TD 17 : Polynômes

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

► L'anneau $\mathbf{K}[X]$

Exercice 17.1 Déterminer le groupe des unités de l'anneau $\mathbf{K}[X]$. PD

Exercice 17.2 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 17.3 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 17.4 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 $\displaystyle\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}$.

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

Exercice 17.5 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 17.6 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 17.7 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 17.8 Soit $P \in \mathbf{K}[X]$. Montrer que $P(X) - X$ divise $P(P(X)) - P(X)$. PD

Exercice 17.9 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 17.10 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 17.11 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 17.12 Montrer que les fonctions $x \mapsto \sin x$, $x \mapsto e^x$ et $x \mapsto \lfloor x \rfloor$ ne sont pas polynomiales. PD

Exercice 17.13 AD

1. Montrer que pour tout $n \in \mathbf{N}$, il existe un unique polynôme $P_n \in \mathbf{R}[X]$ tel que $P_n - P_n' = \dfrac{X^n}{n!}$.
2. Montrer que les racines complexes de P_n sont toutes simples.
3. Déterminer le nombre de racines réelles de P_n.

Exercice 17.14 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 17.15 **(Banque CCP 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 17.16 Soient $a, b \in \mathbf{N}^*$. Montrer que $X^a - 1$ divise $X^b - 1$ si et seulement si $a \mid b$. AD

Exercice 17.17 **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 17.18 Déterminer tous les polynômes $P \in \mathbf{C}[X]$ tels que P' divise P. AD

Exercice 17.19 **(Oral ENS)** D
Quels sont les polynômes $P \in \mathbf{C}[X]$ tels que $P(\mathbf{C}) \subset \mathbf{R}$?

Exercice 17.20 **(Oral Polytechnique)** AD

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

Exercice 17.21 **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 $P \in \Sigma$.

▸ Polynômes d'interpolation de Lagrange

Exercice 17.22 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 $\sum_{k=0}^{n} L_k = 1$. PD

Exercice 17.23 Soit $n \in \mathbf{N}$. Montrer qu'il existe $(\lambda_0, \ldots, \lambda_n) \in \mathbf{R}^{n+1}$ tels que $\forall P \in \mathbf{R}_n[X]$, $\int_0^1 P(t)\,dt = \sum_{k=0}^{n} \lambda_k P\left(\frac{k}{n}\right)$. AD

Exercice 17.24 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 ?

Exercice 17.25 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 17.26 **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 17.27 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 17.28 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 $\prod_{k=1}^{n-1} \sin \frac{k\pi}{n}$.
3. Pour $\theta \in \mathbf{R}$, donner alors une expression de $\prod_{k=1}^{n} \sin\left(\frac{k\pi}{n} + \theta\right)$.
4. Soit $\zeta = e^{\frac{2i\pi}{n}}$. Calculer $\prod_{\substack{0 \leqslant k, \ell \leqslant n-1 \\ k \neq \ell}} \left(\zeta^k - \zeta^\ell\right)$.

Correction des exercices du TD 17

Solution de l'exercice 17.1

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 17.3

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, $a = 1$, $b = 0$ 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 $\deg(P \circ P) = \deg P^2$, donc $\deg(P \circ P) = \deg P \Rightarrow \deg P = 1$.
Ainsi, il existe $(a, b) \in \mathbf{C}^* \times \mathbf{C}$ tels que $P(X) = aX + b$.
Mais alors $P \circ P = a(aX+b) + b = a^2X + ab + b$.
Donc $a^2 = 1 \Leftrightarrow a = \pm 1$. Si $a = 1$, alors $ab + b = b \Leftrightarrow b = 0$.
Si $a = -1$, alors $ab + b = 0$ que que soit $b \in \mathbf{C}$.
Donc les solutions sont X et les $b - X$, $b \in \mathbf{C}$.
3. Si P est une solution non constante, alors $\deg{(P')^2} = 2\deg P'$.

Solution de l'exercice 17.4

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 17.5

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 $(X-1)^3$.
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 $3 \times 2^n(X+1)$.

> **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.

Solution de l'exercice 17.6

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[1] 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.

[1] $2 \in \mathbf{R}^*$ est un inversible de $\mathbf{R}[X]$.

Solution de l'exercice 17.7

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 $P(X^n) = (X^n - 1)Q(X^n)$ est divisible par $X^n - 1$.

Solution de l'exercice 17.8

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

Solution de l'exercice 17.9

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 17.10

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 17.11

1. Soit $r = \frac{p}{q}$ une racine rationnelle de P, avec $p \wedge q = 1$.
   Notons alors $P = \sum_{i=0}^n a_i X^i$, avec $a_i \in \mathbf{Z}$ et $a_n = 1$.
   Alors $0 = P(r) = \sum_{i=0}^n a_i \frac{p^i}{q^i}$. Après multiplication par q^n, il vient donc $p^n + \sum_{i=0}^{n-1} a_i p^i q^{n-i} = 0$.

Mais q divise $\sum_{i=0}^{n-1} a_i p^i q^{n-i}$, 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 17.12

La fonction sin s'annule une infinité de fois[2] 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.

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

SOLUTION DE L'EXERCICE 17.14

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

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

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

SOLUTION DE L'EXERCICE 17.15

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

[3] Après résolution d'un système.

SOLUTION DE L'EXERCICE 17.16

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.
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.

SOLUTION DE L'EXERCICE 17.17

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 $Q = P$ 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 divisibles par 3.

Solution de l'exercice 17.18

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[4], $a = \dfrac{1}{n}$.
Donc quitte à changer b, on a $nP = (X + b)P'$.
En dérivant cette relation $nP' = (X + b)P' + P'' \Leftrightarrow (n - 1)P' = (X + b)P''$.
Puis de proche en proche, on arrive à $P^{(n-1)} = (X + b)P^{(n)}$.
Or, $P^{(n)}$ est une constante : c'est le coefficient dominant de P multiplié par $n!$. Notons le $\lambda \times n!$.
Donc en remontant, $P^{(n-1)} = (X + b)\lambda n!$.
Puis $2P^{(n-2)} = (X + b)P^{(n-1)} = (X + b)^2 \lambda n!$...
De proche en proche, on en déduit que $P = \lambda(X + b)^n$.
Inversement, il est facile de prouver que pour tout $\lambda \in \mathbf{C}^*$, tout $b \in \mathbf{C}$ et tout $n \in \mathbf{N}$, $P = \lambda(X + b)^n$ est divisible par son polynôme dérivé.

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

Solution de l'exercice 17.19

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 17.20

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 17.21

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 $\alpha \prod_{i=1}^{n} (X - \alpha_i)^{2m_i} \prod_{j=1}^{q} Qj(x)$, 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[5], alors sa mise sous forme canonique est

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

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.

[5] Et unitaire.

SOLUTION DE L'EXERCICE 17.22

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

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

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

Donc P possède $\lambda_0, \ldots, \lambda_n$ 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.

> **⚠ 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.

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

SOLUTION DE L'EXERCICE 17.23

Notons $L_0, L_1, \ldots, L_n$ 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 17.24

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[6] double de $X^{mn} - 1$.
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

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

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 $(X - 1)(X^8 - 1)$.

[6] 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.

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 17.25

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[7] : ils sont donc égaux.
Et donc P est à coefficients réels.

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

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

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 17.26

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 $\mathbf{Z}$.

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

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

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

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

Si $r = \dfrac{p}{q}$ est un antécédent de $\dfrac{1}{m}$, où m est nombre premier.

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.

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.

Si $n \geqslant 2$, alors m divise $\dfrac{q^n}{m} = \sum_{i=0}^{n} a_n q^{n-i} p^i$.

Donc m divise $\dfrac{q^n}{m}$ et divise $\displaystyle\sum_{i=0}^{n-1} a_i p^i q^{n-i}$, 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.
Mais a_n ne possède qu'un nombre fini de diviseurs premiers, donc si m est un premier qui ne divise pas a_n, $\dfrac{1}{m}$ n'a pas d'antécédent par P.
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.

SOLUTION DE L'EXERCICE 17.27

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 $\dfrac{a_{n-1}}{n a_n}$.

> **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 17.28

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 trouve alors, après calcul, $\displaystyle\prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n} + \theta\right) = \frac{\sin n\theta}{2^{n-1}}$.