Feuille d'exercices - Chapitre 19

Si rien n'est précisé, les polynômes sont supposés à coefficients dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et on pourra si besoin identifier polynômes et fonctions polynomiales.

Vrai ou Faux ?

1. Soit $P \in \mathbb{R}[X]$. Si P est de degré 2 alors $P + X^2$ aussi.
2. $x^2 + x + 1 \in \mathbb{R}_2[X]$.
3. $x^2 + x + 1 \in \mathbb{R}_3[X]$.
4. $x \mapsto x^2 + x + 1 \in \mathbb{R}_3[X]$.
5. $X^2 + X + 1 \in \mathbb{R}_3[X]$.
6. PQ' et QP' ont même degré.
7. Si P' est scindé alors P est scindé.
8. $2X$ est un diviseur de X.
9. Un polynôme constant est de degré nul.
10. $X - 2$ divise $X^5 - 3X^4 - 2X^3 + 3X^2 + 7X + 6$.
11. Si les seules racines complexes de P sont 0 et 1 alors $P = X(X - 1)$.
12. Si P et Q sont dans $\mathbb{C}[X]$, si $\deg P \leq \deg Q$ et si toutes les racines de P sont racines de Q alors P divise Q.
13. $-j$ est racine de $X^2 - X + 1$.
14. Si j est racine de $P \in \mathbb{R}[X]$ alors j^2 est aussi racine de P.

1 Racines, rigidité

Exercice 1 : ✪ Montrer qu'il existe un unique $P \in \mathbb{R}_n[X]$ tel que pour tout $k \in [\![0\,;\, n]\!], P(k) = k^n$.

Correction : Par analyse-synthèse.

Existence : $P = X^n$ convient.
Unicité : Soit $Q \in \mathbb{R}_n[X]$ un autre polynôme qui convient. Alors P et Q coïncident en $0, \ldots, n$ donc en $n + 1$ points. Puisqu'ils sont de degré inférieur ou égal à n, ils sont égaux. Ce résultat n'étant pas explicitement au programme, on peut dire que $P - Q$ a $n + 1$ racines distinctes et qu'il est de degré inférieur ou égal à n donc est égal au polynôme nul, ce qui permet de conclure.

Exercice 2 : ✪ Soient P, Q deux polynômes tels que pour tout réel $x, P(x)\sin(x) + Q(x)\cos(x) = 0$. Montrer que P et Q sont nuls.

Correction : Montrons que P et Q admettent une infinité de racines. Attention, une somme de termes peut être nulle sans qu'aucun terme soit nul (on pourra se demander combien font $1 - 1$). L'idée est d'abord d'annuler le sinus : on aura alors $Q(x)\cos(x) = 0$, et puisque le cosinus et le sinus ne s'annulent pas en même temps, on aura forcément $Q(x) = 0$. Montrons cela de façon plus précise.

Pour tout $n \in \mathbb{Z}$, $0 = P(2n\pi)\sin(2n\pi) + Q(2n\pi)\cos(2n\pi) = Q(2n\pi)$: Q admet une infinité de racines donc Q est le polynôme nul. Ainsi, pour tout $x \in \mathbb{R}$, $P(x)\sin(x) = 0$. On pourrait recommencer (avec les réels de la forme $\frac{\pi}{2} + 2n\pi$) mais changeons de méthode : pour tout $x \in]\,0\,;\pi\,[$, $\sin(x) \neq 0$ donc $P(x) = 0$. Comme P est nul sur $]\,0\,;\pi\,[$, P admet une infinité de racines donc P est le polynôme nul.

Exercice 3 : ✪ Soient P et Q deux polynômes tels que pour tout $n \in \mathbb{N}, P\left(n^2\right) = Q\left(n^2\right)$. Montrer que $P = Q$.

Correction : Pour $n = 0$, cela donne $P(0) = Q(0)$. Pour $n = 1$, cela donne $P(1) = Q(1)$, mais pour $n = 2$, cela donne $P(4) = Q(4)$, pas $P(2) = Q(2)$! A priori, P et Q ne sont pas égaux en 2. Les polynômes P et Q coïncident sur l'ensemble des carrés parfait qui est un ensemble infini donc sont égaux (si on ne veut pas exploiter ce résultat, on peut dire que $P - Q$

s'annule en tous les carrés parfait, il a une infinité de racines donc est égal au polynôme nul, donc $P = Q$).

Exercice 4 : ✪

1. Soit $n \geq 2$. Donner la multiplicité de la racine $a \neq 0$ de $P = (X-a)^n - (X^n - a^n)$.
2. **Remake :** Donner la multiplicité de 1 en tant que racine de $P = X^{10} - 25X^6 + 48X^5 - 25X^4 + 1$.
3. Soit $n \geq 1$. Trouver les complexes a et b tels que $(X-1)^2$ divise $aX^{n+1} + bX^n + 1$.

Correction : Rappelons que la multiplicité de x_0 en tant que racine de P est le plus petit n tel que $P^{(n)}(x_0) \neq 0$. Par exemple, x_0 est racine triple si et seulement si $P(x_0) = P'(x_0) = P''(x_0) = 0 \neq P^{(3)}(x_0)$.

1. $P(a) = 0$ donc a est racine de P. De plus, $P' = a(X-a)^{n-1} - nX^{n-1}$ si bien que $P'(a) = -na^{n-1} \neq 0$ puisque a est non nul donc a est racine simple de P.
2. $P(1) = 0$ (soit en faisant le calcul, soit en se souvenant que 1 est racine si et seulement si la somme des coefficients est nulle). De plus, $P' = 10X^9 - 150X^5 + 240X^4 - 100X^3$ donc on a aussi $P'(1) = 0$: 1 est racine AU MOINS double (ou est racine multiple). On a aussi $P'' = 90X^8 - 750X^4 + 960X^3 - 300X^2$ donc $P''(1) = 0$. Continuons : $P^{(3)} = 720X^7 - 3000X^3 + 2880X^2 - 600X$ et donc on a encore $P^{(3)}(1) = 0$. Encore : $P^{(4)}(X) = 5040X^6 - 9000X^2 + 5760X - 600$ et là ça ne marche plus, $P^{(4)}(1) \neq 0$ donc 1 est racine de multiplicité 4.
3. On cherche a et b pour que 1 soit racine AU MOINS double : c'est le cas si et seulement si $P(1) = P'(1) = 0$ si et seulement si $a + b + 1 = 0$ et $(n+1)a + nb = 0$. On trouve $a = n$ et $b = -(n+1)$.

Exercice 5 : ✪ Soit $P \in \mathbb{R}[X]$ de degré n et soit $a \in \mathbb{R}$ tel que $P(a), P'(a), \ldots, P^{(n)}(a)$ soient strictement positifs. Montrer que P ne s'annule pas sur $[\,a\,;+\infty\,[$.

Correction : D'après la formule de Taylor pour les polynômes (P est de degré n) :

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)(X-\alpha)^k}{k!}$$

En particulier, pour tout $x \geq \alpha$,

$$P(x) = P(\alpha) + \sum_{k=1}^{n} \frac{P^{(k)}(\alpha)(x-\alpha)^k}{k!}$$

$P(\alpha) > 0$ et les termes de la sommes sont positifs donc $P(x) > 0$.

Exercice 6 : ✪

1. Soient $(m,n,p) \in \mathbb{N}^3$. Montrer que $X^2 + X + 1$ divise $X^{3m+2} + X^{3n+1} + X^{3p}$.
2. **Remake :** Soit $n \in \mathbb{N}$ et soit $P_n \in \mathbb{C}[X]$ défini par $P_n = X^n + 1$. Pour quelles valeurs de n P_n est-il divisible par X^2+1 ?

Correction :

1. Puisque $X^2 + X + 1 = (X-j)(X-j^2)$, pour prouver que $X^2 + X + 1$ divise $X^{3m+2} + X^{3n+1} + X^{3p}$, il suffit de prouver que j et j^2 sont racines de ce polynôme (c'est un résultat de cours : si on a des racines distinctes $a_1, \ldots, a_n$, alors $(X-a_1)\ldots(X-a_n)$ divise le polynôme, cela vient du fait que les $X - a_i$ sont premiers entre eux deux à deux). Rappelons que $j^k = 1$ si $k \equiv 0[3]$, $j^k = j$ si $k \equiv 1[3]$ et $j^k = j^2$ si $k \equiv 2[3]$, et que $1 + j + j^2 = 0$. Dès lors :

$$\begin{aligned} j^{3m+2} + j^{3n+1} + j^{3p} &= j^2 + j + 1 \\ &= 0 \end{aligned}$$

   donc j est racine de $X^{3m+2} + X^{3n+1} + X^{3p}$. On montrerait aisément que j^2 est aussi racine de ce polynôme, mais c'est inutile : il est à coefficients réels et j est racine donc $\overline{j} = j^2$ est aussi racine, ce qui permet de conclure.
2. Puique $X^2 + 1 = (X-i)(X+i)$, X^2+1 divise $X^n + 1$ si et seulement si i et $-i$ sont racines de P_n. Mais puisque P_n est à coefficients réels, i est racine de P_n si et seulement si $\overline{i} = -i$ l'est aussi. En conclusion, $X^2 + 1$ divise P_n si et seulement si i est racine de P_n donc si et seulement si $i^n + 1 = 0$. Dès lors :

$$\begin{aligned} i^n + 1 = 0 &\iff i^n = -1 \\ &\iff e^{in\pi/2} = e^{i\pi} \\ &\iff n\pi/2 \equiv \pi[2\pi] \\ &\iff n \equiv 2[4] \end{aligned}$$

Les entiers n qui conviennent sont donc les entiers congrus à 2 modulo 4 ce qui se voit très bien sur le cercle trigo : les puissances de i successives sont $1, i, i^2 = -1$ et $i^3 = -i$ et on recommence : on se trouve en -1 pour les entiers congrus à 2 modulo 6.

Exercice 7 : ✪ Soit $P \in \mathbb{R}[X]$. Montrer que P est monotone à partir d'une certaine valeur réelle.

Correction : Si P est constant alors P est monotone. Si $\deg(P) = 1$ alors P est strictement monotone. Supposons à présent que P soit de degré $n \geq 2$. Alors $\deg(P') = n-1$ donc P' a un nombre fini de racines (au plus $n-1$). Alors il existe $A \in \mathbb{R}$ tel que P' ne s'annule pas sur $]\,A\,;+\infty\,[$ (soit P' n'admet pas de racines et alors P' ne s'annule pas sur $\mathbb{R}$, soit P' admet un nombre fini de racines, et alors, si on pose A la plus grande des racines de P', ce qui est possible car il y en a un nombre fini, alors P' ne s'annule pas sur $]\,A\,;+\infty\,[$). Puisque P' est un polynôme, c'est une fonction continue donc P' est de signe constant (raisonnement classique à savoir faire). Finalement, soit P' est strictement positive sur $]\,A\,;+\infty\,[$, et alors P est strictement croissante sur cet intervalle, soit P' est strictement négative sur $]\,A\,;+\infty\,[$, et alors P est strictement décroissante.

Exercice 8 : ✪ Montrer qu'il n'existe pas de polynôme $P \in \mathbb{Z}[X]$ non constant tel que, pour tout $n \in \mathbb{Z}$, $P(n)$ soit un nombre premier.

Correction : Supposons qu'un tel polynôme P existe. Notons-le $P = a_n X^n + \cdots + a_1 X + a_0$ avec $n \geq 1$ et $a_n \neq 0$ (il est supposé non constant donc de degré supérieur ou égal à 1). Alors $P(0) = a_0$ est premier. Par conséquent, $P(a_0)$ est aussi premier mais on a :

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

c'est-à-dire que $a_0 | P(a_0)$. Or, $P(a_0)$ est premier et est divisible par a_0 premier donc $P(a_0) = a_0$. De même, pour tout $k \geq 1$, $P\left({a_0}^k\right)$ est divisible par a_0 donc est égal à a_0. a_0 est premier donc $a_0 \geq 2$: les ${a_0}^k$ sont tous distincts, P et le polynôme constant égal à a_0 coïncident en une infinité de points donc sont égaux, et en particulier P est constant, ce qui est absurde.

Exercice 9 : ✪ Soient $P \in \mathbb{C}[X]$ et $n \in \mathbb{N}^*$. Montrer que si $P(X^n)$ est divisible par $X-1$ alors il l'est aussi par $X^n - 1$.

Correction : Supposons que $X-1$ divise $P(X^n)$: il en découle que 1 est racine de $P(X^n)$ donc que $P(1^n) = P(1) = 0$. Par conséquent, pour tout $k \in [\![\, 0\,;\, n-1 \,]\!]$, si on pose $\omega = e^{2ik\pi/n}$ une racine n-ième de l'unité, $0 = P(1) = P(\omega^n)$ donc ω est racine de $P(X^n)$. Les $e^{2ik\pi/n}$ étant deux à deux distincts, $P(X^n)$ est divisible par

$$\prod_{k=0}^{n} (X - e^{2ik\pi/n}) = X^n - 1$$

Exercice 10 : ✪ Soient p et q deux entiers supérieurs ou égaux à 2 premiers entre eux. Montrer que $(X^p-1)(X^q-1)$ divise $(X-1)(X^{pq}-1)$.

Correction : On a tout d'abord :

$$(X^p-1)(X^q-1) = \prod_{k=0}^{p-1} (X - e^{2ik\pi/p}) \times \prod_{k=0}^{q-1} (X - e^{2ik\pi/q})$$

Cherchons les racines communes de ces deux polynômes. Soit z une racine des deux polynômes X^p-1 et X^q-1 : z est donc à la fois une racine p-ième et une racine q-ième de l'unité et donc il existe $k_1 \in [\![\, 0\,;\, p-1 \,]\!]$ et $k_2 \in [\![\, 0\,;\, q-1 \,]\!]$ tels que

$$z = e^{2ik_1\pi/p} = e^{2ik_2\pi/q}$$

Par conséquent : $2k_1\pi/p \equiv 2k_2\pi/q [2\pi]$ si bien que $qk_1 \equiv pk_2 [pq]$: il existe n tel que $qk_1 = pk_2 + npq$: q divise donc pk_2 et puisque $p \wedge q = 1$, alors q divise k_2 mais $k_2 \in [\![\, 0\,;\, q-1 \,]\!]$ donc $k_2 = 0$ donc $z = 1$: 1 est la seule racine commune de ces deux polynômes. En d'autres termes, dans la factorisation ci-dessus, on trouve $(X-1)$ deux fois et tous les autres termes une seule fois. Or, 1 est racine de $X^{pq}-1$ donc 1 est racine double de $(X-1)(X^{pq}-1)$ si bien que ce polynôme est divisible par $(X-1)^2$. De plus, les autres racines p-ièmes et q-ièmes de l'unité sont racines de $X^{pq}-1$: en effet, si ω est racine p-ième de l'unité (idem pour les racines q-ièmes), alors $\omega^p = 1$ donc $\omega^{pq} = 1^q = 1$ donc ω est racine de $X^{pq}-1$. Toutes ces racines étant distinctes, $X^{pq}-1$ est divisible par

$$\prod_{k=1}^{p-1} (X - e^{2ik\pi/p}) \times \prod_{k=1}^{q-1} (X - e^{2ik\pi/q})$$

donc $(X-1)(X^{pq}-1)$ est divisible par

$$(X-1)^2\prod_{k=1}^{p-1}(X-e^{2ik\pi/p})\times\prod_{k=1}^{q-1}(X-e^{2ik\pi/q})=(X^p-1)(X^q-1)$$

Exercice 11 : ✪ Soit $(P,Q,R)\in\mathbb{R}[X]^3$ tel que $Q\circ P=R\circ P$. Montrer que si P n'est pas constant alors $Q=R$.

Correction : P n'étant pas constant, son image est infinie. En effet, P est une fonction continue (on identifie polynôme et fonction polynomiale), $P(\mathbb{R})$ est un intervalle d'après le TVI (l'image d'un intervalle par une fonction continue est un intervalle) donc est infini car n'est pas un singleton (puisque P n'est pas constant). Puisque $Q\circ P=Q\circ R$, Q et R coïncident sur $P(\mathbb{R})$ qui est un ensemble infini donc sont égaux.

Exercice 12 : ✪ Soit $P\in\mathbb{C}[X]$ tel que $P\left(X^2\right)=P(X)P(X+1)$.

1. Donner la valeur de P si P est constant. On suppose dans la suite que ce n'est pas le cas.
2. Montrer que P admet au moins une racine complexe a.
3. Montrer que a^2 est aussi racine de P.
4. En déduire que $a=0$ ou que a est une racine de l'unité.

Correction :

1. Supposons P constant solution égal à λ. Alors $\lambda=\lambda^2$ donc $\lambda=0$ ou 1, qui sont évidemment solutions (ne pas oublier la synthèse).
2. Découle du théorème de d'Alembert Gauß.
3. $P(a^2)=P(a)P(a+1)=0$ puisque a est racine de P.
4. En appliquant ce qui précède à a^2, $(a^2)^2=a^4$ est racine de P, puis $(a^4)^2=a^8$ racine de P etc. Par récurrence, on prouve que a^{2^n} (et pas $(a^2)^n=a^{2n}$) est racine de P pour tout n. P n'étant pas constant, il n'admet qu'un nombre fini de racines : d'après le principe des tiroirs, il existe deux termes (et même une infinité) de la forme a^{2^n} qui sont égaux : il existe $n_1<n_2$ tels que $a^{2^{n_1}}=a^{2^{n_2}}$. Soit $a=0$, et alors c'est bon, soit on peut simplifier par $a^{2^{n_1}}$ ce qui donne : $a^{2^{n_1}-2^{n_2}}=1$, a est une racine de l'unité.

Exercice 13 - Polynômes mystères : ✪

1. Le polynôme P est de degré 4 et vérifie $P(1)=P(2)=P'(2)=0$, $P(0)=4$ et $P(3)=1$. Qui est-il ?
2. Même question avec le polynôme Q de degré 2022, qui admet -3 pour racine d'ordre de multiplicité 794, 3 pour racine d'ordre de multiplicité 1227, 1 pour racine simple et dont le coefficient constant est 6^{2021}.

Correction :

1. P admet 1 comme racine (au moins) simple et 2 comme racine (au moins) double donc est divisible par $(X-1)(X-2)^2$: P étant de degré 4, il existe a et b tels que $P=(aX+b)(X-1)(X-2)^2$. Or, $P(0)=4$ donc $-4b=4$ si bien que $b=-1$. Enfin, $P(3)=1$ donc :

$$(3a-1)(3-1)(3-2)^2=1$$

   et on trouve donc que $(3a-1)\times 2=1$ ce qui donne $a=1/2$. Finalement, P est le polynôme $(X/2-1)(X-1)(X-2)^2$.
2. Par hypothèse, Q est divisible par $(X+3)^{794}(X-3)^{1227}(X-1)$ qui est de degré 2022. Q étant lui-même de degré 2022, si on note a son coefficient dominant (ne pas l'oublier !), $Q=a(X+3)^{794}(X-3)^{1227}(X-1)$. De plus, le coefficient constant, égal à $Q(0)$, vaut 6^{2021} donc :

$$a\times 3^{794}\times(-3)^{1227}\times(-1)=6^{2021}$$

   si bien que $a\times(-1)^{1228}\times 9^{2021}=a\times 9^{2021}=6^{2021}$. On en déduit que $a=(6/9)^{2021}=(2/3)^{2021}$ donc

$$Q=\left(\frac{2}{3}\right)^{2021}(X+3)^{794}(X-3)^{1227}(X-1)$$

Exercice 14 : ✪ Soient P et Q deux polynômes réels distincts. Montrer que :

$$(\exists A\in\mathbb{R},\forall t\geq A,P(t)<Q(t))\qquad\text{ou}\qquad(\exists A\in\mathbb{R},\forall t\geq A,Q(t)<P(t))$$

Correction : $P-Q$ étant non nul, il n'admet qu'un nombre fini de racines donc ne s'annule pas à partir d'une certaine valeur A donc est de signe constant car est une fonction continue (on identifie polynôme et fonction polynomiale) : si $P-Q<0$ à partir de A, alors on est dans le premier cas, sinon on est dans le second cas.

Exercice 15 : ✪ Montrer qu'il n'existe pas de polynôme $P\in\mathbb{R}[X]$ tel que, pour tout $k\in\mathbb{N}^*$:

- $P(k) = 1/k$
- $P(k) = \sqrt{k^2+1}$
- $P(k) = 2^k$

Correction : Raisonnons à chaque fois par l'absurde et supposons qu'un tel polynôme existe.
- Si un tel polynôme P existe, alors pour tout $k \geq 1$, $kP(k) = 1$: en d'autres termes, le polynôme $Q = XP - 1$ s'annule en tout $k \geq 1$ donc admet une infinité de racines donc est le polynôme nul si bien que $XP = 1$ ce qui est absurde car le degré de XP ne peut pas être égal à 0 : si $P = 0$ alors $XP = 0$ et sinon alors $\deg(XP) \geq 1$. Dans tous les cas on a l'absurdité voulue.
- Si un tel polynôme existe, de même, le polynôme $Q = P^2 - X^2 - 1$ est le polynôme nul car admet une infinité de racines donc $P^2 = X^2 + 1$. Or, il n'existe aucun polynôme dont le carré soit $X^2 + 1$. Supposons en effet qu'un tel polynôme P existe : puisque $\deg(P^2) = 2\deg(P) = 2$ alors P est de degré 1 : il existe a et b tels que $P = aX + b$ donc $P^2 = a^2X^2 + 2abX + b^2$ donc $a^2 = 1$ donc $a = \pm 1$, idem pour b, mais $2ab = 0$ donc $a = 0$ ou $b = 0$ ce qui est absurde.
- Le raisonnement précédent ne marche plus, il faut plutôt raisonner avec des croissances comparées. Supposons donc qu'un tel polynôme existe, alors la suite de terme général $P(n)/2^n$ est constante égale à 1. Cependant, par croissances comparées, les suites géométriques l'emportent sur les suites polynomiales donc cette suite tend en fait vers 0 ce qui est absurde.

Exercice 16 : ✪✪ Montrer de deux façons différentes qu'un polynôme réel de degré impair admet au moins une racine (réelle).

Correction : Première méthode : d'après le théorème de factorisation sur $\mathbb{R}$, P s'écrit comme un produit de polynômes de degré 1 ou de degré 2 de discriminant strictement négatif. Si, dans cette factorisation, on ne trouve que des polynômes de degré 2, alors $\deg(P)$ est pair, ce qui est absurde. Ainsi, P est divisible par un polynôme de degré 1. Or, un polynôme de degré 1 admet une racine donc P admet une racine.

Deuxième méthode : notons n le degré de n (impair) et a_n le coefficient dominant (non nul par définition). Alors $P(x) = a_n x^n + \dots$ donc $P(x) \xrightarrow[x\to+\infty]{} +\infty$ si $a_n > 0$ et $-\infty$ si $a_n < 0$, et c'est le contraire en $-\infty$ (car n est impair) et P est une fonction continue (on associe polynôme et fonction polynomiale) donc, d'après le TVI, P s'annule au moins une fois.

Exercice 17 : ✪✪ Montrer qu'il n'existe pas de polynôme $P \in \mathbb{C}[X]$ tel que pour tout $z \in \mathbb{C}, P(z) = \overline{z}$.

Correction : Supposons qu'il existe un polynôme P qui convient. Alors, pour tout $z \in \mathbb{R}$, $P(z) = z$ donc P et X coïncident sur $\mathbb{R}$ qui est un ensemble infini donc sont égaux si bien que $P = X$. En d'autres termes, pour tout $z \in \mathbb{C}$, $P(z) = z$ c'est-à-dire que $\overline{z} = z$ pour tout $z \in \mathbb{C}$ ce qui est absurde (prendre par exemple $z = i$).

Exercice 18 : ✪✪
1. Montrer qu'un polynôme $P \in \mathbb{C}[X]$ non constant est surjectif.
2. On cherche à présent tous les polynômes injectifs. Soit $P \in \mathbb{C}[X]$ injectif.
   (a) P peut-il être constant ?
   (b) Montrer que P a une unique racine complexe (éventuellement de multiplicité supérieure à 1) qu'on notera α. En déduire une expression de P sous forme factorisée.
   (c) Montrer que si $\deg(P) \geq 2$, le coefficient dominant de P admet au moins deux antécédents.
   (d) En déduire tous les polynômes injectifs.

Correction :
1. Soit $P \in \mathbb{C}[X]$ surjectif. Soit $a \in \mathbb{C}$. Alors $P - a$ est toujours non constant donc admet une racine d'après le théorème de d'Alembert-Gauß : il existe $z \in \mathbb{C}$ tel que $P(z) - a = 0$ i.e. tel que $P(z) = a$: a admet un antécédent par P, P est surjectif.
2. (a) Un polynôme constant ne peut pas être injectif puisqu'il prend une infinité de fois la même valeur.
   (b) D'après le théorème de d'Alembert-Gauß, P a au moins une racine complexe. Si P admet au moins deux racines distinctes, alors 0 admet au moins deux antécédents par P ce qui est absurde car P est injectif. Si on note z_0 cette unique racine, $n \geq 1$ le degré de P et $a_n \neq 0$ le coefficient dominant, alors $P = a_n(X - z_0)^n$.
   (c) Supposons donc $n \geq 2$. Soit $z \in \mathbb{C}$. Rappelons que $a_n \neq 0$ par définition d'un coefficient dominant.

$$\begin{aligned} P(z) = a_n &\iff (z - z_0)^n = 1 \\ &\iff z - z_0 \text{ est une racine } n\text{-ième de l'unité} \\ &\iff \exists k \in [\![0\,;\, n-1]\!], z - z_0 = e^{2ik\pi/n} \\ &= \exists k \in [\![0\,;\, n-1]\!], z = z_0 + e^{2ik\pi/n} \end{aligned}$$

Par conséquent, a_n admet exactement $n \geq 2$ antécédents distincts ce qui est absurde par injectivité de P. On en déduit que $n = 1$.

(d) Lors des questions précédentes, on était dans la phase « analyse » d'un raisonnement par analyse-synthèse, et on avait prouvé que les seuls polynômes injectifs possibles étaient les polynômes de degré 1. Synthèse : soit $P = aX+b$ de degré 1 avec $a \neq 0$. Soient z_1, z_2 tels que $P(z_1) = P(z_2)$. Alors $az_1 + b = a_2 + b$ donc $az_1 = a_2$ et $a \neq 0$ donc $z_1 = z_2$: P est injectif. En conclusion, les polynômes injectifs sont exactement les polynômes de degré 1.

Exercice 19 - Un classique : ✪ Soit $P \in \mathbb{R}[X]$ scindé.

1. On suppose que les racines de P sont simples. Montrer que P' est aussi scindé à racines simples.
2. ✪✪✪ Montrer que P' est scindé dans le cas général. On pourra penser à dériver P.
3. On vient donc de montrer que le polynôme dérivé d'un polynôme scindé (sur $\mathbb{R}$) est lui aussi scindé. Ce résultat est un grand classique. Voici trois exercices qui l'utilisent.
   (a) Soit $P \in \mathbb{R}[X]$ scindé. Montrer que si α est une racine multiple de P' alors α est racine de P.
   (b) Soit $\lambda \in \mathbb{R}^*$ et soit $P \in \mathbb{R}[X]$ scindé. Montrer que les racines (complexes) de $P^2 + \lambda^2$ sont simples.
   (c) Montrer que $X^3 + 1$ n'est pas scindé à racines simples sur $\mathbb{R}$. S'inspirer de cet exemple pour montrer qu'un polynôme réel scindé à racines simples ne peut pas avoir deux coefficients consécutifs nuls.

Correction :

1. Soit $n = \deg(P)$. Alors P admet exactement n racines réelles distinctes, puisqu'il est scindé à racines simples. Notons $x_1 < \cdots < x_n$ ses racines. En faisait comme dans le chapitre 15, i.e. en appliquant $n-1$ fois le théorème de Rolle, on trouve que P' admet au moins $n-1$ racines réelles distinctes. Or, $\deg(P') = n-1$ donc P' admet autant de racines réelles que son degré, et celles-ci sont distinctes : P' est scindé à racines simples.
2. Notons $n = \deg(P)$ et $k \leq n$ le nombre de racines réelles distinctes de P. Plus précisément, notons $x_1 < \cdots < x_k$ les racines réelles distinctes de P, de multiplicité respective $n_1, \ldots, n_k$ si bien que
$$P = a_n(X - x_1)^{n_1} \times \cdots \times (X - x_k)^{n_k}$$
On a en particulier $n = \deg(P) = n_1 + \cdots + n_k$. En appliquant encore une fois $k-1$ fois le théorème de Rolle, on obtient $k-1$ racines de P' qu'on peut noter $y_1, \ldots, y_{k-1}$ avec $y_1 \in]\, x_1 \,;\, x_2 \,[\,, \ldots, y_{k-1} \in]\, x_{k-1} \,;\, x_k \,[$. Or, x_1 est racine de multiplicité n_1 de P donc est racine de P' de multiplicité $n_1 - 1$, x_2 est racine de P de multiplicité n_2 donc est racine de P' de multiplicité $n_2 - 1$ etc. Les x_i forment donc des racines de P', et quand on les compte avec multiplicité, cela fait
$$(n_1 - 1) + \cdots + (n_k - 1) = (n_1 + \cdots + n_k) - k = n - k$$
nouvelles racines (distinctes des y_i puisque les y_i appartiennent aux intervalles ouverts). Cela donne $(n-k)+(k-1) = n-1$ racines réelles comptées avec multiplicité : on trouve encore que P' est scindé (mais pas forcément à racines simples).
3. (a) Dans la démonstration ci-dessus, les y_i (i.e. les racines obtenues avec le théorème de Rolle) sont forcément simples : en effet, si l'une au moins est racine double, alors cela donne trop de racines par rapport au degré de P'. Il en découle que les seules racines multiples éventuelles de P' se trouvent parmi les x_i, donc parmi celles qui sont déjà racines de P.
   (b) Soit $Q = P^2 + \lambda^2$, si bien que $Q' = 2PP'$. Oubli dans l'énoncé : il fallait supposer $P \in \mathbb{R}[X]$ scindé. Alors P' est scindé : ses racines sont donc en particulier toutes réelles, et donc les racines de Q' sont aussi toutes réelles. Or, Q n'a aucune racine réelle car est à valeurs strictement positives sur $\mathbb{R}$ (on assimile encore une fois polynôme et fonction polynomiale associée, ce qu'on ne s'est pas privé de faire d'ailleurs pour appliquer le théorème de Rolle) : Q et Q' n'ont donc aucune racine commune, les racines de Q sont toutes simples.
   (c) Si $X^3 + 1$ est scindé à racines simples, son polynôme dérivé également d'après la question 1, ce qui est absurde puisque son polynôme dérivé est $3X^2$ qui admet 0 comme racine double. Plus généralement, soit
$$P = a_n X^n + \cdots + a_{k+2} X^{k+2} + a_{k-1} X^{k-1} + \cdots + a_0$$
un polynôme admettant deux coefficients consécutifs nuls (il n'est dit nulle part que les autres sont non nuls, à part a_n). Si P est scindé à racines simples, alors P' l'est aussi et, par une récurrence finie immédiate, toutes ses dérivées jusqu'à l'ordre n le sont aussi. Or, la dérivée k-ième de P s'écrit
$$P = b_{n-k} X^{n-k} + \cdots + b_2 X^2$$
donc admet 0 comme racine double, ce qui est absurde.

Exercice 20 : ✪✪

1. (a) Soit f dérivable n fois sur $\mathbb{R}$. On suppose qu'il existe $a_1 < a_2 < \cdots < a_{n+1}$ tels que $f(a_1) = f(a_2) = \cdots = f(a_{n+1})$. Montrer qu'il existe $\alpha \in]\,a_1\,;a_{n+1}\,[$ tel que $f^{(n)}(\alpha) = 0$.

   (b) Soit $P \in \mathbb{R}[X]$ de degré n. Montrer que l'équation $P(x) = e^x$ admet au plus $n+1$ solutions.

2. ✪✪✪ Soit $P \in \mathbb{R}[X]$ non constant. Montrer que l'équation $P(x) = \sin(x)$ admet un nombre fini de solutions.

Correction :

1. (a) C'est l'exercice 51 du chapitre 14.

   (b) Raisonnons par l'absurde et supposons qu'elle admet au moins $n+2$ solutions, notées $x_1 < \cdots < x_{n+2}$. En d'autres termes, la fonction $g : x \mapsto P(x) - e^x$ s'annule en $n+2$ points. Puisqu'elle est dérivable $n+1$ fois, d'après la question 1, $g^{(n+1)}$ s'annule. Or, la dérivée $n+1$-ème de P est nulle donc la dérivée $n+1$-ième de g est la dérivée $n+1$-ième de l'exponentielle, c'est-à-dire l'exponentielle elle-même, ce qui est absurde puisqu'elle ne s'annule pas.

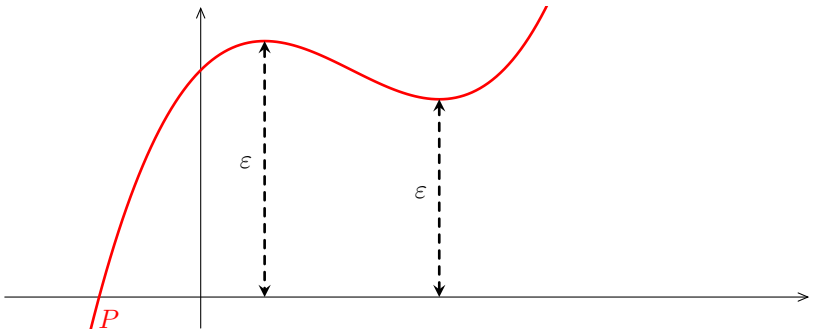
2. Le problème est que cela ne fonctionne plus ici puisque la fonction sinus et toutes ses dérivées s'annulent (et même une infinité de fois). L'idée est de borner l'ensemble des solutions éventuelles. Le polynôme P n'étant pas constant, il tend vers $\pm\infty$ en $\pm\infty$ (selon la parité du degré et le signe du coefficient dominant). En particulier, il existe A tel que, pour tout $x \notin [\,-A\,;A\,]$, $|P(x)| > 1$ donc les solutions éventuelles se trouvent sur $[\,-A\,;A\,]$. Supposons par l'absurde que l'équation $P(x) = \sin(x)$ possède un nombre infini de solutions sur cet intervalle. Notons k le nombre de fois que sin s'annule sur cet intervalle (k est fini car le sinus s'annule un nombre fini de fois sur un intervalle donné). Il en découle que $g : x \mapsto P(x) - \sin(x)$ s'annule au moins $4n+k+1$ fois (où $n = \deg(P)$) fois, si bien que, de même, $g^{(4n)}$ s'annule au moins $k+1$ fois. Or, $4n \geq n+1$ donc la dérivée $4n$-ième de P est nulle si bien que $g^{(4n)} = \sin^{(4n)}$ ce qui est absurde puisque le sinus s'annule au plus k fois sur $[\,-A\,;A\,]$.

Exercice 21 : ✪✪ Soit $P \in \mathbb{R}[X]$ de degré n. Montrer que le nombre de réels ε tels que $P+\varepsilon$ admette des racines multiples est inférieur ou égal à $n-1$. Illustrer par un dessin. En déduire qu'il existe $\alpha > 0$ tel que pour tout $\varepsilon \in]\,0\,;\alpha\,[$, $P+\varepsilon$ n'admette que des racines simples.

Correction : Soit $\alpha \in \mathbb{R}$ et soit $\varepsilon \in \mathbb{R}$. Notons $Q = P + \varepsilon$. Alors :

$$\begin{aligned} \alpha \text{ est racine multiple de } Q &\iff Q(\alpha) = Q'(\alpha) = 0 \\ &\iff \varepsilon = -P(\alpha) \qquad \text{et} \qquad P'(\alpha) = 0 \end{aligned}$$

Par conséquent, Q admet une racine multiple si et seulement s'il existe α racine de P' tel que $\varepsilon = -P(\alpha)$, et donc il y a au plus $n-1$ telles valeurs de ε puisque P' admet au plus $n-1$ racines réelles distinctes. Ci-dessous un dessin : on a une racine multiple quand la fonction coupe l'axe des abscisses avec une tangente horizontale, donc la seule façon d'obtenir une racine multiple « par translation verticale », i.e. en ajoutant un réel, est de soustraire l'image de l'un des points où la tangente est horizontale pour qu'elle coupe l'axe des abscisses en ce point :



En particulier, le nombre de tels ε est fini : si on note α le plus petit de ces $\varepsilon > 0$, alors il n'y a aucun ε dans $]\,0\,;\alpha\,[$ ce qui permet de conclure.

Exercice 22 : ✪✪ Soit $P \in \mathbb{C}[X]$ tel que pour tout x appartenant à $\mathbb{R}$, $P(x)$ soit réel. Montrer que $P \in \mathbb{R}[X]$. Penser au chapitre précédent (ou à l'exercice suivant).

Correction : Notons $P = a_n X^n + \cdots + a_0$. Pour tout $x \in \mathbb{R}$, $P(x) \in \mathbb{R}$ donc $\overline{P(x)} = P(x)$ i.e.

$$\begin{aligned} P(z) &= \overline{a_n x^n + \cdots + a_1 x + a_0} \\ &= \overline{a_n x^n} + \cdots + \overline{a_1 x} + \overline{a_0} \end{aligned}$$

Or, x est réel donc $\overline{x} = x$ si bien que

$$P(z) = \overline{a_n}x^n + \cdots + \overline{a_1}x + \overline{a_0}$$

c'est-à-dire que P et $\overline{a_n}X^n + \cdots + \overline{a_1}X + \overline{a_0}$ coïncident sur $\mathbb{R}$ qui est un ensemble infini donc sont égaux i.e. ont les mêmes coefficients. En d'autres termes, pour tout k, $a_k = \overline{a_k}$ i.e. $a_k \in \mathbb{R}$: les coefficients de P sont réels, $P \in \mathbb{R}[X]$.

Exercice 23 : ✪✪✪ Soit $P \in \mathbb{C}[X]$ de degré n tel qu'il existe $a_1, \ldots, a_{n+1}$ tels que $P(a_i) \in \mathbb{Q}$ pour tout $i \in [\![1\,;\,n+1]\!]$. Montrer que $P \in \mathbb{Q}[X]$. On pourra utiliser les polynômes de Lagrange.

Correction : Notons $b_1 = P(a_1), \ldots, b_n = P(a_n)$. Il existe au plus un polynôme de degré inférieur ou égal à n à coefficients dans $\mathbb{Q}$ (qui est un corps : on obtient le polynôme à l'aide de sommes, produits, quotients d'éléments du corps, cf. cours) et P convient donc ce polynôme est égal à P. En particulier, $P \in \mathbb{Q}[X]$. On aurait pu faire ce raisonnement dans l'exercice précédent.

Exercice 24 - Parce qu'il ne faut quand même pas rêver : ✪ Donner un polynôme $P \notin \mathbb{Z}[X]$ tel que $P(n) \in \mathbb{Z}$ pour tout $n \in \mathbb{Z}$.

Correction : $P = X(X+1)/2$ convient : que n soit pair ou impair, $P(n) \in \mathbb{Z}$. Le résultat sur les polynômes de Lagrange n'est pas valable car $\mathbb{Z}$ n'est pas un corps : on ne peut pas diviser sur $\mathbb{Z}$. Par contre, un tel polynôme est forcément à coefficients rationnels.

Exercice 25 : ✪✪

1. Donner tous les polynômes $P \in \mathbb{R}[X]$ vérifiant
$$\forall k \in \mathbb{N}, \quad \int_k^{k+1} P(t)\,\mathrm{d}t = k$$
2. Donner tous les polynômes $P \in \mathbb{R}[X]$ vérifiant
$$\forall k \in \mathbb{N}^*, \quad \int_k^{k+1} P(t)\,\mathrm{d}t = \frac{1}{k}$$

Correction :

1. Analyse : soit P un polynôme qui convient. Soit Q une primitive de P (une telle primitive existe car P est continue, encore une fois on assimile polynôme et fonction polynomiale : il est légitime d'introduire une primitive de P car on manipule des intégrales). Par conséquent, pour tout k, $Q(k+1) - Q(k) = k$. Par somme (on reconnaît un télescopage) :
$$\sum_{k=0}^{n-1} Q(k+1) - Q(k) = Q(n) = \sum_{k=0}^{n-1} k = \frac{n(n-1)}{2}$$
On en déduit que $Q(n) = \dfrac{n(n-1)}{2} + Q(0)$. Le polynôme Q et le polynôme $\dfrac{X(X-1)}{2} + Q(0)$ coïncident sur $\mathbb{N}$ qui est un ensemble infini donc sont égaux. En dérivant (rappelons que $P = Q'$) il vient : $P = X - 1/2$. Synthèse : il est immédiat que pour tout $k \in \mathbb{N}$,
$$\int_k^{k+1} \left(t - \frac{1}{2}\right) \mathrm{d}t = k$$
donc ce polynôme convient effectivement. Conclusion : $X - 1/2$ est l'unique solution.
2. Deux façons de prouver qu'il n'y a pas de solution. Supposons par l'absurde qu'il existe une solution. L'une est un copier-coller de ce qui précède mais utilise pour conclure un résultat que nous verrons au second semestre. On trouve donc de la même façon que pour tout n,
$$Q(n) - Q(1) = \sum_{k=1}^{n-1} \frac{1}{k}$$
Le problème est que le membre de droite n'est pas polynomial en k donc on ne peut pas conclure de la même façon. Nous verrons au second semestre que ce terme est équivalent (nous verrons aussi ce que ça veut dire au second semestre) à $\ln(n)$ donc que
$$Q(n) \sim \ln(n)$$
ce qui est absurde car $Q(n) \sim a_d n^d$ son terme de plus haut degré : absurde, un tel polynôme n'existe pas. Une autre solution consiste à dire qu'un polynôme est soit constant, soit diverge vers $\pm\infty$ en $+\infty$ (selon son coefficient dominant). S'il est constant égal à λ, alors

$$\int_k^{k+1} P(t)\,\mathrm{d}t = \lambda$$

pour tout k. S'il tend vers $+\infty$, pour t assez grand $P(t) \geq 1$ donc, par croissance de l'intégrale,

$$\int_k^{k+1} P(t)\,\mathrm{d}t \leq 1$$

et s'il tend vers $-\infty$, l'intégrale est inférieure à -1 pour k assez grand par un raisonnement analogue. Dans tous les cas, on ne peut pas avoir

$$\int_k^{k+1} P(t)\,\mathrm{d}t \xrightarrow[k\to+\infty]{} 0^+$$

car la seule façon que cette suite tende vers 0 est que P soit constant égal à 0 mais alors cette suite d'intégrale est constante égale à 0 et ne tend pas vers 0 par valeurs supérieures. Dans les deux cas on conclut à une absurdité : un tel polynôme n'existe pas.

Exercice 26 : ✪✪ Soit $P \in \mathbb{K}[X]$. Montrer que $P-X$ divise $P\circ P-X$ (on commencera par montrer qu'il divise $P\circ P-P$).

Correction : Notons $P = \sum_{k=0}^{n} a_k X^k$ si bien que

$$P \circ P - P = \sum_{k=0}^{n} a_k \left(P^k - X^k\right)$$

Or :

$$P^k - X^k = (P - X) \times \sum_{i=0}^{k-1} P^i X^{k-1-i}$$

En particulier, $P^k - X - k$ est divisible par $P - X$ donc, par somme, $P \circ P - P$ l'est aussi. Enfin,

$$P \circ P - X = (P \circ P - P) + (P - X)$$

donc $P \circ P - X$ est somme de deux polynômes divisibles par $P - X$ donc est lui-même divisible par $P - x$.

Exercice 27 : ✪✪ On se donne dans cet exercice un polynôme $P \in \mathbb{Z}[X]$.

1. Montrer que si $P(0)$ et $P(1)$ sont impairs, alors P n'a aucune racine dans $\mathbb{Z}$.
2. On suppose que P est unitaire et que P admet une racine $r \in \mathbb{Q}$. Montrer que $r \in \mathbb{Z}$.
3. Généraliser le résultat précédent au cas où P n'est pas unitaire.
4. Montrer que $P = X^{2021} + X + 1$ a une unique racine réelle, et que cette racine est irrationnelle.
5. Montrer que si $k \geq 2$ et si $d \in \mathbb{N}$ n'est pas la puissance k-ième d'un entier, alors $\sqrt[k]{d}$ est un irrationnel.

Correction :

1. Montrons que pour tout $n \in \mathbb{Z}$, $P(n)$ est impair : cela impliquera en particulier que $P(n) \neq 0$. Notons $P = \sum_{k=0}^{d} a_k X^k$ avec les a_k dans $\mathbb{Z}$. Supposons n pair. Alors :

   $$P(n) = \sum_{k=1}^{d} a_k n^k + a_0$$

   La somme ci-dessus est paire car n est pair (il fallait mettre à part le terme pour $k = 0$: ne jamais oublier que $X^0 = 1$!) et $a_0 = P(0)$ est impair : on a la somme d'un nombre pair et d'un nombre impair donc la somme est impaire, si bien que $P(n)$ est impair. Supposons à présent n impair. Le même raisonnement n'est plus valide car, même si les puissances de n sont impaires, on ne connaît pas la parité des a_k. Pour tout k, n_k est impair : il existe donc β_k tel que $n^k = 2\beta_k + 1$ donc :

   $$\begin{aligned} P(n) &= \sum_{k=0}^{n} a_k(2\beta_k + 1) \\ &= 2\sum_{k=0}^{n} a_k\beta_k + \sum_{k=0}^{n} a_k \end{aligned}$$

Or, $f(1) = \sum_{k=0}^{n} a_k$ qui est un nombre impair si bien que $P(n)$ est impair car somme d'un nombre pair (car divisible par 2) et d'un nombre impair, ce qui permet de conclure. C'est tout de même fort : il suffit (mais ce n'est pas équivalent sinon ce serait trop facile) que $P(0)$ et $P(1)$ soient impairs pour qu'il n'y ait AUCUNE racine entière !

2. Notons $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ avec les a_i dans $\mathbb{Z}$ (rappelons que P est unitaire). Soit $r = p/q$ avec p et q premiers entre eux (pas forcément premiers mais premiers entre eux) une racine rationnelle de P. Alors $P(r) = 0$ c'est-à-dire :

$$\frac{p^n}{q^n} + a_{n-1} \times \frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \times \frac{p}{q} + a_0 = 0$$

En multipliant par q^n et en mettant tous les termes sauf le premier à droite :

$$p^n = qa_{n-1}p^{n-1} + \cdots + q^{n-1}a_1p + q^na_0$$

Par conséquent, q divise p^n donc $p^n \wedge q = q$ mais p et q sont premiers entre eux donc p^n et q sont premiers entre eux donc $p^n \wedge q = 1$ donc $q = 1$ si bien que $r = p \in \mathbb{Z}$.

3. Si on note a_n le coefficient dominant de P, on arrive à :

$$a_np^n = qa_{n-1}p^{n-1} + \cdots + q^{n-1}a_1p + q^na_0$$

q divise a_np^n et q est premier avec p^n donc, d'après le théorème de Gauß, q divise a_n : en conclusion, les racines rationnelles de P ont un dénominateur (quand elles sont écrites sous forme irréductible) qui divise le coefficient dominant de P. Par exemple, si $P = 3X^n + \cdots$ alors les racines rationnelles de P (s'il en existe) s'écrivent sous la forme $p/3$ avec $p \in \mathbb{Z}$. Cela ne laisse pas beaucoup de choix, comme on le voit dans la question suivante.

4. Théorème de la bijection (on assimile polynôme et fonction polynomiale) pour l'existence et l'unicité (on dérive ou on dit que P est la somme de trois fonctions croissantes dont deux strictement). D'après la question 2, P étant dans $\mathbb{Z}[X]$ unitaire, si cette racine est rationnelle, elle est entière. Mais d'après la question 1, puisque $P(0) = 1$ et $P(1) = 3$ soit impairs, P n'a pas de racine entière : il en découle que P n'a pas de racine rationnelle, donc que l'unique racine réelle de P est irrationnelle.

5. Notons $\alpha = \sqrt[k]{d}$. Alors α est racine de $P = X^k - d$. d n'est pas la puissance k-ième d'un entier donc P n'a pas de racine entière. Or, P est unitaire à coefficients dans $\mathbb{Z}$ donc, d'après la question 2, les racines rationnelles de P sont entières : puisque P n'a pas de racine entière, P n'a pas de racine rationnelle, donc $\alpha = \sqrt[k]{d}$ est un irrationnel.

Exercice 28 : ✪✪ Trouver tous les polynômes $P \in \mathbb{K}[X]$ tels que :

$$\forall (x, y) \in \mathbb{K}^2, P(xy) = P(x) \times P(y)$$

Correction : Supposons P constant égal à λ. Alors P est solution si et seulement si $\lambda = \lambda^2$ si et seulement si $\lambda = 0$ ou 1. Supposons dans la suite P non constant. Analyse : supposons que P convienne. Soit $z \in \mathbb{C}$ une racine complexe de P (rappelons que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ donc, dans tous les cas, P peut être considéré comme un polynôme à coefficients complexes) qui existe d'après le théorème de d'Alembert-Gauß, puisque P n'est pas constant. Alors $P(zy) = 0$ pour tout $y \in \mathbb{C}$. Si $z \neq 0$ alors, pour tout $y \in \mathbb{C}$,

$$\begin{aligned} P(y) &= P\left(z \times \frac{y}{z}\right) \\ &= 0 \end{aligned}$$

donc P est le polynôme nul ce qui est exclu (on a supposé P non constant). Par conséquent, 0 est la seule racine de P donc P s'écrit $P = a_nX^n$ avec n le degré de P et $a_n \neq 0$ son coefficient dominant. Finalement, pour tous x et y :

$$a_n(xy)^n = a_nx^n \times a_ny^n$$

En prenant $x = y = 1$: $a_n = {a_n}^2$ donc $a_n = 1$ puisque $a_n = 0$, c'est-à-dire qu'il existe n tel que $P = X^n$. Synthèse : pour tout n, X^n est évidemment solution. Conclusion : les seuls polynômes solutions sont les polynômes constants égaux à 0 et 1 et tous les polynômes de la forme X^n, pour $n \in \mathbb{N}$.

Exercice 29 : ✪✪ Montrer que le nombre de racines distinctes de $P \in \mathbb{C}[X]$ (non nul) est $\deg(P) - \deg(P \wedge P')$.

Correction : Notons $P = a_n(X - x_1)^{n_1} \times \cdots \times (X - x_k)^{n_k}$ où les x_i sont les racines distinctes de P et les n_i leurs multiplicités respectives (P est forcément scindé puisqu'on est sur $\mathbb{C}$). Il y a donc k racines distinctes et le but de l'exercice est de prouver que $k = \deg(P) - \deg(P \wedge P')$. On a de plus $\deg(P) = n_1 + \cdots + n_k$. Les $x_1, \ldots, x_k$ sont racines de P' de multiplicité respectives $n_1 - 1, \ldots, n_k - 1$ et ce sont les seules racines communes de P et P' (les autres racines de P' ne sont

pas racines de P puisque P n'a pas d'autres racines que les x_k) si bien que (le PGCD de P et P' est le produit de leurs facteurs irréductibles communs à la puissance la plus petite des deux) :

$$P \wedge P' = (X - x_1)^{n_1 - 1} \times \cdots \times (X - x_k)^{n_k - 1}$$

de degré $n_1 + \cdots + n_k - k$ ce qui permet de conclure.

Exercice 30 : ✪✪ Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme unitaire à coefficients complexes. Soit $z \in \mathbb{C}$ une racine de P. Montrer que

$$|z| \leq \max\left(1, \sum_{i=0}^{n-1} |a_i|\right)$$

Correction : Il suffit de prouver que si $|z| > 1$ alors $|z| \leq \sum_{i=0}^{n-1} |a_i|$. En effet, si $|z| \leq 1$ alors c'est bon, et si $|z| > 1$, prouver que $|z|$ est inférieur ou égal à cette somme permet de conclure. Supposons donc que z soit racine de P. Dès lors :

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0$$

si bien que

$$a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = -z^n$$

En prenant le module et en appliquant l'inégalité triangulaire :

$$|z|^n \leq \sum_{k=0}^{n-1} |a_k| \times |z|^k$$

Or, $|z| > 1$ (quand $|z| \leq 1$, les inégalités sont dans l'autre sens) donc, pour tout $k \leq n-1$, $|z|^k \leq |z|^{n-1}$ (l'inégalité est stricte mais, en multipliant par $|a_k|$ qui peut être nul, on obtient de toute façon une inégalité large) donc $|a_k| \times |z|^k \leq |a_k| \times |z|^{n-1}$ et, par somme :

$$|z|^{n-1} \leq \sum_{k=0}^{n-1} |a_k| \times |z|^k = |z|^{n-1} \sum_{k=0}^{n-1} |a_k|$$

En simplifiant par $|z|^{n-1}$ (non nul), on obtient le résultat voulu.

Exercice 31 - Un cas particulier du théorème d'Eneström-Kakeya : ✪✪ Soit

$$P = \sum_{k=0}^{n} a_k X^k \in \mathbb{R}[X]$$

et on suppose que $a_0 \geq a_1 \geq \cdots \geq a_n > 0$. Montrer que les racines complexes de P sont de module supérieur ou égal à 1 (on pourra s'intéresser à $(1 - X) \times P$).

Correction : Raisonnons par l'absurde et supposons que P admette une racine complexe z de module strictement inférieur à 1. Suivons l'indication de l'énoncé et intéressons-nous à $Q = (1 - X) \times P$. Alors $Q(z) = 0$. Or :

$$\begin{aligned}
Q(z) &= (1 - z) \times \sum_{k=0}^{n} a_k z^k \\
&= \sum_{k=0}^{n} a_k z^k - \sum_{k=0}^{n} a_k z^{k+1} \\
&= \sum_{k=0}^{n} a_k z^k - \sum_{k=1}^{n+1} a_{k-1} z^k \\
&= a_0 + \sum_{k=1}^{n} (a_k - a_{k-1}) z^k - a_n z^{n+1}
\end{aligned}$$

Par conséquent, puisque $Q(z) = 0$, il en découle que

$$a_0 = \sum_{k=1}^{n} (a_k - a_{k-1}) z^k - a_{n+1} z^{n+1}$$

Idem, d'après l'inégalité triangulaire :

$$|a_0| \leq \sum_{k=1}^{n} |a_k - a_{k-1}| \times |z|^k + |a_{n+1}| \times |z|^{n+1}$$

Or, a_0 et a_n sont positifs et $|a_k - a_{k-1}| = a_{k-1} - a_k$ par hypothèse sur les coefficients de P, si bien que :

$$a_0 \leq \sum_{k=1}^{n} (a_{k-1} - a_k) \times |z|^k + a_{n+1} \times |z|^{n+1}$$

Or, $|z| < 1$ et $a_{n+1} > 0$ donc $a_{n+1} \times |z|^{n+1} < a_{n+1}$. Cependant, $a_{k-1} - a_k$ peut être nul donc on a seulement $(a_{k-1} - a_k)|z|^k \leq a_{k-1} - a_k$ (l'inégalité n'est pas stricte alors que $|z| < 1$ car $a_{k-1} - a_k$ peut être nul et alors il y a égalité). Cependant, une inégalité est stricte donc la somme l'est, si bien que :

$$a_0 < \sum_{k=1}^{n} (a_{k-1} - a_k) + a_{n+1}$$

On reconnaît une somme télescopique : on obtient finalement $a_0 < a_0 - a_{n+1} + a_{n+1} = a_0$ ce qui est absurde.

Exercice 32 - Polynômes « exponentiels » : ✪✪

Pour tout $n \in \mathbb{N}$, on définit le polynôme $P_n \in \mathbb{R}[X]$ par $P_n = \sum_{k=0}^{n} \frac{X^k}{k!}$.

1. Montrer que les racines complexes de P_n sont toutes simples.
2. Montrer que pour tout $n \in \mathbb{N}$, P_{2n} n'a pas de racine réelle, que P_{2n+1} a une unique racine réelle qu'on note a_n, et que $a_n \neq 0$.
3. Donner le tableau de variation de P_{2n+1} et de P_{2n+3}, ainsi que leurs tableaux de signes.
4. Montrer que $a_n < 0$ pour tout n.
5. Soit $n \geq 0$.
   (a) Soit $p \leq n$. Donner le signe de
   $$\frac{(2n+3)^{2p}}{(2p)!} - \frac{(2n+3)^{2p+1}}{(2p+1)!}$$
   (b) Donner le signe de $P_{2n+1}(-2n-3)$. Comparer a_n et $-2n-3$.
   (c) En calculant le signe de $P_{2n+3}(a_n)$, montrer que la suite (a_n) est décroissante.
6. On admet le résultat suivant (qu'on montrera au deuxième semestre) :
   $$\forall x \in \mathbb{R} \qquad \sum_{k=0}^{n} \frac{x^k}{k!} \xrightarrow[n\to+\infty]{} e^x$$
   Montrer que $a_n \xrightarrow[n\to+\infty]{} -\infty$.

Correction :

1. Remarquons que
   $$P_n{}' = \sum_{k=0}^{n} \frac{kX^k}{k!}$$
   Le terme pour $k = 0$ étant nul, la somme commence en fait en 1, et alors on peut simplifier par k ce qui donne :
   $$\begin{aligned} P_n{}' &= \sum_{k=1}^{n} \frac{X^{k-1}}{(k-1)!} \\ &= \sum_{k=0}^{n-1} \frac{X^k}{k!} \\ &= P_n - \frac{X^n}{n!} \end{aligned}$$
   Soit $z \in \mathbb{C}$ une racine complexe de P_n. Si z est racine multiple, alors z est aussi racine de $P_n{}'$ donc est racine de $X^n/n! = P_n{}' - P_n$. Par conséquent, $z = 0$ car c'est la seule racine de ce polynôme, ce qui est absurde car 0 n'est pas racine de P_n puisque $P_n(0) = 1$. En conclusion, les racines complexes de P_n sont toutes simples.

2. Montrons le résultat par récurrence.
   - Pour $n \geq 0$ on note l'hypothèse H_n : « P_{2n} n'a aucune racine réelle, P_{2n+1} a une unique racine réelle a_n, et celle-ci est non nulle. »
   - Montrons que H_0 est vraie. D'une part $P_{2\times 0} = P_0 = 1$ et n'a aucune racine réelle, d'autre part $P_{2\times 0+1} = 1 + X$ a une unique racine réelle, -1, qui est bien non nulle. Par conséquent, H_0 est vraie.
   - Soit $n \geq 0$. Supposons H_n vraie et montrons que H_{n+1} est vraie, c'est-à-dire qu'on veut montrer que P_{2n+2} ne s'annule jamais sur $\mathbb{R}$, que P_{2n+3} s'annule une unique fois sur $\mathbb{R}$, et que son unique racine n'est pas nulle. On déduit des calculs de la question 1 que ${P_{2n+2}}' = P_{2n+1}$. Or, par hypothèse de récurrence, P_{2n+1} s'annule une unique fois en a_{2n+1}. On en déduit que P_{2n+1} est de signe constant sur chacun des intervalles $]-\infty\,;a_n\,]$ et $[\,a_n\,;+\infty\,[$. En effet, par exemple sur $]\,\infty\,;a_n\,]$, s'il existe deux réels x_0 et x_1 avec $f(x_0) > 0$ et $f(x_1) < 0$ alors, P_{2n+1} étant polynomiale (on confond encore polynôme et fonction polynomiale associée), elle est continue, et d'après le théorème des valeurs intermédiaires, elle s'annule sur $]\,x_0\,;x_1\,[$ ce qui est exclu. De plus, son coefficient dominant étant égal à $1/(n+1)!$, c'est-à-dire un nombre positif, et son degré étant impair :

$$P_{2n+1}(x) \xrightarrow[x\to+\infty]{} +\infty \qquad \text{et} \qquad P_{2n+1}(x) \xrightarrow[x\to-\infty]{} -\infty$$

   On en déduit le tableau de signes de P_{2n+1} et le tableau de variations de P_{2n+2} :

	$-\infty$		a_n		$+\infty$
$P_{2n+1}(x)$		$-$	0	$+$	
P_{2n+2}		$\searrow$	$P_{2n+2}(a_n)$	$\nearrow$	

   Or, on a également $P_{2n+2} = P_{2n+1} + \dfrac{X^{2n+2}}{(2n+2)!}$ donc :

$$P_{2n+2}(a_n) = P_{2n+1}(a_n) + \frac{{a_n}^{2n+2}}{(2n+2)!} = \frac{{a_n}^{2n+2}}{(2n+2)!} > 0$$

   puisque par hypothèse de récurrence, a_n est non nul. D'après le tableau de variations, P_{2n+2} est strictement positif sur $\mathbb{R}$ donc ne s'annule jamais. De plus, on en déduit que P_{2n+3} est strictement croissante sur $\mathbb{R}$ (car sa dérivée P_{2n+2} est strictement positive sur $\mathbb{R}$) et de même que précédemment

$$P_{2n+3}(x) \xrightarrow[x\to+\infty]{} +\infty \qquad \text{et} \qquad P_{2n+3}(x) \xrightarrow[x\to-\infty]{} -\infty$$

   P_{2n+3} étant continue sur $\mathbb{R}$ et strictement croissante, d'après le corollaire du théorème des valeurs intermédiaires, P_{2n+3} s'annule une unique fois sur $\mathbb{R}$. Notons a_{n+1} son unique racine. Pour montrer que a_{n+1} est non nul, il suffit de montrer que $P_{2n+3}(0)$ est non nul, ce qu'on a déjà vu à la question 1. Finalement, H_{n+1} est vraie.
   - D'après le principe de récurrence, H_n est vraie pour tout n.

3. P_{2n} et P_{2n+2} étant strictement positifs d'après la question précédente (je donne uniquement les tableaux de variations, les tableaux de signes s'en déduisent immédiatement) :

	$-\infty$		a_n		$+\infty$
P_{2n}			$+$		
P_{2n+1}	$-\infty$	$\nearrow$	0	$\nearrow$	$+\infty$

	$-\infty$		a_{n+1}		$+\infty$
P_{2n+2}			$+$		
P_{2n+3}	$-\infty$	$\nearrow$	0	$\nearrow$	$+\infty$

4. D'après la question 3, pour tout $n \in \mathbb{N}$: $P_{2n+1}(0) = 1 > 0$, et d'après la question précédente, cela donne le résultat voulu : $\forall n \in \mathbb{N} \qquad a_n < 0$.

5. (a) Soit $p \leq n$. En mettant $(2n+3)^{2p}$ en facteur il vient

$$\frac{(2n+3)^{2p}}{(2p)!} - \frac{(2n+3)^{2p+1}}{(2p+1)!} = \frac{(2n+3)^{2p}}{(2p)!} \times \left(1 - \frac{2n+3}{2p+1}\right)$$

   et puisque $n \geq p, 2n+3 > 2p+1$. En d'autres termes

$$\forall p \leq n \qquad \frac{(2n+3)^{2p}}{(2p)!} - \frac{(2n+3)^{2p+1}}{(2p+1)!} < 0$$

   (b) Par définition de P_{2n+1} :

$$\begin{aligned} P_{2n+1}(-2n-3) &= \sum_{k=0}^{2n+1} \frac{(-2n-3)^k}{k!} \\ &= (1-(2n+3)) + \left(\frac{(2n+3)^2}{2!} - \frac{(2n+3)^3}{3!}\right) + \cdots + \left(\frac{(2n+3)^{2n}}{(2n)!} - \frac{(2n+3)^{2p+1}}{(2p+1)!}\right) \end{aligned}$$

Or, d'après la question précédente, tous les termes entre parenthèses sont strictement négatifs. On en déduit que $P_{2n+1}(-2n-3) < 0$ et d'après la question 3, $-2n-3 < a_n$.

(c) Tout d'abord :

$$P_{2n+3} = P_{2n+2} + \frac{X^{2n+3}}{(2n+3)!} = P_{2n+1} + \frac{X^{2n+2}}{(2n+2)!} + \frac{X^{2n+3}}{(2n+3)!}$$

En particulier

$$\begin{aligned} P_{2n+3}(a_n) &= P_{2n+1}(a_n) + \frac{{a_n}^{2n+2}}{(2n+2)!} + \frac{{a_n}^{2n+3}}{(2n+3)!} \\ &= \frac{{a_n}^{2n+2}}{(2n+2)!} + \frac{{a_n}^{2n+3}}{(2n+3)!} \\ P_{2n+3}(a_n) &= \frac{{a_n}^{2n+2}}{(2n+2)!}\left(1 + \frac{a_n}{2n+3}\right) \end{aligned}$$

D'une part, $\frac{{a_n}^{2n+2}}{(2n+2)!} > 0$ et d'autre part, d'après la question précédente :

$$1 + \frac{a_n}{2n+3} > 1 + \frac{-2n-3}{2n+3} = 0$$

On en déduit que $P_{2n+3}(a_n) > 0$ et d'après le tableau de signes de la fonction, $P_{2n+3}, a_{n+1} < a_n$: la suite (a_n) est décroissante.

6. La suite (a_n) est décroissante, ce qui implique que soit elle converge, soit elle diverge vers $-\infty$. Supposons qu'elle converge vers L. Soit $x \leq L$. La suite (a_n) étant décroissante :

$$\forall n \in \mathbb{N} \qquad a_n \geq L \geq x$$

Toujours d'après le tableau de signes de P_{2n+1}, $P_{2n+1}(x) \leq 0$. Or, $P_{2n+1}(x) \xrightarrow[n\to+\infty]{} e^x$ et l'inégalité large passe à la limite. D'où $e^x \leq 0$: c'est absurde. On en déduit le résultat voulu.

Exercice 33 : ✪✪ Soient $(a_1, a_2, a_3, b_1, b_2, b_3) \in \mathbb{K}^6$ distincts. On se donne le tableau suivant :

a_1+b_1	a_1+b_2	a_1+b_3
a_2+b_1	a_2+b_2	a_2+b_3
a_3+b_1	a_3+b_2	a_3+b_3

On suppose que le produit des termes de chaque colonne vaut 2020. Donner le produit des termes de chaque ligne. On s'intéressera au polynôme $(X+a_1)(X+a_2)(X+a_3)$.

Correction : Oulà, cet exercice retarde... Notons $Q = (X+a_1)(X+a_2)(X+a_3)$. Puisque le produit des termes de chaque colonne fait 2020, $Q(b_1) = Q(b_2) = Q(b_3) = 2020$, c'est-à-dire que b_1, b_2, b_3 sont racines de $Q - 2020$ qui est unitaire de degré 3. Les réels b_1, b_2, b_3 étant distincts, $Q - 2020 = (X-b_1)(X-b_2)(X-b_3)$ et donc

$$(X+a_1)(X+a_2)(X+a_3) = (X-b_1)(X-b_2)(X-b_3) + 2020$$

En évaluant en $-a_1$:

$$0 = (-a_1-b_1)(-a_1-b_2)(-a_1-b_3) - 2020$$

et puisque $(-1)^3 = -1$, il vient :

$$-(a_1+b_1)(a_1+b_2)(a_1+b_3) - 2020 = 0$$

En d'autres termes : $(a_1+b_1)(a_1+b_2)(a_1+b_3) = -2020$: le produit des termes de la première ligne vaut -2020, et c'est la même chose pour les deux autres lignes.

Exercice 34 : ✪✪ Soit $n \geq 1$. Montrer qu'il n'y a qu'un nombre fini de polynômes unitaires de degré n à coefficients dans $\mathbb{Z}$ dont toutes les racines complexes ont un module inférieur ou égal à 1.

Correction : Oubli de l'énoncé : il fallait évidemment supposer que P soit de degré n, sinon ils sont en nombre infini (prendre tous les X^k pour $k \in \mathbb{N}$). De plus, cet exercice a plus sa place dans la section « relations coefficients-racines », mea culpa. En effet, P étant unitaire, pour tout $k \leq n-1$ (il est important que P soit unitaire sinon a_n apparaît dans la formule ci-dessous) :

$$a_k = (-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq n} z_{i_1} \cdots z_{i_k}$$

où on a noté évidemment $z_1, \ldots, z_n$ les racines complexes (pas forcément distinctes) de P. D'après l'inégalité triangulaire, et les z_i étant de module 1 :

$$|a_k \leq \sum_{1 \leq i_1 < \cdots < i_k \leq n} 1$$

On pourrait dire que cette somme est égale à $\binom{n}{k}$ mais sa valeur exacte importe peu : seul compte le fait que les coefficients soient bornés. Puisqu'ils sont entiers, il y a un nombre fini de valeurs possibles pour a_0, disons M_0 valeurs possibles, et ainsi de suite jusque M_{n-1} valeurs possibles pour a_{n-1}. Par principe multiplicatif, il y a $M_0 \times \cdots \times M_{n-1}$ choix possibles pour les coefficients, donc un nombre fini.

Exercice 35 - Polynômes stabilisant le cercle unité : ✪✪✪ On note $E = \{P \in \mathbb{C}[X] \mid P(\mathbb{U}) \subset \mathbb{U}\}$ l'ensemble des polynômes complexes stabilisant le cercle unité.

1. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$ avec $a_n \neq 0$. On pose $\widehat{P} = \sum_{k=0}^{n} \overline{a_{n-k}} X^k$.
   (a) Dans le cas particulier où $P = (3+i)X^4 + 2X^3 + (1+i)X^2 - 2020$, expliciter $\widehat{P}$.
   (b) On revient au cas général. Montrer que pour tout $z \in \mathbb{U}, \widehat{P}(z) = z^n \overline{P(z)}$.
2. Si $P \in E$, que vaut $P\widehat{P}$? En déduire le degré de $\widehat{P}$.
3. Déterminer l'ensemble E.

Correction :

1. (a) La méthode est simple : on change l'ordre des coefficients (le coefficient dominant devient le terme constant, etc.) et on les conjugue. Ici, $n = 4$. Attention, le coefficient de P devant X est nul donc le coefficient de $\widehat{P}$ devant X^3 sera nul aussi. Dès lors :

$$\widehat{P} = -2020X^4 + 0 \times X^3 + (1-i)X^2 + 2X + (3-i)$$

   (b) Soit $z \in \mathbb{U}$. Rappelons que $\overline{z} = 1/z$ puisque z est de module 1.

$$\begin{aligned}
\widehat{P}(z) &= \sum_{k=0}^{n} \overline{a_{n-k}} z^k \\
&= \sum_{j=0}^{n} \overline{a_j} z^{n-j} \qquad j = n-k \\
&= z^n \sum_{j=0}^{n} \overline{a_j} \times \frac{1}{z^j} \\
&= z^n \sum_{j=0}^{n} \overline{a_j} \times \overline{z}^j \\
&= z^n \times \overline{\sum_{j=0}^{n} a_j z^j}
\end{aligned}$$

   ce qui est le résultat voulu.

(c) Soit $P \in E$. D'après la question précédente, pour tout $z \in \mathbb{U}$:

$$\begin{aligned} P(z) \times \widehat{P}(z) &= z^n \times P(z) \times \overline{P(z)} \\ &= z^n \times |P(z)|^2 \end{aligned}$$

Or, $P \in E$ et $z \in \mathbb{U}$ donc $P(z) \in \mathbb{U}$ si bien que $|P(z)|^2 = 1$ donc $P(z) \times \widehat{P}(z) = z^n$. En d'autres termes, les polynômes $P \times \widehat{P}$ et X^n coïncident sur $\mathbb{U}$ qui est un ensemble infini donc sont égaux : $P \times \widehat{P} = X^n$. Par conséquent, $\deg(P) + \deg(\widehat{P}) = n$. Or, $\deg(P) = n$ donc $\deg(\widehat{P}) = 0$.

(d) On en déduit que si $P \in E$ alors $\widehat{P}$ est constant non nul. En d'autres termes, tous les coefficients des X^k, pour $k \geq 1$, de $\widehat{P}$ sont nuls donc $a_{n-k} = 0$ pour tout $k \geq 1$. En d'autres termes, tous les coefficients de P sont nuls à part a_n (tous les a_{n-k} pour $k \geq 1$, cela donne $a_{n-1}, \ldots, a_0$). On en déduit que $P = a_n X^n$: on vient de finir la partie analyse du problème.

Synthèse : soit P de la forme $a_n X^n$ avec $a_n \in \mathbb{C}^*$, cherchons si $P \in E$. Soit $z \in \mathbb{U}$. Alors $P(z) = a_n z^n$ donc $|P(z)| = |a_n|$ puisque $z \in \mathbb{U}$. En particulier, $P(z) \in \mathbb{U}$ si et seulement si $|a_n| = 1$. En conclusion, E est l'ensemble des polynômes de la forme $a_n X^n$ avec $|a_n| = 1$.

Exercice 36 : ✪✪✪ Soient P et Q deux polynômes non constants de $\mathbb{C}[X]$ tels que P et Q aient le même ensemble de racines, ainsi que $P-1$ et $Q-1$. Le but de l'exercice est de prouver que $P = Q$. On pose pour cela $R = P - Q$.

1. Justifier que $P \wedge P'$ et $(P-1) \wedge P'$ sont premiers entre eux.
2. À l'aide de l'exercice 29, prouver que R admet au moins $n+1$ racines distinctes et conclure.

Correction : Oubli dans l'énoncé : il fallait supposer que P et Q sont de degré n.

1. P et $P-1$ n'ont aucune racine commune car, si z est une racine de P, alors $P(z) - 1 = -1 \neq 0$. Par conséquent, si z est une racine de $P \wedge P'$, alors z est une racine de P donc n'est pas racine de $P-1$ donc n'est pas un racine de $(P-1) \wedge P'$: $P \wedge P'$ et $(P-1) \wedge P'$ n'ont aucune racine complexe commune donc sont premiers entre eux.
2. Les racines communes de P et Q sont racines de R, ainsi que les racines de $P-1$ et $Q-1$ puisqu'on a également $R = (P-1) - (Q-1)$. Or, P et $P-1$ n'ont aucune racine commune : on peut donc sommer leur nombre de racines distinctes.

   D'après l'exercice 29, le nombre de racines distinctes de P est $\deg(P) - \deg(P \wedge P')$ et le nombre de racines distinctes de $P-1$ est $\deg(P-1) - \deg((P-1) \wedge (P-1)') = \deg(P) - \deg((P-1) \wedge P')$. Par conséquent, R admet au moins

   $$k = \deg(P) - \deg(P \wedge P') + \deg(P) - \deg((P-1) \wedge P') = 2\deg(P) - (\deg(P \wedge P') + \deg((P-1) \wedge P'))$$

   racines distinctes. Or, d'après la question précédente, les deux PGCD sont premiers entre eux et divisent P' donc leur produit divise P'. En particulier, leur produit a un degré inférieur à celui de P' : en d'autres termes, $\deg(P \wedge P') + \deg((P-1) \wedge P') \leq n-1$ donc le nombre de racines distinctes de R est supérieur à k qui est lui-même supérieur à $2n - (n-1) = n+1$ mais $\deg(R) \leq n$ donc R est le polynôme nul : $P = Q$.

Exercice 37 : ✪✪✪ Soit $P \in \mathbb{C}[X]$ non constant et soit E un sous-ensemble fini de $\mathbb{C}$. Montrer que :

$$\text{card}(P^{-1}(E)) \geq (\text{card}(E) - 1)\deg(P) + 1$$

On pourra utiliser l'exercice 29.

Correction : Notons $E = \{x_1; \ldots; x_n\}$ si bien que $\text{card}(E) = n$. $P^{-1}(E)$ est l'union disjointes des antécédents des x_i si bien que

$$\text{card}(P^{-1}(E)) = \sum_{i=1}^{n} \text{card} P^{-1}(\{x_i\})$$

Soit $i \in [\![1\,;n]\!]$. $P^{-1}(\{x_i\})$ est l'ensemble des racines distinctes du polynôme $P - x_i$. D'après l'exercice 29, cet ensemble a $\deg(P - x_i) - \deg((P-x_i) \wedge (P-x_i)') = \deg(P) - \deg((P-x_i) \wedge P')$ éléments donc :

$$\text{card}(P^{-1}(E)) = \sum_{i=1}^{n} \deg(P) - \deg((P-x_i) \wedge P') = n\deg(P) - \sum_{i=1}^{n} \deg((P-x_i) \wedge P')$$

Or, les $P - x_i$ n'ont aucune racine complexe commune donc sont premiers entre eux donc les $(P-x_i) \wedge P'$ aussi et ceux-ci divisent P' donc leur produit divise P' donc

$$\sum_{i=1}^{n} \deg((P - x_i) \wedge P') \leq \deg(P') = \deg(P) - 1$$

On en déduit que :

$$\text{card}(P^{-1}(E)) \geq n \deg(P) - (\deg(P) - 1)$$

ce qui est le résultat voulu puisque $n = \text{card}(E)$.

2 Factorisation

Exercice 38 - Une factorisation : ✪ Soit $P = (X^2 - 1)^2 - 3X(X^2 + 1)$.

1. Montrer que j est racine de P. Donner une autre racine complexe de P.
2. En déduire toutes les racines de P et sa factorisation sur $\mathbb{R}[X]$.

Correction :

1. On a :

$$\begin{aligned} P(j) &= (j^2 - 1)^2 - 3j(j^2 + 1) \\ &= j^4 - 2j^2 + 1 - 3j^3 - 3j \\ &= j - 2j^2 + 1 - 3 - 3j \\ &= -2(j^2 + j + 1) \\ &= 0 \end{aligned}$$

   De plus, P est à coefficients réels donc $\overline{j} = j^2$ est aussi racine de P.
2. P est donc divisible par $(X - j)(X - j^2) = X^2 + X + 1$. Or,

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

   En effectuant la division euclidienne de P par $X^2 + X + 1$, on trouve : $P = (X^2 + X + 1)(X^2 - 4X + 1)$. Or, $X^2 - 4X + 1 = (X - x_1)(X - x_2)$ avec $x_{1,2} = \dfrac{4 \pm \sqrt{12}}{2} = 2 \pm \sqrt{3}$. Finalement :

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

Exercice 39 : ✪ Soit $n \geq 1$. Factoriser le polynôme

$$P_n = 1 - X + \frac{X(X-1)}{2!} + \cdots + \frac{(-1)^n X(X-1)\cdots(X-n+1)}{n!}$$

Correction : Aucune méthode ne semble fonctionner : regardons pour de petites valeurs de n pour nous donner une idée. On a $P_1 = 1 - X = -(X - 1)$ qui est déjà sous forme factorisée. On a également

$$P_2 = 1 - X + \frac{X(X-1)}{2!} = (1 - X) \times \left(1 - \frac{X}{2!}\right) = (1 - X) \times \left(\frac{2 - X}{2!}\right) = \frac{1}{2!}(1 - X)(2 - X)$$

Finalement, $P_2 = (X - 1)(X - 2)/2!$. Montrons par récurrence que, pour tout $n \geq 1$,

$$P_n = \frac{(-1)^n}{n!} \times (X - 1)\cdots(X - n)$$

Le résultat est vrai aux rangs 1 et 2. Soit $n \geq 2$: supposons le résultat vrai au rang n et prouvons qu'il l'est encore au rang $n + 1$. Remarquons qu'on passe de P_n à P_{n+1} en ajoutant un terme. Plus précisément,

$$P_{n+1} = P_n + \frac{(-1)^{n+1} X(X-1)\cdots(X-n)}{(n+1)!}$$

Par hypothèse de récurrence,

$$P_{n+1} = \frac{(-1)^n}{n!} \times (X - 1)\cdots(X - n) + \frac{(-1)^{n+1} X(X-1)\cdots(X-n)}{(n+1)!}$$

On peut factoriser par P_n qui est en facteur dans les deux termes :

$$P_{n+1} = \frac{(-1)^n}{n!} \times (X-1)\cdots(X-n) \times \left(1 - \frac{X}{n+1}\right) = \frac{(-1)^n}{n!} \times (X-1)\cdots(X-n) \times \left(\frac{n+1-X}{n+1}\right)$$

ce qui permet de conclure en remarquant que $n+1-X = (-1)\times(X-(n+1))$ et que $n!\times(n+1) = (n+1)!$.

Exercice 40 : ✪ Soit $P = (X+1)^7 - X^7 - 1$. Montrer que j est racine de P et factoriser P sur $\mathbb{R}$.

Correction : À l'aide du triangle de Pascal :

$$P_7 = 7X^6 + 21X^5 + 35X^4 + 35X^3 + 21X^2 + 7X$$

On rappelle que $j^3 = 1, j^4 = j, j^5 = j^2, j^6 = 1$ et $j^7 = j$. Le résultat en découle : $P_7(j) = 42 + 42j + 42j^2 = 0$: j est racine de P_7. De plus, P_7 étant à coefficients réels, $j^2 = \overline{j}$ est également racine de P_7, ce qui implique que $(X-j)(X-j^2) = 1+X+X^2$ divise P_7. On cherche à présent des racines évidentes, jusqu'à obtenir un polynôme de degré 2. En évaluant en $x=0$ et $x=-1$, on trouve que 0 et -1 sont racines évidentes. Ainsi, P est divisible par $X(X+1)(X^2+X+1)$: il existe un polynôme Q tel que $P = X(X+1)(X^2+X+1)Q$. Or, P est de degré 6 donc $\deg(Q) = 2$ et il existe a, b, c réels tels que $Q = aX^2 + bX + c$. En développant il vient

$$P = aX^6 + (2a+b)X^5 + (c+2b+2a)X^4 + (2c+2b+a)X^3 + (2c+b)X^2 + cX$$

Par unicité des coefficients, on obtient :

$$Q = 7X^2 + 7X + 7 = 7(X^2+X+1)$$

Finalement, $P_7 = 7X(X+1)(X^2+X+1)^2$.

Exercice 41 : ✪✪ Factoriser sur $\mathbb{R}$ et sur $\mathbb{C}$ les polynômes $X^8 + X^4 + 1$ et $X^{12} + 1$.

Correction : Notons $P_1 = X^8 + X^4 + 1$ et $P_2 = X^{12} + 1$. Soit $z \in \mathbb{C}$. z est racine de P_2 si et seulement si $z^{12} = -1$. Or, $-1 = e^{i\pi}$: les racines 12-ièmes de -1 (cf. chapitre 7) sont donc les

$$e^{i\left(\frac{\pi}{12} + \frac{2k\pi}{12}\right)}$$

pour $k \in [\![0\,;11]\!]$. On a un polynôme de degré 12 avec 12 racines distinctes donc elles sont simples, le polynôme est unitaire, donc on trouve (sur $\mathbb{C}$) :

$$P_2 = \prod_{k=0}^{11} \left(X - e^{i\left(\frac{\pi}{12} + \frac{2k\pi}{12}\right)}\right)$$

Pour factoriser sur $\mathbb{R}$, il faut regrouper les racines conjuguées. Explicitons le produit ci-dessus :

$$\begin{aligned} P_2 &= \left(X - e^{i\pi/12}\right)\left(X - e^{3i\pi/12}\right)\left(X - e^{5i\pi/12}\right)\left(X - e^{7i\pi/12}\right)\left(X - e^{9i\pi/12}\right)\left(X - e^{i11\pi/12}\right) \\ &\quad \times \left(X - e^{i13\pi/12}\right)\left(X - e^{i15\pi/12}\right)\left(X - e^{i17\pi/12}\right)\left(X - e^{19i\pi/12}\right)\left(X - e^{i21\pi/12}\right)\left(X - e^{i23\pi/12}\right) \end{aligned}$$

Or, $e^{23i\pi/12} = \overline{e^{i\pi/12}}$. En effet :

$$\begin{aligned} \overline{e^{i\pi/12}} &= e^{-i\pi/12} \\ &= e^{2i\pi - i\pi/12} \end{aligned}$$

ce qui donne le résultat voulu. De même, $e^{21i\pi/12} = \overline{e^{3i\pi/12}}$ et ainsi de suite. En regroupant chaque terme (correspondants aux indices de k allant de 0 à 5) avec son conjugué :

$$\begin{aligned} P_2 &= \prod_{k=0}^{5} \left(X - e^{i\left(\frac{\pi}{12} + \frac{2k\pi}{12}\right)}\right) \times \left(X - \overline{e^{i\left(\frac{\pi}{12} + \frac{2k\pi}{12}\right)}}\right) \\ &= \prod_{k=0}^{5} \left(X^2 - 2X\cos\left(\frac{\pi}{12} + \frac{2k\pi}{12}\right) + 1\right) \end{aligned}$$

Passons à P_1. Il suffit de voir que $P_1 = (X^4)^2 + X^4 + 1$. Soit $z \in \mathbb{C}$. Alors z est racine de P_1 si et seulement si ${z_1}^4$ est racine de $X^2 + X + 1$ si et seulement si z_1 est quatrième des racines de $X^2 + X + 1$ c'est-à-dire j et j^2. Or :

$$j = e^{2i\pi/3} \qquad \text{et} \qquad j^2 = e^{4i\pi/3}$$

Toujours d'après le chapitre 7, les racines quatrièmes de j sont les $e^{i\left(\frac{2\pi}{12}+\frac{2k\pi}{4}\right)}$ pour $k \in [\![0\,;\,3]\!]$ et les racines quatrièmes de j^2 sont les $e^{i\left(\frac{4\pi}{12}+\frac{2k\pi}{4}\right)}$. On en déduit la factorisation sur $\mathbb{C}$:

$$P_1 = \prod_{k=0}^{3}\left(X - e^{i\left(\frac{\pi}{6}+\frac{k\pi}{2}\right)}\right) \times \prod_{k=0}^{3}\left(X - e^{i\left(\frac{\pi}{3}+\frac{k\pi}{2}\right)}\right)$$

De même :

$$P_1 = \left(X - e^{i\pi/6}\right)\left(X - e^{4i\pi/6}\right)\left(X - e^{7i\pi/6}\right)\left(X - e^{10i\pi/6}\right)\left(X - e^{2i\pi/6}\right)\left(X - e^{i5\pi/6}\right)\left(X - e^{i8\pi/6}\right)\left(X - e^{11i\pi/6}\right)$$

Attention, il y a des trous, il manque des termes (par exemple $e^{3i\pi/6}$) donc on ne peut pas mettre un symbole $\prod$. Tant pis, on le fait à la main. On regroupe les termes conjugués entre eux ($e^{i\pi/6}$ avec $e^{11i\pi/6}$, $e^{2i\pi/6}$ avec $e^{10i\pi/6}$, $e^{4i\pi/6}$ avec $e^{8i\pi/6}$ et enfin $e^{5i\pi/6}$ avec $e^{7i\pi/6}$), on trouve de même :

$$P_1 = \left(X^2 - 2X\cos(\pi/6) + 1\right)\left(X^2 - 2X\cos(2\pi/6) + 1\right)\left(X^2 - 2X\cos(4\pi/6) + 1\right)\left(X^2 - 2X\cos(5\pi/6) + 1\right)$$

Avec les valeurs explicites des cosinus :

$$P_1 = \left(X^2 - X\sqrt{3} + 1\right)\left(X^2 - X + 1\right)\left(X^2 + X + 1\right)\left(X^2 + X\sqrt{3} + 1\right)$$

Exercice 42 : ✪ Soit $n \in \mathbb{N}^*$.

1. Décomposer $P_n = \sum_{k=0}^{n} X^k$ en produit de facteurs irréductibles dans $\mathbb{C}[X]$.
2. En déduire la valeur de $\prod_{k=1}^{n} \sin\left(\frac{k\pi}{n+1}\right)$.

Correction :

1. 1 n'est pas racine de P. Soit $z \in \mathbb{C}\backslash\{1\}$. Alors :

$$\begin{aligned} P(z) = 0 &\iff \frac{1-z^{n+1}}{1-z} = 0 \\ &\iff z^{n+1} = 1 \\ &\iff \exists k \in [\![1\,;\,n]\!], z = e^{2ik\pi/(n+1)} \end{aligned}$$

   On a pris $k \in [\![1\,;\,n]\!]$ et non pas $[\![0\,;\,n]\!]$ car on a supposé $z \neq 1$. P étant de degré n et admettant n racines distinctes, elles sont simples, et P étant unitaire :

$$P = \prod_{k=1}^{n}\left(X - e^{2ik\pi/(n+1)}\right)$$

2. En évaluant en 1, d'une part, $P(1) = n+1$, et d'autre part :

$$\begin{aligned}
P(1) &= \prod_{k=1}^{n}\left(1-e^{2ik\pi/(n+1)}\right)\\
&= \prod_{k=1}^{n} e^{ik\pi/(n+1)}\left(e^{-ik\pi/(n+1)}-e^{2ik\pi/(n+1)}\right) && \text{(angle moitié)}\\
&= \prod_{k=1}^{n+1} e^{ik\pi/(n+1)} \times \prod_{k=1}^{n}(-2i)\times\sin\left(\frac{k\pi}{n+1}\right)\\
&= e^{\sum_{k=1}^{n+1} ik\pi/(n+1)} \times (-2i)^n \prod_{k=1}^{n}\sin\left(\frac{k\pi}{n+1}\right)\\
&= e^{i(n+1)(n+2)\pi/2(n+1)} \times (-2)^n \times e^{in\pi/2}\prod_{k=1}^{n}\sin\left(\frac{k\pi}{n+1}\right)\\
&= e^{i(2n+2)\pi/2} \times (-2)^n \times \prod_{k=1}^{n}\sin\left(\frac{k\pi}{n+1}\right)\\
&= \left(e^{i\pi}\right)^{n+1} \times (-2)^n \times \prod_{k=1}^{n}\sin\left(\frac{k\pi}{n+1}\right)\\
&= (-1)^{n+1} \times (-2)^n \times \prod_{k=1}^{n}\sin\left(\frac{k\pi}{n+1}\right)
\end{aligned}$$

Finalement :

$$\prod_{k=1}^{n}\sin\left(\frac{k\pi}{n+1}\right) = \frac{(-1)^{n+1}(n+1)}{2^n}$$

Exercice 43 : ✪✪ Soit p un entier supérieur ou égal à 1.

1. Donner la factorisation du polynôme $X^{2p}-1$ dans $\mathbb{R}[X]$ (indice : c'est dans le cours).
2. Donner la factorisation sur $\mathbb{R}$ de $1+X+\cdots+X^{2p-1}$. En déduire que

$$\sqrt{2p} = 2^{p-\frac{1}{2}}\prod_{k=1}^{p-1}\sin\left(\frac{k\pi}{2p}\right)$$

Correction :

1. À savoir faire :

$$X^{2p}-1 = (X-1)(X+1)\prod_{k=1}^{n-1}\left(X^2-2\cos(k\pi/n)X+1\right)$$

2. Raisonnons avec les outils du chapitre suivant : on a

$$\begin{aligned}
1+X+\cdots+X^{2p-1} &= \frac{X^{2p}-1}{X-1}\\
&= \frac{(X-1)(X+1)\prod_{k=1}^{n-1}\left(X^2-2\cos(k\pi/n)X+1\right)}{X-1}\\
&= (X+1)\prod_{k=1}^{n-1}\left(X^2-2\cos(k\pi/n)X+1\right)
\end{aligned}$$

Ensuite on fait comme dans l'exercice précédent : on évalue en 1, on utilise la formule de trigo $1-\cos(2u)=2\sin^2(u)$ et on utilise le fait que pour tout $k\in[\![1\,;p-1]\!]$, $k\pi/2p\in[\,0\,;\pi/2\,]$ donc $\sin(k\pi/2p)\geq 0$ si bien que que $\sqrt{\sin^2(k\pi/2p)}=\sin(k\pi/2p)$ et on trouve la valeur voulue.

Exercice 44 : ✪✪ Soit $P \in \mathbb{R}[X]$ unitaire de degré $n \geq 1$. Montrer que P est scindé sur $\mathbb{R}$ si et seulement si $|P(z)| \geq |\mathrm{Im}(z)|^n$ pour tout $z \in \mathbb{C}$.

Correction : P est scindé sur $\mathbb{R}$ si et seulement si ses racines complexes sont toutes réelles i.e. ont toutes une partie imaginaire nulle.

Supposons que $|P(z)| \geq |\Im(z)|^n$ pour tout $z \in \mathbb{C}$. C'est en particulier vrai si z est une racine de P, ce qui donne : $0 \geq |\Im(z)|^n$ donc $\Im(z) = 0$. En d'autres termes, les racines complexes de P sont toutes réelles, P est scindé sur $\mathbb{R}$.

Réciproquement, supposons P scindé sur $\mathbb{R}$, notons $x_1, \dots, x_n$ les racines réelles de P (pas forcément distinctes) et P étant unitaire :

$$P = (X - x_1) \cdots (X - x_n)$$

Soit $z \in \mathbb{C}$. $|P(z)| = |z - x_1| \times \cdots \times |z - x_n|$. Or, le module d'un complexe est supérieur à la valeur absolue de sa partie imaginaire (cf. chapitre 7) donc, pour tout i, $|z - x_i| \geq |\Im(z - x_i)| = |\Im(z)|$ puisque x_i est un réel. Par produit d'inégalités positives, on en déduit que $|P(z)| \geq |\Im(z)|^n$.

Exercice 45 : ✪✪

1. Soit P un polynôme unitaire de degré n tel que pour tout k appartenant à $[\![1 ; n+1]\!]$ on ait $P(k) = \dfrac{1}{k^2}$. Donner $P(n+2)$. On s'intéressera au polynôme $Q = X^2P - 1$.
2. **Remake :** Soit P de degré n tel que pour tout $k \in [\![0 ; n]\!], P(k) = \dfrac{k}{k+1}$. Donner $P(n+1)$.

Correction :

1. Si $k \in [\![1 ; n+1]\!]$, le fait que $P(k) = 1/k^2$ implique que $k^2P(k) - 1 = 0$, c'est-à-dire que $Q(k) = 0$: k est racine de Q. Dès lors, Q est divisible par $B = (X-1) \times \cdots \times (X-(n+1))$. Or, $\deg(P) = n$ donc $\deg(Q) = n+2$. Or, $\deg(B) = n+1$: le quotient est donc de degré 1. Il existe ainsi $(a, b) \in \mathbb{R}^2$ tels que $Q = (X-1) \times \cdots \times (X-n-1) \times (aX+b)$. Comme P est unitaire, Q l'est aussi donc $a = 1$. Nous avons exploité toutes les informations : pour obtenir la valeur de b, il nous faut une nouvelle équation. On remarque que $Q(0) = -1$, ce qui donne :

   $$(-1) \times \cdots \times (-n-1) \times b = (-1)^{n+1}(n+1)!b = -1$$

   si bien que $b = (-1)^n/(n+1)!$. Enfin,

   $$\begin{aligned} Q(n+2) &= (n+2-1) \times \cdots \times (n+2-n-1) \times \left(n+2+\frac{(-1)^n}{(n+1)!}\right) \\ &= (n+1) \times \cdots \times (1) \times \left(\frac{(n+2)(n+1)! + (-1)^n}{(n+1)!}\right) \\ &= (n+1)! \times \left(\frac{(n+2)! + (-1)^n}{(n+1)!}\right) \\ &= (n+2)! + (-1)^n. \end{aligned}$$

   En conclusion, $P(n+2) = \dfrac{Q(n+2)+1}{(n+2)^2} = \dfrac{(n+2)! + (-1)^n + 1}{(n+2)^2}$.
2. Posons $Q = (X+1) \times P - X$. Alors Q est de degré $n+1$ et s'annule en tous les $k \in [\![0 ; n]\!]$ donc admet $n+1$ racines distinctes : si on note a_n le coefficient dominant de P, c'est aussi le coefficient dominant de Q donc $Q = a_nX(X-1)\cdots(X-n)$. On en déduit que $Q(n+1) = a_n \times n(n-1) \times \cdots \times 1 = a_n \times n!$. Dès lors :

   $$P(n+1) = \frac{Q(n+1)}{(n+2)} + n + 1 = \frac{a_n \times n!}{n+2} + n + 1$$

Exercice 46 : ✪✪ Factoriser sur $\mathbb{C}$ le polynôme $8X^3 - 12X^2 - 2X + 3$ sachant que ses racines sont en progression arithmétique.

Correction : Notons h la raison de la progression arithmétique entre les trois (car de degré 3) racines de P. On pourrait noter les racines $a, a + ha + 2h$ mais on va plutôt les noter $a - h, a, a + h$ pour avoir un problème plus symétrique et pour simplifier les calculs. On a trois racines distinctes donc elles sont simples puisque $\deg(P) = 3$, et P est de coefficient dominant égal à 8 donc :

$$P = 8(X-a)(X-a+h)(X-a-h)$$

En développant, il vient :

$$\begin{aligned} P &= 8X^3 - 8\times 3aX^2 + 8\left[a(a-h)+a(a+h)+(a-h)(a+h)\right]X - 8a(a-h)(a+h) \\ &= 8X^3 - 24aX^2 + 8(a^2-ah+a^2+ah+a^2-h^2)X - 8a(a^2-h^2) \\ &= 8X^3 - 24aX^2 + 8(3a^2-h^2)X - 8a(a^2-h^2) \end{aligned}$$

Par unicité des coefficients :

$$-24a = -12, 8(3a^2-h^2) = -2 \qquad \text{et} \qquad -8(a^2-h^2) = 3$$

On trouve donc $a = 1/2$ et $h^2 = 5/8$ donc $a = \pm\sqrt{5/8}$ (il est logique qu'on trouve deux valeurs opposées de h, prendre l'une ou l'autre valeur de h ne fera qu'intervertir $a-h$ et $a+h$). Finalement :

$$P = 8\left(X-\frac{1}{2}\right)\left(X-\frac{1}{2}-\sqrt{\frac{5}{8}}\right)\left(X-\frac{1}{2}+\sqrt{\frac{5}{8}}\right)$$

Exercice 47 : ✪✪ On se place dans cet exercice sur $\mathbb{R}[X]$.

1. Montrer que si A et B sont deux polynômes qui sont sommes de deux carrés (de polynômes), il en est de même pour AB.
2. Montrer qu'un polynôme P est somme de deux carrés si et seulement s'il est positif, c'est-à-dire si et seulement si $P(x) \geq 0$ pour tout $x \in \mathbb{R}$.
3. **Remake :** Montrer qu'un polynôme P est positif sur $\mathbb{R}_+$ si et seulement s'il existe $(C,D) \in \mathbb{R}[X]^2$ tel que $P = C^2 + XD^2$. Le sens indirect est immédiat : s'il existe C et D tels que $P = C^2 + XD^2$ alors P est positif sur $\mathbb{R}_+$.

Correction :

1. Par hypothèse, il existe C, D, E, F dans $\mathbb{R}[X]$ tels que $A = C^2 + D^2$ et $B = E^2 + F^2$ donc

$$\begin{aligned} AB &= (C^2+D^2)(E^2+F^2) \\ &= C^2E^2 + C^2F^2 + D^2E^2 + D^2F^2 \\ &= C^2E^2 + 2CEDF + D^2F^2 + C^2F^2 - 2CEDF + D^2E^2 \\ &= (CE+DF)^2 + (CF-DE)^2 \end{aligned}$$

2. Il est évident qu'un polynôme somme de deux carrés est positif (rappelons qu'on se place sur $\mathbb{R}[X]$), prouvons la réciproque : supposons donc que P soit positif. Écrivons P comme produit de facteurs irréductibles sur $\mathbb{R}$:

$$P = a_n(X-x_1)^{\alpha_1}\cdots(X-x_r)^{\alpha_r}{Q_1}^{\beta_1}\cdots{Q_s}^{\beta_s}$$

où les Q_i sont des polynômes unitaires (car on a factorisé par le coefficient dominant de P) de degré 2 de discriminant strictement négatif. D'après la question précédente, il suffit de prouver que chacun des termes du produit est somme de deux carrés.

Tout d'abord, les α_i sont forcément pairs sinon P s'annule en changeant de signe en x_i ce qui est contraire à l'hypothèse $P(x) \geq 0$: il en découle que, pour tout i, $(X-x_i)^{\alpha_i} = \left((X-x_i)^{\alpha_i/2}\right)^2 + 0^2$.

De plus, $a_n > 0$ car P est positif (si $a_n < 0$ alors P tend vers $-\infty$ en $+\infty$ ce qui est exclu) donc $a_n = \sqrt{a_n}^2 + 0^2$.

Soit $i \in [\![1\,;\, s]\!]$. Prouvons enfin que Q_i est somme de deux carrés. Par produit, on en déduira que ${Q_i}^{\beta_i}$ l'est aussi et donc que P l'est ce qui terminera l'exercice. On note $Q = X^2 + bX + c$ avec $\Delta = b^2 - 4c < 0$. Il suffit d'écrire Q_i sous forme canonique :

$$\begin{aligned} Q_i &= X^2 + 2 \times b \times X + c \\ &= \left(X + \frac{b}{2}\right)^2 - \frac{b^2}{4} + c \\ &= \left(X + \frac{b}{2}\right)^2 + \frac{4c - b^2}{4} \\ &= \left(X + \frac{b}{2}\right)^2 + \frac{-\Delta}{4} \\ &= \left(X + \frac{b}{2}\right)^2 + \left(\sqrt{\frac{-\Delta}{2}}\right)^2 \end{aligned}$$

ce qui permet de conclure (rappelons que $-\Delta > 0$).

3. Erreur d'énoncé : il manque les carrés sur C et D, c'est-à-dire qu'on veut prouver que P est positif sur $\mathbb{R}_+$ si et seulement s'il existe C et D tels que $P = C^2 + XD^2$. Le raisonnement est ensuite le même.

   Prouvons que cette propriété passe au produit i.e. si A et B vérifient cette propriété alors AB aussi. Supposons qu'il existe C, D, E, F tels que $A = C^2 + XD^2$ et $B = E^2 + XF^2$. Par conséquent :

$$\begin{aligned} AB &= C^2E^2 + X(C^2F^2 + D^2E^2) + X^2D^2F^2 \\ &= C^2E^2 + 2XCDEF + X^2D^2F^2 + X(C^2F^2 - 2CDEF + D^2E^2) \\ &= (CE + XCF)^2 + X(CF + DE)^2 \end{aligned}$$

   Supposons que P soit positif sur $\mathbb{R}_+$. Là aussi donnons la décomposition de P en produit de facteurs irréductibles :

$$P = a_n(X - x_1)^{\alpha_1} \cdots (X - x_r)^{\alpha_r} {Q_1}^{\beta_1} \cdots {Q_s}^{\beta_s}$$

   Là aussi, il suffit de prouver que tous les éléments du produit vérifient la condition voulue.

   De même que ci-dessus, $a_n > 0$ donc $a_n = \sqrt{a_n}^2 + X \times 0^2$.

   Soit $i \in [\![1 ; r]\!]$. Si α_i est pair, alors $(X - x_i)^{\alpha_i} = \left((X - x_i)^{\alpha_i/2}\right)^2 + X \times 0^2$.

   Supposons α_i impair. Si $x_i > 0$ alors P change de signe en x_i ce qui est exclu car P est positif sur $\mathbb{R}_+$. Par conséquent, $x_i \leq 0$ donc $-x_i \geq 0$ si bien que $X - x_i = \sqrt{-x_i}^2 + X \times 1^2$.

   Passons aux polynômes Q_i qui sont de la forme $X^2 + bX + c$ avec $b^2 - 4c < 0$. Alors $c > 0$ sinon $b^2 - 4c \geq 0$. Par conséquent :

$$\begin{aligned} Q_i &= (X - \sqrt{c})^2 + 2\sqrt{c}X + bX \\ &= (X + \sqrt{c})^2 + X(b + 2\sqrt{c}) \end{aligned}$$

   Or, $b^2 < 4c$ donc $|b| < 2\sqrt{c}$ donc $-b \leq |b| < 2\sqrt{c}$ si bien que $2\sqrt{c} + b > 0$ et donc on a finalement

$$Q_i = (X + \sqrt{c})^2 + X \times \sqrt{b + 2\sqrt{c}}^2$$

   ce qui permet de conclure en passant au produit.

Exercice 48 : ✪✪✪ Soient $a_1, \ldots, a_n$ deux entiers deux à deux distincts. Montrer que

$$P = \prod_{k=1}^{n} (X - a_k)^2 + 1$$

est irréductible sur $\mathbb{Z}$ (i.e. si $P = AB$ avec A et B dans $\mathbb{Z}[X]$ alors A ou B est constant égal à ± 1).

Correction : Supposons que P s'écrive sous la forme $P = AB$ avec A et B dans $\mathbb{Z}[X]$. Supposons dans un premier temps que A et B soient non constants. En les évaluant en a_k, pour $k \in [\![1 ; n]\!]$, on trouve $A(a_k) \times B(a_k) = P(a_k) = 1$.

Puisque A et B sont à coefficients entiers, $A(a_k)$ et $B(a_k)$ appartiennent à $\mathbb{Z}$ donc $A(a_k) = B(a_k) = \pm 1$. Précisons que P n'a aucune racine réelle puisque ne prend que des valeurs strictement positives sur $\mathbb{R}$ (on identifie encore polynôme et fonction polynomiale). Dès lors, A et B (qui sont des fonctions continues, encore une fois en les identifiant à leur fonction polynomiale associée) sont de signe constant (à savoir faire !). Puisqu'elles coïncident en les a_k, elles sont de signe constant et de même signe : supposons sans perte de généralité que A et B sont strictement positives sur $\mathbb{R}$. On en déduit que :

$$\forall k \in [\![\, , \, ; \, A]\!](a_k) = B(a_k) = 1$$

c'est-à-dire que les a_k sont racines de $A-1$ et $B-1$. Par conséquent, les a_k étant deux à deux distincts, $A-1$ et $B-1$ sont divisibles par $\prod_{k=1}^{n}(X-a_k)$ c'est-à-dire qu'il existe C et D dans $\mathbb{R}[X]$ (en fait dans $\mathbb{Z}[X]$ car on divise par un polynôme unitaire, cf. exercice sur l'âge du fils et l'âge du chien, mais nous n'en avons pas besoin ici) tels que

$$A = C\prod_{k=1}^{n}(X-a_k)+1 \qquad \text{et} \qquad B = D\prod_{k=1}^{n}(X-a_k)+1$$

A et B étant non constants, C et D sont non nuls donc $\deg(A) \geq n$ et $\deg(B) \geq n$. Or, $AB = P$ de degré $2n$ donc $2n = \deg(A) + \deg(B) \geq 2n$: il y a donc égalité, ce qui implique que C et D soient constants. En développant le produit AB :

$$CD\prod_{k=1}^{n}(X-a_k)^2 + (C+D)\prod_{k=1}^{n}(X-a_k)+1 = P = \prod_{k=1}^{n}(X-a_k)^2+1$$

Il en découle que $CD = 1$ et $C + D = 0$ ce qui n'est pas possible sur $\mathbb{R}$: c'est absurde. On en déduit que A ou B est constant. Supposons A constant : alors A fois le coefficient dominant de B donne le coefficient dominant de P c'est-à-dire 1, et puisqu'on a des entiers, A est égal à ± 1.

3 Divers

Exercice 49 : ✪ Soit $n \geq 1$. Soit P un polynôme de degré n. Déterminer le degré des polynômes $Q = X^2P'$ et $R = XP' + P$.

Correction : P n'étant pas constant, P' est de degré $n-1$ donc Q est de degré $n+1$. De plus, XP' est aussi de degré n donc R est la somme de deux polynômes de même degré n : on en déduit que $\deg(P) \leq n$ mais pour donner le degré exact de R, il faut s'intéresser au coefficient dominant. Notons a_n le coefficient dominant de P (non nul par définition d'un coefficient dominant). Le coefficient dominant de XP' est donc na_n si bien que le coefficient devant X^n est $na_n + a_n = (n+1)a_n \neq 0$ donc R est de degré n.

Exercice 50 : ✪ Déterminer tous les polynômes P tels que $P(2) = 6$, $P'(2) = 1$, $P''(2) = 4$ et $P^{(n)}(2) = 0$ pour tout $n \geq 3$.

Correction : Analyse : si P convient. Alors $\deg(P) \geq 2$: en effet, rappelons que si P est de degré d alors $P^{(d+1)} = 0$. Rappelons aussi que si P est de degré $d \geq 0$, alors $P^{(d)}$ est constant non nul. On en déduit que P est de degré 2. Notons $P = aX^2+bX+c$. Alors $P' = 2aX+b$ et $P'' = 2a$. On déduit des données de l'énoncé que $a = 2$ puis que $b = -7$ et enfin $c = 12$.

Synthèse : il est immédiat que $P = 2X^2 - 7X + 12$ convient. C'est donc l'unique solution du problème.

Exercice 51 : ✪ Soit $P \in \mathbb{K}[X]$. Donner le degré de $Q = P(X) - P(X+1)$ en fonction de celui de P.

Correction : Mea culpa : il est trop difficile de donner le degré de Q en fonction de P (cela dépend trop des coefficients, il y a trop de cas à distinguer). Tout ce qu'on peut dire est que si P est nul alors Q aussi, si P est constant non nul, alors Q est nul, et si $\deg(P) = n \geq 1$ alors $\deg(Q) \leq n-1$ puisque Q est différence de deux polynômes de degré n de même coefficient dominant. Je virerai cet exercice l'an prochain.

Exercice 52 : ✪ Soient $n \in \mathbb{N}$ et $P \in \mathbb{K}_n[X]$. Montrer que

$$Q = \sum_{k=0}^{n}(-1)^k \times \frac{P^{(k)}(X) \times X^{k+1}}{(k+1)!}$$

est l'unique polynôme s'annulant en 0 dont la dérivée vaut P.

Correction : Il est immédiat que $Q(0) = 0$. Il suffit de prouver que $Q' = P$.

$$\begin{aligned} Q' &= \sum_{k=0}^{n}(-1)^k \times \frac{P^{(k+1)}(X)\times X^{k+1}}{(k+1)!} + \sum_{k=0}^{n}(-1)^k \times \frac{P^{(k)}(X)\times (k+1)X^k}{(k+1)!} \\ &= \sum_{j=1}^{n+1}(-1)^{j-1} \times \frac{P^{(j)}(X)\times X^j}{j!} + \sum_{k=0}^{n}(-1)^k \times \frac{P^{(k)}(X)\times X^k}{k!} \\ &= \sum_{k=1}^{n} P^{(k)}(X)\times(-1)^k \times \left(\frac{1}{k!}-\frac{1}{k!}\right) + (-1)^n \frac{P^{(n+1)}(X)\times X^{n+1}}{(n+1)!} + (-1)^0 \frac{P^{(0)}(X)\times X^0}{0!} \end{aligned}$$

Or, $P^{(n+1)}(X) = 0$ puisque $P \in \mathbb{K}_n[X]$. Tous les termes ci-dessus sont donc nuls à part le dernier qui vaut P.

Exercice 53 - Polynômes à coefficients alternés : ✪ On dit qu'un polynôme $P \in \mathbb{R}[X]$ est à coefficients alternés s'il peut s'écrire sous la forme

$$P = \sum_{n=0}^{+\infty}(-1)^n a_n X^n$$

où $(a_n)_{n\in\mathbb{N}}$ est une suite presque nulle de réels positifs. Montrer que le produit de deux polynômes à coefficients alternés est encore à coefficients alternés.

Correction : Soient

$$P = \sum_{n=0}^{+\infty}(-1)^n a_n X^n \qquad \text{et} \qquad Q = \sum_{n=0}^{+\infty}(-1)^n b_n X^n$$

deux polynômes alternés i.e. avec (a_n) et (b_n) deux suites presque nulles positives. Par conséquent,

$$PQ = \sum_{n=0}^{+\infty} c_n X^n$$

avec, pour tout $n \in \mathbb{N}$:

$$\begin{aligned} c_n &= \sum_{k=0}^{n}(-1)^k a_k (-1)^{n-k} b_{n-k} \\ &= \sum_{k=0}^{n}(-1)^n a_k b_{n-k} \\ &= (-1)^n \sum_{k=0}^{n} a_k b_{n-k} \end{aligned}$$

Or, par somme et produit, la somme ci-dessus est positive si bien que c_n est égal à $(-1)^n$ multiplié par un terme positif : PQ est alterné.

Exercice 54 : ✪ Soit $n \in \mathbb{N}^*$. Donner le degré et le coefficient dominant de

$$P = \prod_{\ell=1}^{n}\left(64X^6 + 2022X^4 + \ell\right)^{\ell^2}$$

Correction : Le degré d'un produit étant la somme des degrés :

$$\deg(P) = \sum_{\ell=1}^{n} \deg\left(\left(64X^6 + 2022X^4 + \ell\right)^{\ell^2}\right)$$

Or, $\deg(P^k) = k\deg(P)$ si bien que :

$$\deg(P) = \sum_{\ell=1}^{n} \ell^2 \deg\left(64X^6 + 2022X^4 + \ell\right)$$

Finalement :

$$\begin{aligned}\deg(P) &= \sum_{\ell=1}^{n} 6\ell^2 \\ &= n(n+1)(2n+1)\end{aligned}$$

De plus le coefficient dominant est égal à

$$\prod_{\ell=1}^{n} 64^{\ell^2} = 64^{\sum_{\ell=1}^{n} \ell^2} = 64^{n(n+1)(2n+1)/6}$$

Exercice 55 - Un peu de cryptographie : ✪

Pierre le fermier, Jules le métalleux et Jean le musicien décident d'acheter un coffre-fort pour entreposer l'argent du loyer. Comme ils ne se font pas confiance, il doit être impossible à l'un d'entre eux d'ouvrir le coffre seul, ou à deux d'entre eux d'ouvrir le coffre sans le troisième. Par contre, ils doivent quand même pouvoir l'ouvrir une fois par mois pour sortir l'argent du loyer, ou n'importe quand, par exemple pour payer l'électricité, à la condition qu'ils soient tous les trois réunis. Bien sûr, quand ils l'ont ouvert, ils connaissent le code, donc celui-ci doit changer à chaque ouverture. Ils demandent conseil à Antoine le professeur, qui est honnête et en qui tous les trois ont confiance. Dans sa grande sagesse, il leur propose le protocole suivant :

- Antoine le professeur choisit un polynôme $P \in \mathbb{R}_2[X]$, qu'il garde secret.
- Il choisit trois réels distincts a_1, a_2 et a_3, et calcule $b_1 = P(a_1), b_2 = P(a_2)$ et $b_3 = P(a_3)$. Tout cela est gardé secret.
- Il donne à Pierre le fermier le couple (a_1, b_1), à Jules le métalleux le couple (a_2, b_2) et à Jean le musicien le couple (a_3, b_3). Chacun des colocataires connaît son couple, mais pas celui des autres.
- Les colocataires savent que le code du coffre est la valeur en 42 du polynôme d'interpolation de Lagrange passant par les trois points $(a_1, b_1), (a_2, b_2)$ et (a_3, b_3). Ainsi, s'ils veulent ouvrir le coffre, il leur suffit de mettre leurs couples (qu'on appelle leurs clefs privées) en commun, de calculer le polynôme en question (n'oublions pas qu'ils ont fait une classe prépa !) et de trouver le code.
- Une fois le coffre ouvert, ils rappellent Antoine le professeur pour qu'il choisisse un nouveau polynôme et leur donne de nouvelles clefs (c'est-à-dire de nouveaux couples de réels).

1. On rappelle que le polynôme d'interpolation de Lagrange L passant par les trois points est l'unique polynôme de degré ≤ 2 passant par ces trois points (il n'est pas demandé de le montrer). Montrer que $L = P$.
2. La clef de Pierre est $(1, 5)$, celle de Jules est $(2, 3)$ et celle de Jean est $(-1, 36)$. Donner le code du coffre.
3. Pierre et Jules veulent voler l'argent de Jean : Pierre pour s'acheter une trayeuse, et Jules pour aller au Hellfest. Ils mettent donc leurs clefs en commun. Puisqu'ils ne connaissent pas celle de Jean, ils vont essayer de deviner le code. Peut-être qu'après tout ils peuvent déterminer P rien qu'avec leurs deux clefs, ou au moins réduire les possibilités.
   (a) Soit $\alpha \in \mathbb{R}$. Exhiber un polynôme $Q \in \mathbb{R}_2[X]$ vérifiant $Q(1) = 5, Q(2) = 3$ et $Q(42) = \alpha$.
   (b) Pierre et Jules peuvent-ils ouvrir le coffre sans Jean ?

Correction :

1. L et P sont deux polynômes de degré inférieur ou égal à 2 qui coïncident en au moins trois points distincts (a_1, a_2 et a_3)donc ils sont égaux.
2. Comme en cours, le polynôme L est donné par (on n'oublie pas que $-(-1) = +1$)

$$L = 5 \times \frac{(X-2)(X+1)}{(1-2)(1+1)} + 3 \times \frac{(X-1)(X+1)}{(2-1)(2+1)} + 36 \times \frac{(X-1)(X-2)}{(-1-1)(-1-2)}$$

   Après calculs, on trouve $L = \frac{9X^2}{2} - \frac{31X}{2} + 16$. Finalement, le code du coffre est $L(42) = 7303$.
3. (a) Le polynôme d'interpolation passant par les trois points $(1, 5), (2, 3)$ et $(42, \alpha)$ convient (et c'est même le seul !) :

$$Q = 5 \times \frac{(X-2)(X-42)}{(1-2)(1-42)} + 3 \times \frac{(X-1)(X-42)}{(2-1)(2-42)} + \alpha \times \frac{(X-1)(X-2)}{(42-1)(42-2)}$$

   (b) Pour tout $\alpha \in \mathbb{R}$, il existe un polynôme Q tel que $Q(1) = 10, Q(2) = 9$ et $Q(42) = \alpha$. Aucun réel n'est privilégié, et on ne peut exclure aucun réel : Pierre et Jules ne peuvent absolument pas deviner la combinaison du coffre : Pierre et Jules ne peuvent pas ouvrir le coffre sans Jean.

Exercice 56 : ✪✪ Soient P et Q deux polynômes réels distincts de degré $n \geq 0$. Montrer que $\deg\left(P^3 - Q^3\right) \geq 2n$. Le résultat est-il encore valable sur $\mathbb{C}$?

Correction : On a : $P^3 - Q^3 = (P-Q)(P^2+PQ+Q^2)$ si bien que

$$\deg(P^3 - Q^3) = \deg(P-Q) + \deg(P^2+PQ+Q^2)$$

Or, $P-Q \neq 0$ donc $\deg(P-Q) \geq 0$: il suffit donc de prouver que $P^2+PQ+Q^2 \geq 2n$. Notons a_n le coefficient dominant de P et b_n le coefficient dominant de Q (réels et non nuls par définition d'un coefficient dominant). On a des produits de polynômes de degré n donc on a des polynômes de degré $2n$. Plus précisément, le coefficient de X^{2n} dans l'écriture de P^2+PQ+Q^2 est ${a_n}^2 + a_n b_n + {b_n}^2$. Or :

$${a_n}^2 \pm 2a_n b_n + {b_n}^2 = (a_n \pm b_n)^2 \geq 0$$

si bien que ${a_n}^2 + {b_n}^2 \geq 2|a_n b_n| > |a_n b_n| \geq -a_n b_n$ (l'inégalité stricte vient du fait que $a_n b_n$ n'est pas nul). Par conséquent, ${a_n}^2 + a_n b_n + {b_n}^2 > 0$ donc P^2PQ+Q^2 est de degré $2n$ ce qui est le résultat voulu. Le résultat est faux sur $\mathbb{C}$ car on peut avoir $P = jQ$ et alors $P^3 = Q^3$ donc $P^3 - Q^3 = 0$ qui est de degré $-\infty$.

Exercice 57 : ✪✪ Montrer que pour tout $P \in \mathbb{K}[X]$,

$$P(X+1) = \sum_{n=1}^{+\infty} \frac{P^{(n)}(X)}{n!}$$

cette somme étant en fait finie.

Correction : Soit $x \in \mathbb{K}$. D'après la formule de Taylor avec $\alpha = x$:

$$P(X) = \sum_{n=1}^{+\infty} \frac{P^{(n)}(\alpha) \times (X-\alpha)^n}{n!}$$

En évaluant en $x+1$:

$$P(x+1) = \sum_{n=1}^{+\infty} \frac{P^{(n)}(\alpha) \times (x+1-\alpha)^n}{n!}$$

et en se souvenant du fait que $\alpha = x$:

$$P(x+1) = \sum_{n=1}^{+\infty} \frac{P^{(n)}(x)}{n!}$$

Par conséquent, les deux polynômes $P(X)$ et $\displaystyle\sum_{n=1}^{+\infty} \frac{P^{(n)}(X)}{n!}$ sont égaux car coïncident en tout point.

Exercice 58 : ✪✪ Résoudre une équation dont l'inconnue est un polynôme se fait toujours par analyse/synthèse. De façon générale, on s'intéresse à une caractéristique du polynôme P, ce qui réduit considérablement le choix, et ensuite on passe à la synthèse. Il y a en gros trois façons de faire, chacune étudiée dans un exemple ci-dessous.

1. Trouver tous les polynômes P vérifiant $P(2X) = P'(X)P''(X)$ (s'intéresser au degré).
2. Trouver tous les polynômes P vérifiant $(X+4)P(X) = XP(X+1)$ (s'intéresser aux racines de P).
3. Trouver tous les polynômes P vérifiant $(X^2+1)P'' = 6P$ (s'intéresser au coefficient dominant).
4. Trouver tous les polynômes P vérifiant $P\left(X^2\right) = (X^2+1)P(X)$ (débrouillez-vous !).

Correction :

1. On veut s'intéresser au degré : rappelons que, si on veut donner le degré de P' en fonction du degré de P, il faut séparer les cas selon que P est constant ou non. Le polynôme nul est évidemment solution. Si P est constant non nul, alors P n'est pas solution car $P(2X)$ est constant non nul et P' est nul. Examinons le cas où P est de degré 1 (car alors P' est constant et on s'intéresse au degré de P''). Si P est constant alors $P'' = 0$ et $P(2X)$ n'est pas nul donc P n'est pas solution. Supposons à présent P de degré $n \geq 2$.

   Analyse : si P convient. P étant de degré $n \geq 2$, P' est de degré $n-1$ et P'' de degré $n-2$. Alors $\deg(P(2X)) = \deg(P) \times \deg(2X) = \deg(P) = n$ et $\deg(P' \times P'') = \deg(P') + \deg(P'') = n-1+n-2 = 2n-3$. Puisque P est solution, alors $P(2X) = P' \times P''$ donc en particulier ils ont le même degré, c'est-à-dire que $n = 2n-3$ donc $n = 3$. Il en découle qu'il existe a, b, c, d tels que $P = aX^3 + bX^2 + cX + d$. D'une part :

$$\begin{aligned} P(2X) &= a(2X)^3 + b(2X)^2 + c(2X) + d \\ &= 8aX^3 + 4bX^2 + 2cX + d \end{aligned}$$

et d'autre part, $P' = 3aX^2 + 2bX + c$ et $P'' = 6aX + 2b$ si bien que

$$P' \times P'' = 18a^2X^3 + 18abX^2 + (6ac + 4b^2)X + 2bc$$

Par unicité des coefficients :

$$8a = 18a^2, 4b = 18ab, 2c = 6ac + 4b^2 \qquad \text{et} \qquad d = 2bc$$

Or, P est supposé de degré 3 donc $a \neq 0$ (sinon P n'est pas de degré 3) donc $18a = 8$ si bien que $a = 4/9$. Par conséquent, $4b = 8b$ (on réinjecte dans la deuxième égalité) donc $b = 0$. Avec la troisième équation, on trouve $2c = 8c/3$ donc $c = 0$ et $d = 2bc = 0$. Finalement, $P = 4X^3/9$.

Synthèse : Posons $P = 4X^3/9$. Alors $P(2X) = 32X^3/9$ et $P' = 12X^2/9 = 4X^2/3$ et $P'' = 8X/3$ si bien que $P' \times P'' = 32X^3/9 = P(2X)$: P est bien solution. En conclusion, les seules solutions sont le polynôme nul et $4X^3/9$.

2. Suivons l'indication de l'énoncé et cherchons les racines des solutions éventuelles (la démarche précédente ne fonctionne pas ici puisque les deux membres de l'égalité ont le même degré : $\deg(P) + 1$). **Analyse :** Soit P un polynôme qui convient. Alors $(X + 4)P(X) = XP(X + 1)$. En évaluant en 0 : $4P(0) = 0 \times P(1) = 0$ donc $P(0) = 0$: 0 est racine de P. Par conséquent, P est divisible par X : il existe $Q \in \mathbb{R}[X]$ tel que $P = XQ$. En réinjectant dans l'égalité, cela donne :

$$(X + 4)XQ(X) = X(X + 1)Q(X + 1)$$

puisque $P(X) = XQ(X)$ donc $P(X + 1) = (X + 1)Q(X + 1)$. De même, en évaluant en -1 : $(-3)(-1)Q(-1) = (-1) \times 0 \times Q(0)$ donc $Q(-1) = 0$: -1 est racine de Q, Q est donc divisible par $X + 1$ (et pas $X - 1$: α est racine de Q si et seulement si Q est divisible par $X - \alpha$) donc il existe R tel que $Q(X) = (X + 1)R(X)$. En réinjectant dans l'égalité :

$$(X + 4)X(X + 1)R(X) = X(X + 1)(X + 2)R(X + 1)$$

De même, -2 est racine de R donc il existe S tel que $R(X) = (X + 2)S(X)$ et donc :

$$(X + 4)X(X + 1)(X + 2)S(X) = X(X + 1)(X + 2)(X + 3)S(X + 1)$$

De même, -3 est racine de S donc il existe T tel que $S(X) = (X + 3)T(X)$ et donc :

$$(X + 4)X(X + 1)(X + 2)(X + 3)T(X) = X(X + 1)(X + 2)(X + 3)(X + 4)T(X + 1)$$

Ici, par contre, cette méthode ne marche plus : si on évalue en -4, cela donne $0 \times \cdots \times T(-4) = 0$ mais puisqu'on multiplie $T(-4)$ par 0, on ne peut pas affirmer que $T(-4)$ est nul. Dans l'égalité ci-dessus, simplifions par $X(X + 1)(X + 2)(X + 3)(X + 4)$ (on peut simplifier par un polynôme non nul, $\mathbb{K}[X]$ est un anneau intègre, tout élément non nul est régulier) ce qui donne $T(X) = T(X + 1)$: T est périodique donc est constant (cf. cours, ce n'est pas explicitement au programme, à savoir redémontrer !) disons constant égal à λ. Par conséquent, $S = \lambda(X + 3)$, $R = \lambda(X + 2)(X + 3)$, $Q = \lambda(X + 1)(X + 2)(X + 3)$ et finalement $P = \lambda X(X + 1)(X + 2)(X + 3)$.

Synthèse : Soit $\lambda \in \mathbb{R}$ et soit $P = \lambda X(X+1)(X+2)(X+3)$. Alors P est solution (exo). En conclusion, les polynômes solutions sont exactement les polynômes de la forme $P = \lambda X(X + 1)(X + 2)(X + 3)$ avec $\lambda \in \mathbb{R}$.

3. Idem, ici le degré ne marche pas car les degrés sont les mêmes, et aucune racine (réelle) ne saute aux yeux. Suivons l'indication de l'énoncé et intéressons-nous au coefficient dominant. Pour cela, le polynôme doit être non nul. Remarquons que le polynôme nul est solution. Soit à présent P non nul. Tout d'abord, si $\deg(P) \leq 1$ alors $P'' = 0$ donc P n'est pas solution. Supposons à présent P de degré $n \geq 2$ et notons $a_n \neq 0$ son coefficient dominant. Le coefficient dominant de $6P$ est $6a_n$ et le coefficient dominant de P'' est $n(n-1)a_n$ (le terme dominant de P est a_nX^n et on dérive deux fois) donc le coefficient dominant de $(X^2+1)P''$ est aussi $n(n-1)a_n$ si bien que $n(n-1)a_n = 6a_n$ et $a_n \neq 0$ donc $n(n-1) = 6$ si bien que $n^2 - n - 6 = 0$. Par conséquent, $n = 3$ ou $n = -2$ mais n est un entier positif donc $n = 3$: P est de degré 3, donc il existe a, b, c, d avec a non nul (le coefficient dominant) tels que $P = aX^3 + bX^2 + cX + d$. D'une part, $6P = 6aX^3 + 6bX^2 + 6cX + 6d$ et d'autre part, $P' = 3aX^2 + 2bX + c$ et $P'' = 6aX + 2b$ donc

$$(X^2 + 1)P'' = 6aX^3 + 2bX^2 + 6aX + 2b$$

Par unicité des coefficients, $6a = 6a$ (les coefficients dominants sont égaux : on le savait déjà !), $6b = 2b$ donc $b = 0$, $6c = 6a$ donc $a = c$, et enfin $6d = 2b$ donc $d = 0$. Finalement, $P = a(X^3 + X)$.

Synthèse : Soit $a \in \mathbb{R}^*$ et soit $P = a(X^3 + X)$. Alors $6P = 6a(X^3 + X)$ et $P'' = 6aX$ si bien que $(X^2 + 1)P'' = 6aX^2 + 6aX = 6P$: P est solution.

En conclusion, les solutions sont exactement les polynômes du type $P = a(X^3 + X)$ avec $a \in \mathbb{R}$ (y compris $a = 0$ puisque le polynôme nul est solution).

4. Intéressons-nous au degré. Le polynôme nul est solution : supposons à présent que P soit de degré n avec $n \geq 0$. **Analyse :** supposons P solution. Alors $\deg(P(X^2)) = \deg(P) \times \deg(X^2) = 2n$ et $\deg((X^2 + 1)P(X)) = \deg(X^2 + 1) + \deg(P) = n + 2$ donc $2n = n + 2$. On en déduit que $n = 2$: il existe a, b, c tels que $P = aX^2 + bX + c$. Par conséquent, $(X^2 + 1)P(X) = aX^4 + bX^3 + (a + c)X^2 + bX + c$ et d'autre part, $P(X^2) = aX^4 + bX^2 + c$. Par unicité des coefficients, $a = a$, ce qui n'apporte aucune information, $b = 0$, $(a + c) = b$ donc $a = -c$, $b = 0$ et $c = c$. On en déduit que $P = a(X^2 - 1)$.

Synthèse : Soit $a \in \mathbb{R}^*$ et soit $P = a(X^2 - 1)$. Alors P est solution (exo). En conclusion, les solutions sont exactement les polynômes du type $P = a(X^2 - 1)$ avec $a \in \mathbb{R}$ (y compris $a = 0$ puisque le polynôme nul est solution).

Exercice 59 - Polynômes de Legendre : ✪✪ Pour tout $n \in \mathbb{N}$, on pose $P_n = \left(X^2 - 1\right)^n$ et

$$L_n = \frac{1}{2^n \times n!} \times {P_n}^{(n)}$$

1. Déterminer le degré et le coefficient dominant de L_n.
2. Calculer $L_n(1)$ et $L_n(-1)$.

Correction :

1. P_n étant de degré $2n$, sa dérivée n-ième est de degré n donc L_n également. P_n est unitaire de degré $2n$ donc son terme dominant est X^{2n} : en dérivant n fois, le terme dominant est $2n(2n-1)\cdots(n+1)X^n$ donc le coefficient dominant de L_n est

$$\frac{(2n)!}{2^n \times n!^2}$$

2. On sait que $P_n = A_n B_n$ avec $A_n = (X - 1)^n$ et $B_n = (X + 1)^n$. D'après la formule de Leibniz :

$${P_n}^{(n)} = \sum_{k=0}^{n} \binom{n}{k} {A_n}^{(k)} {B_n}^{(n-k)}$$

Or, 1 est racine de multiplicité n de A_n : il en découle que ${A_n}^{(k)}(1) = 0$ pour tout $k \leq n - 1$. En d'autres termes, tous les termes de la somme sont nuls en 1 à part le terme pour $k = n$ qui vaut ${A_n}^{(n)}(1) \times B_n(1)$. Or, ${A_n}^{(n)}$ est le polynôme constant égal à $n!$ et $B_n(1) = 2^n$ si bien que ${P_n}^{(n)}(1) = 2^n \times n!$ et donc $L_n(1) = 1$. On trouve de même que $L_n(-1) = (-1)^n$.

Exercice 60 - Lemme de Gauß : ✪✪✪ Si $P \in \mathbb{Z}[X]$ est non nul, on appelle contenu de P, noté $c(P)$, le PGCD des coefficients de P, et un polynôme est dit primitif lorsque son contenu vaut 1.

1. On se donne dans cette question uniquement deux polynômes primitifs $P = a_n X^n + \cdots + a_0$ et $Q = b_m X^m + \cdots + b_0$. Soit p premier.
   (a) Justifier l'existence de $i_0 = \min\{i \in \mathbb{N} \,|\, p \nmid a_i\}$ et $j_0 = \min\{j \in \mathbb{N} \,|\, p \nmid b_j\}$.
   (b) À l'aide du coefficient d'indice $i_0 + j_0$ de PQ, montrer que PQ est primitif.
2. Montrer que pour tous P et Q non nuls (pas forcément primitifs), $c(PQ) = c(P)c(Q)$.

Correction :

1. (a) Une partie non vide de $\mathbb{N}$ admet toujours un minimum : il suffit de prouver que ces parties sont non vides, donc qu'il existe i et j tel que $p \nmid a_i$ et $p \nmid b_j$. Or, P et Q sont primitifs donc leurs coefficients ne peuvent tous être divisibles par p, sinon le PGCD des coefficients serait divisible par p ce qui n'est pas le cas.
   (b) Suivons l'indication de l'énoncé et intéressons-nous au coefficient d'indice $i_0 + j_0$ de PQ, coefficient qu'on note $c_{i_0+j_0}$. Par définition :

$$c_{i_0+j_0} = \sum_{i=0}^{i_0+j_0} a_i b_{i_0+j_0-i}$$

Si $i < i_0$, alors $p \mid a_i$ puisque, par définition de i_0, p divise tous les coefficients avant a_{i_0}, donc $p \mid a_i b_{i_0+j_0-i}$. Si $i > i_0$, alors $i_0 - i < 0$ donc $i_0 + j_0 - i < j_0$ et, de même, p divise $b_{i_0+j_0-i}$ donc $a_i b_{i_0+j_0-i}$. On en déduit que p divise tous les termes de la somme sauf (peut-être) celui d'indice i_0. Dès lors :

$$c_{i_0+j_0} \equiv a_{i_0} b_{j_0} [p]$$

Cependant, p ne divise par a_{i_0} ni b_{j_0} donc ne divise pas leur produit (car p est premier !). Il en découle que $c_{i_0+j_0} \not\equiv 0[p]$ donc p ne divise pas ce coefficient. On en déduit que les coefficients de PQ n'ont aucun facteur premier commun puisque, pour tout p premier, il existe un coefficient qui n'est pas divisible par p. Finalement, PQ est primitif : si d est le PGCD des coefficients de PQ, alors d n'est divisible par aucun nombre premier d'après ce qui précède donc $d = 1$ (un PGCD est forcément strictement positif).

2. Notons $A = P/c(P)$ et $B = Q/c(Q)$. A et B sont non nuls et à coefficients dans $\mathbb{Z}$ puisque $c(P)$ est le PGCD des coefficients de P donc les divise tous, et idem pour $c(Q)$. De plus, A et B sont primitifs : en effet, si d est le PGCD des coefficients de A donc tous les coefficients de A sont divisibles par d donc tous les coefficients de P sont divisibles par $c(P) \times d$: or, $c(P)$ est le plus grand diviseur commun des coefficients donc $d = 1$. Idem pour B. D'après la question précédente, AB est primitif. Or, $PQ = c(P)c(Q)AB$. En d'autres termes, tous les coefficients de AB sont multipliés par $c(P)c(Q)$: leur PGCD est donc aussi multiplié par $c(P)c(Q)$ (cf. chapitre 6). En d'autres termes, $c(PQ) = c(P)c(Q)c(AB)$ mais $c(AB) = 1$, ce qui permet de conclure.

Exercice 61 : ✪✪✪ Donner tous les polynômes $P \in \mathbb{Q}[X]$ tels que $P(\mathbb{R}\backslash\mathbb{Q}) \subset \mathbb{R}\backslash\mathbb{Q}$. On pourra utiliser l'exercice 27.

Correction : Les polynômes non constants (à valeurs dans $\mathbb{Q}$) ne sont évidemment pas solutions. Soit $P = aX + b \in \mathbb{Q}[X]$ de degré 1 (donc avec $a \neq 0$). Soit $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. Si $P(\alpha) \in \mathbb{Q}$ alors

$$\alpha = \frac{P(\alpha) - b}{a} \in \mathbb{Q}$$

en tant que quotient de rationnels, ce qui est absurde. En d'autres termes, $P(\alpha) \in \mathbb{R}\backslash\mathbb{Q}$: les polynômes de degré 1 conviennent. Montrons que ce sont les seuls. Soit $P \in \mathbb{Q}[X]$ de degré $n \geq 2$, qu'on note comme d'habitude $P = a_n X^n + \cdots + a_1 X + a_0$ avec $a_n \neq 0$. Suivons l'indication de l'énoncé et utilisons l'exercice 27. Cet exercice parlant de polynômes à coefficients entiers, transformons P de manière à ce qu'il soit à coefficients entiers. Plus précisément, soit m le PPCM des dénominateurs des coefficients de P. Alors $mP \in \mathbb{Z}[X]$. Notons $Q = mP = b_n X^n + \cdots + b_1 X + b_0 \in \mathbb{Z}[X]$ avec $b_n \neq 0$.

Supposons $b_n > 0$ (raisonnement analogue dans l'autre cas). Alors (on identifie polynôme et fonction polynomiale) $Q(x) \xrightarrow[x\to+\infty]{} +\infty$: tout $k \in \mathbb{Z}$ et supérieur à $Q(0)$ est atteint par Q (TVI, Q est continu). Puisque l'exercice 29 parle de racine, transformons ceci en racine : un réel x_k est solution de $Q(x_k) = k$ si et seulement si x_k est racine de $Q_k = Q - k$. Soit donc $k \in \mathbb{Z}$ tel que $k \geq Q(0)$. Supposons que $x_k \in \mathbb{Q}$. D'après l'exercice 29, x_k est de la forme a/b_n avec b_n le coefficient dominant de Q_k donc de Q (Q et Q_k ont même coefficient dominant, seul change leur terme constant). En d'autres termes, tous les antécédents d'entiers (assez grands) par Q sont de la forme a/b_n. En particulier, deux antécédents d'entiers sont distants d'au moins $1/b_n$, c'est-à-dire que si x_k est l'antécédent de k et x_{k+1} celui de $k+1$, alors $x_{k+1} - x_k \geq 1/b_n$. Montrons que ce n'est pas possible pour k assez grand car « Q devient de plus en plus raide donc, en un laps de temps $1/b_n$, fait des bonds plus grands que 1 ».

Puisque Q est de degré supérieur ou égal à 2, alors Q' est de degré supérieur ou égal à 1 et de coefficient dominant $nb_n > 0$ donc $Q'(x) \xrightarrow[x\to+\infty]{} +\infty$. En particulier, il existe A tel que, pour tout $x \geq A$, $Q'(x) > b_n$. Soit $k \in \mathbb{Z}$ tel que $k \geq Q(A)$: d'après le TVI, il existe $x_k \leq x_{k+1}$ supérieurs à A tels que $Q(x_k) = k$ et $Q(x_{k+1}) = k + 1$. Si x_k et x_{k+1} sont rationnels, d'après ce qui précède, $x_{k+1} - x_k \geq 1/b_n$. Or, d'après l'IAF, Q' étant strictement supérieur à b_n à partir de A, il vient :

$$Q(x_{k+1}) - Q(x_k) > b_n \times (x_{k+1} - x_k) \geq b_n \times \frac{1}{b_n} = 1$$

ce qui est absurde puisque $Q(x_{k+1}) = k + 1$ et $Q'x_k) = k$: il en découle que l'un des deux est irrationnels, et puisqu'il a une image entière (donc rationnelle), Q n'envoie pas les irrationnels sur des irrationnels, Q n'est pas solution du problème. En conclusion, les seuls polynômes qui conviennent sont exactement les polynômes de degré 1.

4 Arithmétique des polynômes

Exercice 62 : ✪ Effectuer à chaque fois la division euclidienne de A par B.

1. $A = 6X^6 - 3X^5 - 5X^2 + 10X - 6, B = 4X^3 + X - 1$.
2. $A = 7X^7 - 5X^5 + 3X^3 - X, B = 6X^6 - 4X^4 + 2X^2$.

1. Rappelons qu'on s'arrête quand on a un reste qui a un degré strictement inférieur au polynôme par lequel on divise.

$$\begin{array}{rrrrrrrrrrrrr|l}
6X^6 & - & 3X^5 & & & & & - & 5X^2 & + & 10X & - & 6 & 4X^3 + X + 1 \\
\cline{14-14}
-(6X^6 & & & + & 3X^4/2 & + & 3X^3/2) & & & & & & & 3X^3/2 - 3X^2/4 - 3X/8 - 3/16 \\
\cline{1-13}
 & & -3X^5 & - & 3X^4/2 & - & 3X^3/2 & - & 5X^2 & + & 10X & - & 6 & \\
 & - & (-3X^5 & & & - & 3X^3/4 & - & 3X^2/4) & & & & & & \\
\cline{2-13}
 & & & - & 3X^4/2 & - & 3X^3/4 & - & 17X^2/4 & + & 10X & - & 6 & \\
 & & - & (-3X^4/2 & & & & - & 3X^2/8 & - & 3X/8) & & & \\
\cline{3-13}
 & & & & & - & 3X^3/4 & - & 31X^2/8 & + & 83X/8 & - & 6 & \\
 & & & & - & (-3X^3/4 & & & & - & 3X/16 & - & 3/16) & \\
\cline{5-13}
 & & & & & & & - & 31X^2/8 & + & 169X/16 & - & 93/16 &
\end{array}$$

2. Là, c'est beaucoup plus simple :

$$\begin{array}{rrrrr|l}
7X^7 & - & 5X^5 & + & 3X^3 & - X & 6X^6 - 4X^4 + 2X^2 \\
\cline{6-6}
-(7X^7 & - & 14X^5/3 & + & 7X^3/3) & & 7X/6 \\
\cline{1-5}
 & & -X^5/3 & + & 2X^3/3 & - X & \\
\end{array}$$

Exercice 63 : ✪ Calculer, pour $n \geq 2$, les restes des divisions euclidiennes de $P = (X-3)^{2n} + (X-2)^n - 2$ par, respectivement, $(X-3)(X-2)$ et $(X-2)^2$. Pour la deuxième, on pourra dériver l'expression obtenue en écrivant la division euclidienne. Recommencer en donnant le reste de la division euclidienne de $(X^n+1)^2$ par $(X+1)^2$, puis en donnant le reste de la division euclidienne de X^n par $(X-1)^3$.

Correction : Effectuer la division euclidienne n'est pas imaginable : P est de degré $2n$, le quotient serait de degré $2n-2$, nous n'y arriverions pas. Heureusement, on ne demande que le reste ! Il suffit d'appliquer le théorème de division euclidienne (on peut le faire car on ne divise pas par le polynôme nul) : il existe Q et R uniques tels que $P = Q \times (X-3)(X-2) + R$ avec $\deg(R) < \deg((X-3)(X-2)) = 2$. Ainsi, $\deg(R) \leq 1$: il existe a et b tels que $R = aX + b$ donc tels que

$$(X-3)^{2n} + (X-2)^n - 2 = Q \times (X-3)(X-2) + aX + b.$$

On cherche la valeur de a et la valeur de b. Évaluons l'égalité ci-dessus en 2 : on ne connaît pas $Q(2)$, mais puisque Q est multiplié par $(X-3)(X-2)$ qui est nul en 2, ce n'est pas grave. On a donc :

$$(2-3)^{2n} + (2-2)^n - 2 = Q(2) \times (2-3)(2-2) + 2a + b$$

c'est-à-dire que $(-1)^{2n} - 2 = -1 = 2a + b$. De même, en évaluant en 3, on obtient $-1 = 3a + b$. On a donc $a = 0$ et $b = -1$, si bien que $R = -1$. De même, il existe $Q \in \mathbb{R}[X]$ et $(a, b) \in \mathbb{R}^2$ (distincts des Q, a, b du cas précédent) tels que (nous noterons (E) cette égalité dans la suite) :

$$(X-3)^{2n} + (X-2)^n - 2 = Q \times (X-2)^2 + aX + b.$$

En évaluant en 2, il vient $2a + b = -1$. Cependant, on ne peut pas évaluer en un autre réel ici : si on évalue en un autre réel que 2, $X - 2$ ne sera pas nul et donc on aura une égalité faisant intervenir $Q(2)$, dont on ne connaît pas la valeur. Suivons l'indication de l'énoncé et dérivons l'égalité (E) :

$$2n(X-3)^{2n-1} + n(X-2)^{n-1} = Q' \times (X-2)^2 + Q \times 2(X-2) + a.$$

En évaluant en 2, il vient $a = 2n \times (-1)^{2n-1} = -2n$, si bien (à l'aide de l'égalité $2a + b = -1$ obtenue précédemment) que $b = 4n - 1$. Finalement, $R = -2nX + 4n - 1$.

De même, il existe Q et a et b uniques tels que $(X^n+1)^2 = Q \times (X+1)^2 + aX + b$. En évaluant en -1, on trouve que $b - a = ((-1)^n + 1)^2$. En dérivant l'égalité précédente, on trouve :

$$2nX^{n-1}(X^n+1) = Q' \times (X+1)^2 + Q \times 2(X+1) + a$$

et donc, en évaluant en -1, on trouve que $a = 2n \times (-1)^{n-1} \times ((-1)^n + 1)$ ce qui permet de trouver b et donc de conclure.

Idem, il existe Q et a, b, c uniques tels que $X^n = (X-1)^3 Q + aX^2 + bX + c$. En évaluant en 1, on trouve $a + b + c = 1$. En dérivant, il vient : $nX^{n-1} = 3(X-1)^2 Q + (X-1)^3 Q' + 2aX + b$ et en évaluant en 1 on trouve $n = 2a + b$. En dérivant encore une fois et en évaluant en 1 on trouve $a = n(n-1)$ et donc on trouve b et ensuite c.

Exercice 64 : ✪✪ Soit $(n, p) \in (\mathbb{N}^*)^2$. S'inspirer de l'exercice 60 du chapitre 6 pour prouver que $(X^n - 1) \wedge (X^p - 1) = X^{n \wedge p} - 1$.

Correction : Notons r le division euclidienne de la division euclidienne (d'entiers) de n par p. Puisque $r < p$ et $a \geq 2$, alors $\deg(X^r - 1) < \deg(X^p - 1)$. De l'écriture

$$X^n - 1 = X^r \times (X^{qp} - 1) + X^r - 1$$

on déduit que le reste dans la division euclidienne de $X^n - 1$ par $X^p - 1$ vaut $X^r - 1$. On itère ensuite le procédé : si on note $(r_1, \dots, r_k, 0)$ les restes successifs dans l'algorithme d'Euclide donnant $n \wedge p$ (et donc $r_k = n \wedge p$), les restes successifs dans l'algorithme d'Euclide donnant $(X^n - 1) \wedge (X^p - 1)$ sont $\left(X^{r_0} - 1, \dots, X^{r_k} - 1, X^0 - 1 = 0\right)$ si bien que $(X^n - 1) \wedge (a^p - 1)$, le dernier reste non nul, est égal à $X^{r_k} - 1 = X^{n \wedge p} - 1$.

Exercice 65 : ✪ Trouver les réels a tels que $X^2 - aX + 1$ divise $X^4 - X + a$ dans $\mathbb{R}[X]$.

Correction : Effectuons la division euclidienne de $X^4 + X + a$ par $X^2 - aX + 1$. Au bout de deux étapes, comme dans l'exercice 62, on se retrouve avec l'égalité suivante :

$$X^4 - X + a = (X^2 - aX + 1) \times (X^2 + aX) + (a^2 - 1)X^2 - (a + 1)X + a$$

On peut se dire qu'on n'a pas terminé puisque le reste n'est pas de degré < 2, mais attention : $a^2 - 1$ peut être nul, il faut différencier les cas. Si $a = \pm 1$, le reste n'est pas nul donc $X^2 - aX + 1$ ne divise pas $X^4 - X + a$. Supposons donc $a \neq 1$. Avec une dernière étape de division euclidienne, on obtient finalement que le reste est égal à

$$\left(-2a - 1 + a^2\right) X + (a - a^2 + 1)$$

et les deux coefficients ne sont jamais nuls en même temps : il n'y a aucune valeur de a qui convienne.

Exercice 66 : ✪ Montrer que $X^5 - 1$ et $X^2 + X + 1$ sont premiers entre eux. Déterminer une relation de Bézout entre ces polynômes.

Correction : Pour prouver qu'ils sont premiers entre eux, il suffit de prouver qu'ils n'ont aucune racine complexe commune donc que j et j^2 (les racines de $X^2 + X + 1$) ne sont pas racines de $X^5 - 1$. Puisque $X^5 - 1$ est à coefficients réels, il suffit même de prouver que j n'est pas racine de $X^5 - 1$ ce qui est immédiat puisque $j^5 = j \neq 1$. Cependant, on demande une relation de Bézout : on n'y coupe pas, il faut appliquer l'algorithme d'Euclide étendu. Je ne détaille pas les calculs de division euclidienne.

$$\begin{array}{r|l} X^5 - 1 & X^2 + X + 1 \\ \hline & X^3 - X^2 + 1 \\ -X - 2 & \end{array} \qquad \begin{array}{r|l} X^2 + X + 1 & -X - 2 \\ \hline & -X + 1 \\ 3 & \end{array} \qquad \begin{array}{r|l} -X - 2 & 3 \\ \hline & -X - 2 \\ 0 & \end{array}$$

Puisque le dernier reste non nul est constant, les deux polynômes sont premiers entre eux. De plus,

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

donc :

$$\begin{aligned} 1 &= -\frac{1}{3}(X^2 + X + 1) + \frac{1}{3}(-X - 2)(-X + 1) \\ &= -\frac{1}{3}(X^2 + X + 1) + \frac{1}{3}(-X + 1) \times \left[(X^5 - 1) - (X^2 + X + 1)(X^3 - X^2 + 1)\right] \\ &= \frac{1}{3} \times (-X + 1) \times (X^5 - 1) + (X^2 + X + 1) \times \left[-\frac{1}{3} - \frac{1}{3} \times (X + 1) \times (X^3 - X^2 + 1)\right] \end{aligned}$$

ce qui est bien une relation de Bézout.

Exercice 67 - Introduction au résultant : ✪ Soient n, m deux entiers naturels non nuls et P et Q deux éléments de $\mathbb{K}[X]$ de degrés respectifs n et m. Montrer que P et Q ne sont pas premiers entre eux si et seulement s'il existe deux polynômes A et B non nuls de $\mathbb{K}[X]$ de degrés $\deg A < m$ et $\deg B < n$ tels que $AP = BQ$.

Correction : Rappelons que, sur $\mathbb{C}$, « ne pas être premiers entre eux » est équivalent à « admettre une racine complexe commune ». Supposons que P et Q admettent une racine complexe commune notée z_0. Alors il existe A de degré $m - 1$ et B de degré $n - 1$ tels que $P = (X - z_0)B$ et $Q = (X - z_0)A$ et $AP = BQ = AB(X - z_0)$. Réciproquement, supposons qu'il existe de tels polynômes A et B. Raisonnons par l'absurde et supposons que P et Q soient premiers entre eux. $AP = BQ$ donc P divise BQ donc, d'après le théorème de Gauß (P et Q sont premiers entre eux) P divise B ce qui est absurde

puisque B est non nul de degré strictement inférieur au degré de P : P et Q ne sont pas premiers entre eux, d'où l'équivalence.

Exercice 68 - Pour tous les âges : ✪✪

Pierre le fermier et Jules le métalleux discutent :

« Devine l'âge de mon fils sachant qu'il est racine d'un polynôme P à coefficients entiers relatifs.
- Je crois qu'il a 7 ans.
- Ah non, $P(7) = 77$, il est plus vieux.
- Dans ce cas il a le même âge que mon chien.
- Non plus ! Si y est l'âge de ton chien, $P(y) = 85$. Il est encore plus vieux.
- C'est bon, j'ai trouvé. »

Le but de l'exercice est de faire comme Jules le métalleux et de trouver l'âge du fils... ainsi que l'âge du chien ! On reprend les notations du dialogue et on appelle $\alpha \in \mathbb{N}$ l'âge du fils.

1. Montrer que le théorème de la division euclidienne est encore valable sur $\mathbb{Z}$ si B est unitaire.
2. Quel âge a le fils ? et le chien ?

Correction :

1. Recopier la preuve du cours en remplaçant b_p par 1.
2. D'après le théorème de la division euclidienne sur $\mathbb{Z}$ (car $X - 7$ est unitaire), il existe Q_1 et R_1 uniques dans $\mathbb{Z}[X]$ tels que $P = Q_1 \times (X - 7) + R_1$ et $\deg(R_1) < \deg(X - 7)$. Donc, $\deg(R_1) < 1$ ce qui implique que R_1 est constant. En évaluant en $x = 7$ on obtient $P(7) = 0 + R_1$ c'est-à-dire que $R_1 = 77$. La méthode pour trouver R_2 est tout-à-fait analogue. Ainsi, il existe Q_1 et Q_2 dans $\mathbb{Z}[X]$ tels que $P = Q_1 \times (X - 7) + 77 = Q_2 \times (X - y) + 85$.

   En évaluant en y on obtient $Q_1(y) \times (y - 7) + 77 = 85$. Puisque $Q_1(y) \in \mathbb{Z}$ (car Q_1 est à coefficients dans $\mathbb{Z}$ et $y \in \mathbb{Z}$, il vient, en posant $k = Q_1(y)$: il existe $k \in \mathbb{Z}$ tel que $k \times (y - 7) = 8$. Or, $y - 7 > 0$ d'après l'énoncé, et les seuls diviseurs entiers positifs sont $1, 2, 4$ et 8, si bien que $y - 7 = 1, 2, 4$ ou 8.

   On a également $P = Q_1 \times (X - y) + 77$. α étant racine de P, on a $-Q_1(y) \times (\alpha - 7) = 77 = 7 \times 11$. $\alpha - 7$ est par conséquent positif (d'après l'énoncé) et un diviseur dans $\mathbb{Z}$ de 77 (car $Q_1(y) \in \mathbb{Z}$) et les seuls diviseurs de 77 étant $1, 7, 11, 77$, ce qui implique également que $\alpha - 7 = 1, 7, 11$ ou 77.

   De même en utilisant l'écriture $P = Q_2 \times (X - y) + 85$ et en voyant que $85 = 5 \times 17$: $\alpha - y = 1, 5, 17$ ou 85. D'après ce qui précède, $y = 8, 9, 11$ ou 15 et $\alpha = 8, 14, 18$ ou 84 (dans ce cas le père ne doit plus être tout jeune...). Enfin, on a aussi $\alpha - y = 1, 5, 17$ ou 85.
   - Si $y = \alpha = 8, \alpha - y = 0$ ce qui n'est pas possible (déjà car le chien est plus jeune que le fils).
   - Si $y = 8$ et $\alpha = 14, \alpha - y = 6$ ce qui n'est pas possible.

   Et ainsi de suite : la seule possibilité est d'avoir $\alpha = 14$ et $y = 9$: le fils a 14 ans et le chien a 9 ans.

Exercice 69 : ✪✪ Soit $n \geq 2$ un entier. Déterminer les polynômes de degré n, divisibles par $X + 1$ et dont les restes dans la division euclidienne par $X + 2, \ldots, X + n + 1$ sont égaux.

Correction : Raisonnons par analyse synthèse.
Analyse : Notons R le reste commun des divisions euclidiennes de P par $(X + 2), \ldots, (X + n + 1)$. D'après le théorème de division euclidienne, $\deg(R) < \deg(X + 2) = 1$ si bien que R est constant, disons égal à β. Notons respectivement $Q_1, \ldots, Q_{n+1}$ les restes dans les divisions euclidiennes de P par, respectivement, $X + 2, \ldots, X + n + 1$, si bien que

$$P = (X + 2) \times Q_2 + \beta = \cdots = (X + n + 1) \times Q_{n+1} + \beta$$

Il en découle que $P(-2) = P(-3) = \cdots = P(-(n + 1)) = \beta$. En d'autres termes, $-2, \ldots, -(n + 1)$ sont racines de $P - \beta$. Or, ce polynôme est de degré n (car P est de degré n) et admet n racines distinctes : celles-ci sont donc simples, et si l'on note a_n le coefficient dominant de P, on obtient :

$$P - \beta = a_n(X + 2) \times \cdots \times (X + n + 1)$$

Si bien que $P = a_n(X + 2) \times \cdots \times (X + n + 1) + \beta$. Enfin, $X + 1$ divise P donc $P(-1) = 0$, d'où :

$$0 = a_n(-1 + 2) \times \cdots \times (-1 + n + 1) + \beta$$

et donc $\beta = -a_n \times n!$. Finalement, $P = a_n \times [(X + 2) \times \cdots \times (X + n + 1) - n!]$.

Synthèse : Soit $a_n \in \mathbb{R}^*$ et soit $P = a_n \times [(X+2) \times \cdots \times (X+n+1) - n!]$. Montrons que P convient. Rappelons qu'il y a unicité dans le théorème de division euclidienne. Ainsi, si on a une écriture du type $P = BQ + R$ avec $\deg(R) < \deg(B)$ alors Q est le quotient et R est le reste. En particulier, si on a une écriture du type $P = BQ + R$ avec $\deg(B) = 1$ et R constant, alors R est le reste. Or,

$$P = (X+2) \times a_n(X+3)\cdots(X+n+1) - a_n \times n!$$

est une écriture de ce type : le reste de la division de P par $X+2$ est donc $-a_n \times n!$. On montre de même que c'est aussi le reste quand on divise par $(X+3), \ldots, (X+n+1)$. Enfin, un calcul simple donne bien $P(-1) = 0$ donc $X+1$ divise P : P est bien solution.

Conclusion : les polynômes solutions sont exactement les polynômes de la forme

$$P = a_n \times [(X+2) \times \cdots \times (X+n+1) - n!]$$

avec $a_n \neq 0$.

Exercice 70 : ✪✪✪ Soient P et Q appartenant à $\mathbb{Z}[X]$ n'ayant aucune racine complexe commune.

1. Montrer qu'il existe A et B appartenant à $\mathbb{Z}[X]$ et $d \in \mathbb{N}^*$ tels que $AP + BQ = d$.
2. Montrer que pour tout $n \in \mathbb{N}$, $P(n+d) - P(n)$ est divisible par d.
3. En déduire que la suite de terme général $u_n = P(n) \wedge Q(n)$ est d-périodique.

Correction :

1. A et B sont premiers entre eux car n'ont aucune racine complexe commune. D'après le théorème de Bézout, il existe U et V dans $\mathbb{Q}[X]$ tels que $AU + BV = D$, où D est **un** PGCD de A et B (pas forcément $A \wedge B$). En effet, U et V sont obtenus à l'aide de divisions d'entiers donc sont à coefficients rationnels (ou, si on veut faire les choses proprement : l'algorithme d'Euclide étendu et le théorème de Bézout qui en découle sont valables sur un corps, A et B sont à coefficients dans $\mathbb{Q}$ qui est un corps donc U, V et D sont à coefficients rationnels, pas forcément entiers car $\mathbb{Z}$ est un anneau et pas un corps). En multipliant par m le PPCM des dénominateurs de U, V, D, on obtient : $(mU)P + (mV)Q = (mD)$. Or, m étant un multiple de tous les dénominateurs, mU, mV et mD sont à coefficients entiers. Enfin, P et Q étant premiers entre eux, tous leurs PGCDs sont constants donc mD est constant (entier). Il suffit de poser $A = mU, B = mV$ et $d = mD$ pour conclure.
2. Notons $P = \sum_{k=0}^{d} a_k X^k$ avec d le degré de P (et donc a_d est le coefficient dominant de P). Soit $n \in \mathbb{N}$.

$$P(n+d) - P(n) = \sum_{k=0}^{d} a_k (n+d)^k - \sum_{k=0}^{d} a_k n^k$$

   Or, pour $k = 0$, $a_k(n+d)^k = a_0 = a_k n^k$ donc les deux termes se compensent : les deux sommes commencent en 1. Dès lors :

$$P(n+d) - P(n) = \sum_{k=1}^{d} a_k \left((n+d)^k - n^k\right)$$

   Or, pour tout $k \geq 1$:

$$(n+d)^k - n^k = (n+d-n)\sum_{i=0}^{k-1}(n+d)^i n^{k-1-i}$$

   Puisque $n + d - n = d$, ce terme est divisible par d donc tous les termes de la somme ci-dessus sont divisibles par d, ce qui permet de conclure.
3. Soit $n \in \mathbb{N}$. D'après la question 1, $A(n)P(n) + B(n)Q(n) = d$ donc, d'après le théorème de Bézout (pour les entiers), u_n (le PGCD de $P(n)$ et $Q(n)$) divise d. Par conséquent, d'après la question précédente, u_n divise $P(n+d) - P(n)$. Or, u_n divise $P(n)$ donc u_n divise $P(n+d)$. Par symétrie des rôles, u_n divise $Q(n+d)$ donc u_n divise u_{n+d} car est un diviseur commun de $P(n+d)$ et $Q(n+d)$. On prouve de même que u_{n+d} divise u_n donc u_n et u_{n+d} sont associés : ils sont soit égaux soit opposés, et puisqu'ils sont positifs, ils sont égaux, ce qui permet de conclure.

5 Relations coefficients-racines

Exercice 71 : ✪ Donner la somme et le produit des racines complexes (comptées avec multiplicité) de $P = 2X^5 + 3X^4 + 2X^3 + X^2 + X + 2022$.

Correction : Pour un polynôme de degré n dont les coefficients sont notés $a_0, \dots, a_n$, On sait que la somme des racines vaut $-a_{n-1}/a_n$ et le produit des racines $(-1)^n a_0/a_n$. On en déduit que la somme cherchée vaut $-3/2$ et le produit -1011 (car $(-1)^5 = -1$).

Exercice 72 : ✪ Soit $n \geq 1$. Calculer le produit

$$P = \prod_{k=1}^{n-1} \left(1 - e^{2ik\pi/n}\right)$$

Correction : Mea culpa, je ne vois pas ce que cet exercice fait dans cette section... On définit le polynôme

$$Q = \prod_{k=1}^{n} (X - e^{2ik\pi/n})$$

si bien que $P = Q(1)$. Or, Q est presque égal à

$$R = \prod_{k=0}^{n-1} (X - e^{2ik\pi/n}) = X^n - 1$$

Finalement, $X^n - 1 = (X-1) \times Q$ (je préfère ne pas faire de quotient de polynômes avant le chapitre suivant). Or, on a aussi : $X^n - 1 = (X-1)(1 + X + \cdots + X^{n-1})$. Un polynôme non nul étant régulier puisque $\mathbb{K}[X]$ est un anneau intègre :

$$Q = 1 + X + \cdots + X^{n-1}$$

si bien que $P = Q(1) = n$.

Exercice 73 : ✪ Soit $P \in \mathbb{C}[X]$ de degré $n \geq 1$. On note

$$\mu(P) = \frac{1}{n} \sum_{P(z)=0} z$$

la moyenne arithmétique des racines de P comptées avec multiplicité. Montrer que $\mu(P) = \mu(P')$.

Correction : Notons $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ avec $a_n \neq 0$. D'après le cours, la somme des racines est égale à $-a_{n-1}/a_n$ donc

$$\mu(P) = -\frac{a_{n-1}}{n \times a_n}$$

De plus, $P' = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \cdots + 2a_2 X + a_1$. Par conséquent, la somme des racines de P' est $-(n-1)a_{n-1}/na_n$ (moins l'avant dernier coefficient divisé sur le dernier i.e. le coefficient dominant). Par conséquent (en n'oubliant pas que P' est de degré $n-1$ donc on divise par $n-1$ et pas par n) :

$$\begin{aligned} \mu(P') &= \frac{1}{n-1} \times \frac{-(n-1)a_{n-1}}{na_n} \\ &= -\frac{a_{n-1}}{na_n} \\ &= \mu(P) \end{aligned}$$

Exercice 74 : ✪✪ Résoudre le système suivant :

$$\begin{cases} x + y + z = 1 \\ x^2 + y^2 + z^2 = 9 \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1 \end{cases}$$

Correction : Utilisons les relations coefficients racines pour un polynôme de degré 3 (puisqu'on a trois inconnues x, y et z) :

$$\begin{aligned}(X-x)(X-y)(X-z) &= X^3-(x+y+z)X^2+(xy+xz+yx)X-xyz\\ &= X^3-X^2+(xy+xz+yx)X-xyz\end{aligned}$$

Or,

$$\begin{aligned}(x+y+z)^2 &= x^2+y^2+z^2+2xy+2yz+2zx\\ &= x^2+y^2+z^2+2(xy+yz+zx)\end{aligned}$$

Or, $x+y+z=1$ et $x^2+y^2+z^2=9$ donc $2(xy+yz+zx)=-8$ donc $xy+yz+zx=-4$. Enfin, en mettant au même dénominateur :

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{yz+xz+xy}{xyz}$$

c'est-à-dire que $1=\dfrac{-4}{xyz}$ donc $xyz=-4$. Finalement :

$$(X-x)(X-y)(X-z)=X^3-X^2-4X+4$$

1 est racine évidente. En factorisant, il vient : $X^3-X^2+4X-4=(X-1)(X^2-4)=(X-1)(X-2)(X+2)$, c'est-à-dire que les racines de $(X-x)(X-y)(X-z)$ sont 1 et ± 2. Or, ce sont aussi x,y,z donc x,y,z valent 1 et ± 2. Qui est qui ? x,y,z jouent des rôles symétriques donc ils peuvent valoir n'importe quelle valeur. En conclusion, il y a 6 triplets solutions : tous les triplets contenant 1 et ± 2 dans les 6 ordres possibles (6 car il y a $3!=6$ permutations d'un ensemble à 3 éléments).

Exercice 75 : ✪✪ Soit $(p,q)\in\mathbb{C}^2$. Soit $P=X^3+pX+q$. Soient x,y,z les trois racines complexes de P comptées avec multiplicité.

1. Montrer que $P'(x)P'(y)P'(z)=4p^3+27q^2$.
2. En déduire une CNS pour que P admette une racine multiple.

Correction :

1. $P'=3X^2+p$ donc

$$\begin{aligned}P'(x)P'(y)P'(z) &= (3x^2+p)(3y^2+p)(3z^2+p)\\ &= (9x^2y^2+p(3x^2+3y^2)+p^2)(3z^2+p)\\ &= 27x^2y^2z^2+p(9x^2y^2+9x^2z^2+9y^2z^2)+p^2(3z^2+3x^2+3y^2)+p^3\end{aligned}$$

Or, $P=(X-x)(X-y)(X-z)$ donc, d'après les relations coefficients racines :

$$-x-y-z=0,\qquad xy+xz+yz=p\qquad\text{et}\qquad -xyz=q$$

Dès lors, $P'(x)P'(y)P'(z)=27q^2+9p(x^2y^2+x^2z^2+y^2z^2)+3p^2(z^2+x^2+y^2)+p^3$. D'une part, $(x+y+z)^2=0$, et d'autre part :

$$\begin{aligned}(x+y+z)^2 &= x^2+y^2+z^2+2xy+2xz+2yz\\ &= x^2+y^2+z^2+2p\end{aligned}$$

si bien que $x^2+y^2+z^2=-2p$. Enfin, $(xy+xz+yz)^2=p^2$ et

$$\begin{aligned}(xy+xz+yz)^2 &= x^2y^2+x^2z^2+y^2z^2+2x^2yz+2y^2xz+2z^2xy\\ &= x^2y^2+x^2z^2+y^2z^2+2xyz(x+y+z)\\ &= x^2y^2+x^2z^2+y^2z^2+0\end{aligned}$$

Finalement, $x^2y^2+x^2z^2+y^2z^2=p^2$. On en déduit que :

$$\begin{aligned}P'(x)P'(y)P'(z) &= 27q^2+9p\times p^2+3p^2\times -2p+p^3\\ &= 27q^2+4p^3\end{aligned}$$

2. P admet une racine multiple si et seulement si x, y ou z est racine de P' donc si et seulement si $27q^2 + 4p^3 = 0$. Par analogie avec le degré 2, cette quantité est donc appelée le discriminant de P.

Exercice 76 : ✪✪ Soit $P \neq 0$ et soit $n = \deg(P)$. Montrer que les sommes des racines de $P, P', \dots, P^{(n-1)}$ forment une progression arithmétique.

Correction : Notons $P = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$. Notons, pour tout $k \in [\![0 ; n-1]\!]$, S_k la somme des racines (comptées avec multiplicité) de $P^{(k)}$. D'après les relations coefficients racines, $S_0 = -a_{n-1}/a_n$ (moins l'avant-dernier coefficient divisé par le dernier). Calculons S_1. Tout d'abord :

$$P' = \sum_{k=1}^{n} k a_k X^{k-1}$$

Par conséquent (toujours : moins l'avant-dernier coefficient divisé par le dernier) :

$$\begin{aligned} S_1 &= \frac{-(n-1)a_{n-1}}{n a_n} \\ &= \frac{n-1}{n} \times S_0 \\ &= \left(1 - \frac{1}{n}\right) \times S_0 \\ &= S_0 - \frac{S_0}{n} \end{aligned}$$

Ensuite :

$$P'' = \sum_{k=2}^{n} k(k-1) a_k X^{k-2}$$

donc

$$\begin{aligned} S_2 &= \frac{(n-1)(n-2)a_{n-1}}{-n(n-1)a_n} \\ &= \frac{n-2}{n} \times S_0 \\ &= \left(1 - \frac{2}{n}\right) \times S_0 \\ &= S_0 - \frac{2S_0}{n} \end{aligned}$$

On généralise facilement le résultat : pour tout k, $S_k = S_0 - kS_0/n$, donc cette famille est en progression arithmétique (de raison $-S_0/n$).

Exercice 77 : ✪✪ Soit $n \geq 1$ et soit $f : \mathbb{C}^n \to \mathbb{C}^n$ qui à $(z_1, \dots, z_n)$ associe $(\sigma_1, \dots, \sigma_n)$ où σ_k désigne la k-ième fonction symétrique élémentaire des z_i.

1. L'application f est-elle surjective ?
2. Montrer que f n'est pas injective.
3. Montrer cependant que si $(z_1, \dots, z_n)$ et $(a_1, \dots, a_n)$ sont deux éléments de $\mathbb{C}^n$ qu'on ne peut pas déduire l'un de l'autre par permutation des coordonnées, alors $f(z_1, \dots, z_n) \neq f(a_1, \dots, a_n)$.

Correction : Rappelons que si $z_1, \dots, z_n$ sont les racines de P de degré n, alors on a :

$$P = a_n \left(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \sigma_3 X^{n-3} + \dots + (-1)^n \sigma_n\right)$$

avec les σ_k les fonctions symétriques élémentaires.

1. Soit $(\sigma_1, \dots, \sigma_n) \in \mathbb{C}^n$ et posons

$$P = -\sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \sigma_3 X^{n-3} + \cdots + (-1)^n \sigma_n$$

Notons $z_1, \dots, z_n$ les racines complexes de P. Alors les fonctions symétriques élémentaires des z_i sont exactement les σ_i c'est-à-dire que $f(z_1, \dots, z_n) = (\sigma_1, \dots, \sigma_n)$: f est surjective.

2. f n'est pas injective car tout n-uplet de racines qu'on peut déduire l'un de l'autre a les mêmes fonctions symétriques élémentaires. Par exemple, les racines $(1, 0, \dots, 0)$ et les racines $(0, \dots, 0, 1)$ donnent les mêmes polynômes donc les mêmes coefficients donc les mêmes fonctions symétriques élémentaires.

3. Supposons que $(z_1, \dots, z_n)$ et $(a_1, \dots, a_n)$ sont deux éléments de $\mathbb{C}^n$ qu'on ne peut pas déduire l'un de l'autre par permutation des coordonnées, et notons

$$P = (X - z_1) \dots (X - z_n) \qquad \text{et} \qquad Q = (X - a_1) \dots (X - a_n)$$

Notons $(\sigma_1, \dots, \sigma_n)$ l'image de $(z_1, \dots, z_n)$ par f, et $(\tau_1, \dots, \tau_n)$ l'image de $(a_1, \dots, a_n)$. Par conséquent, en utilisant les relations coefficients racines :

$$P = X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \sigma_3 X^{n-3} + \cdots + (-1)^n \sigma_n \qquad \text{et} \qquad Q = X^n - \tau_1 X^{n-1} + \tau_2 X^{n-2} - \sigma_3 X^{n-3} + \cdots + (-1)^n \tau_n$$

P et Q n'ont pas les mêmes racines donc ne sont pas égaux donc n'ont pas les mêmes coefficients c'est-à-dire que $(\sigma_1, \dots, \sigma_n) \neq (\tau_1, \dots, \tau_n)$: les deux images sont bien distinctes.

6 Quantités polynomiales en quelque-chose

Exercice 78 : ✪

1. Montrer que, pour tout $n \in \mathbb{N}$, il existe un unique $P_n \in \mathbb{N}[X]$ (dont la définition est évidente) tel que $\tan^{(n)} = P_n(\tan)$. En déduire que, pour tout $n \in \mathbb{N}$ et tout $x \in \left[0 ; \frac{\pi}{2}\right[$, $\tan^{(n)}(x) \geq 0$.

2. **Remake :** Soit $f : x \mapsto e^{e^x}$. Montrer que, pour tout $n \in \mathbb{N}$, il existe un unique $P_n \in \mathbb{R}[X]$ tel que, pour tout $x \in \mathbb{R}$, $f^{(n)}(x) = P_n\left(e^x\right)$.

Correction :

1. Montrons que les dérivées successives de la tangente sont des polynômes à coefficients entiers positifs évalués en la tangente (cf les polynômes de Tchebychev, c'est un argument du même genre). Montrons cela de façon plus précise.
   - Si $n \geq 0$, soit l'hypothèse de récurrence H_n : « Il existe $P_n \in \mathbb{N}[X]$ tel que $\tan^{(n)} = P_n(\tan)$ ».
   - Si $n = 0$, $\tan^{(0)} = \tan$: $P_0 = X$ convient donc H_0 est vraie. De plus, $\tan^{(1)} = 1 + \tan^2$: $P_1 = 1 + X^2$ convient, H_1 est également vraie.
   - Soit n quelconque supérieur ou égal à 1. Supposons H_n vraie et montrons que H_{n+1} est vraie. Par hypothèse de récurrence, il existe $d \geq 0$ (le degré de P_n) et $a_0, \dots, a_d$ entiers positifs (ses coefficients) tels que

$$\tan^{(n)} = \sum_{k=0}^{d} a_k \tan^k$$

   En dérivant cette égalité, il vient (le terme pour $k = 0$ est nul, la somme commence donc en $k = 1$)

$$\begin{aligned} \tan^{(n+1)} &= \sum_{k=1}^{d} k a_k \tan^{k-1}(1 + \tan^2) \\ &= \sum_{k=1}^{d} k a_k \tan^{k-1} + \sum_{k=1}^{d} k a_k \tan^{k+1} \end{aligned}$$

   Il suffit de poser

$$P_{n+1} = \sum_{k=1}^{d} k a_k X^{k-1} + \sum_{k=1}^{d} k a_k X^{k+1}$$

   qui est bien à coefficients entiers positifs (car somme de deux polynômes à coefficients entiers positifs) pour conclure : H_{n+1} est vraie.
   - D'après le principe de principe de récurrence, H_n est vraie pour tout $n \geq 0$.

Ainsi, pour tout $n \geq 0, \tan^{(n)}(x)$ est un polynôme à coefficients entiers positifs évalué en $\tan(x)$, qui est un nombre positif. Or, un polynôme à coefficients positifs évalué en un nombre positif est lui-même positif : $\tan^{(n)}(x) \geq 0$.

Pour l'unicité : si deux polynômes P_n et Q_n conviennent, alors $P_n(\tan(x)) = Q_n(\tan(x))$ pour tout $x \in \left[0\,;\frac{\pi}{2}\right[$ donc P_n et Q_n coïncident en tout élément de la forme $\tan(x)$ avec $x \in \left[0\,;\frac{\pi}{2}\right[$ donc P_n et Q_n coïncident sur $\mathbb{R}_+$ qui est infini donc sont égaux : ceci prouve l'unicité.

2. Pour l'existence, raisonnons par récurrence sur n.
   - Si $n \in \mathbb{N}$, notons H_n : « $\exists P_n \in \mathbb{R}[X], \forall x \in \mathbb{R}, f_n(x) = P_n(e^x) \times e^{e^x}$ ».
   - Puisque, pour tout $x \in \mathbb{R}$, $f_0(x) = 1 \times e^{e^x}$, $P_0 = 1$ convient : H_0 est vraie.
   - Bien que ce ne soit pas nécessaire, montrons que H_1 et H_2 sont vraies pour nous donner une idée. Soit $x \in \mathbb{R}$. On a $f_1(x) = {f_0}'(x) = e^x \times e^{e^x}$. Ainsi, $P_1 = X$ convient. Attention, ne pas écrire « Donc $P_1 = X$ » ou, pire avec des équivalences ! Pour l'instant, nous ne montrons que l'existence et nous nous contentons d'exhiber des polynômes qui **conviennent**.

     En effet, $P_1(e^x) = e^x$ et donc on a bien $f_1(x) = P_1(e^x) \times e^{e^x}$. De plus, $f_2 = {f_1}'(x)$, si bien que $f_2(x) = (e^x + e^x \times e^x) \times e^{e^x} = \left(e^x + e^{2x}\right) \times e^{e^x}$. Dès lors, $P_2 = X + X^2$ convient. En effet, $P_2(e^x) = e^x + e^{2x}$ et on a bien l'égalité voulue.
   - Soit $n \in \mathbb{N}$. Supposons H_n vraie et prouvons que H_{n+1} est vraie. Par hypothèse de récurrence, il existe $P_n \in \mathbb{R}[X]$ tel que, pour tout $x \in \mathbb{R}$, $f_n(x) = P_n(e^x) \times e^{e^x}$. Soit $x \in \mathbb{R}$. En dérivant, il vient $f_{n+1}(x) = \left(e^x \times {P_n}'(e^x) + P_n(e^x) \times e^x\right) \times e^{e^x}$. Ainsi, $P_{n+1} = XP_n' + XP_n \in \mathbb{R}[X]$ convient : H_{n+1} est vraie.
   - D'après le principe de récurrence, H_n est vraie pour tout n.

   Unicité : Soit $n \in \mathbb{N}$. Soit Q_n un autre polynôme qui convient. Ainsi, pour tout $x \in \mathbb{R}$, $P_n(e^x) = Q_n(e^x)$. Attention, cela ne signifie pas (encore) que $P_n = Q_n$! En effet, on ne peut pas encore dire que P_n et Q_n coïncident en tout réel (par exemple, quoi qu'on fasse, on ne peut pas trouver de réel x tel que $e^x = -1$ et donc on ne peut pas encore affirmer que $P_n(-1) = Q_n(-1)$). On sait juste que, pour tout $x \in \mathbb{R}$, $P_n(e^x) = Q_n(e^x)$, c'est-à-dire que P_n et Q_n coïncident en tout réel de la forme e^x. Ils coïncident donc sur $\{e^x \,|\, x \in \mathbb{R}\} = \mathbb{R}_+^*$, qui est un ensemble infini, donc sont égaux. D'où l'unicité.

Exercice 79 : ✪✪

1. Soit $n \in \mathbb{N}$ et soit $x \neq 0$. Développer $\left(x^n + \frac{1}{x^n}\right) \times \left(x + \frac{1}{x}\right)$.
2. Montrer que, pour tout $n \in \mathbb{N}$, il existe un unique polynôme P_n tel que, pour tout $x \neq 0$, $P_n\left(x + \frac{1}{x}\right) = x^n + \frac{1}{x^n}$.

Correction :

1. On trouve :
$$\left(x^n + \frac{1}{x^n}\right) \times \left(x + \frac{1}{x}\right) = x^{n+1} + \frac{x^{n+1}}{+} x^{n-1} + \frac{1}{x^{n-1}}$$
2. **Existence :** Par récurrence sur n. Vu la question précédente, on se dit qu'il va y avoir un lien entre les rangs $n-1$, n et $n+1$: on va donc faire une récurrence double et, pour cela, il faut montrer l'initialisation pour au moins deux valeurs. Ici, donc, montrer que H_1 est vraie est indispensable.
   - Si $n \in \mathbb{N}$, notons H_n : « $\exists P_n \in \mathbb{R}[X], \forall x \in \mathbb{R}^*, P_n\left(x + \frac{1}{x}\right) = x^n + \frac{1}{x^n}$ ».
   - Soit $x \neq 0$. On a $x^0 + \frac{1}{x^0} = 2$, si bien que $P_0 = 2$ convient : H_0 est vraie.
   - Soit $x \neq 0$. Le polynôme $P_1 = X$ convient. En effet, $P_1\left(x + \frac{1}{x}\right) = x + \frac{1}{x}$: H_1 est donc vraie.
   - Bien que ce ne soit pas nécessaire, montrons que H_2 est vraie. Soit $x \neq 0$. Tout d'abord, $\left(x + \frac{1}{x}\right)^2 = x^2 + \frac{1}{x^2} + 2$ donc $x^2 + \frac{1}{x^2} = \left(x + \frac{1}{x}\right)^2 - 2$. Par conséquent, $P_2 = X^2 - 2$ convient. En effet, pour tout $x \neq 0$,
   $$P_2\left(x + \frac{1}{x}\right) = \left(x + \frac{1}{x}\right)^2 - 2 = x^2 + \frac{1}{x^2}$$
   ce qui est le résultat voulu. Ainsi, H_2 est vraie.
   - Soit $n \geq 1$. Supposons H_n et H_{n-1} vraies, et prouvons que H_{n+1} est vraie. Soit $x \neq 0$. D'après la question 1,
   $$x^{n+1} + \frac{1}{x^{n+1}} = \left(x + \frac{1}{x}\right) \times \left(x^n + \frac{1}{x^n}\right) - \left(x^{n-1} + \frac{1}{x^{n-1}}\right).$$

Or, par hypothèse de récurrence, il existe $(P_n, P_{n-1}) \in \mathbb{R}[X]^2$ tels que, pour tout $x \in \mathbb{R}^*$,

$$x^n + \frac{1}{x^n} = P_n\left(x + \frac{1}{x}\right) \qquad \text{et} \qquad x^{n-1} + \frac{1}{x^{n-1}} = P_{n-1}\left(x + \frac{1}{x}\right).$$

Ainsi, $x^{n+1} + \dfrac{1}{x^{n+1}} = \left(x + \dfrac{1}{x}\right) \times P_n\left(x + \dfrac{1}{x}\right) - P_{n-1}\left(x + \dfrac{1}{x}\right)$. Finalement, $P_{n+1} = XP_n - P_{n-1}$ convient : H_{n+1} est vraie.

- D'après le principe de récurrence, H_n est vraie pour tout $n \in \mathbb{N}$.

Unicité : Soit $n \in \mathbb{N}$. Soit Q_n un polynôme qui convient. Alors, pour tout $x \neq 0$, $P_n\left(x + \dfrac{1}{x}\right) = Q_n\left(x + \dfrac{1}{x}\right)$, c'est-à-dire que P_n et Q_n coïncident en tout point de la forme $x + \dfrac{1}{x}$. Soit φ la fonction définie sur $\mathbb{R}^*$ par $\varphi : x \longmapsto x + \dfrac{1}{x}$. Alors P_n et Q_n coïncident sur $\{\varphi(x) \,|\, x \in \mathbb{R}^*\}$. On trouve facilement le tableau de variations de φ :

x	$-\infty$		-1		0		1		$+\infty$
$\varphi'(x)$		$+$	0	$-$	‖	$-$	0	$+$	
$\varphi(x)$	$-\infty$	↗	-2	↘	$-\infty$ ‖ $+\infty$	↘	2	↗	$+\infty$

Comme φ est continue, strictement croissante sur $[\,1\,;+\infty\,[$ et telle que $\varphi(1) = 2$ et $\varphi(x) \xrightarrow[x\to+\infty]{} +\infty$, c'est une bijection de $[\,1\,;+\infty\,[$ dans $[\,2\,;+\infty\,[$. φ étant impaire, c'est également une bijection de $]\,-\infty\,;-1\,]$ dans $]\,-\infty\,;-2\,]$. Enfin, d'après le tableau de variations, φ ne prend aucune valeur dans $]\,-2\,;2\,[$. En conclusion, $\{\varphi(x) \,|\, x \in \mathbb{R}^*\} =]\,-\infty\,;-2\,] \cup [\,2\,;+\infty\,[$ donc est un ensemble infini : P_n et Q_n coïncident sur un ensemble infini donc $Q_n = P_n$. D'où l'unicité.

Exercice 80 - Polynômes de Tchebychev de seconde espèce : ✪✪✪ Soit $n \geq 1$. S'inspirer du cours pour montrer l'existence d'un unique polynôme Q_n vérifiant, pour tout $\theta \in \mathbb{R}$, $\sin(\theta)Q_n(\cos(\theta)) = \sin((n+1)\theta)$.

Correction : Existence : Montrons l'existence par récurrence sur n.

- Si $n \geq 1$, notons H_n : « il existe $Q_n \in \mathbb{R}[X]$ tel que, pour tout $\theta \in \mathbb{R}$, $\sin(\theta)Q_n(\cos(\theta)) = \sin((n+1)\theta)$ ».
- Pour $n = 1$: pour tout $\theta \in \mathbb{R}$, $\sin(2\theta) = 2\sin(\theta)\cos(\theta) = \sin(\theta) \times 2\cos(\theta)$ donc $2X$ convient : H_1 est vraie.
- Pour $n = 2$: pour tout $\theta \in \mathbb{R}$,

$$\begin{aligned}
\sin(3\theta) &= 3\sin(\theta) - 4\sin^3(\theta) \\
&= \sin(\theta) \times (3 - 4\sin^2(\theta)) \\
&= \sin(\theta) \times (3 - 4(1 - \cos^2(\theta))) \\
&= \sin(\theta) \times (4\cos^2(\theta) - 1)
\end{aligned}$$

  c'est-à-dire que $4X^2 - 1$ convient : H_2 est vraie.
- Soit $n \geq 2$. Supposons H_n et H_{n-1} vraies (on pense à faire une récurrence double puisque c'est une récurrence double pour les polynômes de Tchebychev classiques, mais si on n'y pense pas, on s'en rend compte plus tard et on revient sur ses pas) et prouvons que H_{n+1} est vraie. Soit $\theta \in \mathbb{R}$.

$$\begin{aligned}
\sin((n+2)\theta) &= \sin((n+1)\theta + \theta) \\
&= \sin((n+1)\theta)\cos(\theta) + \sin(\theta)\cos((n+1)\theta)
\end{aligned}$$

  Or, à l'aide de la formule $\sin(a)\cos(b)$:

$$\sin(\theta)\cos((n+1)\theta) = \frac{1}{2}\left(\sin((n+2)\theta) - \sin(n\theta)\right)$$

  donc :

$$\sin((n+2)\theta) = \sin((n+1)\theta)\cos(\theta) + \frac{1}{2}\left(\sin((n+2)\theta) - \sin(n\theta)\right)$$

  Par conséquent :

$$2\sin((n+2)\theta) = 2\sin((n+1)\theta)\cos(\theta) + \sin((n+2)\theta) - \sin(n\theta)$$

  Finalement, en mettant tous les $\sin((n+2)\theta)$ du même côté :

$$\sin((n+2)\theta) = 2\sin((n+1)\theta)\cos(\theta) - \sin(n\theta)$$

Par hypothèse de récurrence, il existe Q_n et Q_{n-1} tels que $\sin((n+1)\theta) = Q_n(\cos(\theta)) \times \sin(\theta)$ et $\sin(n\theta) = Q_{n-1}(\cos(\theta)) \times \sin(\theta)$ (c'est-là qu'on se rend compte qu'il faut une récurrence double) si bien que :

$$\begin{aligned}\sin((n+2)\theta) &= 2Q_n(\cos(\theta)) \times \sin(\theta)\cos(\theta) - Q_{n-1}(\cos(\theta)) \times \sin(\theta) \\ &= \sin(\theta) \times (2\cos(\theta)Q_n(\cos(\theta)) - Q_{n-1}(\cos(\theta)))\end{aligned}$$

En conclusion, $Q_{n+1} = 2XQ_n - Q_{n-1}$ convient (on remarque que c'est la même relation de récurrence que les polynômes de Tchebychev « classiques ») : H_{n+1} est vraie.

- D'après le principe de récurrence, H_n est vraie pour tout $n \geq 1$. D'où l'existence.

Unicité : Soit $n \geq 1$, soient P_n et Q_n deux polynômes qui conviennent. Alors, pour tout $\theta \in \mathbb{R}$, $\sin(\theta)P_n(\cos(\theta)) = \sin(\theta)Q_n(\cos(\theta))$. En particulier, pour tout $\theta \not\equiv 0[\pi]$, le sinus n'est pas nul donc $P_n(\cos(\theta)) = Q_n(\cos(\theta))$: P_n et Q_n coïncident sur $\cos(\mathbb{R}\backslash\pi\mathbb{Z})$ donc sur $]-1\,;1[$ (ou on peut dire aussi qu'ils coïncident au moins sur $\cos(]\,0\,;\pi\,[) =]-1\,;1\,[$) qui est un ensemble infini donc sont égaux. D'où l'unicité.

7 Polynômes à coefficients dans un corps quelconque (HP)

Exercice 81 : ✪ On dit qu'un corps $\mathbb{K}$ est algébriquement clos si tout polynôme non constant à coefficients dans $\mathbb{K}$ admet une racine dans $\mathbb{K}$. Montrer qu'un corps algébriquement clos est infini. Réciproque ?

Correction : Supposons $\mathbb{K}$ fini et notons $\mathbb{K} = \{a_1; \ldots; a_n\}$. Soit $P = (X - a_1)\ldots(X - a_n) + 1$ (avec 1 le neutre du produit sur $\mathbb{K}$ i.e. $1_{\mathbb{K}}$). Alors P est constant égal à 1 sur $\mathbb{K}$ donc n'admet aucune racine dans $\mathbb{K}$. Il existe un polynôme à coefficients dans $\mathbb{K}$ qui n'admet aucune racine sur $\mathbb{K}$ donc $\mathbb{K}$ n'est pas algébriquement clos. Par contraposée, on a le résultat voulu.

Exercice 82 : ✪✪ Soit $\mathbb{K}$ un corps fini et soit $f : \mathbb{K} \to \mathbb{K}$. Montrer que f est polynomiale i.e. qu'il existe $P \in \mathbb{K}[X]$ tel que pour tout $x \in \mathbb{K}$, $f(x) = P(x)$.

Correction : Notons $\mathbb{K} = \{a_1; \ldots; a_n\}$ (avec les a_i deux à deux distincts) et $b_1 = f(a_1), \ldots, a_n = f(a_n)$ (les b_i ne sont pas forcément distincts). À l'aide d'un polynôme d'interpolation de Lagrange, il existe $P \in \mathbb{K}_{n-1}[X]$ tel que $P(a_1) = b_1, \ldots, P(a_n) = b_n$ i.e. $P \in \mathbb{K}_{n-1}[X]$ tel que pour tout $x \in \mathbb{K}, f(x) = P(x)$.

Exercice 83 - Théorème de Wilson (le retour) : ✪✪✪ Cet exercice fait appel au théorème de Lagrange et à la notion d'ordre dans un groupe (cf. chapitre 18). Soit p un nombre premier.

1. Sur $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, montrer que
$$X^{p-1} - 1 = \prod_{k=1}^{p-1}(X - k)$$
2. En déduire que $(p-1)! \equiv -1[p]$.

Correction :

1. On sait (cf. chapitre 18) que, dans un groupe d'ordre n, $y^n = e$. Or, $\mathbb{Z}/p\mathbb{Z}$ est un corps car p est premier donc $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ est un groupe d'ordre $p-1$. Par conséquent, pour tout $k \neq 0$ (on travaille dans $\mathbb{Z}/p\mathbb{Z}$), $k^{p-1} = 1$ (le neutre du produit). Les $p-1$ éléments de $\mathbb{Z}/p\mathbb{Z}^*$ sont donc racines de $X^{p-1} - 1$: on a $p-1$ racines distinctes, le polynôme est de degré $p-1$ donc les racines sont simples, le polynôme est unitaire donc on a la factorisation voulue.
2. Si $p = 2$ le résultat est immédiat. Supposons $p \geq 3$. Il suffit d'évaluer en 0 : dans $\mathbb{Z}/p\mathbb{Z}$, cela donne : $-1 = (-1)^{p-1} \times (p-1)!$ et p est impair (c'est un nombre premier différent de 2) donc $-1 = -(p-1)!$. Rappelons que l'égalité dans $\mathbb{Z}/p\mathbb{Z}$ est équivalente à la congruence modulo p ce qui permet de conclure.

Exercice 84 : ✪✪✪ Cet exercice fait appel au théorème de Lagrange et à la notion d'ordre dans un groupe (cf. chapitre 18). Soit p un nombre premier et soit $x \in \mathbb{Z}/p\mathbb{Z}$. Montrer que $x \neq 0$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$.

Correction : Supposons p impair sinon il n'y a rien à prouver (il n'y a qu'un élément qui est un carré et qui vérifie la deuxième condition). Si x est un carré alors il existe y tel que $x = y^2$ si bien que $x^{\frac{p-1}{2}} = y^{p-1}$ et on sait (cf. chapitre 18) que, dans un groupe d'ordre n, $y^n = e$. Or, $\mathbb{Z}/p\mathbb{Z}$ est un corps car p est premier donc $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ est un groupe d'ordre $p-1$. Par conséquent, $y^{p-1} = 1$ (le neutre du produit) donc $x^{\frac{p-1}{2}} = 1$.

Réciproquement : montrons que $\mathbb{Z}/p\mathbb{Z}^*$ admet exactement $(p-1)/2$ carrés. L'application $f : x \mapsto x^2$ est évidemment un morphisme de groupes de $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ dans lui-même (il est impératif d'enlever 0 car ce n'est pas un morphisme de groupe de $(\mathbb{Z}/p\mathbb{Z}, +)$ dans lui-même). Son noyau (i.e. l'ensemble des antécédents de 1) est $\{\pm 1\}$ qui a deux éléments ($1 \neq -1 = p-1$, rappelons qu'on travaille modulo p, car p est impair donc différent de 2) donc, d'après l'exercice 32 du chapitre 18, l'image de f est de cardinal $(p-1)/2$, c'est-à-dire qu'il y a exactement $(p-1)/2$ carrés qui sont, d'après ce qui précède, racines du polynôme $X^{\frac{p-1}{2}} - 1$. Or, il ne peut pas admettre d'autre racines à cause de son degré, donc les nombres qui ne sont pas des carrés ne sont pas des racines de ce polynôme donc ne vérifient pas l'égalité $x^{\frac{p-1}{2}} = 1$, d'où l'équivalence.