Feuille d'exercices n° 10

Polynômes

Exercice 1. Quelles sont les racines (dans $\mathbf{C}$, dans $\mathbf{R}$ et dans $\mathbf{Q}$) des polynômes suivants ?

a) $X^3 - 7X^2 + 14X - 8$, b) $X^n - 1$, où n est un entier, c) $X^6 - 4$,

d) $X^4 - 13X^2 + 36$, e) $X^4 + 6X^2 + 25$.

Solution :

a) $X^3 - 7X^2 + 14X - 8 = (X-1)(X-2)(X-4)$. Donc ses racines dans $\mathbf{C}$, dans $\mathbf{R}$ ou dans $\mathbf{Q}$ sont $1, 2, 4$.

b) Pour tout entier $n \geq 1$, les racines complexes du $X^n - 1$ sont $X = e^{i\frac{2k\pi}{n}}$ avec $k = 0, 1, \cdots, n-1$. Si $n \in \mathbf{N}^*$ est impaire, les racines réelles/rationnelles sont $X = 1$; si $n \in \mathbf{N}^*$ est paire, les racines réelles/rationnelles sont $X = \pm 1$. Si $n = 0$, $X^n - 1 \equiv 0$.

c) $X^6 - 4 = (X^3 - 2)(X^3 + 2)$. Donc ses racines complexes sont $\pm\sqrt[3]{2}$, $\pm\sqrt[3]{2}e^{i\frac{2\pi}{3}}$ et $\pm\sqrt[3]{2}e^{i\frac{4\pi}{3}}$. Ses racines réelles sont $\pm\sqrt[3]{2}$. Il n'y a pas de racines dans $\mathbf{Q}$.

d) On a $X^4 - 13X^2 + 36 = (X^2 - 4)(X^2 - 9)$. Donc ses racines complexes/réelles/rationnelles sont ± 2 et ± 3.

e) On a $X^4 + 6X^2 + 25 = (X^2 + 3)^2 + 16 = (X^2 + 3 + 4i)(X^2 + 3 - 4i)$. Les racines complexes de $X^2 + 3 + 4i$ sont $\pm(1 - 2i)$ et les racines complexes de $X^2 + 3 - 4i$ sont $\pm(1 + 2i)$. Donc les racines complexes de $X^4 + 6X^2 + 25$ sont $\pm(1 - 2i)$ et $\pm(1 + 2i)$. Il n'existe pas de racine réelle.

$\square$

Exercice 2. Pour chacun des polynômes suivants, dresser la liste complète des polynômes qui le divisent dans l'anneau de polynômes précisé :

a) $X + 1$ dans $\mathbf{R}[X]$, b) $X^2 - 1$ dans $\mathbf{R}[X]$,

c) $X^2 + 1$ dans $\mathbf{C}[X]$, d) $X^2 + 1$ dans $\mathbf{R}[X]$.

Solution :

a) Dans $\mathbf{R}[X]$, pour tout $a \in \mathbf{R}^*$, a et $aX + a$ divisent $X + 1$.

b) Dans $\mathbf{R}[X]$, pour tout $a \in \mathbf{R}^*$, a, $aX + a$, $aX - a$ et $aX^2 - a$ divisent $X^2 - 1$.

c) Dans $\mathbf{C}[X]$, pour tout $a \in \mathbf{C}^*$, a, $a(X + i)$, $a(X - i)$ et $a(X^2 + 1)$ divisent $X^2 + 1$.

d) Dans $\mathbf{R}[X]$, pour tout $a \in \mathbf{R}^*$, a et $a(X^2 + 1)$ divisent $X^2 + 1$.

$\square$

Exercice 3.

1. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbf{C}[X]$. On définit $\overline{P} = \sum_{k=0}^{n} \overline{a_k} X^k$ le polynôme conjugué de P. Montrer que, pour tout $z \in \mathbf{C}$, on a $\overline{P(z)} = \overline{P}(\overline{z})$. En déduire que si $P \in \mathbf{R}[X]$, alors pour tout $z \in \mathbf{C}$, on a $\overline{P(z)} = P(\overline{z})$.
2. Soit P, Q deux polynômes à coefficients complexes tels que $P(x) = Q(x)$ pour tout $x \in \mathbf{R}$. Montrer que $P = Q$.
3. Soit $P \in \mathbf{C}[X]$ tel que $P(x) \in \mathbf{R}$ pour tout $x \in \mathbf{R}$. Montrer que $P \in \mathbf{R}[X]$.

Solution :

1. Soit $z \in \mathbf{C}$. Alors
$$\overline{P(z)} = \overline{\sum_{k=0}^{n} a_k z^k} = \sum_{k=0}^{n} \overline{a_k} \cdot \overline{z^k} = \sum_{k=0}^{n} \overline{a_k} \cdot (\overline{z})^k = \overline{P}(\overline{z}).$$
Si $P \in \mathbf{R}[X]$, alors $\overline{a_k} = a_k$ pour tout k, ce qui implique $\overline{P} = P$, d'où $\overline{P(z)} = P(\overline{z})$.
2. On pose $R = P - Q$. Alors R est un polynôme dans $\mathbf{C}[X]$. De plus, pour tout $x \in \mathbf{R}$, $R(x) = P(x) - Q(x) = 0$. Ceci implique que R possède une infinité de racines dans $\mathbf{C}$. On en déduit que R est la fonction nulle. Autrement dit, $P = Q$.
3. Disons que P est de degré n et écrivons $P = \sum_{k=0}^{n} a_k X^k$ avec $a_k \in \mathbf{C}$.
Première méthode. Pour tout réel x on a $\overline{x} = x$. De plus, puisque $P(x)$ est réel, on a aussi $\overline{P(x)} = P(x)$. D'où, un utilisant la question 1
$$P(x) = \overline{P(x)} = \overline{P}(\overline{x}) = \overline{P}(x).$$
D'après la question 2. cela implique que $P = \overline{P}$, c'est-à-dire $a_k = \overline{a_k}$ pour tout k. Autrement dit $P \in \mathbf{R}[X]$.
Deuxième méthode. Si x et h désignent deux variables réelles avec $h \neq 0$, on a par hypothèse $P(x+h) - P(x) \in \mathbf{R}$, donc
$$P'(x) = \lim_{h \to 0} \frac{P(x+h) - P(x)}{h} \in \mathbf{R}$$
pour tout $x \in \mathbf{R}$. Par récurrence immédiate, on a $P^{(k)}(x) \in \mathbf{R}$ pour tout entier k et tout réel x, en particulier $P^{(k)}(0) \in \mathbf{R}$. On conclut avec la formule
$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k \in \mathbf{R}[X]$$
(cas particulier de la formule $P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$).
Troisième méthode. Utiliser l'exo suivant en choisissant $x_0, \ldots, x_n \in \mathbf{R}$ deux-à-deux distincts. On trouve
$$P(X) = \sum_{k=0}^{n} P(x_k) \left[\prod_{\substack{j=0 \\ j \neq k}}^{n} \frac{X - x_j}{x_k - x_j} \right] \in \mathbf{R}[X],$$
puisque $P(x_k) \in \mathbf{R}$ pour tout k...

□

Exercice 4. Soit $n \in \mathbf{N}$ et soient $f_0, \ldots, f_n \in \mathbf{C}$ et $x_0, \ldots, x_n \in \mathbf{C}$. On suppose les x_k deux-à-deux distincts.

1. Pour tout $k = 0, \ldots, n$, montrez qu'il existe un unique polynôme $Q_k(X) \in \mathbf{C}[X]$ de degré n vérifiant
$$Q_k(x_k) = 1 \quad \text{et} \quad Q_k(x_j) = 0 \text{ pour tout } j \neq k.$$
2. En utilisant les polynômes Q_k définis à la question précédentes, construisez un polynôme $Q \in \mathbf{C}[X]$ de degré au plus n tel que
$$Q(x_k) = f_k \text{ pour } k = 0, \ldots, n.$$
3. Application : montrez que si $P \in \mathbf{C}[X]$ est de degré $n \in \mathbf{N}$, alors
$$P(X) = \sum_{k=0}^{n} P(x_k) \left[\prod_{\substack{j=0 \\ j \neq k}}^{n} \frac{X - x_j}{x_k - x_j} \right].$$

Solution :

1. Soit k un entier avec $0 \leq k \leq n$. Par hypothèse, x_j est une racine de Q_k pour tout $j \neq k$. Comme les x_j sont deux-à-deux distincts, Q_k a au moins n racines (distinctes). Comme $\deg Q_k = n$, ce sont les seules racines et elles sont de multiplicité 1. Donc il existe $\lambda \in \mathbf{R}$ tel que
$$Q_k(X) = \lambda \prod_{\substack{j=0 \\ j \neq k}}^{n} (X - x_j).$$
En utilisant $Q_k(x_k) = 1$, on trouve
$$\lambda = \Big(\prod_{\substack{j=0 \\ j \neq k}}^{n} (x_k - x_j) \Big)^{-1}.$$
2. Il suffit de poser $Q(X) = \sum_{j=0}^{n} f_j Q_j(X)$. On a $\deg P \leq n$ et puisque $Q_j(x_k) = 0$ pour tout $j \neq k$ on vérifie aisément que $Q(x_k) = f_k Q_k(x_k) = f_k$.
3. On applique ce qui précède avec $f_k = P(x_k)$. On construit ainsi un polynôme Q de degré au plus n tel que $Q(x_k) = P(x_k)$ pour tout k. Le polynôme $Q - P$ a au moins $n+1$ racines et de degré $\leq n$: c'est donc le polynôme nul.

□

Exercice 5. Développer $P = (X^3 - X^2 + 1)(X^2 + X + 1) \in \mathbf{R}[X]$. En déduire une preuve que 100011 n'est pas un nombre premier.

Solution : On a $P(X) = (X^3 - X^2 + 1)(X^2 + X + 1) = X^5 + X + 1$. Donc $100011 = P(10) = (10^3 - 10^2 + 1) \times (10^2 + 10 + 1) = 901 \times 111$. Donc 100011 n'est pas un nombre premier.

□

Exercice 6. Soit P un polynôme de $\mathbf{R}[X]$, et soient a et b deux réels distincts. Soient λ (respectivement, μ) le reste de la division euclidienne de $P(X)$ par $X-a$ (respectivement, par $X-b$). Calculer le reste de la division euclidienne de P par $(X-a)(X-b)$. Commenter le cas $\lambda=\mu=0$.

Solution : Il existent Q_1 et Q_2 dans $\mathbf{R}[X]$ tels que

$$\begin{cases} P(X) = Q_1(X)(X-a)+\lambda; \\ P(X) = Q_2(X)(X-b)+\mu. \end{cases}$$

Ecrivons aussi

$$P(X) = Q(X)(X-a)(X-b)+cX+d,$$

avec $Q(X)\in\mathbf{R}[X]$ et $c,d\in\mathbf{R}$ à déterminer (division euclidienne de $P(X)$ par $(X-a)(X-b)$). En utilisant les trois identités précédentes, on trouve

$$\begin{cases} P(a) &= \lambda = ca+d \\ P(b) &= \mu = cb+d. \end{cases}$$

On résout ce système. On peut faire par exemple $P(a)-P(b)$, ce qui conduit à $c=(\lambda-\mu)/(a-b)$ (ici on utilise l'hypothèse $a\neq b$). En considérant $bP(a)-aP(b)$ on trouve $d=(b\lambda-a\mu)/(b-a)$.
On en déduit que le reste de la division euclidienne de P par $(X-a)(X-b)$ est

$$\frac{\mu-\lambda}{b-a}X+\frac{b\lambda-a\mu}{b-a}.$$

En particulier, si $\lambda=\mu=0$, P est divisible par $(X-a)(X-b)$.

$\square$

Exercice 7. Établir les identités, pour $n\in\mathbf{N}^*$

$$X^n-1=(X-1)(X^{n-1}+X^{n-2}+\cdots+X+1),$$

$$X^{2n+1}+1=(X+1)(X^{2n}-X^{2n-1}+X^{2n-2}-\cdots+(-1)^pX^p\cdots-X+1).$$

En déduire les résultats suivants

1. Si le nombre de Mersenne $M_n=2^n-1$ est premier, alors n est premier.
2. Si le nombre de Fermat $F_n=2^n+1$ est premier, alors n est soit nul, soit une puissance de 2.

Solution : Notons que

$$X^{n-1}+X^{n-2}+\cdots+X+1=\sum_{k=0}^{n-1}X^k=\begin{cases}\frac{1-X^n}{1-X}, \text{ si } X\neq 1; \\ n, \text{ si } X=1.\end{cases}$$

On en déduit que

$$X^n-1=(X-1)(X^{n-1}+X^{n-2}+\cdots+X+1), \forall X\in\mathbf{C}.$$

Similairement, on peut montrer que $X^{2n+1}+1=(X+1)(X^{2n}-X^{2n-1}+X^{2n-2}-\cdots+(-1)^pX^p\cdots-X+1)$.

1. Par contraposée, supposons que n n'est pas premier. Si $n=1$ alors $M_1=1$ n'est pas premier. Si $n\geq 2$, alors il existent des entiers positifs $m,k\in\mathbf{N}^*$ tels que $n=mk$, avec $2\leq k<n$. On applique la première identité avec $X=2^k$ (et m à la place de n). On trouve

   $$M_n=(2^k-1)(2^{k(m-1)}+2^{k(m-2)}+\cdots+2^k+1).$$

   Donc 2^k-1 est un diviseur de M_n. De plus, comme $2\leq k<n$, on a $\leq 2^k-1<M_n$. Donc M_n n'est pas premier.

2. Soit $n \in \mathbf{N}$ tel que $F_n = 2^n + 1$ est premier. Supposons que $n \neq 0$ et n n'est pas une puissance de 2. Alors, on a
$$n = 2^k(2m+1) \text{ avec } (k,m) \in \mathbf{N} \times \mathbf{N}^*.$$
Observons que $2^{2^k} + 1 \neq F_n$ car $m \geq 1$. Or, on voit que $F_n = (2^{2^k})^{2m+1} + 1$ qui est divisible par $2^{2^k} + 1$. C'est une contradiction. Par l'absurde, on conclut que n soit nul, soit une puissance de 2.

□

Exercice 8. Pour quels entiers n le polynôme $X^{2n} + X^n + 1$ est-il divisible par $X^2 + X + 1$ dans $\mathbf{R}[X]$?

Solution : Observons que si $n = 1$, $X^2 + X + 1$ divise $X^{2n} + X^n + 1$. Soit $n \in \mathbf{N}^*$. Par l'ex 6, on voit que
$$X^3 - 1 \text{ divise } X^{3n} - 1.$$
Notons que
$$X^3 - 1 = (X-1)(X^2 + X + 1),$$
et que
$$X^{3n} - 1 = (X^n - 1)(X^{2n} + X^n + 1) = (X-1)(X^{n-1} + \cdots + 1)(X^{2n} + X^n + 1).$$
Puisque $X - 1$ et $X^2 + X + 1$ sont premiers entre eux, on obtient que $X^2 + X + 1$ divise $(X^{n-1} + \cdots + 1)(X^{2n} + X^n + 1)$. Dans $\mathbf{R}[X]$, $X^2 + X + 1$ est premier. Donc soit $X^2 + X + 1$ divise $(X^{n-1} + \cdots + 1)$ soit $X^2 + X + 1$ divise $X^{2n} + X^n + 1$. Notons de plus que $(X^{n-1} + \cdots + 1)$ et $(X^{2n} + X^n + 1)$ sont premiers entre eux car $X^n - 1$ et $X^{2n} + X^n + 1$ sont premiers entre eux. Donc,
$$\text{soit } X^2 + X + 1 \text{ divise } X^{n-1} + \cdots + 1 \text{ et } X^2 + X + 1 \text{ ne divise pas } X^{2n} + X^n + 1;$$
$$\text{soit } X^2 + X + 1 \text{ divise } X^{2n} + X^n + 1 \text{ et } X^2 + X + 1 \text{ ne divise pas } X^{n-1} + \cdots + 1.$$
Observons que pour $n \in \mathbf{N}^*$, on a $n = 3k + r$ avec $k \in \mathbf{N}$ et $r \in \{0, 1, 2\}$. Alors, le reste de la division de $X^{n-1} + \cdots + 1$ par $X^2 + X + 1$ est $X^{r-1} + \cdots + 1$ si $r \geq 1$ et 0 si $r = 0$ car
$$X^{n-1} + \cdots + 1 = (X^{n-1} + X^{n-2} + X^{n-3}) + \cdots + (X^{n-3k+2} + X^{n-3k+1} + X^{n-3k}) + X^{r-1} + \cdots + 1.$$
C'est-à-dire, $X^2 + X + 1$ divise $(X^{n-1} + \cdots + 1)$ si et seulement si $3|n$ et $n \geq 3$. Réciproquement, si et seulement si $n \in \mathbf{N}^*$ et 3 ne divise pas n, $X^2 + X + 1$ divise $X^{2n} + X^n + 1$.

□

Exercice 9. Factoriser les polynômes suivants en polynômes irréductibles

1. $X^n + X^{n-1} + \cdots + 1$ dans $\mathbf{C}[X]$,
2. $X^{11} + 2^{11}$ dans $\mathbf{C}[X]$ puis dans $\mathbf{R}[X]$,
3. $X^4 + 4$ dans $\mathbf{C}[X]$ puis dans $\mathbf{R}[X]$, et enfin dans $\mathbf{Q}[X]$,
4. $X^4 - j$ dans $\mathbf{C}[X]$, où $j = \exp(2i\pi/3)$.
5. $X^8 + X^4 + 1$ dans $\mathbf{R}[X]$.
6. $X^5 - 1$ dans $\mathbf{R}[X]$.

Solution :

1. Notons que $(X^{n+1}-1)=(X-1)(X^n+X^{n-1}+\cdots+X+1)$. On sait que les racines complexes de $X^{n+1}-1$ sont $e^{i\frac{2k\pi}{n+1}}$ avec $k=0,1,\cdots,n$. Donc,
$$X^{n+1}-1=(X-1)\times\prod_{k=1}^{n}(X-e^{i\frac{2k\pi}{n+1}}).$$
On en déduit que
$$X^n+X^{n-1}+\cdots+1=\prod_{k=1}^{n}(X-e^{i\frac{2k\pi}{n+1}}).$$
2. Notons que les racines complexes de $X^{11}+2^{11}$ sont $(-2)e^{i\frac{2k\pi}{11}}$ où $k=0,\cdots,10$. Donc, dans $\mathbf{C}[X]$,
$$X^{11}+2^{11}=\prod_{k=0}^{10}(X+2e^{i\frac{2k\pi}{11}})$$
De plus, les racines $(-2)e^{i\frac{2k\pi}{11}}$ et $(-2)e^{i\frac{2(11-k)\pi}{11}}$ sont conjuguées. En conséquence,
$$\begin{aligned}X^{11}+2^{11}=\prod_{k=0}^{10}(X+2e^{i\frac{2k\pi}{11}}) &=(X+2)\prod_{k=1}^{5}[(X+2e^{i\frac{2k\pi}{11}})(X+2e^{i\frac{2(11-k)\pi}{11}})]\\ &=(X+2)\prod_{k=1}^{5}(X^2+4\cos(\frac{2k\pi}{11})X+4),\end{aligned}$$
dans $\mathbf{R}[X]$.
3. Les racines complexes de X^4+4 sont $\sqrt{2}e^{i\frac{(2k+1)\pi}{4}}$ où $k=0,1,2,3$. Donc, dans $\mathbf{C}[X]$,
$$X^4+4=(X-\sqrt{2}e^{i\frac{2\pi}{4}})(X-\sqrt{2}e^{i\frac{3\pi}{4}})(X-\sqrt{2}e^{i\frac{5\pi}{4}})(X-\sqrt{2}e^{i\frac{7\pi}{4}}).$$
Dans $\mathbf{R}[X]$ (ou dans $\mathbf{Q}[X]$), on a
$$X^4+4=X^4+4X^2+4-4X^2=(X^2+2)^2-(2X)^2=(X^2-2X+2)(X^2+2X+2).$$
4. Les racines complexes de X^4-j sont $e^{i\frac{(3k+1)\pi}{6}}$ où $k=0,1,2,3$. Dans $\mathbf{C}[X]$,
$$X^4-j=(X-e^{i\frac{\pi}{6}})(X-e^{i\frac{4\pi}{6}})(X-e^{i\frac{7\pi}{6}})(X-e^{i\frac{11\pi}{6}})$$
5. Observons que
$$\begin{aligned}X^8+X^4+1=&X^8+2X^4+1-X^4\\ =&(X^4+1)^2-X^4=(X^4+X^2+1)(X^4-X^2+1)\\ =&(X^4+2X^2+1-X^2)(X^4+2X^2+1-3X^2)\\ =&[(X^2+1)^2-X^2][(X^2+1)^2-3X^2]\\ =&(X^2+X+1)(X^2-X+1)(X^2+\sqrt{3}X+1)(X^2-\sqrt{3}X+1)\end{aligned}$$
6. Notons que les racines complexes de X^5-1 sont $X=e^{i\frac{2k\pi}{5}}$ avec $k=0,1,2,3,4$. Donc,
$$\begin{aligned}X^5-1=&(X-1)(X-e^{i\frac{2\pi}{5}})(X-e^{i\frac{4\pi}{5}})(X-e^{i\frac{6\pi}{5}})(X-e^{i\frac{8\pi}{5}})\\ =&(X-1)[(X-e^{i\frac{2\pi}{5}})(X-e^{i\frac{8\pi}{5}})]\times[(X-e^{i\frac{4\pi}{5}})(X-e^{i\frac{6\pi}{5}})]\\ =&(X-1)[(X-e^{i\frac{2\pi}{5}})(X-e^{-i\frac{2\pi}{5}})]\times[(X-e^{i\frac{4\pi}{5}})(X-e^{-i\frac{4\pi}{5}})]\\ =&(X-1)(X^2-2\cos(\frac{2\pi}{5})X+1)(X^2-2\cos(\frac{4\pi}{5})X+1)\end{aligned}$$
$\square$

Exercice 10. Soit $P = (X^2 - X + 1)^2 + 1$.

1. Vérifier que i est racine de P et que $P = X^4 - 2X^3 + 3X^2 - 2X + 2$.
2. En déduire alors la décomposition en produit de facteurs irréductibles de P sur $\mathbf{R}[X]$ et sur $\mathbf{C}[X]$. *Indication : On pourra penser à effectuer la division euclidienne de P par un polynôme de degré 2 bien choisi.*

Solution :

1. On calcule : $P(i) = (-i)^2 + 1 = 0$.
2. Puisque P $\mathbb{R}[X]$ on a aussi $-i$ qui est racine. Donc $X^2 + 1 | P$. On effectue la division eucidienne : $P = (X^2 + 1)(X^2 - 2X + 2)$. Puisque P n'a pas de racines réelles ($P(x) \geq 1$ pour tout x) on a la décompostion de P dans $\mathbb{R}$. Dans $\mathbf{C}$, on cherche les racines via le discriminant. On obtient $P = (X - i)(X + i)(X - 1 + i)(X - 1 - i)$.

□

Exercice 11. Soit $a \in \mathbf{R}$, $n \in N$, et le polynôme $P = (\cos a + X \sin a)^n \in \mathbf{R}[X]$. Calculer le reste de la division euclidienne de P par $X^2 + 1$.

Solution :
On peut écrire ce reste sous la forme $bX + c$. On a alors

$$P = Q \cdot (X^2 + 1) + bX + c.$$

De là, on obtient $P(i) = bi + c = exp(ina)$ et $P(i) = -bi + c = exp(-ina)$. On en déduit que $b = sin(na)$ et $c = cos(na)$.

□

Exercice 12. On rappelle que $j = e^{2i\pi/3}$. Soit le polynôme $P = X^8 + 2X^6 + 3X^4 + 2X^2 + 1$.

1. Montrer que j est racine de ce polynôme. Déterminer son ordre de multiplicité.
2. Décomposer P en facteurs irréductibles dans $\mathbf{C}[X]$ et dans $\mathbf{R}[X]$ (on pourra utiliser judicieusement le fait que P est pair).

Solution :

1. On utilise la relation $j^3 = 1$ pour obtenir

$$P(j) = j^2 + 2 + 3j + 2j^2 + 1 = 3j^2 + 3j + 3.$$

Or, j est racine de $X^2 + X + 1$, donc $j^2 = -j - 1$. On a donc

$$P(j) = 0.$$

On calcule maintenant la dérivée :

$$P' = 8X^7 + 12X^5 + 12X^3 + 4X = 4X(2X^6 + 3X^4 + 3X^2 + 1).$$

On a alors

$$P'(j) = 4j(2 + 3j + 3j^2 + 1) = 4jP(j) = 0.$$

Ensuite, on calcule la dérivée seconde :

$$P'' = 4(2X^6 + 3X^4 + 3X^2 + 1) + 4X(12X^5 + 12X^3 + 6X).$$

On a donc

$$P''(j) = 24j^2(2j + 2j^2 + 1) = -24j^2 \neq 0.$$

Donc j est racine de P d'ordre de multiplicité 2.

2. Puisque P est pair, pour chacune de ses racines, comptées avec multiplicité, l'opposé est racine aussi.

   Donc $-j$ est racie de multiplicité 2.

   D'autre part, puisque P est un polynôme réel, on a $\overline{j}$ et $-\overline{j}$ qui sont racines de multiplicité 2.

   Finalement,

$$P = (X - j)^2(X + j)^2(X - j^2)^2(X + j^2)^2.$$

□

<u>Exercice 13.</u> Soit le polynôme $P = X^6 + 4X^5 + 8X^4 + 10X^3 + aX^2 + 4X + 1 \in \mathbf{R}[X]$. On suppose que -1 est une racine de P.

1. Déterminer a.
2. Montrer que -1 est racine double de P.
3. Montrer que j est racine multiple de P.
4. Factoriser P en facteurs irréductibles, d'abord dans $\mathbf{C}[X]$ puis dans $\mathbf{R}[X]$.

Solution :

1. $P(-1) = 1 - 4 + 8 - 10 + a - 4 + 1 = -8 + a$ donc $P(-1) = 0 \Leftrightarrow a = 8$.
2. Deux solutions : faire la division euclidienne de P par $X+1$ et voir si 1 est racine puis recommencer, ou calculer les dérivées.

$$P' = 6X^5 + 20X^4 + 32X^3 + 30X^2 + 16X + 4.$$

   On a bien $P'(-1) = 0$. De plus,

$$P'' = 30X^4 + 80X^3 + 96X^2 + 60X + 16 \text{ et } P''(-1) = 2 \neq 0$$

   donc -1 est racine double de P.

3. $P(j) = 1 + 4j^2 + 8j + 10 + 8j^2 + 4j + 1$ et en utilisant $j^2 = -j - 1$ on obtient $P(j) = 0$.

   On calcule

$$P'(j) = 2(3j^2 + 10j + 16 + 15j^2 + 8j + 2) = 36(j^2 + j + 1) = 0.$$

   De même,

$$P''(j) = 30j + 80 + 96j^2 + 60j + 16 = -6j \neq 0$$

   donc j est racine double de P.

4. Puisque P est à coefficients réels, j^2 est racine double de P et on a alors

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

   Dans $\mathbf{R}$ on a alors

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

□

Exercice 14. Soit θ un réel, et n un entier supérieur ou égal à 2. Démontrer que le reste de la division euclidienne dans $\mathbf{C}[X]$ de $X^n \sin(\theta) - X\sin(n\theta) + \sin((n-1)\theta)$ par $X^2 - 2X\cos(\theta) + 1$ est nul. Qu'en est-il dans $\mathbf{R}[X]$?

Solution : On écrit $X^2 - 2\cos(\theta)X + 1 = (X - e^{i\theta})(X - e^{-i\theta})$, donc il s'agit de vérifier si

$$e^{in\theta}\sin(\theta) - e^{i\theta}\sin(n\theta) + \sin((n-1)\theta) = 0$$

et la même chose pour $e^{-i\theta}$. On écrit $e^{i\theta} = \cos(\theta) + i\sin(\theta)$ et on a

$$\begin{aligned} e^{in\theta}\sin(\theta) - e^{i\theta}\sin(n\theta) + \sin((n-1)\theta) &= \cos(n\theta)\sin(\theta) + i\sin(n\theta)\sin(\theta) \\ &\quad - \cos(\theta)\sin(n\theta) - i\sin(n\theta)\sin(\theta) + sin((n-1)\theta) \\ &= \cos(n\theta)\sin(\theta) - \cos(\theta)\sin(n\theta) + sin((n-1)\theta) \\ &= -sin((n-1)\theta) + sin((n-1)\theta) \\ &= 0. \end{aligned}$$

Puisque P est à coefficients réels on a alors aussi $e^{-i\theta}$ qui est racine de P. Le reste de la division euclidienne dans $\mathbf{C}$ est donc 0, on peut écrire $P = Q \cdot (X^2 - 2cos(\theta)X + 1)$ avec $Q \in \mathbf{C}[X]$.
Supposons que le reste de la division eucidienne dans $\mathbf{R}$ n'est pas 0. On a alors $P = Q_1 \cdot (X^2 - 2cos(\theta)X + 1) + aX + b$ pour un polynôme réel Q_1 et des réels a et b. Cela donne alors, dans $\mathbf{C}$,

$$Q_1 \cdot (X^2 - 2cos(\theta)X + 1) + aX + b = Q \cdot (X^2 - 2cos(\theta)X + 1)$$

et donc $X^2 - 2cos(\theta)X + 1 \mid aX + b$ donc $a = b = 0$.

□

Exercice 15.

1. Calculer le PGCD unitaire des polynômes $2X^4+X^2+X+1$ et de $X^6-X^5+X^4-2X^3+3X^2-3X+1$.
2. Montrer que les polynômes $X^4 - 1$ et $X^3 + 2X^2 - X - 1$ sont premiers entre eux, et établir un relation de Bézout entre eux.
3. Soient les polynômes complexes $A = X^5 - X^4 + 2X^3 + 1$ et $B = X^5 + X^4 + 2X^2 - 1$. Calculer leur PGCD unitaire. En déduire une relation de Bézout entre A et B. Déterminer tous les couples de polynômes (U, V) vérifiant cette identité.
4. Reprendre la question 3. avec $A = X^4 - X^3 + 2X^2 - 2X + 1$ et $B = X^3 - X^2 + 2X - 1$.

Solution :

4. La division euclidienne de A par B donne $A = Q_1B + R_1$ avec $Q_1 = X$ et $R_1 = -X + 1$. La division euclidienne de B par R_1 donne $B = Q_2R_1 + R_2$, avec $Q_2 = -(X^2 + 2)$ et $R_2 = 1$. Donc le pgcd de A et B vaut 1 : ils sont premiers entre eux. Pour avoir une relation de Bézout, on remonte à partir du pgcd en écrivant $R_2 = B - Q_2R_1$ et $R_1 = A - Q_1B$. On trouve

$$\begin{aligned} 1 = R_2 &= B + (X^2 + 2)R_1 \\ &= B + (X^2 + 2)(A - XB) \\ &= (-X^3 - 2X + 1)B + (X^2 + 2)A. \end{aligned}$$

□

Exercice 16. Soit n et m deux entiers. Calculer le PGCD unitaire des polynômes $X^n - 1$ et $X^m - 1$.

Solution : On note d le pgcd de n par m. Montrons que

$$\mathrm{pgcd}(X^n - 1, X^m - 1) = X^d - 1.$$

Ecrivons $n = qm + r$ avec $0 \leq r < m$ (division euclidienne). Alors en utilisant la formule de factorisation habituelle $a^q - b^q = (a-b)\sum_{k=0}^{q-1} a^k b^{q-1-k}$, on trouve

$$X^n - 1 - (X^r - 1) = X^{qm+r} - X^r = X^r((X^m)^q - 1) = X^r(X^m - 1)((X^m)^{q-1} + \cdots + X^m + 1),$$

autrement dit

$$X^n - 1 = Q(X)(X^m - 1) + X^r - 1,$$

avec $Q(X) = X^r(X^{m(q-1)} + \cdots + X^m + 1)$. Comme $\deg(X^r - 1) = r < m = \deg(X^m - 1)$, on trouve que le reste de la division euclidienne de $X^n - 1$ par $X^m - 1$ est précisément $X^r - 1$. Les restes successifs $r_1 = r, r_2, \ldots$ de l'algorithme de la division euclidienne de n par m fournissent les restes successifs $X^{r_1} - 1, X^{r_2} - 1, \ldots$ de l'algorithme de la division euclidienne du polynôme $X^n - 1$ par $X^m - 1$! En particulier, le dernier reste non nul d est le pgcd de m et n et correspond au dernier reste non nul $X^d - 1$ qui est le PGCD de $X^n - 1$ et $X^m - 1$.

Exercice 17. Donner une condition nécessaire et suffisante sur λ, μ pour que $X^2 + 1$ divise $X^4 + X^3 + \lambda X^2 + \mu X + 2$.

Solution :

P divise $X^2 + 1 \Leftrightarrow P$ divise $X - i$ et $X + i \Leftrightarrow i$ et $-i$ sont des racines de $P \Leftrightarrow P(i) = P(-i) = 0$ $\Leftrightarrow \begin{cases} 1 - i - \lambda + \mu i + 2 = 0 \\ 1 + i - \lambda - \mu i + 2 = 0. \end{cases} \quad \Leftrightarrow \lambda = 3, \mu = 2.$

Exercice 18. Montrer que, pour tout $n \in \mathbf{N}^*$, on a

$$\prod_{k=0}^{n-1}(X^2 - 2X\cos(2k\pi/n) + 1) = (X^n - 1)^2.$$

Solution :
On a $X^n - 1 = \prod_{k=0}^{n-1}\left(X - e^{\frac{2k\pi}{n}}\right) = \prod_{k=0}^{n-1}\left(X - e^{-\frac{2k\pi}{n}}\right)$ cela donne :

$$(X^n - 1)^2 = \prod_{k=0}^{n-1}\left(X - e^{\frac{2k\pi}{n}}\right)\prod_{k=0}^{n-1}\left(X - e^{\frac{2k\pi}{n}}\right) = \prod_{k=0}^{n-1}\left(X - e^{\frac{2k\pi}{n}}\right)\left(X - e^{\frac{-2k\pi}{n}}\right) = \prod_{k=0}^{n-1}(X^2 - 2X\cos(2k\pi/n) + 1)$$

Exercice 19. Soit $n \in \mathbf{N}$, $n \geq 1$, et soient $z_1, \ldots, z_n$ des nombres complexes (pas nécessairement distincts). On pose $e_0 = 1$ et, pour k compris entre 1 et n :

$$e_k = \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq n} z_{j_1} z_{j_2} \cdots z_{j_k}.$$

Voici quelques valeurs des e_k :

$$\begin{aligned}
e_0 &= 1,\\
e_1 &= z_1 + z_2 + \cdots + z_n,\\
e_2 &= (z_1z_2 + z_1z_3 + \cdots + z_1z_n) + (z_2z_3 + \cdots + z_2z_n) + \cdots + (z_{n-1}z_n),\\
&\vdots\\
e_{n-1} &= z_2\cdots z_n + z_1z_3\cdots z_n + \cdots + z_1\cdots z_{n-1},\\
e_n &= z_1z_2\cdots z_n.
\end{aligned}$$

1. Pour $n = 2$ (resp. $n = 3$), écrire explicitement e_1, e_2 (resp. e_1, e_2, e_3) et montrer que

   $$(X - z_1)(X - z_2) = X^2 - e_1X + e_2 \qquad \big(\text{resp. } (X - z_1)(X - z_2)(X - z_3) = X^3 - e_1X^2 + e_2X - e_3\big).$$

2. Pour n quelconque, montrer que l'on a :

   $$\prod_{j=1}^{n}(X - z_j) = \sum_{k=0}^{n}(-1)^k e_k X^{n-k} \ .$$

3. Sachant que $2i$ et $3-i$ sont des racines de $X^3+(i+1)X^2-(8+4i)X-4+28i$, calculer la troisième racine complexe de ce polynôme.
4. Pour $n \in \mathbf{N}$, $n \geq 2$, déterminer sans calcul $\sum_{1\leq j\leq n} e^{2\pi ij/n}$ et $\sum_{1\leq j<k\leq n} e^{2\pi i(j+k)/n}$.

Solution :

1. $\underline{n = 2}$:

$e_0 = 1,\ e_1 = z_1 + z_2,\ e_2 = z_1z_2.$

Donc $(X - z_1)(X - z_2) = X^2 - X(z_1 + z_2) + z_1z_2 = X^2 - e_1X + e_2.$

$\underline{n = 3}$:

$e_0 = 1,\ e_1 = z_1 + z_2 + z_3,\ e_2 = z_1z_2 + z_1z_2 + z_2z_3,\ e_3 = z_1z_2z_3.$

Donc $(X - z_1)(X - z_2)(X - z_3) = X^3 - (z - 1 + z_2 + z_3)X^2 + (z_1z_2 + z_1z_2 + z_2z_3)X - z_1z_2z_3 = X^3 - e_1X^2 + e_2X - e_3.$

2. On demontre le resultat par recurrence :

Initialisation : pour $n = 2$, le resultat est vrai.

Heridite : on suppose que (P_n) est vraie et on demontre que P_{n+1} l'est aussi,

Soient $\{e_k, k \in \{0, .., n\}\}$ comme precedement definits et :

$$\begin{aligned}
d_0 &= 1,\\
d_1 &= z_1 + z_2 + \cdots + z_{n+1},\\
d_2 &= (z_1z_2 + z_1z_3 + \cdots + z_1z_{n+1}) + (z_2z_3 + \cdots + z_2z_{n+1}) + \cdots + (z_nz_{n+1}),\\
&\vdots\\
d_n &= z_2\cdots z_{n+1} + z_1z_3\cdots z_{n+1} + \cdots + z_1\cdots z_n,\\
d_{n+1} &= z_1z_2\cdots z_{n+1}.
\end{aligned}$$

Le but est de montrer que :

$$\prod_{j=1}^{n+1}(X - z_j) = \sum_{k=0}^{n+1}(-1)^k d_k X^{n+1-k}.$$

On a :

$$\begin{aligned}\prod_{j=1}^{n+1}(X-z_j) &= (X-z_{n+1})\prod_{j=1}^{n}(X-z_j)\\
&= (X-z_{n+1})\sum_{k=0}^{n}(-1)^k e_k X^{n-k} \quad (P_n)\\
&= \sum_{k=0}^{n} z_{n+1}(-1)^{k+1}e_k X^{n-k} + \sum_{k=0}^{n}(-1)^k e_k X^{n+1-k}\\
&= \sum_{k=1}^{n+1} z_{n+1}(-1)^{k}e_{k-1} X^{n+1-k} + \sum_{k=0}^{n}(-1)^k e_k X^{n+1-k}\\
&= (-1)^{n+1}z_{n+1}e_n + \sum_{k=1}^{n} z_{n+1}(-1)^{k}e_{k-1} X^{n+1-k} + \sum_{k=1}^{n}(-1)^k e_k X^{n+1-k} + e_0X^{n+1}\\
&= d_0X^{n+1} + \sum_{k=1}^{n} z_{n+1}\Big((-1)^k e_{k-1} + (-1)^k e_k\Big) X^{n+1-k} + (-1)^{n+1}d_{n+1} \quad \text{car } z_{n+1}e_n = d_{n+1},\ e_0 = d_0\\
&= d_0X^{n+1} + \sum_{k=1}^{n} z_{n+1}((-1)^k d_k) X^{n+1-k} + (-1)^{n+1}d_{n+1} \quad \text{car } e_{k-1}+e_k = d_k\\
&= \sum_{k=0}^{n+1}(-1)^k d_k X^{n+1-k}.\end{aligned}$$

Conclusion : $\forall n \in \mathbf{N} \quad \prod_{j=1}^{n}(X-z_j) = \sum_{k=0}^{n}(-1)^k e_k X^{n+1-k}$.

3. D'apres la question 2., si on note z la troisieme racine de $X^3+(i+1)X^2-(8+4i)X-4+28i$ on a : $(2i)+(3-i)+z_3 = e_1 = -i-1$ donc : $z_3 = -4-2i$.

4. Si $n \geq 2$, les $e^{i\frac{2\pi j}{n}}, j\{1,..,n\}$ sont les racines du polynome X^n-1 donc : $\sum_{1\leq j\leq n} e^{2\pi ij/n} = e_1 = 0$

On a : $e^{2\pi i(j+k)/n} = e^{i\frac{2\pi j}{n}}e^{i\frac{2\pi k}{n}}$, donc, Idem : $\sum_{1\leq j<k\leq n} e^{2\pi i(j+k)/n} = e_2 = \begin{cases} 0 \text{ si } n\geq 3.\\ -1 \text{ si } n=2.\end{cases}$

<u>Exercice 20.</u> Soit $P(X) = X^4+12X-5$. Décomposer ce polynôme en facteurs irréductibles dans $\mathbf{R}[X]$, en sachant qu'il admet deux racines dont la somme vaut 2. **Solution :**

On suppose que a, b sont les racines tels que : $a+b = 2$,. Soient maintenant c, d les deux autres racines de ce polynome.

D'apres l'exercie 18. on a $0 = e_1 = a+b+c+d$ et donc $c+d = -2$.

Puisque : $P = ((X-a)(X-b))((X-c)(X-d)) = (X^2-2X+ab)(X^2+2X+cd) = X^4+(-4+ab+cd)X^2+(2ab-2cd)X+(ab)(cd)$ on a :

$$\begin{cases} a+b=2.\\ c+d=-2\\ ab+cd=4\\ ab-cd=6\\ (ab)(cd)=-5.\end{cases} \Longrightarrow \begin{cases} a+b=2.\\ ab=5\\ c+d=-2\\ cd=-1.\end{cases} \Longrightarrow \begin{cases}(a,b)\in(1+2i,1-2i)\\ (c,d)\in(-1+\sqrt{2},-1-\sqrt{2}).\end{cases}$$

La decomposition dans $\mathbf{C}[X]$ est donnee par :

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

La decomposition dans $\mathbf{R}[X]$ est donnee par :

$$P = (X+1-\sqrt{2})(X+1+\sqrt{2})(X^2-2X+5).$$

Exercice 21. Quels sont les polynômes $P \in \mathbf{C}[X]$ tels que P' divise P ? **Solution :**

$P \in \mathbf{C}[X]$, on suppose que $P'|P$ et que $P \neq 0$
Si $deg(P) = 0$ alors $P' = 0$ ce qui est exclu. Par consequent $deg(P) \geq 1$.
Alors $\exists Q \in \mathbf{C}[X]$ tel que $P = QP'$, or $deg(P) = deq(P') + deg(Q) \implies deq(Q) = 1$.
Soit r une racine de P, comme $P = QP'$ on a :

$$\text{multiplicite de } r \text{ pour } P = \text{multiplicite de } r \text{ pour } P' + \text{multiplicite de } r \text{ pour } Q$$

Or par definition, on a :

$$\text{multiplicite de } r \text{ pour } P = \text{multiplicite de } r \text{ pour } P' + 1$$

Donc r est une racine de Q, comme Q est de la forme $x \mapsto ax + b, a \neq 0$ alors il admet une seule racine qui est r, cela implque que P admet une seule racine, cette racine est de multiplicite $deg(P)$.
En consequence, $\exists c \in \mathbf{C}^*, r \in \mathbf{C}$ tel que : $P = c(X - r)^{deg(P)}$.Reciproquement, on peut verifier que les polynomes de cette forme satisfont : $P'|P$.

Exercice 22.

1. Factoriser le polynôme $X^2 - X + 1$ dans $\mathbf{C}[X]$.
2. Soit n un entier naturel. Montrer que $(X - 1)^{n+2} + X^{2n+1}$ est divisible par $X^2 - X + 1$.

Solution :
1. On a $X^2 - X + 1 = (X - e^{i\frac{\pi}{3}})(X - e^{-i\frac{\pi}{3}})$
2. $n \in \mathbf{N}$, on a : $X^2 - X + 1|(X - 1)^{n+2} + X^{2n+1} \Leftrightarrow (X - e^{i\frac{\pi}{3}})(X - e^{-i\frac{\pi}{3}})|(X - 1)^{n+2} + X^{2n+1} \Leftrightarrow$ $e^{i\frac{\pi}{3}}$ et $e^{-i\frac{\pi}{3}}$sont des racines de $(X - 1)^{n+2} + X^{2n+1}$.
Or, $e^{i\frac{\pi}{3}} - 1 = e^{i\frac{\pi}{6}}(e^{i\frac{\pi}{6}} - e^{i\frac{-\pi}{6}}) = e^{i\frac{\pi}{6}}(2isin(\frac{\pi}{6})) = e^{i\frac{\pi}{6}+i\frac{\pi}{2}} = e^{i\frac{2\pi}{3}}$
Alors,
$(e^{i\frac{\pi}{3}} - 1)^{n+2} + (e^{i\frac{\pi}{3}})^{2n+1} = (e^{i\frac{2\pi}{3}})^{n+2} + (e^{i\frac{\pi}{3}})^{2n+1} = (e^{i\frac{\pi}{3}})^{2n+4} + (e^{i\frac{2\pi}{3}})^{2n+1} = (e^{i\frac{\pi}{3}})^{2n+1}\Big((e^{i\frac{\pi}{3}})^3 + 1\Big) =$ $(e^{i\frac{\pi}{3}})^{2n+1}(e^{i\pi} + 1) = 0$
Le polynome $(X - 1)^{n+2} + X^{2n+1}$ est dans $\mathbf{R}[X]$ et donc il admet $e^{-i\frac{\pi}{3}}$ comme racine, par consequent $X^2 - X + 1|(X - 1)^{n+2} + X^{2n+1}$.

Exercice 23. Soit $P \in \mathbf{C}[X]$ défini par $P(X) = X^3 + 3X^2 + 2X + i$.

1. Déterminer les racines du polynôme dérivé P'.
2. Montrer que P n'admet aucune racine réelle.
3. Déduire des questions précédentes que P admet 3 racines distinctes dans $\mathbf{C}$, notées α, β et γ.
4. Calculer $\alpha + \beta + \gamma$, $\alpha^2 + \beta^2 + \gamma^2$ et $\alpha^3 + \beta^3 + \gamma^3$.

Solution :
1. $P' = 3X^2 + 6X + 2$ donc les racines de P' sont : $x_1 = -2 + \frac{2}{\sqrt{3}}$ et $x_2 = -2 - \frac{2}{\sqrt{3}}$.
2. On a : $P(X) = 0 \Leftrightarrow -i = -(X^3 + 3X^2 + 2X)$ qui ne peut jamais etre vraie si $X \in \mathbf{R}$.
3. P n'admet aucune racine reelle, donc toutes ces racines sont complexes, comme la derive de P n'admet

aucune racince complexes, alors P n'admet aucune racine de multiplicite ≥ 2.Enfin, P admet 3 racine complexes (non reelles) distinctes.
4. Supposons que a, b et c sont les racince de P, d'apres l'exercice 18. on a :

$$\begin{cases} a+b+c=(-1)^1e_1=-3 \\ ab+ac+bc=(-1)^2e_2=2 \\ abc=(-1)^3e_3=-i \end{cases}$$

Cela implique que :

$$a^2+b^2+c^2=(a+b+c)^2-2(ab+ac+bc)=(-3)^2-2(2)=5.$$

Et,

$$a^3+b^3+c^3=(a+b+c)^3-3(ab+ac+bc)(a+b+c)+3abc=-27-3(2)(-3)+3(-i)=-9-3i.$$

<u>Exercice 24.</u> On note $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ et α_5 les racines complexes du polynôme $P(X)=X^5-29X^4+117X^3-11X^2+4X+1$. Montrer que ces nombres sont différents de 0. Écrire le polynôme unitaire de degré 5 dont les racines sont $1/\alpha_1, 1/\alpha_2, 1/\alpha_3, 1/\alpha_4$ et $1/\alpha_5$.

Solution : $P(0)=1\neq 0$, donc aucun des α_i n'est nul. Remarquons que

$$Q(X):=X^5P(1/X)=1-29X+117X^2-11X^3+4X^4+X^5$$

est un polynôme donc les racines sont également non nulles, et que $Q(\lambda)=0$ est équivalent à $P(1/\lambda)=0$. Donc les racines de Q sont précisément $1/\alpha_1, 1/\alpha_2, 1/\alpha_3, 1/\alpha_4$ et $1/\alpha_5$.

<u>Exercice 25.</u> Déterminer le PGCD unitaire de $P(X)=X^5+X^4+X^3+X^2+X+1$ et de $Q(X)=X^4-1$, considérés comme éléments de $\mathbf{Q}[X]$.

Solution : *Première méthode.* Faire l'algorithme d'Euclide (long).

Deuxième méthode. On a $Q(X)=(X^2-1)(X^2+1)=(X-1)(X+1)(X-i)(X+i)$. On vérifie que parmi $\pm 1, \pm i$, seul -1 est aussi racine de $P(X)$. Donc le plus grand facteur commun (rationnel) de $P(X)$ et $Q(X)$ est $X+1$.

<u>Exercice 26.</u> Déterminer tous les polynômes de degré 3, divisibles par $X-1$, et tels que les restes des divisions euclidiennes par $X-2$, par $X-3$ et par $X-4$ soient égaux (mais certainement non nuls).

Solution : Un polynôme, disons P, de degré 3 divisible par $X-1$, se décompose nécessairement comme

$$P(X)=(X-1)(aX^2+bX+c$$

où $a, b, c \in \mathbf{C}$ sont à déterminer. Par hypothèse, il exite $R\in\mathbf{C}$ et trois polynômes Q_1, Q_2, Q_3 tels que

$$P(X)=(X-2)Q_1(X)+R=(X-3)Q_2(X)+R=(X-4)Q_3(X)+R.$$

En évaluant P sur 2 (donc $P(2)=R$)) 3 et 4 on trouve 3 équations :

$$2^2a+2b+c=R, 2(3^2a+3b+c)=R \text{ et } 3(4^2a+4b+c)=R.$$

On trouve une seule solution qui dépend du reste R (et dons une famille de solutions à un paramètre).

Exercice 27. Soit $n \in \mathbf{N}^*$, et considérons le polynôme à coefficients réels $P(X) = aX^{n+1} + bX^n + c$. Peut-on choisir a, b, c (avec $c \neq 0$) pour que P admette 1 comme racine multiple ? Quel est alors l'ordre de cette racine ?

Solution : Remarquons que $P'(X) = a(n+1)X^n + bnX^{n-1}$. Supposons que 1 soit une racine multiple de P (c'est-à-dire d'ordre au moins 2). On doit avoir alors

$$\begin{cases} P(1) = a + b + c = 0 \\ P'(1) = a(n+1) + bn = 0. \end{cases}$$

Cela conduit à $0 = P'(1) - nP(1) = a - nc$, i.e. $a = nc$. Combiné avec la deuxième équation, on trouve aussi $b = -(n+1)c$, donc finalement

$$P(X) = c(nX^{n+1} - (n+1)X^n + 1).$$

Réciproquement, on vérifie aisément que si P est de cette forme alors $P(1) = P'(1) = 0$. Montrons que dans ce cas, si $c \neq 0$, alors 1 et d'ordre exactement 2. Si $n = 1$ c'est clair puisqu'on a alors $\deg P = n + 1 = 2$. Si $n \geq 3$, on a $P''(X) = cn(n+1)(nX^{n-1} - (n-1)X^{n-2})$ et on trouve

$$P''(1) = cn(n+1) \neq 0.$$

D'où le résultat.

□

Exercice 28. Factoriser $P = X^6 + X^3 + 1$ sous forme d'un produit de polynômes irréductibles de $\mathbf{R}[X]$.

Solution : Rappelons que $j = e^{2i\pi/3}$. Posons $Y = X^3$. On a alors

$$P(X) = Y^2 + Y + 1 = (Y - j)(Y - \overline{j}) = (X^3 - e^{2i\pi/3})(X^3 - e^{-2i\pi/3}).$$

Pour factoriser $X^3 - e^{\pm 2i\pi/3}$ on cherche les solutions de l'équation $x^3 = e^{\pm 2i\pi/3}$ de la manière habituelle (on prend une racine 3ème de $e^{\pm 2i\pi/3}$ qu'on multiple par les racines 3-ème de l'unité). Cela conduit à

$$P(X) = (X - e^{2i\pi/9})(X - je^{2i\pi/9})(X - \overline{j}e^{2i\pi/9})(X - e^{-2i\pi/9})(X - je^{-2i\pi/9})(X - \overline{j}e^{-2i\pi/9}).$$

Pour avoir la factorisation sur $\mathbf{R}$ on regroupe les termes avec des racines conjuguées et on utilise la formule $(X - e^{i\theta})(X - e^{-i\theta}) = X^2 - 2\cos(\theta)X + 1$ (cas particulier de la formule plus générale $(X - \alpha)(X - \overline{\alpha}) = X^2 - 2\Re(\alpha)X + |\alpha|^2$). Par exemple, puisque $je^{2i\pi/9} = e^{8i\pi/9}$, on a

$$(X - je^{2i\pi/9})(X - \overline{j}e^{-2i\pi/9}) = (X - je^{2i\pi/9})(X - \overline{je^{2i\pi/9}}) = X^2 - 2\cos(8\pi/9)X + 1.$$

Finalement on trouve

$$P(X) = (X^2 - 2\cos(2\pi/9)X + 1)(X^2 - 2\cos(4\pi/9)X + 1)(X^2 - 2\cos(8\pi/9)X + 1)$$

Exercice 29. Soit $n \in \mathbf{N}^*$. Montrer que les polynômes $P(X) = 1+\dfrac{X}{1!}+\ldots+\dfrac{X^n}{n!}$ et $Q(X) = 1+X+X^n$ n'ont que des racines simples dans $\mathbf{C}$.

Solution : On remarque que

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

Par l'absurde, supposons que P ait une racine λ d'ordre ≥ 2. Alors $P(\lambda) = P'(\lambda) = 0$, donc $\lambda^n/n! = 0$ par ce qui précède. On en déduit que $\lambda = 0$: contradiction (puisque $P(0) = 1 \neq 0$).

Si $n = 1$ le résultat est clair (Q a alors une unique racine car de degré 1). On suppose $n \geq 2$. On a $Q'(X) = 1 + nX^{n-1}$. Par l'absurde, supposons que Q ait une racine λ d'ordre ≥ 2. Alors $Q(\lambda) = 0$ et $Q'(\lambda) = 0$. La deuxième équation donne $\lambda^{n-1} = -1/n$. En particulier

$$|\lambda| < 1 \quad \text{et} \quad \lambda^n = -\frac{\lambda}{n}.$$

Or la première équation donne $0 = 1 + \lambda + \lambda^n = 1 + (1 - 1/n)\lambda$, d'où

$$\lambda = -\frac{1}{1 - 1/n},$$

et donc $|\lambda| > 1$: contradiction.

$\square$

Exercice 30. Montrer que le polynôme $P = X^{163} - 24X^{57} - 6$ possède au moins une racine réelle, mais ne possède pas de racine rationnelle.

Solution : On a $\lim_{x\to+\infty} P(x) = +\infty$ et $\lim_{x\to-\infty} P(x) = -\infty$. Par le TVI il existe $\lambda \in \mathbf{R}$ tel que $P(\lambda) = 0$. Par l'absurde, supposons qu'il existe $p/q \in \mathbf{Q}$ avec $p \in \mathbf{Z}$ et $q \in \mathbf{N}^*$ premiers entre eux, tels que

$$0 = P(p/q) = \left(\frac{p}{q}\right)^{163} - 24\left(\frac{p}{q}\right)^{57} - 6.$$

Cela implique (en multipliant par q^{163}) que

$$0 = p^{163} - 24p^{57}q^{106} - 6q^{163}.$$

En particulier, comme q divise $-24p^{57}q^{106} - 6q^{163}$, on doit avoir q divise p^{163}, donc $q = 1$ (car p et q sont premiers entre eux). (Remarquons que de même, p divise $p^{163} - 24p^{57}q^{106}$, on doit avoir p divise $6q^{163}$, donc p divise 6, puisque p et q sont premiers entre eux... ici nous allons conclure autrement). Puisque $0 = p^{163} - 24p^{57} - 6$, on a p^57 qui divise $p^{163} - 24p^{57}$, donc p^{57} divise 6, ce qui n'est possible que si $p = \pm 1$. On vérifie enfin facilement que $\pm$ ne sont pas racines de P : contradiction.

Exercice 31. Soient a, b des réels, et $P = X^4 + 2aX^3 + bX^2 + 2X + 1$. Pour quelles valeurs de a et b le polynôme P est-il le carré d'un polynôme de $\mathbf{R}[X]$?

Solution : Puisque P est de degré 4, il ne peut être le carré que d'un polynôme de degré deux. On cherche donc les valeurs de a et b telles qu'il existe λ, c et d tels que

$$X^2 + 2aX^3 + bX^2 + 2X + 1 = (\lambda X^2 + cX + d)^2 = \lambda^2 X^4 + 2\lambda c X^3 + (2\lambda d + c^2)X^2 + 2cdX + d^2.$$

Par identification, si la solution existe si et seulement si le système

$$\begin{cases} \lambda^2 = 1 \\ 2\lambda c = 2a \\ 2\lambda d + c^2 = b \\ 2cd = 2 \\ d^2 = 1 \end{cases}$$

a une solution. Puisque $d^2 = 1$ et $cd = 1$, alors $c = d = \pm 1$. De plus $\lambda = \pm 1$. On a donc que $a = \lambda c$ et $b = 2\lambda c + 1$. Puisqu'il n'y a que deux valeurs possibles à λc, à savoir 1 ou -1, le système a donc deux solutions, $a = 1$ et $b = 3$ ou $a = -1$ et $b = -1$.
Ainsi, il faut et il suffit que $(a, b) \in \{(1, 3); (-1, -1)\}$ pour que le polynôme P soit un carré.

Exercice 32.

1. Soient p_1, p_2, p_3 et p_4 quatre entiers. Trouver deux entiers q_1 et q_2 tels que $(p_1^2+p_2^2)(p_3^2+p_4^2) = q_1^2+q_2^2$. *(Indication : manipuler les nombres complexes $p_1 + ip_2$ et $p_3 + ip_4$).*
2. Soient P_1, P_2, P_3 et P_4 quatre polynômes de $\mathbf{R}[X]$. En s'inspirant de la question précédente, trouver deux polynômes réels Q_1, Q_2 tels que $(P_1^2 + P_2^2)(P_3^2 + P_4^2) = Q_1^2 + Q_2^2$.
3. Soit $P \in \mathbf{R}[X]$. Montrer l'équivalence entre les deux assertions suivantes :
   (a) Pour tout réel x, on a $P(x) \geq 0$.
   (b) Il existe Q_1, Q_2 dans $\mathbf{R}[X]$ tels que $P = Q_1^2 + Q_2^2$.

Solution :

1. Posons $p = p_1 + ip_2$, $p' = p_3 + ip_4$. Le problème devient de trouver $q = q_1 + iq_2$ où $(q_1, q_2) \in \mathbf{Z}^2$ tel que $|p|^2|p'|^2 = |q|^2$. Il est donc clair que poser $q = pp'$ convient, et de plus ses parties réelles et imaginaires sont entières. En développant, on trouve en effet $q_1 = p_1p_3 - p_2p_4 \in \mathbf{Z}$ et $q_2 = p_2p_3 + p_1p_4$.
2. On pose $Q_1 = P_1P_3 - P_2P_4$ et $Q_2 = P_2P_3 + P_1P_4$, qui sont des polynômes réels, et en développant on retrouve bien que $(P_1^2 + P_2^2)(P_3^2 + P_4^2) = Q_1^2 + Q_2^2$.
3. L'implication $b) \Rightarrow a)$ est évidente. Montrons la réciproque. Soit P un polynôme tel que pour tout $x \in \mathbf{R}$, $P(x) \geq 0$. On sait alors que P se décompose en facteurs irréductibles de la forme $X^2 + 2bX + c^2$, avec $b^2 - c^2 \leq 0$, car sinon P aurait une racine simple, ce qui n'est pas possible à cause de son signe. On note $P = P_1 \dots P_r$ la décomposition en facteurs irréductibles de P. Pour $1 \leq n \leq r$. Posons l'hypothèse de récurrence H_n : "Il existe deux polynômes Q_1 et Q_2 tels que $P_1 \dots P_n = Q_1^2 + Q_2^2$".
   Initialisons. $P_1 = X^2 + 2bX + c^2 = (X - b)^2 + \sqrt{c^2 - b^2}$, donc H_1 est vraie.
   La question 2 montre que si H_n est vraie, alors H_{n+1}. Par récurrence, on a donc pour tout $1 \leq n \leq r$, H_n est vraie. En particulier H_r est vraie et donc il existe deux polynômes Q_1 et Q_2 tels que $P = Q_1^2 + Q_2^2$.

Exercice 33. Déterminer tous les polynômes P vérifiant les relations suivantes :

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

b) $P(2X+1) = P(X)$,

c) $(1-X)P'(X) - P(X) = X^n$, où $n \in \mathbf{N}$,

d) $P'(X)^2 = 4P(X)$,

e) $P(P(X)) = P(X)$.

Solution :

a) Considérons les degrés : $\deg[P(X^2+1)] = 2\deg P$, mais doit être aussi égal à $\deg P$, donc $\deg P \in \{-\infty, 0\}$. Réciproquement, tous les polynômes constant conviennent. Ce sont donc les seules solutions.

b) Si le polynôme P est non nul, il s'écrit de manière unique comme $P = \sum_{k=0}^{n} a_k X^k$, avec $a_n \neq 0$. Or, $P(2x+1) = \sum_{k=0}^{n} a_k (2X+1)^k$. Par identification du terme de plus haut degré, on a $a_n = 2^n a_n$. Puisque $a_n \neq 0$, on a donc $2^n = 1$, c'est à dire $n = 0$. Puisque les polynômes constant et le polynôme nul conviennent, ce sont les seules solutions.

c) Puisque le polynôme nul n'est pas solution, P s'écrit de façon unique comme $P = \sum_{k=0}^{d} a_k X^k$, avec $a_d \neq 0$. Si $d = 0$, il n'existe de solution que si $n = 0$ et alors $P = 1$. On suppose donc désormais que $d \geq 1$. On a donc

$$\begin{aligned}(1-X)P'(X) - P(X) &= \sum_{k=1}^{d} k a_k X^{k-1} - \sum_{k=1}^{d} k a_k X^k - \sum_{k=0}^{d} X^k \\ &= a_1 - a_0 + \sum_{k=1}^{d-1} [(k+1)a_{k+1} - k a_k - a_k] X^k - (d+1) a_d X^d.\end{aligned}$$

Ainsi, commençons par voir que puisque $-(d+1)a_d \neq 0$, alors $d = n$ nécessairement. On a alors par identification $a_n = -\frac{1}{n+1}$, $a_1 - a_0 = 0$ et pour tout $1 \leq k \leq d-1$, $[(k+1)a_{k+1} - k a_k - a_k] = 0$, c'est à dire $a_{k+1} = a_k$. Ainsi, pour tout $0 \leq k \leq d$, $a_k = a_n = \frac{1}{n+1}$. Il ne peut y avoir au plus qu'une seule solution, et l'on vérifie facilement que le polynôme $P = -\frac{1}{n+1} \sum_{k=0}^{n} X^k$ convient en effet.

d) Puisque $\deg[P'(X)^2] = 2(\deg P - 1)$, on a donc $2(\deg P - 1) = \deg$ c'est à dire $\deg P = 2$. On cherche donc une solution de la forme $P = aX^2 + bX + c$. On a donc $(2aX+b)^2 = 4aX^2 + 4bX + 4c$, et donc par identification $4a^2 = 4a$, $4ab = 4b$ et $b^2 = 4c$. Donc $a = 1$ puisque $a \neq 0$, et $c = b^2/4$. Réciproquement les polynômes $P = X^2 + bX + b^2/4 = (X - b/2)^2$ sont tous solutions.
Une autre façon de le prouver est de remarquer que puisque P est de degré plus grand que 1, P a une racine α dans $\mathbf{C}$. C'est à dire $(X-\alpha)|P$. Or $P = P'^2$ donc $(X-\alpha)|P'^2$, donc $(X-\alpha)|P'$, donc $(X-\alpha)^2|P'^2$, c'est à dire $(X-\alpha)^2|P$. Reste à montrer que le polynôme est unitaire pour conclure.

e) Puisque $\deg[P(P(X))] = (\deg P)^2$, on a donc que P est le polynôme nul ou $\deg P \in \{0, 1\}$. On cherche donc les solutions parmi les polynômes $P = aX + b$. On a alors $a(aX+b) + b = ax + b$ donc par identification $a^2 = a$ et $ab + b = b$, d'où $a = 0$ ou $a = 1$, et si $a = 1$, alors $b = 0$. Puisque qu'ils conviennent, les solutions sont donc les polynômes constants et le polynôme X.

Exercice 34.

1. Soient P_1, P_2 et Q trois polynômes. Montrer que $P_1 - P_2$ divise $Q(P_1) - Q(P_2)$.
2. Soit P un polynôme. Montrer que $P(X) - X$ divise $P(P(X)) - X$.

Solution :

1. Si Q est le polynôme nul, c'est trivial, sinon $Q = \sum_{k=0}^{d} q_k X^k$. On a alors

$$\begin{aligned} Q(P_1) - Q(P_2) &= \sum_{k=0}^{d} a_k[(P_1(X))^k - (P_2(X))^k] \\ &= \sum_{k=0}^{d} \left(a_k(P_1(X) - P_2(X)) \sum_{j=0}^{k-1} (P_1(X))^j (P_2(X))^{k-j-1} \right) \\ &= (P_1(X) - P_2(X)) \sum_{k=0}^{d} \left(a_k \sum_{j=0}^{k-1} (P_1(X))^j (P_2(X))^{k-j-1} \right). \end{aligned}$$

   Puisque le terme dans la somme est un polynôme, $P_1 - P_2$ divise $Q(P_1) - Q(P_2)$.
2. D'après la question précédent, $P(X) - X$ divise$P(P(X)) - P(X)$. Mais $P(X) - X$ se divise lui même, donc $P(X) - X$ divise $P(P(X)) - P(X) + P(X) - X = P(P(X)) - X$.

Exercice 35. **(Polynômes de Tchebychev)** On considère la suite de polynômes $P_n(x)$ définie par $P_0(X) = 1$, $P_1(X) = X$, et pour $n \in \mathbf{N}$,

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

1. Préciser P_2, P_3, P_4.
2. Déterminer le terme de plus haut degré de P_n.
3. Étudier la parité de P_n.
4. Montrer que pour tout $n \in \mathbf{N}$ et $\theta \in \mathbf{R}$, on a $P_n(\cos\theta) = \cos(n\theta)$.

Solution :

1. $P_2 = 2X^2 - 1$,
   $P_3 = 2X(2X^2 - 1) - X = 4X^3 - 3X$,
   $P_4 = 2X(4X^3 - 3X) - (2X^2 - 1) = 8X^4 - 8X^2 + 1$.
2. Par récurrence double, montrons que $P_n = 2^n X^n + Q_n$ où Q_n est de degré au plus $n - 1$. Cette proposition est vraie aux rangs 1 et 2 (au rang 0 éventuellement aussi, mais pour éviter l'ambiguïté du degré du polynôme nul, initialisons à 1 et 2.).

   Supposons cet énoncé vrai aux rangs n et $n + 1$. On a alors d'après l'hypothèse de récurrence :

$$P_{n+2} = 2XP_{n+1} - P_n = 2X(2^{n+1}X^{n+1} + Q_{n+1}) - P_n = 2^{n+2}X^{n+2} + 2XQ_{n+1} - P_n.$$

   De plus d'après l'hypothèse de récurrence, $2XQ_{n+1}$ est un polynôme de degré au plus $n + 1$, et P_n est de degré n. Donc $Q_{n+2} = 2XQ_{n+1} - P_n$ est un polynôme de degré au plus $n + 1$, donc la récurrence est prouvée.

3. Montrons par récurrence double que P_n est de la parité de n. C'est vrai aux rangs 1 et 2. De plus, si P est un polynôme qui a une parité, XP est un polynôme de parité inverse. Soit donc n tel P_n est de la parité de n et P_{n+1} est de la parité de $n+1$. Ainsi P_{n+2} est la somme d'un polynôme de la parité de n et un polynôme de la parité inverse de $n+1$, soit deux polynômes de la parité de $n+2$. Le résultat est ainsi prouvé par récurrence.
4. Raisonnons une nouvelle fois par récurrence sur $\mathbf{N}$. Il est clair que pour tout $\theta \in \mathbf{R}$, $1(\cos(\theta)) = 1 = \cos(0\theta)$, et $X(\cos(\theta)) = \cos(\theta)$, donc l'affirmation est vraie aux rangs 0 et 1.

   On la suppose vraie aux rangs n et $n+1$. Soit $\theta \in \mathbf{R}$. Alors $P_{n+2}(\cos(\theta)) = 2\cos(\theta)\cos((n+1)\theta) - \cos(n\theta)$. Or $\cos(n\theta) = \cos((n+1-1)\theta) = \cos(-\theta)\cos((n+1)\theta) - \sin(-\theta)\sin((n+1)\theta)$, donc

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

   Ce qui achève la preuve.

Exercice 36. Soit P un polynôme réel scindé à racines simples.

1. Montrer que P' est aussi scindé à racines simples.
2. Montrer que si a et b sont respectivement la plus petite et la plus grande racine de P alors les racines de P' sont comprises entre a et b.

Solution :

1. Soit n le degré de P. Soit $x_1 < \ldots < x_n$ les n racines du polynômes réel P scindé à racines simples. D'après le théorème de Rolle, puisque la fonction polynômiale associée à P satisfait à $P(x_1) = P(x_2) = \ldots = P(x_n)$, alors sa dérivée s'annule au moins au n-1 points $y_1, \ldots, y_{n-1}$ tels que $x_1 < y_1 < x_2$, $x_2 < y_2 < x_3$, …, $x_{n-1} < y_{n-1} < x_n$, et donc en particulier $y_1 < \ldots < y_{n-1}$. Le polynôme P' a donc au moins $n-1$ racines différentes dans $\mathbf{R}$, or il est de degré $n-1$, donc ce sont toutes ses racines et P' est scindé à racines simples.
2. D'après la question précédente, on a $x_1 < y_1 < \ldots < y_{n-1} < x_n$ ce qui répond à la question.

Exercice 37. Soit P et Q deux polynômes rationnels.

1. Montrer que $P|Q$ dans $\mathbf{Q}[X]$ si, et seulement si $P|Q$ dans $\mathbf{C}[X]$. (*En particulier, si $P \mid Q$ dans $\mathbf{C}[X]$, alors le quotient de la division de P par Q appartient à $\mathbf{Q}[X]$*).
2. Montrer que P et Q ont le même PGCD considérés comme polynômes à coefficients dans $\mathbf{Q}$ ou dans $\mathbf{C}$.
3. Montrer que si P est irréductible dans $\mathbf{Q}[X]$ alors P et P' sont premiers entre eux (on dit alors que $\mathbf{Q}$ est un *corps parfait*).

Solution :

1. Si $P|Q$ dans $\mathbf{Q}[X]$, alors $P|Q$ dans $\mathbf{C}[X]$. Réciproquement, supposons que $P|Q$ dans $\mathbf{C}[X]$, et écrivons la division euclidienne de Q par P dans $\mathbf{Q}[X]$: il existe deux polynômes T et R de $\mathbf{Q}[X]$ avec $\deg R < \deg P$ tels que $Q = TP + R$. Mais $P|Q$ dans $\mathbf{C}[X]$, donc il existe $S \in \mathbf{C}[X]$ tel que $Q = PS$. Donc $PS = TP + R$, c'est à dire $P(S - T) = R$. Or si $S - T$ n'est pas le polynôme nul, alors $\deg(P(S - T)) \geq \deg P$, ce qui est absurde puisque $\deg R < \deg P$. Donc $S - T$ est le polynôme nul, c'est à dire que $Q = TP$, et puisque $T \in \mathbf{Q}[X]$, c'est que $P|Q$ dans $\mathbf{Q}[X]$.
2. Puisque la divisibilité est la même dans $\mathbf{C}[X]$ que $\mathbf{Q}[X]$, l'algorithme d'Euclide conduit au même résultat.
3. Soit P un polynôme irréductible dans $\mathbf{Q}[X]$. Le PGCD dans $\mathbf{Q}[X]$ de P et P' divise P et P'. Or, puisque P est irréductible, par définition, les seuls polynômes rationnels unitaires qui divisent P sont 1 et P. Il reste donc à vérifier que P n'est pas un diviseur de P', ce qui est évident puisque $\deg P' < \deg P$. On déduit que $\mathrm{pgcd}_{\mathbf{Q}}(P, P') = 1$, et donc $\mathrm{pgcd}_{\mathbf{C}}(P, P') = 1$.