TD 18 : Polynômes

Sauf mention explicite du contraire, $\mathbf{K}$ est un corps quelconque.

► L'anneau $\mathbf{K}[X]$

Exercice 18.1 Déterminer le groupe des unités de l'anneau $\mathbf{K}[X]$. PD

Exercice 18.2 Un polynôme $P \in \mathbf{R}[X]$ est dit pair (respectivement impair) si $P(-X) = P(X)$ (resp. $P(-X) = -P(X)$). PD

1. Montrer qu'un polynôme $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbf{R}[X]$ est pair si et seulement si $\forall k \in \mathbf{N}$, $a_{2k+1} = 0$.
   Donner alors une condition nécessaire et suffisante portant sur les $P^{(k)}(0)$ pour que P soit pair.
2. Déterminer des conditions similaires pour qu'un polynôme soit impair.
3. Prouver qu'un polynôme P est pair si et seulement si $\forall k \in \mathbf{N}$, $P(k) = P(-k)$. La même condition est-elle valable pour une fonction continue ?

Exercice 18.3 Déterminer tous les polynômes $P \in \mathbf{C}[X]$ tels que : PD

1. $P(X^2) = (X^2+1)P(X)$
2. $P \circ P = P$
3. $(P')^2 = 4P$.

Exercice 18.4 Formule de Vandermonde PD
Soient $m, n, r \in \mathbf{N}$. En développant de deux manières le produit $(1+X)^m(1+X)^n$, déterminer la valeur de $\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}$.

► Divisibilité dans $\mathbf{K}[X]$, racines d'un polynôme

Exercice 18.5 PD

1. Soit $n \in \mathbf{N}^*$. Montrer que $(X-1)^3$ divise $nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$.
2. Soit $n \in \mathbf{N}^*$. Quelle est la multiplicité de 1 comme racine de $nX^{n+1} - (n+1)X^n + 1$?
3. Soit $n \in \mathbf{N}^*$. Déterminer le reste de la division de $X^n(X+1)^2$ par $(X+1)(X-2)$.

Exercice 18.6 Pour quelles valeurs de $n \in \mathbf{N}$ le polynôme $P_n = (X-1)^n - X^n + 2X - 1$ est-il divisible (dans $\mathbf{R}[X]$) par $Q = 2X^3 - 3X^2 + X$? PD

Exercice 18.7 Soit $n \in \mathbf{N}^*$ et $P \in \mathbf{K}[X]$. Montrer que si $P(X^n)$ est divisible par $X-1$, alors il est divisible par $X^n - 1$. PD

Exercice 18.8 Soit $P \in \mathbf{K}[X]$. Montrer que $P(X) - X$ divise $P(P(X)) - P(X)$. PD

Exercice 18.9 Soit $P \in \mathbf{R}[X]$. On suppose qu'il existe $a \in \mathbf{R}$ tel que $P(a) > 0$ et $\forall k \in \mathbf{N}^*$, $P^{(k)}(a) \geqslant 0$. PD
Prouver que P n'a pas de racine dans $[a, +\infty[$.

Exercice 18.10 La fonction $z \mapsto \overline{z}$ est-elle polynomiale ? PD

Exercice 18.11 Déterminer tous les polynômes $P \in \mathbf{R}[X]$ tels que $\forall n \in \mathbf{N}$, PD

1. $P(n) = n^2$
2. $P(n) = n^2 + (-1)^n$

Exercice 18.12 Soient $a, b \in \mathbf{N}^*$. Montrer que $X^a - 1$ divise $X^b - 1$ si et seulement si $a \mid b$. AD

Exercice 18.13 Soit $P \in \mathbf{R}[X]$ un polynôme unitaire dont tous les coefficients sont des entiers relatifs. PD

1. Prouver que toute racine rationnelle de P est dans $\mathbf{Z}$.
2. Soient $k, d \in \mathbf{N}^*$. Montrer que $\sqrt[k]{d}$ est soit entier, soit irrationnel.

Exercice 18.14 Déterminer la forme scindée (dans $\mathbf{C}[X]$) des polynômes suivants (où $n \in \mathbf{N}^*$) F

1. $X^4 - 16$
2. $X^3 + 1$
3. $X^n - 1$
4. $X^n + 2^n$.

Exercice 18.15 Montrer que les fonctions $x \mapsto \sin x$, $x \mapsto e^x$ et $x \mapsto \lfloor x \rfloor$ ne sont pas polynomiales. PD

Exercice 18.16 Discriminant d'un polynôme réel de degré 3 AD
Soient $p, q \in \mathbf{R}$. Montrer que $X^3 + pX + q$ est scindé sur $\mathbf{R}$ si et seulement si $4p^3 + 27q^2 \leqslant 0$.

Exercice 18.17 Soit $n \in \mathbf{N}$, et soit $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbf{C}[X]$. On note alors $M = \sup\{|P(z)|, |z| = 1\}$. AD

1. Justifier que M est bien défini.
2. On note $\zeta = e^{\frac{2i\pi}{n+1}}$. En calculant $P(1) + P(\zeta) + \cdots + P(\zeta^n)$, prouver que $|a_0| \leqslant M$.
3. Prouver que pour tout $k \in [\![0, n]\!]$, $|a_k| \leqslant M$.

Exercice 18.18 Montrer que $X^8 + 2X^6 + 3X^4 + 2X^2 + 1$ possède j comme racine double. En déduire sa factorisation irréductible sur $\mathbf{R}$ et sur $\mathbf{C}$. **AD**

Exercice 18.19 **(Banque CCINP 85)** **PD**
Déterminer deux réels a et b pour que 1 soit racine double du polynôme $P = X^5 + aX^2 + bX$ et factoriser alors ce polynôme comme produit de polynômes irréductibles de $\mathbf{R}[X]$.

Exercice 18.20 **La divisibilité dans $\mathbf{C}[X]$ de polynômes réels implique leur divisibilité dans $\mathbf{R}[X]$** **AD**

1. Soient A et B deux polynômes à coefficients réels, tels que A divise B dans $\mathbf{C}[X]$. Justifier que A divise B dans $\mathbf{R}[X]$.
2. Quels sont les entiers naturels n tels que $X^2 + X + 1$ divise $X^{2n} + X^n + 1$?

Exercice 18.21 Déterminer tous les polynômes $P \in \mathbf{C}[X]$ tels que P' divise P. **AD**

Exercice 18.22 **(Oral ENS)** **D**
Quels sont les polynômes $P \in \mathbf{C}[X]$ tels que $P(\mathbf{C}) \subset \mathbf{R}$?

Exercice 18.23 **(Oral Polytechnique)** **AD**

Soient $a_1, \ldots, a_n$ des réels. Déterminer le reste de la division euclidienne de $P(X) = \displaystyle\prod_{k=1}^{n} (\cos(a_k) + \sin(a_k)X)$ par $X^2 + 1$.

Exercice 18.24 **AD**

1. Soit $n \in \mathbf{N}^*$. Factoriser sur $\mathbf{C}$ le polynôme $P_n = 1 + X + X^2 + \cdots + X^{n-2} + X^{n-1}$.
2. En déduire une expression de $\displaystyle\prod_{k=1}^{n-1} \sin \frac{k\pi}{n}$.
3. Pour $\theta \in \mathbf{R}$, donner alors une expression de $\displaystyle\prod_{k=1}^{n} \sin\left(\frac{k\pi}{n} + \theta\right)$.
4. Soit $\zeta = e^{\frac{2i\pi}{n}}$. Calculer $\displaystyle\prod_{\substack{0 \leqslant k, \ell \leqslant n-1 \\ k \neq \ell}} \left(\zeta^k - \zeta^\ell\right)$.

Exercice 18.25 Soient m, n deux entiers supérieurs ou égaux à 2, premiers entre eux. Montrer que $(X^n - 1)(X^m - 1)$ divise $(X^{mn} - 1)(X - 1)$. **D**
Ce résultat reste-t-il vrai si m et n ne sont pas premiers entre eux ?

▸ Polynômes d'interpolation de Lagrange

Exercice 18.26 Soit $n \in \mathbf{N}^*$ et soient $\lambda_0, \ldots, \lambda_n$ des éléments deux à deux distincts de $\mathbf{K}$, et soient $L_0, \ldots, L_n$ les polynômes d'interpolation de Lagrange associés. Montrer que $\displaystyle\sum_{k=0}^{n} L_k = 1$. **PD**

Exercice 18.27 Soit $n \in \mathbf{N}$. Montrer qu'il existe $(\lambda_0, \ldots, \lambda_n) \in \mathbf{R}^{n+1}$ tels que $\forall P \in \mathbf{R}_n[X]$, $\displaystyle\int_0^1 P(t)\,dt = \sum_{k=0}^{n} \lambda_k P\left(\frac{k}{n}\right)$. **AD**

Exercice 18.28 Déterminer tous les polynômes $P \in \mathbf{C}[X]$ tels que $P(\mathbf{R}) \subset \mathbf{R}$, puis $P(\mathbf{Q}) \subset \mathbf{Q}$. **D**

Exercice 18.29 **Fait suite au précédent** **(Oral ENS)** **TD**
Déterminer tous les polynômes $P \in \mathbf{C}[X]$ qui induisent une surjection de $\mathbf{Q}$ sur $\mathbf{Q}$.

▸ Relations racines coefficients

Exercice 18.30 Soit $P \in \mathbf{C}[X]$, de degré n. Pour tout $k \in [\![0, n-1]\!]$, on note s_k la somme des racines (comptées avec multiplicité) de $P^{(k)}$. **AD**
Montrer que $s_0, s_1, \ldots, s_{n-1}$ est une progression arithmétique dont on précisera la raison.

Exercice 18.31 On note $(\mathscr{S})$ le système (non linéaire !) d'équations suivantes : $\begin{cases} x+y+z=1 \\ x^2+y^2+z^2=21 \\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1 \end{cases}$, d'inconnues $(x,y,z)\in(\mathbf{C}^*)^3$. **AD**

1. Pour $(x,y,z)\in(\mathbf{C}^*)^3$, on pose $P=(X-x)(X-y)(X-z)\in\mathbf{C}[X]$.
   Si (x,y,z) est solution de $\mathscr{S}$, déterminer P.
2. En déduire les solutions de $(\mathscr{S})$.

▶ Divers

Exercice 18.32 **(Oral Mines)** **AD**

1. Montrer que $\alpha=\cos\left(\frac{\pi}{9}\right)$ est racine d'un polynôme de degré 3 à coefficients entiers.
2. En déduire que α est irrationnel.

Exercice 18.33 **Sommes de deux carrés dans $\mathbf{R}[X]$** **D**

On note $\Sigma=\{A^2+B^2,\ (A,B)\in\mathbf{R}[X]\}$ l'ensemble des polynômes qui sont somme de deux carrés.

1. En utilisant l'application $\mathbf{C}[X]\to\mathbf{R}[X]$ définie par $Q\mapsto Q\overline{Q}$, montrer que Σ est stable par produit.
2. Montrer que si $P\in\Sigma$, alors $\forall x\in\mathbf{R}$, $P(x)\geqslant 0$.
3. Inversement, soit $P\in\mathbf{R}[X]$ tel que $\forall x\in\mathbf{R}$, $P(x)\geqslant 0$.
   (a) Montrer que toutes les racines réelles de P sont d'ordre de multiplicité pair.
   (b) En utilisant la décomposition de P en produit de facteurs irréductibles, prouver que $P\in\Sigma$.

Correction des exercices du TD 18

Solution de l'exercice 18.1

Il est évident que si P est un polynôme constant non nul, disons λ, alors il es inversible, d'inverse $\frac{1}{\lambda}$.
Inversement, soit P un inversible de $\mathbf{K}[X]$. Alors il existe $Q \in \mathbf{K}[X]$ tel que $PQ = 1$.
Et donc en particulier, $\deg P + \deg Q = 0$, donc $\deg P = \deg Q = 0$, de sorte que P est un polynôme constant **non nul.**
Autrement dit, l'ensemble des inversibles de $\mathbf{K}[X]$ est exactement l'ensemble des polynômes constants non nul, c'est-à-dire l'ensemble des polynômes de degré 0.

Rappel
Le polynôme nul n'est pas de degré 0.

Solution de l'exercice 18.2

1. Notons tout de suite que par dérivations successives d'une composée, pour tout $P \in \mathbf{R}[X]$ et tout $k \in \mathbf{N}$, $(P(-X))^{(k)} = (-1)^k P^{(k)}(-X)$.
En particulier si P est pair, pour tout $k \in \mathbf{R}[X]$, $P^{(k)}(X) = (-1)^k P^{(k)}(-X)$.
Et donc en évaluant en 0, $P^{(k)}(0) = (-1)^k P^{(k)}(0)$, de sorte que pour k impair, $P^{(k)}(0) = 0$.
Mais nous savons également que $P^{(k)}(0) = k! a_k$, et donc pour k impair, $a_k = 0$.

Inversement, si les a_k, pour k impair sont nuls, alors $P(X) = \sum_{k=0}^{+\infty} a_{2k} X^{2k}$, et donc $P(-X) = \sum_{k=0}^{+\infty} a_{2k}(-X)^{2k} = \sum_{k=0}^{+\infty} a_{2k} X^{2k} = P(X)$, donc P est pair.

2. De même, si P est impair, alors pour tout $k \in \mathbf{N}$, $-P^{(k)}(X) = (-1)^k P^{(k)}(-X)$, et donc $-P^{(k)}(0) = (-1)^k P^{(k)}(0)$ de sorte que pour tout k pair, $P^{(k)}(0) = 0$, et donc $a_k = 0$.
La réciproque se traite comme pour le cas des polynômes pairs.

3. Il est évident que si $P \in \mathbf{R}[X]$ est pair, alors pour tout $k \in \mathbf{N}$, $P(-k) = P(k)$.
Et inversement, si pour tout $k \in \mathbf{N}$, $P(k) = P(-k)$, notons $Q = P(X) - P(-X)$. Alors Q est un polynôme, qui s'annule en tous les entiers. Puisqu'il existe une infinité d'entiers, Q est dont le polynôme nul, de sorte que $P(X) = P(-X)$, et donc P est pair.

Ceci n'est pas vrai pour les fonctions continues, où la connaissance de f aux entiers relatifs ne détermine pas du tout son comportement sur $\mathbf{R} \setminus \mathbf{Z}$, et donc on peut imaginer des fonctions qui ne sont pas paires mais qui coïncident à tous les entiers. Par exemple, $f : x \mapsto \sin((2x+1)\pi)$ s'annule en tous les entiers relatifs, donc pour tout $k \in \mathbf{N}$, $f(k) = f(-k)$.
Mais pourtant, f est impaire, et n'étant pas la fonction nulle[1], elle n'est pas paire.

[1] Qui est la seule fonction à la fois paire et impaire.

Solution de l'exercice 18.3

1. Un tel polynôme, s'il est non nul, doit vérifier $\deg P \times 2 = 2 + \deg P$, donc être de degré 2.
Donc il existe $a, b, c \in \mathbf{K}$ tels que $P(X) = aX^2 + bX + c$.
Et alors $P(X^2) = aX^4 + bX^2 + c$, alors que $(X^2+1)P(X) = aX^4 + bX^3 + (c+a)X^2 + bX + c$.
Donc par identification, $b = 0$ puis $c = -a$.
Et par conséquent, $P = a(X^2 - 1)$.
Inversement, si $P = a(X^2-1)$, alors $(X^2+1)P(X) = a(X^2-1)(X^2+1) = a(X^4-1) = P(X^2)$.

2. Les polynômes constants sont évidemment solutions.
Et si P est non constant, alors $\deg(P \circ P) = \deg P$, donc $\deg(P)^2 = \deg P \Rightarrow \deg P = 1$.
Ainsi, il existe $(a, b) \in \mathbf{C}^* \times \mathbf{C}$ tels que $P(X) = aX + b$.
Mais alors $P \circ P = a(aX+b) + b = a^2 X + ab + b$.
Donc $a^2 = a$, et puisque $a \neq 0$, $a = 1$. Et donc $ab + b = b \Leftrightarrow b = 0$.
Inversement, le polynôme X est solution, et donc les polynômes vérifiant $P \circ P = P$ sont les polynômes constants et le polynôme X.

Détails
Les deux seules solutions de $x^2 = x$ sont 0 et 1, et on a écarté le cas $\deg P = 0$, puisque P est non constant.

3. Si P est une solution non constante, alors $\deg(P')^2 = \deg(4P) = \deg(P)$.
Mais $\deg P' = \deg P - 1$, et donc $\deg(P'^2) = 2\deg P' = 2\deg P - 2$.
On en déduit que $\deg P = 2$.
Notons alors $P = aX^2 + bX + c$, avec $a \neq 0$ un polynôme de degré 2. Alors $P' = 2aX + b$ et

donc $P'^2 = 4a^2X^2 + 4abX + b^2$, de sorte que

$$P'^2 = 4P \Leftrightarrow 4a^2X^2 + 4abX + b^2 = 4aX^2 + 4bX + 4c \Leftrightarrow \begin{cases} a^2 = a \\ ab = b \\ b^2 = 4c \end{cases}$$

Donc P est solution si et seulement si $a = 1$ et $c = \frac{b^2}{4}$.
Par ailleurs, la seule solution constante est le polynôme nul, puisque si P est constant, alors $P' = 0$, et donc $4P = 0_{\mathbf{C}[X]} \Leftrightarrow P = 0_{\mathbf{C}[X]}$.

Solution de l'exercice 18.4

On a clairement $(1+X)^m(1+X)^n = (1+X)^{m+n} = \displaystyle\sum_{k=0}^{m+n} \binom{n+m}{k} X^k$.

En particulier, son coefficient de degré r est $\binom{n+m}{r}$.

D'autre part, ce coefficient est donné par

$$\sum_{k=0}^{r} a_k b_{r-k}$$

où a_k (resp. b_k) est le coefficient de degré k de $(1+X)^m$ (resp. $(1+X)^n$).
Mais par le binôme, $a_k = \binom{m}{k}$ et $b_k = \binom{n}{k}$, donc

$$\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} = \sum_{k=0}^{r} a_k b_{r-k} = \binom{n+m}{r}.$$

Solution de l'exercice 18.5

1. Il s'agit donc de prouver que 1 est racine de multiplicité supérieure ou égale à 3 de $P_n = nX^{n+2} - (n+2)X^{n+1} + (n+2)X^{-}n$.
   Or, $P_n(1) = n - (n+2) + (n+2) - n = 0$. Donc 1 est racine de P_n.
   Puis $P_n' = n(n+2)X^{n+1} - (n+2)(n+1)X^n + n + 2$, de sorte que $P_n'(1) = 0$.
   Enfin, $P_n'' = n(n+1)(n+2)X^n - n(n+1)(n+2)X^{n-1}$ et donc $P_n''(1) = 0$.
   Donc 1 est racine d'ordre au moins 3 de P_n, qui est donc divisible par $(X-1)^3$.

> **Remarque**
> Nul besoin de calculer $P_n^{(3)}(1)$ pour voir si elle s'annule ou non.
> En effet, l'ordre de multiplicité ne nous intéresse pas vraiment, tout ce que nous voulons savoir à son égard, c'est qu'il est au moins égal à 3.

2. Notons $P_n = nX^{n+1} - (n+1)X^n + 1$.
   Alors $P_n(1) = 0$, $P_n'(1) = 0$ et $P_n''(1) = 2n(n+1) \neq 0$.
   Donc la multiplicité de 1 est égale à 2.
3. Il suffit d'utiliser les deux racines du diviseur, on obtient $3 \times 2^n(X+1)$.

Solution de l'exercice 18.6

Les racines de Q sont 0, 1 et $\frac{1}{2}$.
Si Q divise P_n, alors nécessairement ce sont des racines de P_n.
Or, $P_n(0) = (-1)^n - 1$, qui est nul si et seulement si n est pair.
Donc déjà les valeurs impaires de n ne conviennent pas.

Si n est pair, on a $P_n(1) = 0$, et $P_n\left(\frac{1}{2}\right) = \left(\frac{1}{2}\right)^n - \left(\frac{1}{2}\right)^n + 1 - 1 = 0$.

Donc P_n est divisible par $\left(X - \frac{1}{2}\right)(X-1)X$, et donc[2] par $2\left(X - \frac{1}{2}\right)(X-1)X = Q$.
Donc au final, P_n est divisible par Q si et seulement si n est pair.

[2] $2 \in \mathbf{R}^*$ est un inversible de $\mathbf{R}[X]$.

Solution de l'exercice 18.7

Puisque $P(X^n)$ est divisible par $X - 1$ si et seulement si $P(1) = 0$, c'est-à-dire si et seulement si 1 est racine de P.
Et donc il existe $Q \in \mathbf{K}[X]$ tel que $P = (X-1)Q$.
Mais alors par composition $P(X^n) = (X^n - 1)Q(X^n)$ est divisible par $X^n - 1$.

Solution de l'exercice 18.8

Notons $P = \sum_{k=0}^{n} a_k X^k$. Alors

$$P(P(X)) - P(X) = \sum_{k=0}^{n} a_k P(X)^k - \sum_{k=0}^{n} a_k X^k = \sum_{k=1}^{n} a_k (P(X)^k - X^k).$$

Mais pour $k \geqslant 1$, $P(X)^k - X^k = (P(X) - X)\left(\sum_{i=0}^{k-1} P(X)^i X^{k-1-i}\right)$.

Donc $P(X) - X$ divise $P(X)^k - X^k$.

Détails
La troisième identité remarquable généralisée est valable dans $\mathbf{K}[X]$ puisqu'il s'agit d'un anneau commutatif.

Solution de l'exercice 18.9

Appliquons la formule de Taylor en a :

$$P(X) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!}(X-a)^k.$$

En particulier, pour $x \geqslant a$, $P(x) = P(a) + \underbrace{\sum_{k=1}^{\deg P} \frac{P^{(k)}(a)}{k!}(x-a)^k}_{\geqslant 0} \geqslant P(a) > 0$.

Et donc P n'a pas de racine dans $[a, +\infty[$.

Solution de l'exercice 18.10

Supposons qu'il existe un polynôme $P \in \mathbf{C}[X]$ tel que pour tout $z \in \mathbf{C}$, $P(z) = \overline{z}$.
Alors en particulier, pour tout $x \in \mathbf{R}$, $P(x) = x$.
Donc $P - X$ s'annule en tous les réels, donc est nul.
Et par conséquent, $P = X$.
Mais alors pour $z \in \mathbf{C} \setminus \mathbf{R}$, $\overline{z} = P(z) = z$, ce qui est absurde.
Donc la fonction $z \mapsto \overline{z}$ n'est pas polynomiale.

Solution de l'exercice 18.11

1. Soit P un tel polynôme, et soit $Q = P - X^2$.
Alors $Q(n) = 0$, pour tout $n \in \mathbf{N}$. Donc Q possède une infinité de racines, et par conséquent est nul.
Et donc $P = X^2$. Inversement, $P = X^2$ est évidemment solution.
Donc seul le polynôme X^2 convient.
2. Soit P un tel polynôme, et soit $Q(X) = P(X) - X^2 - 1$.
Alors pour tout $n \in \mathbf{N}$, $Q(2n) = P(2n) - (2n)^2 - 1 = (2n)^2 + 1 - (2n)^2 - 1 = 0$.
Comme précédemment, on en déduit que Q est nul, et donc que $P(X) = X^2 + 1$.
Mais alors $P(3) = 10 \neq 3^2 - 1$, ce qui est absurde.
Autrement dit, il n'existe pas de tel polynôme.

Solution de l'exercice 18.12

Si a divise b, notons $b = aq$. Alors

$$X^b - 1 = (X^a)^q - 1^q = (X^a - 1)\sum_{k=0}^{q-1} X^{ak}$$

et donc $X^a - 1$ divise $X^b - 1$.

Remarque
Puisque $\mathbf{K}[X]$ est un anneau commutatif, la troisième identité remarquable généralisée y est valable.

Plus généralement, notons $b = aq + r$ la division euclidienne de b par a, avec donc $0 \leqslant r < a$.
Alors

$$X^b - 1 = X^{aq+r} - X^r + X^r - 1 = X^r(X^{aq} - 1) + X^r - 1 = X^r(X^a - 1)(1 + X^a + \cdots + X^{a(q-1)}) + X^r - 1.$$

Puisque $\deg(X^r - 1) < \deg(X^a - 1)$, on a donc la division euclidienne de $X^b - 1$ par $X^a - 1$, dont le reste est $X^r - 1$.
En particulier, $X^a - 1$ divise $X^b - 1$ si et seulement si ce reste est nul, donc si et seulement si $r = 0$, soit si et seulement si a divise b.

Alternative : la solution précédente a l'avantage de fonctionner dans n'importe quel corps (l'énoncé ne disait d'ailleurs pas grand chose à ce sujet).
Supposons qu'on travaille dans $\mathbf{C}[X]$
Alors les racines complexes de $X^a - 1$ sont les éléments de $\mathbf{U}_a$. Il y en a donc $a = \deg(X^a - 1)$, donc toutes ces racines sont simples.
Et par conséquent $X^a - 1$ divise $X^b - 1$ si et seulement si toute racine $a^{\text{ème}}$ de l'unité est une racine $b^{\text{ème}}$ de l'unité.

Remarque
L'exercice suivant justifie que nos deux polynômes étant à coefficients dans $\mathbf{Q}$, chercher à quelle condition ils se divisent dans $\mathbf{Q}[X]$, dans $\mathbf{R}[X]$ ou dans $\mathbf{C}[X]$ revient au même.

Solution de l'exercice 18.13

1. Soit $r = \dfrac{p}{q}$ une racine rationnelle de P, avec $p \wedge q = 1$.

   Notons alors $P = \displaystyle\sum_{i=0}^{n} a_i X^i$, avec $a_i \in \mathbf{Z}$ et $a_n = 1$.

   Alors $0 = P(r) = \displaystyle\sum_{i=0}^{n} a_i \frac{p^i}{q^i}$. Après multiplication par q^n, il vient donc $p^n + \displaystyle\sum_{i=0}^{n-1} a_i p^i q^{n-i} = 0$.

   Mais q divise $\displaystyle\sum_{i=0}^{n-1} a_i p^i q^{n-i}$, et donc divise p^n.

   Puisque p et q sont premiers entre eux, q et p^n sont premiers entre eux, donc $q = 1$.
   Et par conséquent, $r = p \in \mathbf{Z}$.

2. $\sqrt[k]{d}$ est racine de $X^k - d$, qui est bien un polynôme unitaire à coefficients entiers.
   Donc soit c'est un irrationnel, soit il est rationnel, auquel cas la question 1 prouve qu'il s'agit d'un entier.

Remarque
On retrouve notamment l'irrationnalité de tous les $\sqrt{k}$, où k n'est pas un carré parfait.

Solution de l'exercice 18.15

La fonction sin s'annule une infinité de fois[3] et ne saurait donc être polynomiale, puisqu'elle aurait une infinité de racines.
Même remarque pour $x \mapsto \lfloor x \rfloor$, qui est nulle sur tout $]0,1[$, qui contient bien une infinité de réels.
Enfin, le même raisonnement ne vaut plus pour l'exponentielle.
Mais s'il existait $P \in \mathbf{R}_n[X]$ tel que $\forall x \in \mathbf{R}$, $P(x) = e^x$, alors $P_n^{(n+1)} = 0 \Rightarrow \forall x \in \mathbf{R}$, $\exp^{(n+1)}(x) = 0 \Rightarrow \forall x \in \mathbf{R}$, $e^x = 0$, ce qui est absurde.

[3] En tous les $2k\pi$, $k \in \mathbf{Z}$.

Solution de l'exercice 18.16

Notons $f : x \mapsto x^3 + px + q$ la fonction polynomiale associée à $X^3 + pX + q$.
Alors elle est dérivable sur $\mathbf{R}$, de dérivée $f' : x \mapsto 3x^2 + p$.
▸ Si $p \geqslant 0$, alors pour tout $x \in \mathbf{R}$, $f'(x) \geqslant 0$, et f' s'annule au plus[4] une fois, si bien que f est strictement croissante.
Puisque $\displaystyle\lim_{x\to+\infty} f(x) = +\infty$ et $\displaystyle\lim_{x\to-\infty} f(x) = -\infty$, par le théorème des valeurs intermédiaires[5], f possède une unique racine α.

[4] Seulement en 0 si $p = 0$.

[5] f est continue.

▸ Si $p < 0$, alors f' s'annule deux fois, en $\pm\sqrt{\dfrac{-p}{3}}$.

Notons $\alpha = \sqrt{\dfrac{-p}{3}}$.

Alors $f(\alpha) = \left(\sqrt{\dfrac{-p}{3}}\right)^3 + p\sqrt{\dfrac{-p}{3}} + q = -\dfrac{p\sqrt{-p}}{3\sqrt{3}} + \dfrac{p\sqrt{-p}}{\sqrt{3}} + q$.

Et de même, $f(-\alpha) = \dfrac{p\sqrt{-p}}{3\sqrt{3}} - \dfrac{p\sqrt{-p}}{\sqrt{3}} + q$.

Le tableau de variations de f est donc donné par :

x	$-\infty$		$-\alpha$		α		$+\infty$
$f'(x)$		$+$	0	$-$	0	$+$	
$f(x)$	$-\infty$	$\nearrow$	$f(-\alpha)$	$\searrow$	$f(\alpha)$	$\nearrow$	$+\infty$

Par stricte monotonie de f sur chacun des intervalles $]-\infty, -\alpha]$, $]-\alpha, \alpha]$ et $]\alpha, +\infty[$, f ne peut posséder qu'au plus une racine sur chacun de ces intervalles.

Donc f possède trois racines réelles distinctes si et seulement si elle en possède exactement une sur chacun de ces intervalles.
Ce qui est le cas si et seulement si $f(-\alpha) > 0$ et $f(\alpha) < 0$.
Puisqu'on a toujours $f(-\alpha) > f(\alpha)$, ces deux nombres sont de signes opposés si et seulement si $f(-\alpha) > 0$ et $f(\alpha) < 0$. Donc f possède trois racines distinctes si et seulement si $f(\alpha)f(-\alpha) \leqslant 0$.

Détails
Le théorème des valeurs intermédiaires se cache ici : si $f(-\alpha) > 0$, alors il existe une racine dans $]-\infty, -\alpha]$.

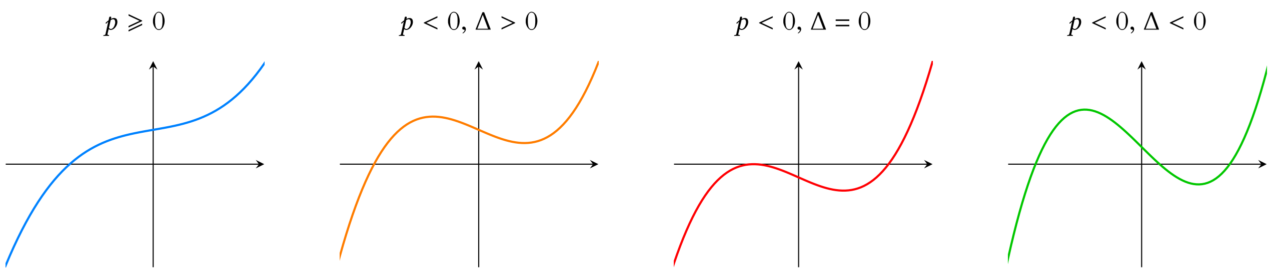
Mais

$$\begin{aligned} f(-\alpha)f(\alpha) &= \left[q + \left(\frac{p\sqrt{-p}}{\sqrt{3}} - \frac{p\sqrt{-p}}{3\sqrt{3}}\right)\right]\left[q - \left(\frac{p\sqrt{-p}}{\sqrt{3}} - \frac{p\sqrt{-p}}{3\sqrt{3}}\right)\right] \\ &= q^2 - \left(\frac{p\sqrt{-p}}{\sqrt{3}} - \frac{p\sqrt{-p}}{3\sqrt{3}}\right)^2 = q^2 - \left(-\frac{p^3}{3} + \frac{2}{9}p^3 - \frac{p^3}{27}\right) \\ &= \frac{27q^2 + 4p^3}{27}. \end{aligned}$$

Et donc on a bien $f(\alpha)f(-\alpha) < 0 \Leftrightarrow 27q^2 + 4p^3 < 0$.
Ainsi, f possède trois racines distinctes si et seulement si $4p^3 + 27q^2 < 0$.
Si $4p^3 + 27q^2 > 0$, alors $f(\alpha)$ et $f(-\alpha)$ sont tous deux de même signe, et non nuls. Donc f possède une unique racine, qui n'est pas une racine triple puisque 0 est la seule racine de f''.
Enfin, si $4p^3 + 27q^2 = 0$, alors $q = \pm\sqrt{\frac{-4p^3}{27}}$.
Dans ce cas, le produit $f(\alpha)f(-\alpha)$ est nul, et donc un[6] de ces deux nombres est nul.
Si $f(-\alpha) = 0$, puisque $f'(\alpha) = 0$, α est une racine de f de multiplicité au moins 2.
Et de plus, f possède, par le théorème des valeurs intermédiaires, une autre racine sur $]\alpha, +\infty[$. Donc f possède bien trois racines si on les compte avec multiplicités, et donc est scindé.
On prouve de même que si $f(\alpha) = 0$, alors c'est une racine double, et f possède une autre racine, donc est scindé.
Ainsi, si $4p^3 + 27q^2 = 0$, f est scindé.

[6] Et un seul par stricte décroissance de f sur $[-\alpha, \alpha]$.

Au final, on a bien prouvé que f est scindé si et seulement si $4p^3 + 27q^2 \leqslant 0$.



SOLUTION DE L'EXERCICE 18.17

1. Si $|z| = 1$, alors $|P(z)| \leqslant \sum_{k=0}^{n} |a_k|$.
Donc $\{|P(z)|, |z| = 1\}$ est une partie non vide et majorée de $\mathbf{R}$, elle admet donc un plus grand élément.

Mieux, on peut noter que $\{|P(z)|, z \in \mathbf{U}\} = \{|P(e^{i\theta})|, \theta \in \mathbf{R}\} = \{|P(e^{i\theta})|, \theta \in [0, 2\pi]\}$.
Or la fonction $\theta \mapsto P(e^{i\theta})$ est continue sur $[0, 2\pi]$ et donc il en est de même de $\theta \mapsto |P(e^{i\theta}|$, qui par le théorème des bornes atteintes possède donc un maximum (et donc a fortiori une borne sup) sur le segment $[0, 2\pi]$.

2. Rappelons que $1 + \zeta + \cdots + \zeta^n = 0$.
Et que le même calcul[7] prouve que pour $1 \leqslant k < n+1$, $1 + \zeta^k + \cdots + \zeta^{kn} = \frac{1 - \zeta^{k(n+1)}}{1 - \zeta^k} = 0$.
En revanche, ceci ne fonctionne plus pour $k = n+1$ ou $k = 0$, puisqu'il s'agit alors d'une

[7] Qui utilise la formule pour la somme des termes consécutifs d'une suite géométrique de raison $\neq 1$.

somme de termes tous égaux à 1, qui vaut donc $n+1$.
On en déduit que

$$P(1)+P(\zeta)+\cdots+P(\zeta^n)=\sum_{\ell=0}^{n}\sum_{k=0}^{n}a_k\zeta^{k\ell}=\sum_{k=0}^{n}a_k\sum_{\ell=0}^{n}\zeta^{k\ell}=a_0(n+1).$$

Et donc

$$|a_0|(n+1)=|P(1)+\cdots+P(\zeta^n)|\leqslant|P(1)|+\cdots+|P(\zeta^n)|\leqslant(n+1)M$$

et donc $|a_0|\leqslant M$.

3. On a

$$P(1)+\zeta^{-1}P(\zeta)+\zeta^{-2}P(\zeta^2)+\cdots+\zeta^{-n}P(\zeta^n)=\sum_{\ell=0}^{n}\zeta^{-\ell}\sum_{k=0}^{n}a_k\zeta^{k\ell}=\sum_{k=0}^{n}a_k\sum_{\ell=0}^{n}\zeta^{-\ell}\zeta^{k\ell}=\sum_{k=0}^{n}a_k\sum_{\ell=0}^{n}\zeta^{(k-1)\ell}.$$

Donc comme précédemment,

$$\sum_{\ell=0}^{n}\zeta^{(k-1)\ell}=\begin{cases}0 & \text{si } \zeta^{k-1}\neq 1\\ (n+1) & \text{sinon}\end{cases}.$$

Mais $-1\leqslant k-1<n$, donc $\zeta^{k-1}=1\Leftrightarrow k=1$.
Donc $\displaystyle\sum_{\ell=0}^{n}\zeta^{-\ell}P(\zeta^\ell)=(n+1)a_1$.
Et donc $(n+1)|a_1|\leqslant(n+1)M$, si bien que $|a_1|\leqslant M$.

Plus généralement, pour tout $k\in[\![0,n]\!]$,

$$\sum_{\ell=0}^{n}\zeta^{-k\ell}P(\zeta^{k\ell})=\sum_{i=0}^{n}a_i\sum_{\ell=0}^{n}\zeta^{(k-i)\ell}.$$

Or, $\displaystyle\sum_{\ell=0}^{n}\zeta^{(k-i)\ell}=\begin{cases}0 & \text{si } \zeta^{k-i}\neq 1\\ n+1 & \text{sinon}\end{cases}$ si bien que $\displaystyle\sum_{\ell=0}^{n}\zeta^{-k\ell}P(\zeta^{k\ell})=(n+1)a_k$.

Et donc toujours par l'inégalité triangulaire, $(n+1)|a_k|\leqslant\displaystyle\sum_{\ell=0}^{n}\left|\zeta^{-k}\right|\left|(\zeta^{k\ell})\right|\leqslant(n+1)M$.

Et donc $|a_k|\leqslant M$.

Solution de l'exercice 18.18

On a $P(j)=j^8+2j^6+3j^4+2j^2+1=j^2+2+3j+2j^2+1=3(j^2+j+1)=0$.
Donc j est racine de P.
Par ailleurs, $P'=8X^7+12X^5+12X^3+4X$, et donc

$$P'(j)=8j^7+12j^5+12j^3+4j=8j+12j^2+12+4j=12(j^2+j+1)=0.$$

Donc j est racine de multiplicité au moins 2 de P.
Notons que si j est racine double, alors $\overline{j}$ l'est aussi.
Donc on a déjà 4 racines comptées avec multiplicité parmi les 8 que compte P.
Mais puisque P est pair, $-j$ est aussi racine de P. Et même $-j$ est racine double, puisque si P est pair, alors P' est impair, et donc si x est racine de P', $-x$ l'est aussi.
Mais si $-j$ est racine double, alors $\overline{-j}=-\overline{j}=-j^2$ l'est aussi.
Donc nous avons bien un total de 8 racines lorsque comptées avec leurs multiplicités.
Donc $P=1(X-j)^2(X-\overline{j})^2(X+j)^2(X+\overline{j})^2$ est la décomposition en produit de facteurs irréductibles dans $\mathbf{C}[X]$.

> **Remarque**
> À ce stade, il se pourrait que j soit racine de multiplicité 3 ou plus.

Puisque $(X-j)(X-\overline{j})=X^2+X+1$ et $(X+j)(X+\overline{j})=X^2-X+1$, la décomposition de P en produit de facteurs irréductibles dans $\mathbf{R}[X]$ est donc $P=(X^2+X+1)^2(X^2-X+1)^2$.

Solution de l'exercice 18.19

On a $P(1)=1+a+b$, et $P'(1)=5+2a+b$.
Ces deux quantités seront nulles si et seulement si[8] $a=-4$ et $b=3$.
On a alors $P(X)=X(X-1)^2(X^2+2X+3)$, et il est facile de constater Xp^2+2X+3 est irréductible sur $\mathbf{R}[X]$ puisque de discriminant strictement négatif.

[8] Après résolution d'un système.

SOLUTION DE L'EXERCICE 18.20

1. Soit donc $P \in \mathbf{C}[X]$ tel que $A = BP$.
D'autre part, notons $A = BQ + R$ la division euclidienne de A par B dans $\mathbf{R}[X]$, c'est-à-dire avec $Q, R \in \mathbf{R}[X]$, et $\deg R < \deg B$.
Puisque ces polynômes sont également dans $\mathbf{C}[X]$, l'écriture $A = BQ + R$ est également une division euclidienne de A par B dans $\mathbf{C}[X]$.
Or, $A = BP + 0$ est aussi une division euclidienne de A par B dans $\mathbf{C}[X]$.
Par unicité de cette division, on a donc $Q = P \quad$ et $R = 0$.
Puisque $R = 0$, B divise A dans $\mathbf{R}[X]$.

> **Remarque**
> Notons qu'on a prouvé au passage que nécessairement, P est à coefficients réels.

2. Ce que nous enseigne la question précédente, c'est que la divisibilité dont il est question, a priori dans $\mathbf{R}[X]$, est aussi une divisibilité dans $\mathbf{C}[X]$.
Or, dans $\mathbf{C}[X]$, il est aisé de tester la divisibilité : elle se lit sur les racines.
Les racines complexes de $X^2 + X + 1$ sont j et $\overline{j} = j^2$.
Il s'agit donc de déterminer pour quelles valeurs de n j et j^2 sont des racines de $X^{2n} + X^n + 1$.
Étant conjugués, et $X^{2n} + X^n + 1$ étant à coefficients réels, l'un sera racine si et seulement si l'autre l'est.
On cherche donc les valeurs de n pour lesquelles $j^{2n} + j^n + 1 = 0$.
▸ Si $n \equiv 0 \ [3]$, alors $j^n = j^{2n} = 1$, donc $1 + j^n + j^{2n} = 3 \neq 0$.
▸ Si $n \equiv 1 \ [3]$, alors $j^n = j$, donc $j^{2n} = j^2$ et donc $1 + j + j^2 = 0$.
▸ Si $n \equiv 2 \ [3]$, alors $j^n = j^2$ et $j^{2n} = j^4 = j$, de sorte que $1 + j + j^2 = 0$.
Donc $X^2 + X + 1$ divise $X^{2n} + X^n + 1$ si et seulement si n n'est pas divisible par 3.

SOLUTION DE L'EXERCICE 18.21

Il est évident que les polynômes constants conviennent.
Si P est non constant et divisible par P', puisque $\deg P' = \deg P - 1$, il existe $(a, b) \in \mathbf{K}^2$ tels que $P = (aX + b)P'$.

Notons n le degré de P, de sorte que par identification des coefficients dominants[9], $a = \dfrac{1}{n}$.
Donc en posant $\lambda = -nb$, on a $nP = (X - \lambda)P'$.
En dérivant cette relation $nP' = (X - \lambda)P'' + P' \Leftrightarrow (n-1)P' = (X - \lambda)P''$.
Donc λ est racine de P', et puisqu'il est déjà racine de P, c'est une racine de P de multiplicité au moins égale à 2.
En dérivant de nouveau, $(n-2)P'' = (X - \lambda)P'$, et donc λ est racine de P''.

Puis de proche en proche, on arrive à $P^{(n-1)} = (X - \lambda)P^{(n)}$, et donc λ est racine de $P, P', P'', \dots, P^{(n-1)}$, et donc est racine de P de multiplicité au moins n.
Puisque $\deg P = n$, c'est donc la seule racine de P, qui est scindé. Et donc il existe $\alpha \in \mathbf{C}$ tel que $P = \alpha(X - \lambda)^n$.

> **Remarque**
> α n'est rien d'autre que le coefficient dominant de P.

Inversement, il est facile de prouver que pour tous $\alpha, \lambda \in \mathbf{C} \times \mathbf{C}^*$ et tout $n \in \mathbf{N}$, $P = \alpha\lambda(X - \lambda)^n$ est divisible par son polynôme dérivé.
Alternative : donnons une autre preuve, un peu moins calculatoire, mais spécifique à $\mathbf{C}[X]$, puisqu'elle utilise le fait que P est scindé.
Soit $P \in \mathbf{C}[X]$ non constant, tel que P' divise P.
Alors P est scindé, notons n le nombre de ses racines distinctes, notons $\lambda_1, \dots, \lambda_n$ ces racines et $m_1, \dots, m_n$ leur multiplicités.

On a alors $P = \alpha \displaystyle\prod_{i=1}^{n} (X - \lambda_i)^{m_i}$, avec $\alpha \in \mathbf{C}^*$.

On a donc $\displaystyle\sum_{i=1}^{n} m_i = \deg P$.

Puisque P' divise P, toutes les racines de P' sont racines de P. Autrement dit, les racines de P' sont parmi $\lambda_1, \dots, \lambda_n$.
Or nous savons que λ_i est racine de P', de multiplicité $m_i - 1$ (avec cette multiplicité éventuellement nulle si λ_i n'est pas racine de P').

Et donc $\displaystyle\sum_{i=1}^{n} (m_i - 1) = \deg P'$.

Soit encore $\displaystyle\sum_{i=1}^{n} m_i - n = \deg P - 1 \Leftrightarrow n = 1$.

Autrement dit, P possède une unique racine, et donc est de la forme $P = \alpha(X - \lambda)^k$.

> **Remarque**
> Le raisonnement que nous avons tenu ici n'est pas spécifique à $\mathbf{C}[X]$, et reste valable dans $\mathbf{R}[X]$ ou dans $\mathbf{Q}[X]$.
> Il faut tout de même rester dans un corps «suffisamment raisonnable» pour que $\deg P' = \deg P - 1$ (ce sont aussi les corps pour lesquels nous avons une caractérisation de la multiplicité d'une racine à l'aide des dérivées).

[9] Le coefficient dominant de P' est n fois celui de P : le n provenant de la dérivée de X^n.

Solution de l'exercice 18.22

Si $P \in \mathbf{C}[X]$ est non constant, alors, par le théorème de d'Alembert-Gauss, il réalise une bijection de $\mathbf{C}$ sur $\mathbf{C}$.
En effet, pour tout $y \in \mathbf{C}$, $P - y$ possède au moins une racine, donc y possède au moins un antécédent par P.
Et donc en particulier, on ne peut avoir $P(\mathbf{C}) \subset \mathbf{R}$ que si P est constant. Et alors, il faut nécessairement que la constante en question soit réelle.
Inversement, si P est un polynôme constant à coefficient réel, nécessairement, l'image de $\mathbf{C}$ est incluse dans $\mathbf{R}$ (elle est même réduite à un singleton de $\mathbf{R}$).
Donc les solutions sont les polynômes constants à coefficient(s) réel(s).

Solution de l'exercice 18.23

Notons $Q \in \mathbf{R}[X]$ et $R(X) = aX + b \in \mathbf{R}_1[X]$ le quotient et le reste de cette division euclidienne.
Alors, dans $\mathbf{C}[X]$, on a toujours $P = (X^2+1)Q + R$, donc Q et R sont également les quotient et reste de la division euclidienne dans $\mathbf{C}[X]$.
Donc en particulier, on peut évaluer cette relation en un complexe, prenons donc i et $-i$, les racines de $X^2 + 1$.

$$P(i) = Q(i)\underbrace{(i^2+1)}_{=0} + ai + b \Leftrightarrow \prod_{k=1}^{n} e^{ia_k} = ai + b \Leftrightarrow e^{i(a_1+\cdots+a_n)} = ai + b.$$

De même, l'évaluation en $-i$ nous conduit à $-ai + b = e^{-i(a_1+\cdots+a_n)}$.
Reste à déterminer a et b, c'est-à-dire à résoudre un système linéaire de deux équations à deux inconnues, qui nous donne

$$b = \frac{e^{i(a_1+\cdots+a_n)} + e^{-i(a_1+\cdots+a_n)}}{2} = \cos(a_1+\cdots+a_n) \text{ et } a = \sin(a_1+\cdots+a_n).$$

Donc le reste cherché est $\sin(a_1+\cdots+a_n)X + \cos(a_1+\cdots+a_n)$.

Solution de l'exercice 18.24

1. Si $z \in \mathbf{U}_n$ est différent de 1, alors $1 + z + z^2 + \cdots + z^{n-1} = \dfrac{z^n - 1}{z - 1} = 0$.
Donc les $n-1$ éléments de $\mathbf{U}_n \setminus \{1\}$ sont racines de P_n, qui est de degré $n-1$. Il n'y a donc pas d'autres racines, et P_n étant unitaire

$$P_n = \prod_{\substack{z\in \mathbf{U}_n\\ z\neq 1}} (X - z) = \prod_{k=1}^{n-1}\left(X - e^{i\frac{2k\pi}{n}}\right).$$

⚠ Attention !
Ne jamais oublier le coefficient dominant lors d'une factorisation par les racines ! Ici ça : il vaut 1.

2. Il s'agit de remarquer que

$$\begin{aligned}
P_n(1) &= \prod_{k=1}^{n-1}\left(1 - e^{i\frac{2k\pi}{n}}\right) = \prod_{k=1}^{n-1} e^{i\frac{k\pi}{n}}\left(-2i\sin\frac{k\pi}{n}\right)\\
&= (-2i)^{n-1} e^{i\frac{\pi}{n}(1+2+\cdots+n-1)} \prod_{k=1}^{n-1}\sin\frac{k\pi}{n}\\
&= (-2i)^{n-1} \underbrace{e^{i(n-1)\frac{\pi}{2}}}_{i^{n-1}} \prod_{k=1}^{n-1}\sin\frac{k\pi}{n}\\
&= 2^{n-1}\prod_{k=1}^{n-1}\sin\frac{k\pi}{n}.
\end{aligned}$$

Puisque d'autre part, $P_n(1) = 1 + 1 + \cdots + 1 = n$, on en déduit que $\displaystyle\prod_{k=1}^{n-1}\sin\frac{k\pi}{n} = \frac{n}{2^{n-1}}$.

3. Même principe en utilisant le polynôme $Q_n = X^n - e^{2in\theta}$.
On a alors $Q_n = \displaystyle\prod_{k=1}^{n}\left(X - e^{i\left(2\theta + \frac{2k\pi}{n}\right)}\right)$.

Et alors[10] $Q_n(1) = 1 - e^{i2n\theta} = -2i\sin(n\theta)e^{in\theta}$.
Et d'autre part,

$$\begin{aligned}
Q_n(1) &= \prod_{k=1}^{n}\left(1 - e^{i\left(2\theta + \frac{2k\pi}{n}\right)}\right)\\
&= \prod_{k=1}^{n} e^{i\frac{k\theta}{n}} \prod_{k=1}^{n}(-2i)\sin\left(\frac{k\pi}{n}+\theta\right)\\
&= (-2i)^n e^{i\frac{n(n+1)\theta}{2n}} \prod_{k=1}^{n}\sin\left(\frac{k\pi}{n}+\theta\right)\\
&= (-2i)^n i^{n+1} \prod_{k=1}^{n}\sin\left(\frac{k\pi}{n}+\theta\right).
\end{aligned}$$

[10] Toujours par factorisation par l'angle moitié.

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

4. Il s'agit donc de calculer

$$\begin{aligned}
P &= \prod_{k=0}^{n-1}\prod_{\substack{\ell=0\\k\neq\ell}}^{n-1}\left(\zeta^k - \zeta\ell\right)\\
&= \prod_{k=0}^{n-1}\zeta^k\left(1-\zeta^{\ell-k}\right)\\
&= \prod_{k=0}^{n-1}\left(\left(\prod_{\substack{\ell=1\\\ell\neq k}}^{n-1}\zeta^k\right)\left(\prod_{\substack{\ell=0\\\ell\neq k}}^{n-1}\left(1-\zeta^{\ell-k}\right)\right)\right)
\end{aligned}$$

Or, $\left\{\zeta^{\ell-k},\ 0\leqslant \ell\leqslant n-1, l\neq k\right\} = \mathbf{U}_n\setminus\{1\}$.

On en déduit que $\displaystyle\prod_{\substack{\ell=0\\\ell\neq k}}^{n-1}\left(1-\zeta^{\ell-k}\right) = P_n(1) = n$.

Donc $\displaystyle P = \prod_{k=0}^{n-1}\left(n\zeta^{k(n-1)}\right) = n^n\prod_{k=0}^{n-1}\zeta^{-k}$.

Soit encore $P = n^n\zeta^{-(0+1+\cdots+(n-1))} = n^n\zeta^{-\frac{n(n-1)}{2}} = n^n e^{-i(n-1)\pi} = (-1)^{n-1}n^n$.

Solution de l'exercice 18.25

Les racines de X^n-1 (resp. X^m-1) sont les racines $n^{\text{èmes}}$ (resp. $m^{\text{èmes}}$) de l'unité.
Mais m, n étant premiers entre eux, il existe deux entiers p et q tels que $np+mq=1$. Et alors si $z\in\mathbf{U}_n\cap\mathbf{U}_m$, alors $z = z^1 = z^{np+mq} = (z^n)^p\,(z^m)^q = 1$.
Autrement dit, $\mathbf{U}_n\cap\mathbf{U}_m = \{1\}$.
Ainsi, $(X^n-1)(X^m-1)$ possède $n+m-1$ racines simples (qui sont les éléments différents de 1 de $\mathbf{U}_m\cup\mathbf{U}_n$) et une racine double, qui est 1.
Mais 1 est racine $mn^{\text{ème}}$ de l'unité, donc racine de $X^{mn}-1$, et donc racine au moins[11] double de $(X^{mn}-1)\,(X-1)$.
De plus, si $z\in\mathbf{U}_m$, alors $z^{mn} = (z^m)^n = 1^n = 1$, donc $z\in\mathbf{U}_{mn}$.
Autrement dit, toutes les racines simples de $(X^n-1)(X^m-1)$ sont racines de $(X^{mn}-1)$.
Ainsi, ce dernier polynôme est divisible par

[11] Il n'est pas très dur de prouver que c'est une racine double, et donc de multiplicité exactement égale à 2, mais ce n'est pas vraiment nécessaire ici.

$$(X-1)^2\prod_{z\in\mathbf{U}_n\setminus\{1\}}(X-z)\prod_{z\in\mathbf{U}_m\setminus\{1\}}(X-z) = \prod_{z\in\mathbf{U}_n}(X-z)\prod_{z\in\mathbf{U}_m}(X-z) = (X^n-1)(X^m-1).$$

Ce résultat ne vaut plus si p et q ne sont plus premiers entre eux, par exemples pour $p=2$ et $q=4$, -1 est racine de X^2-1 et de X^4-1, donc est racine double de $(X^2-1)(X^4-1)$, alors qu'il n'est que racine simple de X^8-1.
Donc $(X^2-1)(X^4-1)$ ne divise pas $(X-1)(X^8-1)$.

Mieux
Prouver qu'en fait, dès que $p\wedge q\neq 1$, $(X^p-1)(X^q-1)$ ne divise pas $(X-1)(X^8-1)$.

Solution de l'exercice 18.26

Notons $P = \sum_{i=0}^{n} L_i - 1$. Alors pour tout $j \in [\![0, n]\!]$, on a

$$P(\lambda_j) = \sum_{i=0}^{n} L_i(\lambda_j) - 1 = L_j(\lambda_j) - 1 = 1 - 1 = 0.$$

Donc P possède $\lambda_0, \dots, \lambda_n$ comme racines : il possède $n+1$ racines distinctes.
Mais les L_i sont de degré exactement n, donc P est de degré au plus n.
Donc P possède strictement plus de racines que son degré : c'est le polynôme nul.

Et par conséquent, $\sum_{i=0}^{n} L_i = 1$.

Rappel

$$L_i(\lambda_j) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon} \end{cases}$$

⚠ Attention !

Ne pas dire que P est de degré exactement n : la somme de polynômes de même degré peut être de degré strictement inférieur, et c'est bien ce qui se produit ici.

Solution de l'exercice 18.27

Notons $L_0, L_1, \dots, L_n$ les polynômes d'interpolation de Lagrange associés aux $\frac{k}{n}, k \in [\![0, n]\!]$.

Alors tout polynôme $P \in \mathbf{R}_n[X]$ s'écrit $P = \sum_{k=0}^{n} P\left(\frac{k}{n}\right) L_k$.

Et donc par linéarité de l'intégrale,

$$\int_0^1 P(t)\,dt = \sum_{k=0}^{n} P\left(\frac{k}{n}\right) \int_0^1 L_k(t)\,dt.$$

En posant $\lambda_k = \int_0^1 L_k(t)\,dt$, on a alors le résultat souhaité.

Solution de l'exercice 18.28

Il est clair que les polynômes à coefficients réels satisfont $P(\mathbf{R}) \subset \mathbf{R}$.
Inversement, soit $P \in \mathbf{C}[X]$ un tel polynôme. Alors pour tout $x \in \mathbf{R}$, $P(x) = \overline{P(x)} = \overline{P}(\overline{x}) = \overline{P}(x)$.
Ainsi, les polynômes $\overline{P}$ et P coïncident en une infinité de nombres[12] : ils sont donc égaux.
Et donc P est à coefficients réels.

[12] Tous les réels.

Il est évident que les polynômes à coefficients rationnels conviennent.
Inversement, soit $P \in \mathbf{C}[X]$ tel que $P(\mathbf{Q}) \subset \mathbf{Q}$, de degré n.
Notons alors $L_0, L_1, \dots, L_n$ les polynômes d'interpolation de Lagrange associés aux entiers $0, 1, \dots, n$.

Alors $L_i = \prod_{\substack{k=0\\k\neq i}}^{n} \frac{X-k}{i-k} \in \mathbf{Q}[X]$.

Mais nous savons que $P = \sum_{i=0}^{n} \underbrace{P(i)}_{\in \mathbf{Q}} L_i \in \mathbf{Q}[X]$.

Et donc $P \in \mathbf{Q}[X]$.

Remarque

Prendre les polynômes d'interpolation associés à $n+1$ rationnels distincts aurait fonctionné tout aussi bien, il n'est pas nécessaire de prendre précisément ceux associés à $0, 1, \dots, n$.

Solution de l'exercice 18.29

Par l'exercice précédent, P est à coefficients rationnels.
Nous allons prouver que son degré ne peut pas être supérieur ou égal à 2 c'est-à-dire que P est de la forme $aX + b$.
Soit donc $P \in \mathbf{Q}[X]$ de degré $n \geqslant 2$. Quitte à multiplier P par le PPCM des dénominateurs de ses coefficients, on peut supposer que P est à coefficients dans $\mathbf{Z}$.

Remarque

Noter qu'une telle multiplication ne change pas la surjectivité : en effet, si tout rationnel r possède un antécédent par P, c'est en particulier le cas de $\frac{r}{n}$, de sorte que r possède un antécédent par nP.

Notons alors $P = \sum_{i=0}^{n} a_i X^i$, avec les a_i entiers.

Soit alors $r = \frac{p}{q}$ un rationnel, avec $p \in \mathbf{Z}$, $q \in \mathbf{N}^*$ et $p \wedge q = 1$.

Alors $P(r) = \sum_{i=0}^{n} a_i r^i = \sum_{i=0}^{n} a_i \frac{p^i}{q^i}$.

Et en particulier, $q^n P(r) = \sum_{i=0}^{n} a_i q^{n-i} p^i$.

Soit m un nombre premier, et supposons qu'il existe $r = \frac{p}{q}$ un antécédent de $\frac{1}{m}$.

Alors $q^n \dfrac{1}{m} = \displaystyle\sum_{i=0}^{n} a_i q^{n-i} p^i \Leftrightarrow q^n = m \sum_{i=0}^{n} a_i q^{n-i} p^i$.
Ainsi, m divise q^n, et m étant premier, il divise donc q.
Par conséquent, m^n divise q^n.
Si $n \geqslant 2$, alors m divise $\dfrac{q^n}{m} = \displaystyle\sum_{i=0}^{n} a_n q^{n-i} p^i$.
Donc m divise $\dfrac{q^n}{m}$ et divise[13] $\displaystyle\sum_{i=0}^{n-1} a_i p^i q^{n-i}$, donc il divise leur différence qui est $a_n p^n$.
Mais $p \wedge q = 1$, donc par le lemme de Gauss, m divise a_n.
Ainsi, si m est un nombre premier qui ne divise pas[14] a_n, alors $\frac{1}{m}$ n'a pas d'antécédent, et donc P n'est pas surjectif.

Inversement, il est évident qu'un polynôme de degré 1 à coefficients rationnels réalise une surjection de $\mathbf{Q}$ sur $\mathbf{Q}$.
Donc les polynômes $P \in \mathbf{C}[X]$ qui réalisent une surjection de $\mathbf{Q}$ sur $\mathbf{Q}$ sont les polynômes de degré 1 à coefficients rationnels.

[13] Il s'agit d'une somme d'entiers dont tous les termes sont divisibles par q, donc par m.

[14] Et il en existe puisque a_n n'a qu'un nombre fini de diviseurs premiers.

SOLUTION DE L'EXERCICE 18.30

Notons $P = \displaystyle\sum_{i=0}^{n} a_i X^i$. Alors pour tout $k \in [\![0, n-1]\!]$, $P^{(k)}$ est de degré $n-k$, son coefficient dominant est $a_n \dfrac{n!}{(n-k)!}$ et son coefficient de degré $n-k-1$ est $a_{n-1}\dfrac{(n-1)!}{(n-k-1)!}$.
Donc $s_k = -\dfrac{a_{n-1}(n-1)!}{(n-k-1)!}\dfrac{(n-k)!}{n!a_n} = -\dfrac{a_{n-1}}{a_n}\left(1-\dfrac{k}{n}\right)$.
On reconnaît là une suite arithmétique de raison $\dfrac{a_{n-1}}{na_n}$.

Détails
Calculer les dérivées successives de X^i si vous avez besoin d'être convaincu de la validité de ces formules.

SOLUTION DE L'EXERCICE 18.31

1. Notons $P = X^3 + aX^2 + bX + c$.
Nous savons, via les relations racines coefficients, que $a = -\sigma_1 = -x-y-z = -1$.
D'autre part, $b = \sigma_2 = xy + yz + xz$. Il s'agit donc de déterminer cette quantité. Mais nous savons que
$$(x+y+z)^2 = x^2+y^2+z^2+2(xy+yz+xz) \Leftrightarrow 1^2 = 21 + 2\sigma_2 \Leftrightarrow \sigma_2 = -10.$$
Donc $b = -10$.
Enfin, nous avons[15] $c = -\sigma_3 = -xyz$.
Mais $\dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z} = \dfrac{yz+xz+yz}{xyz} = \dfrac{\sigma_2}{\sigma_3}$.
Et donc $\sigma_3 = \sigma_2 = -10$.
Ainsi, $P = X^3 - X^2 - 10X + 10$.
2. Il est clair que 1 est racine de P, et donc $P = (X-1)(X^2-10) = (X-1)\left(X-\sqrt{10}\right)\left(X+\sqrt{10}\right)$.
Donc si on a une solution, $\{x,y,z\} = \left\{1, \sqrt{10}, -\sqrt{10}\right\}$.
Inversement, on vérifie que si $\{x,y,z\} = \left\{1, \sqrt{10}, -\sqrt{10}\right\}$, alors le système est bien satisfait, donc l'ensemble des solutions est
$$\left\{\left(1,\sqrt{10},-\sqrt{10}\right), \left(1,-\sqrt{10},\sqrt{10}\right), \left(\sqrt{10},-\sqrt{10},1\right),\right.$$
$$\left.\left(\sqrt{10},1,-\sqrt{10}\right), \left(-\sqrt{10},1,\sqrt{10}\right), \left(-\sqrt{10},\sqrt{10},1\right)\right\}.$$

[15] Toujours par les relations racines-coefficients.

Ensemble
Noter que nous donnons ici un ensemble, et pas un triplet : l'ordre des trois solutions n'est pas imposé, et de toutes façons, vu que les trois variables jouent un rôle symétrique dans le système, elles sont interchangeables : dès qu'on a une solution, on en a jusqu'à 6, en permutant les trois variables.

SOLUTION DE L'EXERCICE 18.32

1. On a $\frac{1}{2} = \cos\left(\frac{\pi}{3}\right) = \cos\left(3\frac{\pi}{9}\right)$.
Mais pour $x \in \mathbf{R}$,
$$\begin{aligned}\cos(3x) &= \cos(2x+x) = \cos(2x)\cos(x) + \sin(2x)\sin(x)\\ &= \left(2\cos^2 x - 1\right)\cos(x) + 2\cos(x)\sin^2(x)\end{aligned}$$

$$= 2\cos^3 x - \cos x + 2\cos^3 x - 2\cos(x) = 4\cos^3(x) - 4\cos(x).$$

Donc en particulier,

$$\frac{1}{2} = 4\alpha^3 - 3\alpha$$

si bien que α est racine de $8X^3 - 6\alpha X - 1$, qui est bien à coefficients entiers.

2. Supposons par l'absurde que $\alpha \in \mathbf{Q}$, avec $\alpha = \frac{p}{q}$, p et q deux entiers naturels[16] premiers entre eux.
Alors $8\frac{p^3}{q^3} - 6\frac{p}{q} - 1 = 0$, et donc $8p^3 - 6pq^2 - q^3 = 0$.
Donc p divise q^3. Or p et q sont premiers entre eux, donc p et q^3 sont premiers entre eux.
Ainsi $p = p \wedge q^3 = 1$.
On en déduit que q^2 divise $8p^3 = 8$, et donc $q^2 \in \{1, 2, 4, 8\}$.
Mais parmi ces nombres, seuls 1 et 4 sont des carrés, donc $\alpha = 1$ ou $\alpha = \frac{1}{2}$.
Or il est clair, par stricte décroissance de cos sur $\left[0, \frac{\pi}{2}\right]$ que $1 > \alpha > \cos\left(\frac{\pi}{3}\right) = \frac{1}{2}$.
Donc α n'est pas rationnel.

[16] Car α est clairement positif.

Solution de l'exercice 18.33

1. Soient P, Q deux polynômes de Σ, avec $P = A^2 + B^2$, $Q = C^2 + D^2$, où A, B, C, D sont des polynômes à coefficients réels.
Alors $P = (A + iB)(A - iB)$, et de même $Q = (C + iD)(C - iD)$.
Donc $PQ = [(A + iB)(C + iD)]\,\overline{[(A + iB)(C + iD)]} = (AC - BD)^2 + (AD + BC)^2 \in \Sigma$.

2. C'est assez clair...

3.a. Soit α une racine de P, soit m sa multiplicité, et soit $Q \in \mathbf{R}[X]$ tel que $P(X) = (X - \alpha)^m Q(X)$ et $Q(\alpha) \neq 0$.
Alors en considérant la limite quand x tend vers α par valeurs supérieures, on constate que

$$Q(\alpha) = \lim_{x \to \alpha^+} Q(x) = \lim_{x \to \alpha^+} \frac{P(x)}{(x - \alpha)^m} \geqslant 0.$$

Donc $Q(\alpha) > 0$. Puisque Q est continue, il existe $\eta > 0$ tel que pour $x \in]\alpha - \eta, \alpha + \eta[$, $Q(x) > 0$.
Et donc, pour $x \in]\alpha - \eta, \alpha + \eta[$, $P(x) = (x - a)^m Q(x)$ est du signe de $(x - a)^m$.
Si m est impair, alors $(x - a)^m$ change de signe en a, et donc P aussi.
Plus précisément, $P(x) < 0$ pour $x \in]\alpha - \eta, \alpha[$ et $P(x) > 0$ pour $x \in]\alpha, \alpha + \eta[$.
Mais ceci vient contredire notre hypothèse, donc m est pair.

Remarque
Sur cet intervalle, α est donc la seule racine de P.

3.b. Nous savons que P s'écrit $\alpha \prod_{i=1}^{n} (X - \alpha_i)^{2m_i} \prod_{j=1}^{q} Q_j(x)$, avec Q_j irréductible de degré 2.
Donc déjà, α est positif, donc somme de deux carrés
$(X - \alpha_i)^{2m_i}$ est un carré, et donc s'écrit $0^2 + ((X - \alpha_i)^{m_i})^2$.
Enfin, si $P = X^2 + bX + c$ est irréductible[17], de discriminant $\Delta < 0$, alors sa mise sous forme canonique est

$$\left(X - \frac{b}{2}\right)^2 - \frac{\Delta}{4} = \left(X - \frac{b}{2}\right)^2 + \left(\frac{\sqrt{-\Delta}}{2}\right)^2.$$

Donc un tel polynôme est somme de carrés.
Donc tous les facteurs de la décomposition de P sont dans Σ, par la question 1, P l'est aussi.

[17] Et unitaire.