \mathbb{N}$, notons n le degré de P et soit
$$Q(X) = P(X) - \sum_{i=0}^{n} P(i)H_i(X).$$
Le polynôme Q est de degré n et possède $n+1$ racines $0, 1, \dots, n$. On en déduit que Q est nul. Les polynômes cherches sont donc des combinaisons linéaires entières des polynômes de Hermite.
3. (i) On a
$$\begin{aligned} X^k = (X+1-1)^k &= \sum_{i=0}^{k}\binom{k}{i}(X+1)^i(-1)^{k-i} = \sum_{i=0}^{k}\binom{k}{i}\left(\sum_{j=0}^{i}\binom{i}{j}X^j\right)(-1)^{k-i} \\ &= \sum_{j=0}^{k}\left(\sum_{i=j}^{k}(-1)^{k-i}\binom{k}{i}\binom{i}{j}\right)X^j. \end{aligned}$$
Ainsi, en identifiant les coefficients, la somme cherchée est nulle pour $0 \leqslant j \leqslant k-1$ et vaut 1 pour $j = k$.

   (ii) Pour prouver que 1. implique 2., si P est de degré n, on peut écrire
$$P(X) = \sum_{i=0}^{n} P(i)H_i(X).$$
On a alors pour tout entier $j \geqslant 0$.
$$P(j) = \sum_{k=0}^{n}\binom{j}{k}P(k)$$
et
$$\sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}u_j = \sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}P(j) = \sum_{j=0}^{i}\sum_{k=0}^{n}(-1)^{i-j}\binom{i}{j}\binom{j}{k}P(k).$$

D'après ce qui précède, cette somme est nulle pour $i \geqslant n+1$.

Pour montrer que 2. implique 1., on voit que le polynôme

$$P(X) = \sum_{i=0}^{n} u_i H_i(X)$$

convient en utilisant un raisonnement similaire.

Solution de l'exercice 11 On met P sous forme canonique : $P = a(x-b)^2 + c$. On translate de b selon l'axe des abscisses, de $-c$ selon l'axe des ordonnées, et on applique une homothétie de rapport $\frac{1}{\sqrt{a}}$.

Solution de l'exercice 12 Soit (x, y, z) une solution. Visiblement, aucun de ces nombres n'est nul. En retranchant la troisième équation à la deuxième équation, on en déduit que $zx = xy$, puis, en simplifiant par x (qui est non nul), on obtient que $z = y$. En retranchant la troisième équation à la première équation, on obtient : $y^2 - xy = 8$, ou encore $xy = y^2 - 8$. La deuxième équation se réécrit $y^2x + xy = 4$. Il vient donc :

$$y(y^2-8) + y^2 - 8 = 4,$$

ou encore $y^3 + y^2 - 8y - 12 = 0$. On remarque que $y = 3$ est une solution. En effectuant la division euclidienne de $y^3 + y^2 - 8y + 12$ par $y - 3$, on trouve :

$$y^3 + y^2 - 8y - 12 = (y-3)(y^2+4y+4) = (y-3)(y+2)^2.$$

On en déduit que $y = z = 3$ ou $y = z = -2$. Dans le premier cas, $x = \frac{1}{3}$ et dans le deuxième cas, $x = 2$. Réciproquement, les triplets $(2, -2, -2)$ et $(\frac{1}{3}, 3, 3)$ sont solution et ce sont donc les seules.

Solution de l'exercice 13 Supposons que $ax^2 - (a+3)x + 2 = 0$ admette deux racines de signe opposé, notées z_1, z_2. Alors d'après les relations de Viète, $z_1z_2 = 2/a$. Or z_1 et z_2 sont de signe opposés si, et seulement si, $z_1z_2 < 0$. On en déduit que $a < 0$. Réciproquement, si a<0, alors le discriminant de l'équation vaut $a^2 - 2a + 9$. Pour montrer qu'il est positif, utilisons la forme canonique en écrivant $a^2 - 2a + 9 = (a-1)^2 + 8 \geqslant 0$. Ainsi, lorsque $a < 0$, il y a deux solutions réelles notées z_1, z_2. D'après les relations de Viète, $z_1z_2 = 2/a < 0$, de sorte que z_1 et z_2 sont de signe opposés.

Remarquons que dans la preuve de la réciproque, il a d'abord fallu montrer que le polynôme avait deux racines réelles avant d'utiliser les relations de Viète.

Solution de l'exercice 14 On pose $P = \sum a_k X^k$, et on appelle n le degré de P. La somme des racines de $P^{(k)}$ vaut $\frac{a_{n-1}(n-1)(n-2)\ldots(n-k)}{a_n n(n-1)\ldots(n-k+1)} = \frac{a_{n-1}(n-k)}{a_n n}$. La suite est donc arithmétique, de raison $\frac{-a_{n-1}}{n a_n}$.

Solution de l'exercice 15 Indication : introduire $\sigma_1 = x + y$ et $\sigma_2 = xy$, puis écrire les équations correspondantes pour σ_1 et σ_2, puis les résoudre.

Solution de l'exercice 16 On a clairement $x/(x+y) + y/(x+y) = 1$ et

$$\frac{x}{x+y} \cdot \frac{y}{x+y} = \frac{xy}{x^2+2xy+y^2} = 1.$$

Ainsi, $x/(x+y)$ et $y/(x+y)$ sont les racines de $t^2 - t + 1 = 0$, de sorte que les sommes $S_k = (x/(x+y))^k + (y/(x+y))^k$ vérifient $S_0 = 2$, $S_1 = 1$ et

$$S_{k+2} = S_{k+1} - S_k$$

pour $k \geqslant 0$. On en déduit que la suite (S_k) est période de période 6, ses valeurs étant successivement $2, 1, -1, -2, -1, 1, 2, 1, -1, \ldots$. On en déduit que $S_{2013} = -2$.

<u>*Solution de l'exercice 17*</u> On écrit les relations de Newton :

$$S_1 - \sigma_1 = 0, \qquad S_2 - \sigma_1 S_1 + 2\sigma_2 = 0, \qquad S_3 - \sigma_1 S_2 + \sigma_2 S_1 - 3\sigma_3 = 0.$$

Ainsi, $\sigma_1 = 3$, $\sigma_2 = 3$, $\sigma_3 = 1$. On en tire que x, y, z sont racines de $t^3 - 3t^2 + 3t - 1 = 0$. Or $t^3 - 3t^2 + 3t - 1 = (t-1)^3$. Donc $x = y = z = 1$.

<u>*Solution de l'exercice 18*</u> Si un tel P existait, on aurait $a - b | P(a) - P(b)$, i.e $a - b | b - c$ et de même $b - c | c - a$ et $c - a | a - b$ donc $|a - b| \leqslant |b - c| \leqslant |c - a| \leqslant |a - b|$, donc on doit avoir égalité partout, ce qui est impossible car, si par exemple $a > b > c$, alors $|a - c| > |a - b|$ et on vérifie de même les autres cas...

<u>*Solution de l'exercice 19*</u> Écrivons

$$P(P(x)) - Q(Q(x)) = (Q(P(x)) - Q(Q(x))) + S(P(x)),$$

où $S(x) = P(x) - Q(x)$. Suppsons que $S \neq 0$. Soient k le degré de S et n le degré de Q. On voit aisément que le degré de $Q(P(x)) - Q(Q(x))$ est $n^2 - n + k$ et que le degré de $R(P(x))$ est kn.

Si $k \geqslant 1$, on a $kn < n^2 - n + k$, et donc le degré de $P(P(x)) - Q(Q(x))$ est $n^n - n + k$, absurde.

Si $k = 0$, S est constant. Écrivons $S = c$. On obtient alors que $Q(Q(x) + c) = Q(Q(x) - c)$. Ainsi, $Q(z + c) = Q(z) - c$ pour une infinité de réels z, et donc $Q(x + c) = Q(x) - c$. Donc $Q(kc) = Q(0) - kc$ pour tout entier k, et donc $Q(x) = Q(0) - x$. Ceci contredit le fait que Q est unitaire.

<u>*Solution de l'exercice 20*</u> Écrivons $P(x) = x^n Q(x)$ pour un certain entier $n \geqslant 0$ et $Q(x)$ un polynôme tel que $Q(0) \neq 0$. Alors Q vérifie la propriété de l'énoncé. Si Q n'est pas constant, en faisant tendre x vers l'infini, on voit que forcément $Q(0) = 0$, absurde. Donc Q est constant est P est de la forme $P(x) = cx^n$ avec $c \in \mathbb{R}$ et $n \geqslant 0$. Réciproquement, on vérifie que les polynômes de la forme $P(x) = cx^n$ avec $|c| \leqslant 1$ et $n \geqslant 0$ conviennent.

<u>*Solution de l'exercice 21*</u> Soit $P(x) = 1 + x + \cdots + x^{n-1} = (1 - x^n)/(1 - x)$. Ainsi, $P(x)$ divise $P(x^2)$ si et seulement si il existe un polynôme $Q(x)$ tel que

$$\frac{1 - x^{2n}}{1 - x^2} = Q(x) \frac{1 - x^n}{1 - x},$$

ou encore

$$(1 + x^n) = Q(x)(1 + x).$$

Ainsi, $P(X)$ divise $P(X^2)$ si et seulement si -1 est racine de $1 + X^n$, autrement dit si et seulement si n est impair.

<u>*Solution de l'exercice 22*</u> La première assertion est vraie (utiliser le théroème de Bézout pour les nombres entiers avec 7 et 12). La seconde assertion est fausse (prendre $x = 2^{1/3}$).

<u>*Solution de l'exercice 23*</u> Supposons par l'absurde que P admette une racine réelle, α. Alors $\alpha^2 + \alpha + 1$ est une autre racine du polynôme, strictement supérieure à la précédente. On construit ainsi une infinité de racines distinctes, contradiction. Donc toutes les racines de P sont complexes, donc P est de degré pair.

<u>*Solution de l'exercice 24*</u> On écrit P comme produit de polynômes irréductibles dans $\mathbb{R}$. P est le produit de polynômes de degrés 2 de discriminant négatifs et de polynômes de la forme $(x-a)^{2k}$ (en effet si la multiplicité d'une racine était impaire, au voisinage de cette racine on pourrait rendre P négatif). Pour exprimer la partie complexe comme somme de carrés, on la sépare en deux termes conjugués l'un de l'autre (en séparant les termes $(X-z)$ des $(X-\bar{z})$). Cela termine, car $(P-iQ)(P+iQ) = P^2 + Q^2$.

<u>*Solution de l'exercice 25*</u> On démarre par diviser P par son contenu, ce qui ne modifie pas les hypothèses (car ce contenu est impair). Supposons par l'absurde que P a toutes ces racines rationnelles. Comme $c(P) = 1$, ces racines sont entières. Comme d est impair, ces trois racines sont impaires, et les relations coefficients racines montrent que b et c sont impairs, c'est absurde.

<u>*Solution de l'exercice 26*</u> Supposons qu'il existe deux polynômes g et h, à coefficients entiers, tels que $f = gh$. Comme $f(0) = 3$, on peut supposer, sans perte de généralité que $|g(0)| = 3$ et on écrit : $g(x) = x^k + a_{k-1}x^{k-1} + ... + a_0$ ($a_0 = \pm 3$). On s'inspire maintenant de la démonstration du critère d'Eisenstein : soit j le plus petit indice tel que a_j ne soit pas divisible par 3. On pose $h(x) = x^p + b_{p-1}x^{p-1} + ... + b_0$ et $f(x) = x^n + c_{n-1}x^{n-1} + ... + c_0$, il apparaît que le coefficient $c_j = a_j b_0 + a_{j-1}c_1 + ...$ n'est pas divisible par 3 car $b_0 a_0 = 3$ et $a_0 = \pm 3$. Compte tenu de l'expression de $f, j \geqslant n-1$, donc $k \geqslant n-1$ donc $p \leqslant 1$ donc le polynôme h s'écrit $\pm x \pm 1$, ce qui est absurde car $f(\pm 1) = 0$.

<u>*Solution de l'exercice 27*</u>

Dans ce genre d'exercice, on cherche un polynôme "proche" de P ayant (presque) autant de racines que son degré, pour l'avoir sous forme factorisée. Avec un soupçon d'observation, on se rend compte que $P(1) - 1^2 = P(2) - 2^2 = P(3) - 3^2 = P(4) - 4^2 = 0$. $P(X) - X^2$ est de degré au plus 4, donc il existe un réel c tel que $P(X) - X^2 = c(X-1)(X-2)(X-3)(X-4)$. Pour $X = 0$, on trouve $c = \frac{1}{24}$.

<u>*Solution de l'exercice 28*</u> Une méthode sûre même si, en l'occurrence, on peut trouver plus rapide, est de chercher l'équation ayant pour racines $\frac{1-\alpha}{1+\alpha}, \frac{1-\beta}{1+\beta}, \frac{1-\gamma}{1+\gamma}$ et de calculer la somme des racines de cette dernière équation à partir de ses coefficients. Si x est racine de $x^3 - x - 1$, de quelle équation est racine $y = \frac{1-x}{1+x}$? On remarque que $x = \frac{1-y}{1+y}$ (la fonction est involutive), donc $\left(\frac{1-y}{1+y}\right)^3 - \left(\frac{1-y}{1+y}\right) - 1 = 0$, soit : $(1-y)^3 - (1-y)(1+y)^2 - (1+y)^3 = 0$. L'équation en y s'écrit donc : $-y^3 + y^2 - 7y - 1$, la somme de ses racines vaut 1.

Autre méthode : on aurait aussi pu tout mettre au même dénominateur, développer en haut et en bas, et tout exprimer en fonction des polynômes symétriques élémentaires.

<u>*Solution de l'exercice 29*</u>

Puisque nous sommes chez les polynômes, débarassons-nous de ces vilaines racines. $a, c, -b, -d$ sont racines de $X^4 - 8X^2 + X + 11$. Donc $abcd = bd \times (-a) \times (-c) = 11$ et on a fini... eh non ! pour être sûr d'avoir les quatre racines du polynôme (dont le produit des opposés fait le terme constant) sans avoir de problème de multiplicité, il serait bien de pouvoir montrer que ces quatre racines sont distinctes. a, c sont positives, $-b, -d$ sont négatives. Si $a = c$,

$\sqrt{5-a} = -\sqrt{5-a} = 0$. Donc $a = 5$, et en partant de l'énoncé, $a = \sqrt{4} = 2$, contradiction. Donc $a \neq c$, $b \neq d$ de même et on a bien le résultat voulu.

Solution de l'exercice 30 On écrit P sous la forme $P(X) = Q(X)(X-a)(X-b)(X-c)(X-d)+5$, et on suppose par l'absurde que $P(k) = 8$. Alors $Q(k)(k-a)(k-b)(k-c)(k-d) = 13$. Or $(k-a)$, $(k-b)$, $(k-c)$ et $(k-d)$ sont des entiers distincts, et comme 3 est premier, il ne peut pas être écrit comme produit de 4 entiers distincts, contradiction.

Solution de l'exercice 31
Avec $x = 1$, on a $P(2) = 0$. Puis $x = 2$ donne $P(4) = 0$. De même, $P(8) = P(16) = 0$. On peut ainsi écrire $P(X) = (X-2)(X-4)(X-8)(X-16)Q(X)$. En réinjectant dans l'équation, on trouve $Q(x) = Q(2x)$ pour tout x (sauf $x = 2, 4, 8, 16$), donc $Q(X) - Q(2X)$ est le polynôme nul.
Si $r \neq 0$ est racine de Q, $2^n r$ l'est aussi pour tout $n \in \mathbb{N}$, donc $Q = 0$ ou $r = 0$. Donc $Q(X) = aX^k$, et il est facile de voir que $k = 0$. Donc Q est constant.
On en déduit que $P = c(X-2)(X-4)(X-8)(X-16)$ avec c un réel. Réciproquement, ce genre de polynôme est bien solution.

Solution de l'exercice 32 On note $a = x^2 - x$. Si $a = 0$, $x = 0$ ou $x = 1$. Si, $a \leqslant -1$, l'équation $x^2 - x$ n'a pas de racines réelles, donc $a \geqslant 1$.

Montrons par récurrence que, pour tout $\ell \in \mathbb{N}$, $\ell \geqslant 3$, in existe deux entiers positifs A_ℓ et B_ℓ tels $A_\ell \geqslant 2$ et

$$x^\ell = A_\ell x + B_\ell.$$

Pour $\ell = 3$ on a $x^3 = (a+1)x + a$. Supposons le résultat vrai pour ℓ. Ainsi $x^\ell = A_\ell x + B_\ell$. D'où $x^{\ell+1} = (A_\ell + B_\ell)x + aA_\ell$. $A_{\ell+1} := A_\ell + B_\ell$ et $B_{\ell+1} = aA_\ell$ conviennent. Cela finit la récurrence.

Ainsi, pour $\ell = n$, on a $x^n = A_n x + B_n$. D'autre par, d'après l'énoncé, $x^n = x + b$ pour un b entier. Donc $x = \frac{b-B_n}{A_n-1}$. On peut diviser car $A_n \geqslant 2$. Ainsi $x \in \mathbb{Q}$.

Comme x vérifie $x^2 - x - a$ qui est à coefficients entiers, le dénominateur de x divise le coefficient de tête. Ainsi x est entier.

Solution de l'exercice 33
Reformulons classiquement et légèrement l'énoncé : on veut une racine réelle au polynôme $R(X) = P(X-1) - Q(X+1)$. A quoi peut-il ressembler ? Il est clairement de degré au plus 2013 (le coefficient du terme de degré 2014 étant nul). S'il est de degré 2013, donc impair, alors il aura bien une racine impaire. Regardons de plus près, en posant $P(X) = X^{2014} + aX^{2013} + S(X)$ et $Q(X) = X^{2014} + bX^{2013} + T(X)$, où S et T sont de degré au plus 2012. Soit de plus c le coefficient de degré 2013 de R. On obtient $c = -2014 - 2014 + a - b = a - b - 4028$ (on regarde, dans $(X-1)^{2014}$, le terme de degré 2013, et de même pour $(X+1)^{2014}$). Se posent deux questions : comment gérer ce $a - b$? Et à quoi sert la condition $P(x) \neq Q(x)$ pour tout x réel ? Heureusement, elles sont liées !
$P - Q$ n'a pas de racine réelle, donc n'est pas de degré impair. Or $P - Q$ est de degré au plus 2013, et le coefficient du terme de degré 2013 est $a - b$. Donc $a - b = 0$.
Ainsi $c \neq 0$, et R est bien de degré 2013, ce que l'on voulait.

Solution de l'exercice 34 En injectant $a = b = c = 0$, on trouve $P(0) = 0$. En prenant $b = c = 0$, on obtient $P(2a) = 3P(a) + P(-a)$, et ce pour tout a. On suppose P de degré n. En examinant les coefficients dominants, on obtient $2^n = (-1)^n + 3$, donc n vaut 1 ou 2, et P est de la forme $aX^2 + bX$. On vérifie réciproquement que ces polynômes conviennent.

Solution de l'exercice 35
En $+\infty$ et $-\infty$, le polynôme tend vers $+\infty$ car de degré pair. Pour avoir une racine réelle, il

suffit que le polynôme soit négatif a un moment, le pauvre sera bien obligé de passer par zéro. Si Alcina met un coefficient c devant x^3, Bajazet met un nombre négatif c' de valeur absolue assez grande devant x^2 de sorte que $x^4+cx^3+c'x^2+1$ soit strictement négatif en 1 et -1. Alors si Alcina met un coefficient positif (ou négatif) devant x, $P(-1)$ sera encore strictement négatif (ou $P(1)$), donc Bajazet gagne. De même si Alcina joue d'abord sur x.
Si Alcina met un coefficient c devant x^2, c'est un petit peu plus compliqué puisqu'on ne peut plus rendre le polynôme négatif en un réel et son opposé. On va alors se focaliser sur la taille des monômes en fonction de celle de x (pour lequel on choisit une valeur > 1. Posons $D = 10^4+c10^2+1$, $D' = 5^4+c5^2+1$. Bajazet place b devant x^3, et Alcina place a devant x. On a $P(10) + P(-10) = 2D$ (les termes impairs s'annulent, les pairs s'ajoutent). Si P est toujours positif, avec $b = -D$, on trouve $a > 99D$. Donc $P(-5) = D' + 125D - 5 \times 99D < -2D'$ car $D > D'$. Or $P(5) + P(-5) = 2D'$ donc $P(5) < 0$ et Bajazet gagne avec ce choix de b.

<u>*Solution de l'exercice 36*</u> Supposons par l'absurde qu'il existe $Q, R \in \mathbb{Z}[X]$ non constants tels que $P = QR$. Alors $P(a_i) = Q(a_i)R(a_i) = -1$ donc $Q(a_i) = \pm 1$ et $R(a_i) = -Q(a_i)$ soit $(Q+R)(a_i) = 0$. Comme Q et R sont de degrés strictement inférieurs à n, on obtient $Q+R = 0$ donc $P = -Q^2$, donc P est négatif sur les réels. Ceci est absurde car P tend vers $+\infty$ en $+\infty$.

<u>*Solution de l'exercice 37*</u> L'inégalité est équivalente, après multiplication par $Q(x)^2 = (\prod_{k=1}^{70}(x-k))^2$ et passage du second membre dans le premier, à $P(x) \geqslant 0$ où $P(X) = Q(X)R(X)$ avec $R(X) = 4\sum_{k=1}^{70} k \prod_{1\leqslant i\neq k\leqslant 70}(X-i) - 5Q(X)$.

On remarque $R(1) < 0$, $R(2) > 0$, $R(3) < 0$, ..., $R(70) > 0$ et $R(+\infty) = -\infty$ donc R a pour racines les r_i tels que $1 < r_1 < 2 < r_2 < \cdots < 70 < r_{70}$, et P a pour racines les r_i et les entiers compris entre 1 et 70 inclus. Or P est négatif en $\pm\infty$ donc P est positif sur la réunion des intervalles $[k, r_k]$ pour $1 \leqslant k \leqslant 70$, dont la longueur totale vaut $\sum_{i=1}^{70}(r_i - i)$. Par les relations coefficients racines, on déduit du coefficient de X^{69} dans R que $\sum_{i=1}^{70} r_i = \frac{9}{5}\sum_{i=1}^{70} i$ donc la longueur totale des intervalles vaut $\frac{4}{5}\sum_{i=1}^{70} i = 1988$.

<u>*Solution de l'exercice 38*</u> Supposons par l'absurde que P n'est pas constant. Si z_0 est une racine, alors $z_0^2, z_0^4, \ldots$ sont aussi des racines. Si on a des racines $|z_0| < 1$ ou $|z_0| > 1$ alors P aurait une infinité de racines. Donc toute les racines sont de module 1.

L'équation s'écrit également $P((x+1)^2) = P(x+1)P(x)$. Donc si z_0 est une racine , alors $(z+1)^2$ est une racine aussi. Comme toute racine est de module 1, on a $|z_O + 1| = 1$. Pour chercher les nombres complexes qui vérifient $|z| = |z+1| = 1$ on pose $z = a + ib$. On trouve $a^2 + b^2 = 1 = a^2 + b^2 + 2a + 1$. Alors $a = \frac{-1}{2}$ et $b = \pm\frac{\sqrt{3}}{2}$. Donc $P(x) = (x-\epsilon)^a(x-\frac{1}{\epsilon})^b$ pour $\epsilon = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$. Comme $P \in \mathbb{R}[x]$, $a = b$, donc $P = (x^2+x+1)^a$. Réciproquement tout polynôme de ce type convient.

<u>*Solution de l'exercice 39*</u> Soit p_0 et p_1 le nombre de racines distinctes respectivement de P et $P-1$. Soit n le degré de P, qu'on peut supposer par symétrie supérieur ou égal à celui de Q. Comme P et $P-1$ sont premiers entre eux, ils n'ont aucune racine commune. On remarque que $P - Q = (P-1) - (Q-1)$, donc ce polynôme admet comme racines à la fois les racines de P et celles de $P-1$, donc $p_0 + p_1$ racines. Il suffit de montrer que ce nombre est strictement supérieur à n pour conclure que $P - Q$ est le polynôme nul, soit $P = Q$.

Pour cela, on étudie les racines multiples en considérant le polynôme dérivé $P' = (P-1)'$. Soit $D_0 = \gcd(P, P')$ et $D_1 = \gcd(P-1, P')$. On sait que $\deg(D_i) = n - p_i$. Par ailleurs, D_0 et D_1 sont premiers entre eux car P et $P-1$ le sont, et divisent P' donc D_0D_1 divise P' d'où en considérant les degrés : $n - p_1 + n - p_2 \geqslant n - 1$ soit $p_0 + p_1 > n$, $\square$.

<u>*Solution de l'exercice 40*</u> On pose $P(x) - \Pi_{j=1}^{n}(x+b_j) - c$. D'après l'hypothèse $a_1, \dots, a_n$ sont racines de P. Comme P est unitaire, $P = \Pi_{i=1}^{n}(x - a_i)$. Soit j un indice de colonne. Le produit de $\Pi_{i=1}^{n}(b_j + a_i)$ vaut $(-1)^n P(-b_j) = -c$. Comme c ne dépend pas de j, les produits des colonnes sont tous égaux.

<u>*Solution de l'exercice 41*</u> On remarque tout d'abord, en prenant $b = c = 0$, que P est pair, et ne contient donc que des termes de degré pair. En évaluant en zéro, on trouve que le terme constant doit être nul. On essaie ensuite $a = 6x$, $b = 3x$ et $c = -2x$. Cela donne $P(3x)+P(5x)+P(-8x) = 2P(7x)$. On note n le degré de P. En comparant les coefficients dominants, on trouve $3^n + 5^n + (-8)^n = 2 \cdot 7^n$. C'est impossible pour $n \geqslant 5$. P est donc de la forme $aX^4 + bX^2$. On vérifie réciproquement que ces polynômes conviennent.

<u>*Solution de l'exercice 42*</u> Notons $c_n(k)$ le nombre de permutations de longueur n. Pour résoudre l'exercice, nous établissons une relation de récurrence sur les $c_n(k)$. Nous allons, pour cela, dénombrer les permutations $\sigma \in \mathfrak{S}_n$ tel que $\mathrm{cyc}(\sigma) = k$ en les comptant séparément selon la valeur de $\sigma(n)$. Si $\sigma(n) = n$, on remarque que se donner une telle permutation revient simplement à se donner une permutation de $\{1, \dots, n-1\}$ ayant $(k-1)$ cycles (puisque n est tout seul dans son cycle). Il y a donc $c_{n-1}(k-1)$ permutations qui relèvent de ce cas.

Examinons maintenant le cas où $\sigma(n)$ est un entier m fixé strictement inférieur à n. L'entier n apparaît alors dans un cycle de σ qui est de longueur au moins 2 (puisqu'il contient au moins n et m) et on peut construire une permutation τ de $\{1, \dots, n-1\}$ simplement en retirant n de ce cycle et en laissant les autres cycles inchangés. Par construction, il est évident que τ a encore k cycles. Par ailleurs, on peut reconstruire σ à partir de τ et l'entier m comme suit : on regarde le cycle de τ qui contient m et, dans ce cycle, on insère l'entier n juste avant m. On déduit de cela qu'il y a $c_{n-1}(k)$ permutations à k cycles telles $\sigma(n)$ est égal à un entier $m < n$ fixé.

En mettant ensemble les deux raisonnements précédents, on aboutit à $c_n(k) = c_{n-1}(k-1) + (n-1)c_{n-1}(k)$. En tenant compte du fait que $c_{n-1}(0) = c_{n-1}(n) = 0$ trivialement, et en sommant l'égalité précédente pour k variant de 1 à n, il vient :

$$P_n(x) = \sum_{k=1}^{n} c_n(k)x^k = \sum_{k=1}^{n-1} c_{n-1}(k)x^{k+1} + (n-1) \cdot \sum_{k=1}^{n-1} c_{n-1}(k)x^k = (x+n-1) \cdot P_{n-1}(x).$$

<u>*Solution de l'exercice 43*</u> L'hypothèse sur les coefficients impairs nous donne envie de réduire modulo 2 : si on note $\overline{P}$ le réduit de P modulo 2, on a $\overline{P} = X^n + ... + X + 1$ et, dans $\mathbb{Z}/2\mathbb{Z}[X]$, $(X-1)2^k$ divise $\overline{P}$ si $m \geqslant 2^k$, i.e $(X+1)^{2^k} | X^n + ... + X + 1$.

Or, $(X+1)^{2^k} = \sum_{i=0}^{2^k} \binom{2^k}{i} X^i$ et pour $i \neq 0, 2^k$ on a d'après la formule de Legendre :

$$v_2\left(\binom{2^k}{i}\right) = \sum_{j=0}^{k} \lfloor \frac{2^k}{2^j} \rfloor - \lfloor \frac{i}{2^j} \rfloor - \lfloor \frac{2^k - i}{2^j} \rfloor \geqslant 1 - \lfloor \frac{i}{2^k} \rfloor - \lfloor \frac{2^k - i}{2^j} \rfloor = 1$$

donc dans $\mathbb{Z}/p\mathbb{Z}$, $(X+1)^{2^k} = X^{2^k}+1$ divise $\overline{P}$. On pose donc $\overline{P} = (X^{2^k}+1)Q$: comme $\overline{P} \neq X^{2^k}+1$, on a $n > m$. Mais alors, pour faire apparaître le coefficient X^{2^k-1} en développant le produit, il faut que Q ait un coefficient non nul devant X^{2^k-1}, soit $\deg(Q) \geqslant 2^k - 1$, d'où $\deg(P) = \deg(\overline{P}) \geqslant 2^{k+1} - 1$.

<u>*Solution de l'exercice 44*</u> On remarque $w(P \pm Q) \leqslant w(P) + w(Q)$ (inégalité triangulaire), et en ce qui concerne la multiplication, si $\deg(P) < k$ alors $w((1+X^k)P) = w(P) + w(PX^k) = 2w(P)$ $(*)$.

En calculant $w(Q_i)$ pour des i petits, on remarque l'égalité polynômiale dans $\mathbb{Z}/2\mathbb{Z}$ suivante, qui est démontrée dans l'exercice précédent : $(1+X)^{2^k} \equiv 1+X^{2^k}[2]$. Cela nous permet de simplifier le calcul de w, car si $i = 2^k+i'$ avec $i' < 2^k$, $w(Q_i) = w((1+X^{2^k})(1+X)^{i'}) = 2w(Q_{i'})$. Cela va nous permettre de procéder par récurrence sur i_n.

On suppose le résultat acquis pour $i_n < N$ et on considère le cas $i_n = N$. Soit k tel que $2^k \leqslant N < 2^{k+1}$. Si $i_1 \geqslant 2^k$, posons $i_l = 2^k + i'_l$, alors d'après le calcul précédent, $w(Q_{i_1} + \cdots + Q_{i_n}) = 2w(Q_{i'_1} + \cdots + Q_{i'_n})$, $w(Q_{i_n}) = 2w(Q_{i'_n})$ et par hypothèse de récurrence, $w(Q_{i'_1} + \cdots + Q_{i'_n}) \geqslant w(Q_{i'_1})$ donc en multipliant par 2, on obtient $w(Q_{i_1} + \cdots + Q_{i_n}) \geqslant w(Q_{i_1})$.

Si $i_1 < 2^k$ soit r tel que $i_r < 2^k \leqslant i_{r+1}$, alors $w(Q_{i_1} + \cdots + Q_{i_n}) = w(\sum_{1\leqslant l\leqslant r} Q_{i_l} + \sum_{r<l\leqslant n} Q_{i'_l}) + w(\sum_{r<l\leqslant n} Q_{i'_l}) \geqslant w(\sum_{1\leqslant l\leqslant r} Q_{i_l}) \geqslant w(Q_{i_1})$ en appliquant successivement la remarque $(*)$, l'inégalité triangulaire, et l'hypothèse de récurrence, ce qui conclut.

<u>*Solution de l'exercice 45*</u> Si (n, m) est un tel couple, soit $P_n(X) = X^n+X^2-1$ et $P_m(X) = X^m+X-1$, alors le reste R dans la division euclidienne de P_m par P_n est de degré strictement inférieur à n, et s'il est non nul, pour une infinité d'entiers k, $P_n(k)$ divise $R(k)$ et $|P_n(k)| \leqslant |R(k)|$, ce qui est impossible car P_n domine R d'où $R = 0$ et P_n divise P_m. En travaillant modulo $X^n + X^2 - 1$, on a $\frac{X^n}{1+X} \equiv 1 - X$ ($1 + X$ est inversible car -1 n'est pas racine de $X^n + X^2 - 1$) et $X^m + X - 1 \equiv 0$ donc $X^m \equiv 1 - X$, d'où $X^{m+1} + X^m - X^n \equiv 0$ d'où $P_k(X) = X^{k+1} + X^k - 1$ est divisible par P_n où $k = m - n$. Si $k + 1 = n$ alors P_n divise $P_k - P_n = X^{n-1} - X^2$ donc $n = 3$, et $m = 5$ qui convient. Sinon, $k \geqslant n$, et pour $x \in]0; 1[$ $x^{k+1} < x^n$ et $x^k < x^2$ car $n > 2$, d'où $P_k(x) < P_n(x)$, ce qui absurde car $P_n(0) = -1$ et $P_n(1) = 1$ donc P_n a une racine sur $]0; 1[$ que P_k ne partage pas.

Ainsi, seul le couple $(3, 5)$ convient.