TD 34 : Arithmétique des polynômes, fractions rationnelles

▶ Arithmétique des polynômes

Exercice 34.1 F
Dans les deux cas suivants, calculer $A \wedge B$ et déterminer des polynômes U et V tels que $AU + BV = A \wedge B$.

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

Exercice 34.2 PD
Montrer que deux polynômes P et Q de $\mathbf{K}[X]$ sont premiers entre eux si et seulement si PQ et $P+Q$ le sont.

Exercice 34.3 PD
Soient P, R deux polynômes à coefficients dans $\mathbf{Z}$, premiers entre eux.
Pour tout $n \in \mathbf{N}$, on pose $u_n = P(n) \wedge R(n)$. Montrer que (u_n) est bornée.

Exercice 34.4 PD
Soit $P \in \mathbf{K}[X]$ un polynôme scindé. Déterminer $P \wedge P'$ en fonction des racines de P et de leurs multiplicités.
En déduire un algorithme permettant de déterminer le nombre de racines complexes distinctes d'un polynôme $P \in \mathbf{R}[X]$.

Exercice 34.5 AD

1. Soient A et B deux polynômes non constants de $\mathbf{K}[X]$, premiers entre eux. Montrer qu'il existe un unique couple $(U, V) \in \mathbf{K}[X]^2$ tel que $AU + BV = 1$ avec $\deg U < \deg B$ et $\deg V < \deg A$.
2. Soient $A, B \in \mathbf{K}[X]$ non constants, avec $p = \deg A$ et $q = \deg B$.
   Donner une condition nécessaire et suffisante pour que $\Phi : \left| \begin{array}{ccc} \mathbf{K}_{q-1}[X] \times \mathbf{K}_{p-1}[X] & \longrightarrow & \mathbf{K}_{p+q-1}[X] \\ (U, V) & \longmapsto & AU + BV \end{array} \right.$ soit une bijection.

Exercice 34.6 PD
Soient P et Q deux polynômes à coefficients réels.

1. Montrer, à l'aide de la factorisation en produit d'irréductibles, que P et Q sont premiers entre eux en tant qu'éléments de $\mathbf{R}[X]$ si et seulement si ils le sont en tant qu'éléments de $\mathbf{C}[X]$.
2. En déduire que le PGCD de P et Q dans $\mathbf{R}[X]$ est égal au PGCD de P et Q dans $\mathbf{C}[X]$.
3. Retrouver ce résultat en utilisant l'algorithme d'Euclide.

Exercice 34.7 PD
Soient $A, B \in \mathbf{K}[X]$ tels que $A^2 \mid B^2$. Prouver que $A \mid B$.

Exercice 34.8 Arithmétique et idéaux AD
Un partie I de $\mathbf{K}[X]$ est appelée un idéal de $\mathbf{K}[X]$ si c'est un sous-groupe de $(\mathbf{K}[X], +)$, et si pour tout $P \in I$, pour tout $Q \in \mathbf{K}[X]$, $PQ \in I$.

1. Montrer que pour tout $P \in \mathbf{K}[X]$, $(P) = \{PQ, Q \in \mathbf{K}[X]\}$ est un idéal de $\mathbf{K}[X]$. *(P) est appelé l'idéal engendré par P.*
2. En utilisant la division euclidienne prouver que pour tout idéal I de $\mathbf{K}[X]$, il existe un unique polynôme unitaire P tel que $I = (P)$.
   On dit alors que $\mathbf{K}[X]$ est un anneau principal, ce qui est également le cas de $\mathbf{Z}$.
3. Soient $A, B \in \mathbf{K}[X]$. Montrer que $(A) + (B) = \{P + Q,\ P \in (A), Q \in (B)\}$ et $(A) \cap (B)$ sont deux idéaux de $\mathbf{K}[X]$. Reconnaissez-vous les polynômes unitaires qui engendrent ces idéaux ?

Exercice 34.9 Polynômes de Fibonacci AD
Soit $(P_n)_{n \in \mathbf{N}}$ la suite de polynômes définis par $P_0 = 0$, $P_1 = 1$ et pour tout $n \in \mathbf{N}$, $P_{n+2}(X) = XP_{n+1}(X) - P_n(X)$.

1. Quel est le degré de P_n ?
2. Prouver que pour tout $n \geqslant 2$, $P_n^2 - P_{n+1}P_{n-1} = 1$.
3. En déduire que pour tout $n \geqslant 2$, P_{n-1} et P_n sont premiers entre eux.
4. Montrer que pour tout $n \geqslant 2$ et tout $p \in \mathbf{N}^*$, $P_{n+p} = P_nP_{p+1} - P_{n-1}P_p$, puis en déduire que $P_{n+p} \wedge P_p = P_n \wedge P_p$.
5. Conclure alors que $P_n \wedge P_p = P_{n \wedge p}$.

Exercice 34.10 AD
Montrer que pour $n, p \in \mathbf{N}^*$, on a $(X^n - 1) \wedge (X^p - 1) = X^{n \wedge p} - 1$.

Exercice 34.11 AD

1. Soient $P, Q \in \mathbf{Q}[X]$ irréductibles, unitaires et distincts. Montrer que P et Q n'ont pas de racine complexe commune.

2. Soit P un polynôme irréductible de $\mathbf{Q}[X]$. Montrer que P n'a pas de racine complexe de multiplicité supérieure ou égale à 2.

Exercice 34.12 **$\mathbf{Q}[X]$ contient des irréductibles de tout degré** D
Montrer que pour tout $n \in \mathbf{N}^*$, $P_n = X^n - 2$ est irréductible dans $\mathbf{Q}[X]$.

Exercice 34.13 **(Oral X)** D
Soient P et Q deux polynômes non constants de $\mathbf{C}[X]$ qui ont mêmes racines, et tels que $P-1$ et $Q-1$ aient aussi les mêmes racines.

1. Prouver que $\deg(P \wedge P') + \deg((P-1) \wedge P') \leqslant \deg P - 1$.
2. En déduire alors que $P = Q$.

► Fractions rationnelles

Exercice 34.14 Un scalaire peut-il être à la fois un zéro et un pôle d'une fraction rationnelle ? F

Exercice 34.15 **Un air de déjà vu...** PD
En utilisant la décomposition en éléments simples de $\frac{P'}{P}$, déterminer tous les polynômes P de $\mathbf{C}[X]$ tels que $P' \mid P$.

Exercice 34.16 **Image d'une fraction rationnelle complexe** AD
Soit $F \in \mathbf{C}(X)$ non constante, et soit A l'ensemble des pôles de F.
Déterminer l'image $\mathbf{C} \setminus A$ par $\widetilde{F}$, la fonction rationnelle associée à F.

Exercice 34.17 Montrer que $\displaystyle\sum_{\omega \in \mathbf{U}_7} \frac{1}{2-\omega} = \frac{448}{127}$. PD

Exercice 34.18 Soit $n \geqslant 2$. Donner la forme irréductible de la fraction $\displaystyle\sum_{\omega \in \mathbf{U}_n} \frac{\omega^2}{X-\omega}$. AD

Exercice 34.19 **Polynômes de Tchebychev** AD

1. Soit $n \in \mathbf{N}^*$. Montrer qu'il existe un unique $P_n \in \mathbf{R}[X]$ tel que pour tout $x \in \mathbf{R}$, $P_n(\cos(x)) = \cos(nx)$.
2. Déterminer les racines de P_n.
3. Quelle est la décomposition en éléments simples de $\frac{1}{P_n}$?

Exercice 34.20 Soit $P = \displaystyle\sum_{k=0}^{n} a_k X^k$ un polynôme de $\mathbf{R}[X]$, scindé sur $\mathbf{R}$. AD

1. Justifier que pour tout $x \in \mathbf{R}$, $P'(x)^2 - P(x)P''(x) \geqslant 0$.
2. En déduire que $\forall k \in [\![1, n-1]\!]$, $a_{k-1}a_{k+1} \leqslant a_k^2$.

Exercice 34.21 **Zéros des polynômes trigonométriques** AD
Soit $n \in \mathbf{N}^*$ et soient $a_0, a_1, \ldots, a_n, b_0, \ldots, b_n$ des réel et soit $f : x \mapsto \displaystyle\sum_{k=0}^{n} (a_k \cos(kx) + b_k \sin(kx))$.
En utilisant une formule d'Euler, montrer que soit f est la fonction nulle, soit f s'annule au plus $2n$ fois dans $[0, 2\pi[$.

Exercice 34.22 **Le logarithme n'est pas une fonction rationnelle** D
Soit $F = \frac{P}{Q} \in \mathbf{C}(X)$, irréductible et telle que $F' = \frac{P'Q - PQ'}{Q^2} = \frac{1}{X}$.

1. Justifier que $X \mid Q$.
2. Soit $n \geqslant 1$ tel que $X^n \mid Q$. Prouver que $X^n \mid Q'$.
3. Qu'en déduit-on ?

Exercice 34.23 **Théorème de Mason et grand théorème de Fermat pour les polynômes (Oral ENS)** TD

1. Soient A, B, C trois polynômes de $\mathbf{C}[X]$, non constants, premiers entre eux dans leur ensemble, et tels que $A+B=C$.
   On note m le nombre de racines **distinctes** de ABC. Montrer que $A\left(\frac{A'}{A} - \frac{C'}{C}\right) = B\left(\frac{C'}{C} - \frac{B'}{B}\right)$.
   En déduire que $\max(\deg A, \deg B, \deg C) < m$.
2. Soit $n \geqslant 3$. Montrer que s'il existe trois polynômes P, Q, R de $\mathbf{C}[X]$ tels que $P^n + Q^n = R^n$, alors P, Q et R sont associés.

CORRECTION DES EXERCICES DU TD 34

SOLUTION DE L'EXERCICE 34.1

1. Il s'agit de faire des divisions euclidiennes successives :

$$A = (X+1)B + \underbrace{(-2X^3 - 10X^2 - 16X - 8)}_{=R_1},\quad B = \frac{1}{2}(-X+3)R_1 + \underbrace{9X^2 + 27X + 18}_{=R_2},\quad R_1 = R_2\left(-\frac{2}{9}X - \frac{4}{9}\right) + 0.$$

Donc les PGCD de A et B sont les associés à R_2, et donc $A \wedge B$, qui doit être unitaire est $\frac{R_2}{9} = X^2 + 3X + 2$.
Et alors en remontant les calculs,

$$X^2+3X+2 = \frac{1}{9}B + \frac{1}{18}(X-3)R_1 = \frac{1}{9}B + \frac{1}{18}(X-3)\left(A - (X+1)B\right) = \left(\frac{1}{18}X - \frac{1}{6}\right)A + \left(-\frac{1}{18}X^2 + \frac{1}{-}X + \frac{5}{18}\right)B.$$

2. Sur le même principe, on trouve $A \wedge B = 1$ et

$$1 = A(-X^3) + B(X^5 + X^3 + X + 1).$$

SOLUTION DE L'EXERCICE 34.2

Si PQ et $P+Q$ sont premiers entre eux, alors par le théorème de Bézout, il existe $U, V \in \mathbf{K}[X]$ tels que $PQU+(P+Q)V = 1$, et alors $P(QU+V)+QV = 1$, donc P et Q sont premiers entre eux.

Inversement, si P et Q sont premiers entre eux, soit $D = (PQ) \wedge (P+Q)$, et soit R un diviseur irréductible de D. Alors R divise PQ, donc[1] divise P ou divise Q.
Mais puisqu'il divise $P+Q$, s'il divise P, alors il divise Q et inversement.
Donc il divise P et Q et donc divise $P \wedge Q = 1$.

[1] C'est là qu'on utiliser le fait que P et Q sont premiers entre eux.

SOLUTION DE L'EXERCICE 34.3

Plaçons-nous dans l'anneau $\mathbf{Q}[X]$.
Par le théorème de Bézout, il existe deux polynômes U, V à coefficients dans $\mathbf{Q}$ tels que $PU + RV = 1$.
Notons alors m le PGCD[2] des dénominateurs des coefficients de U et V, de sorte que mU et mV sont à coefficients dans $\mathbf{Z}$.
On a alors $PmU + RmV = m$. Et donc pour tout $n \in \mathbf{N}$, $P(n)mU(n) + R(n)mV(n) = m$, de sorte que $u_n = P(n) \wedge R(n)$ divise m.
Mais m ne possède qu'un nombre fini de diviseurs, et donc (u_n) ne peut prendre qu'un nombre fini de valeurs.

[2] Mais on aurait tout aussi bien pu prendre le produit.

SOLUTION DE L'EXERCICE 34.4

Notons $\alpha_1, \dots, \alpha_n \in \mathbf{K}$ les racines distinctes de P, de multiplicité respectives $m_1, \dots, m_n$, de sorte que $P = \lambda \prod_{i=1}^{n} (X - \alpha_i)^{m_i}$.
Nous savons qu'il s'agit là de la décomposition de P en produit de facteurs irréductibles.
Et puisque tout facteur irréductible de $P \wedge P'$ est facteur irréductible de P, les seuls facteurs irréductibles de $P \wedge P'$ sont parmi les $X - \alpha_i$.
Nous savons déjà que si $m_i \geqslant 2$, alors α_i est racine de P' de multiplicité $m_i - 1$. Donc $(X - \alpha_i)^{m_i - 1}$ divise P', et divise évidemment P.
Inversement, si $(X - \alpha_i)^k$ divise $P \wedge P'$, avec $k \geqslant 1$, alors α_i est racine de P, et est racine de P' de multiplicité supérieur ou égale à k. Donc est racine de P de multiplicité supérieure ou égale à $k+1$.
Et donc $k+1 \leqslant m_i \Leftrightarrow k \leqslant m_i - 1$. Notons qu'en particulier, $m_i \geqslant 2$.
On en déduit donc que $P \wedge P' = \prod_{i=1 \mid m_i \geqslant 2}^{n} (X - \alpha_i)^{m_i - 1}$.

En particulier, si $P \in \mathbf{R}[X]$, alors il est possible de voir P comme un polynôme scindé de $\mathbf{C}[X]$.

Et alors il est possible de calculer $P' \wedge P$ par l'algorithme d'Euclide[3].
Avec les notations précédentes, on a donc

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

Et donc $n = \deg P - \deg(P' \wedge P)$ est le nombre de racines complexes distinctes de P.

[3] Tout en restant dans $\mathbf{R}[X]$, puisque le PGCD est le même dans $\mathbf{R}[X]$ ou dans $\mathbf{C}[X]$.

Solution de l'exercice 34.5

1. Commençons par l'existence d'un tel couple. Partons pour cela d'une relation de Bézout : $AU + BV = 1$.
Soit alors $U = BQ + U_1$ la division euclidienne de U par B, et soit $V_1 = V + AQ$, de sorte que

$$AU_1 + BV_1 = A(U - BQ) + BV + ABQ = AU + BV = 1.$$

Puisqu'on n'a pas $\deg(AU_1 + BV_1) = \max(\deg AU_1, \deg BV_1)$, c'est donc que ces deux polynômes sont de même degré. .
Donc $\deg(V_1) = \deg(AU_1) - \deg(B) = \deg(A) + \underbrace{\deg(U_1) - \deg(B)}_{<0} < \deg(A)$.

> **Rappel**
> Si $\deg P \neq \deg Q$, alors
> $\deg(P+Q) = \max(\deg(P), \deg(Q))$.

Pour l'unicité, supposons que deux tels couples (U_1, V_1) et (U_2, V_2) existent. Alors

$$AU_1 + BV_1 = 1 = AU_2 + BV_2 \Rightarrow A(U_1 - U_2) = B(V_2 - V_1).$$

Donc A divise $B(V_2 - V_1)$, et étant premier avec B, $A \mid V_2 - V_1$.
Mais $\deg(V_2 - V_1) < \deg A$, donc $V_2 - V_1 = 0 \Leftrightarrow V_1 = V_2$.
Et par conséquent, $U_1 - U_2 = 0$, donc $U_1 = U_2$.

2. Commençons par noter que Φ est linéaire : pour (U_1, V_1), (U_2, V_2) dans $\mathbf{K}_{q-1}[X] \times \mathbf{K}_{p-1}[X]$, et pour $\lambda \in \mathbf{K}$, on a

$$\begin{aligned}\Phi(\lambda(U_1, V_1) + (U_2, V_2)) &= \Phi((\lambda U_1 + U_2, \lambda V_1 + V_2)) \\ &= A(\lambda U_1 + U_2) + B(\lambda V_1 + V_2) \\ &= \lambda(AU_1 + BV_1) + (AU_2 + BV_2) \\ &= \lambda\Phi(U_1, V_1) + \Phi(U_2, V_2).\end{aligned}$$

Par ailleurs, $\dim \mathbf{K}_{q-1}[X] \times \mathbf{K}_{p-1}[X] = \dim \mathbf{K}_{q-1}[X] + \dim \mathbf{K}_{p-1}[X] = q+p = \dim \mathbf{K}_{p+q-1}[X]$.
Donc Φ est bijective si et seulement si elle est injective.

Si c'est une bijection, alors en particulier, 1 possède un (unique) antécédent (U, V), et donc par Bézout, A et B sont premiers entre eux.
Inversement, si A et B sont premiers entre eux, alors la question précédente prouve que 1 possède un unique antécédent (U_0, V_0) par Φ.
Mais alors , pour $(U, V) \in \mathbf{K}_{q-1}[X] \times \mathbf{K}_{p-1}[X]$, (U, V) est un antécédent de Φ si et seulement si

$$\Phi(U, V) = 1 = \Phi(U_0, V_0) \Leftrightarrow \Phi((U_0 - U, V_0 - V)) = 0 \Leftrightarrow (U_0 - U, V_0 - V) \in \operatorname{Ker}\Phi.$$

> **Plus généralement**
> Pour une application linéaire, soit tous les éléments de l'image ont un unique antécédent (et alors on a l'injectivité), soit tous ont une infinité d'antécédents.

Donc l'unicité de l'antécédent de 1 fournie par la première question garantit que $\operatorname{Ker}\Phi = \{0\}$.

Et donc Φ est une bijection.
Alternative, ne nécessitant pas la question 1 : supposons P et Q premiers entre eux, et soit $(U, V) \in \operatorname{Ker}\Phi$.
Alors $AU + BV = 0 \Leftrightarrow AU = -BV$. Mais alors, par Gauss, $A \mid V$, et en utilisant de plus les conditions de degré, il vient $V = 0$, puis $A = 0$.
Donc $\operatorname{Ker}\Phi = \{(0, 0)\}$, si bien que Φ est injective, donc bijective.

Solution de l'exercice 34.6

1. Soient P, Q deux polynômes premiers entre eux dans $\mathbf{C}[X]$. Alors ils n'ont aucun diviseur commun non constant à coefficients complexe.
Donc a fortiori, n'ont aucun diviseur commun non constant à coefficients réels, et donc sont premiers entre eux dans $\mathbf{R}[X]$.

Inversement, supposons que P et Q soient premiers entre eux dans $\mathbf{R}[X]$, et raisonnons par l'absurde en supposant que leur PGCD, en tant que polynômes à coefficients complexes ne soit pas égal à 1.
Alors il existe un facteur $D \in \mathbf{C}[X]$, irréductible (dans $\mathbf{C}[X]$) commun à P et Q.
Mais les irréductibles de $\mathbf{C}[X]$ sont les $X-\lambda$, $\lambda \in \mathbf{C}$. Soit donc $\lambda \in \mathbf{C}$ tel que $X-\lambda \mid P$ et $X-\lambda \mid Q$, c'est-à-dire tel que λ soit à la fois racine de P et de Q.
Un tel λ ne peut pas être réel, faute de quoi P et Q seraient tous les deux divisibles (dans $\mathbf{R}[X]$) par $X-\lambda$, et donc non premiers entre eux dans $\mathbf{R}[X]$.
Donc $\lambda \in \mathbf{C} \setminus \mathbf{R}$, de sorte que $\overline{\lambda}$ est également une racine de P, et de Q.
Donc $X-\lambda \mid P$ et $X-\overline{\lambda} \mid P$. Mais ces deux polynômes sont premiers entre eux, car irréductibles[4] et non associés. Donc $(X-\lambda)(X-\overline{\lambda}) \mid P$.
Et de même $(X-\lambda)(X-\overline{\lambda}) \mid Q$.
Donc P et Q sont tous deux divisibles par $(X-\lambda)(X-\overline{\lambda}) = X^2 - 2\operatorname{Re}(\lambda) + |\lambda|^2 \in \mathbf{R}[X]$.
Et donc P et Q ne sont pas premiers dans $\mathbf{R}[X]$.
Remarque *: il se cache ici une petite subtilité quand on parle de divisibilité, entend-on divisibilité dans $\mathbf{R}[X]$ ou dans $\mathbf{C}[X]$?*
En réalité, peu importe, car si A et B sont deux polynômes à coefficients réels, alors $A \mid B$ dans $\mathbf{R}[X]$ si et seulement si $A \mid B$ dans $\mathbf{C}[X]$.
L'implication de gauche à droite est évidente. Et réciproquement, si $A = BQ$, avec $Q \in \mathbf{C}[X]$, alors $\overline{A} = \overline{BQ} \Leftrightarrow A = B\overline{Q}$.
Et donc si $B \neq 0$, $\overline{Q} = Q$, donc $Q \in \mathbf{R}[X]$. Et si $Q = 0$, alors $A = 0$, et alors le résultat est trivial.

2. Notons $D_{\mathbf{R}}$ le PGCD de P et Q dans $\mathbf{R}[X]$ et $D_{\mathbf{C}}$ leur PGCD dans $\mathbf{C}[X]$.
Alors il existe deux polynômes à coefficients réels P_1 et Q_1, premiers entre eux tels que $P = D_{\mathbf{R}}P_1$ et $Q = D_{\mathbf{R}}Q_1$.
Par la question 1, P_1 et Q_1 sont également premiers entre eux dans $\mathbf{C}[X]$, et donc $D_{\mathbf{R}}$ est un PGCD de P et Q dans $\mathbf{C}[X]$. Étant unitaire, c'est **le** PGCD unitaire.

3. Notons que la division euclidienne ne dépend pas du corps choisi. Plus précisément, si $A, B \in \mathbf{R}[X]$, alors leur division euclidienne dans $\mathbf{R}[X]$ est $A = BQ + R$, avec $Q, R \in \mathbf{R}[X]$ et $\deg R < \deg B$.
Mais alors $A = BQ + R$, avec $Q, R \in \mathbf{C}[X]$ et $\deg R < \deg B$, donc par unicité de la division euclidienne dans $\mathbf{C}[X]$, il s'agit là de la division euclidienne, dans $\mathbf{C}[X]$, de A par B.

Ainsi, lorsque P et Q sont à coefficients dans $\mathbf{R}$, notons $R_0 = P$, $R_1 = Q$ et $R_2, \dots, R_n$ les reste successifs des divisions euclidiennes de l'algorithme d'Euclide appliqué dans $\mathbf{R}[X]$, avec R_n associé à $P \wedge Q$ le dernier reste non nul.
Alors nous avons là aussi des restes de divisions euclidiennes dans $\mathbf{C}[X]$, et l'algorithme d'Euclide étant valable lui aussi dans $\mathbf{C}[X]$, R_n est également associé au PGCD de P et Q en tant que polynômes complexes.
Et donc le PGCD de P et Q est le même qu'on considère P et Q comme polynômes réels ou complexes.

SOLUTION DE L'EXERCICE 34.7

Notons $D = A \wedge B$. Alors $D^2 = A^2 \wedge B^2$.
En effet, on a $A = DA_1$ et $B = DB_1$ avec $A_1 \wedge B_1 = 1$.
Donc $A^2 = D^2A_1^2$ et $B^2 = D^2B_1^2$, et A_1^2 et B_1^2 sont premiers entre eux.
Mais A^2 est un diviseur commun de A^2 et B^2, donc divise D^2.
Puisque nous avons prouvé ci-dessus que $D^2 \mid A^2$, A^2 et D^2 sont associés, et donc ont même degré.
Donc A et D ont également même degré, et $D \mid A$. Donc A et D sont associés. Puisque $D \mid B$, alors $A \mid B$.

SOLUTION DE L'EXERCICE 34.8

1. Il est évident que (P) contient $0 = P \times 0$.
Soient $A, B \in (P)$. Alors il existe $Q_1, Q_2 \in \mathbf{K}[X]$ tels que $A = PQ_1$ et $B = PQ_2$. Et donc $A - B = P(Q_1 - Q_2) \in (P)$.
Ainsi, (P) est un sous-groupe de $(\mathbf{K}[X], +)$.
Par ailleurs, si $A \in (P)$ et $R \in \mathbf{K}[X]$, alors soit $Q \in \mathbf{K}[X]$ tel que $A = PQ$. Alors $AR = PQR = P(QR) \in (P)$.
Donc (P) est bien un idéal de $\mathbf{K}[X]$.

Plus généralement
Le même raisonnement prouve que deux polynômes sont premiers entre eux dans $\mathbf{C}[X]$ si et seulement si ils n'ont aucune racine complexe commune.

Rappel
Si P est un polynôme **à coefficients réels**, alors pour tout $\lambda \in \mathbf{C}$, $P(\lambda) = 0 \Leftrightarrow P(\overline{\lambda}) = 0$.

[4] Comme tous les polynômes de degré 1, et ce quel que soit le corps de base.

Remarque
Le même raisonnement est valable dans n'importe quels corps tels que $\mathbf{k} \subset \mathbf{K}$: le PGCD de deux polynômes à coefficients dans $\mathbf{k}$ est le même que l'on considère ces polynômes comme éléments de $\mathbf{k}[X]$ ou de $\mathbf{K}[X]$.

2. Soit I un idéal de $\mathbf{K}[X]$. Si $I = \{0\}$, alors $I = \{0\}$.
Et si $I \neq \{0\}$, soit P un polynôme de degré minimal parmi les éléments de $I \setminus \{0\}$.
Alors pour $A \in I$, la division euclidienne de A par P est de la forme $A = PQ + R$, avec $\deg R < \deg P$.
Mais $R = A - PQ$, avec $A \in I$, et $P \in I$, donc $PQ \in I$, et donc $R \in I$.
Puisque R est de degré strictement inférieur à P, on a donc $R = 0$, de sorte que $A = PQ \in (P)$.
Et donc $I \subset (P)$. L'inclusion réciproque découle directement du second point de la définition d'idéal, donc $I = (P)$.

Notons que quitte à diviser P par son coefficient dominant (ce qui fournit encore un polynôme dans I, de degré minimal parmi les polynômes non nuls), on peut supposer P unitaire.
Ne reste alors qu'à prouver l'unicité d'un tel P. Mais si P, Q sont deux polynômes unitaires tels que $I = (P) = (Q)$, alors $Q \in (P)$, et donc $P \mid Q$, et de même $Q \mid P$, donc P et Q sont associés. Étant tous deux unitaires, ils sont égaux.

3. La vérification du fait que $(A) + (B)$ et $(A) \cap (B)$ soient des idéaux ne pose pas de problème.
Soit donc P unitaire tel que $(A) + (B) = (P)$. Puisque $A = A + 0 \in (A) + (B) = (P)$, P divise A. Et de même, $P \mid B$. Donc P divise $A \wedge B$.
Et inversement, puisque $A \wedge B$ divise tous les polynômes de la forme $AU + BV$, en particulier il divise P.
Et donc $P = A \wedge B$.

Détails

P est bien de la forme $AU + BV$, puisque par définition, tous les éléments de $(A) + (B)$ sont de cette forme.

De plus (A) étant l'ensemble des multiples de A, $(A) \cap (B)$ est l'ensemble des multiples communs de A et de (B).
Nous savons déjà que $A \vee B$ est un tel multiple, et donc que $(A \vee B) \subset (A) \cap (B)$.
Par ailleurs, un multiple commun de A et de B est un multiple de $A \vee B$, donc $(A) \cap (B) \subset (A \vee B)$, de sorte que $(A) \cap (B) = (A \vee B)$.

Solution de l'exercice 34.9

1. Une récurrence rapide[5] prouve que $\deg P_n = n - 1$.

2. Par récurrence sur n. Pour $n = 2$, on a

$$P_2^2 - P_3 P_1 = X^2 - (X^2 - 1) = 1.$$

Et alors

$$\begin{aligned} P_{n+1}^2 - P_n P_{n+2} &= (XP_n - P_{n-1})^2 - P_n(XP_{n+1} - P_n) \\ &= X^2 P_n^2 - 2XP_nP_{n-1} + P_{n-1}^2 - P_n(X^2 P_n - XP_{n-1} - P_n) \\ &= X^2 P_n^2 - 2XP_nP_{n-1} + P_{n-1}^2 - X^2 P_n^2 + XP_nP_{n-1} + P_n^2 \\ &= P_n^2 - XP_nP_{n-1} + P_{n-1}^2 = P_n^2 - P_{n-1}(XP_n - P_{n-1}) \\ &= P_n^2 - P_{n-1}P_{n+1}. \end{aligned}$$

3. C'est tout simplement Bézout.

4. Par récurrence sur p. Pour $p = 1$, c'est la définition de F_{n+1}.
Et on a ensuite $Pn + 1 + p = P_{(n+1)+p} = P_{n+1}P_{p+1} - P_nP_p = (XP_n - P_{n-1})P_{p+1} - P_nP_p$.
Et d'autre part,

$$P_nP_{p+2} - P_{n-1}P_{p+1} = P_n(Xp_{p+1} - P_p) - P_{n-1}P_{p+1} = P_{n+p+1}.$$

Un diviseur commun D à P_{n+p} et P_p divise alors P_nP_{p+1}.
Mais $P_{p+1} \wedge P_p = 1$, donc $P_{p+1} \wedge D = 1$, donc par Gauss, $D \mid P_n$. Et donc D divise à la fois P_n et P_p, donc divise leur PGCD.

Réciproquement, un diviseur commun à P_p et P_n divise $P_nP_{p+1} = -P_{n-1}P_p = P_{n+p}$, donc divise $P_p \wedge P_{n+p}$.

5. Supposons $p < n$ et soit $n = pq + r$ la division euclidienne de n par p.
Alors $P_n \wedge P_p = P_{n-p} \wedge P_p = P_{n-2p} \wedge P_p = \cdots = P_{n-qp} \wedge P_p = P_r \wedge P_p$.
Et alors si on note $a_0 = n$, $a_1 = p$ et $a2, \ldots, a_k, 0$ les restes successifs obtenus dans l'algorithme d'Euclide pour le calcul de $n \wedge p = a_k$, on obtient

$$P_n \wedge P_p = P_p \wedge P_{a_1} = \cdots = P_{a_k} \wedge P_0 = P_{a_k} = P_{n \wedge p}.$$

[5] Qui nécessite tout de même de se souvenir à quelle condition le degré d'une somme est le degré maximal des deux termes.

SOLUTION DE L'EXERCICE 34.10

L'énoncé comporte une petite ambiguïté, puisqu'il ne précise pas dans quel corps nous voyons ces polynômes : sont-ils à coefficients dans $\mathbf{R}$, dans $\mathbf{C}$ ou dans $\mathbf{Z}/17\mathbf{Z}$?

Donnons une première solution dans $\mathbf{C}[X]$, par le résultat de l'exercice 34.6, cela traitera également le cas où on voit nos polynômes comme étant à coefficients réels, rationnels, ou dans n'importe quel sous-corps de $\mathbf{C}$.

Rappelons que $X^n - 1 = \prod_{\omega \in \mathbf{U}_n} (X - \omega)$ et de même $X^p - 1 = \prod_{\omega \in \mathbf{U}_p} (X - \omega)$.
Puisque les racines de $X^n - 1$ sont simples, celles de $(X^n - 1) \wedge (X^p - 1)$ le sont aussi, et donc $(X^n - 1) \wedge (X^p - 1) = \prod_{\omega \in \mathbf{U}_p \cap \mathbf{U}_q} (X - \omega)$.
Mais nous avons déjà prouvé dans un exercice du TD d'arithmétique que $\mathbf{U}_n \cap \mathbf{U}_p = \mathbf{U}_{n \wedge p}$.
Et donc

$$(X^n - 1) \wedge (X^p - 1) = \prod_{\omega \in \mathbf{U}_{n \wedge p}} (X - \omega) = X^{n \wedge p} - 1.$$

Alternative : supposons, quitte à inverser n et p, que $n \geqslant p$, et soit $n = pq + r$ la division euclidienne de n par p.
Alors,

$$X^n - 1 = X^{pq+r} - X^r + X^r - 1 = X^r(X^{pq} - 1) + (X^r - 1).$$

Et par la troisième identité remarquable généralisée,

$$X^{pq} - 1 = (X^p - 1)(1 + X^p + \cdots + X^{p(q-1)}).$$

Puisque $\deg(X^r - 1) = r < p = \deg(X^p - 1)$, la division euclidienne de $X^n - 1$ par $X^q - 1$ est donc

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

Et donc le reste est $X^r - 1$.
Donc par le lemme d'Euclide[6], $(X^n - 1) \wedge (X^p - 1) = (X^p - 1) \wedge (X^r - 1)$.
Notons alors $r_1 = r, r_2, \ldots, r_k$ les restes successifs obtenus lors du calcul du PGCD de n et p par l'algorithme d'Euclide[7], avec $r_k = n \wedge p$ le dernier reste non nul.
Alors $(X^n - 1) \wedge (X^p - 1) = (X^p - 1) \wedge (X^r - 1) = \cdots = (X^{r_{k-1}} - 1) \wedge (X^{r_k} - 1)$.
Et alors on prouve que le reste de la division euclidienne de $X^{r_{k-1}} - 1$ par $X^{r_k} - 1$ est nul (car r_k divise r_{k-1}), et donc par l'algorithme d'Euclide[8], $(X^n - 1) \wedge (X^p - 1) = X^{r_k} - 1 = X^{n \wedge p} - 1$.
Si vous avez l'impression d'avoir déjà rencontré ces calculs, allez voir l'exercice 16.14, le raisonnement y est quasiment identique.

[6] Celui qui justifie la validité de l'algorithme d'Euclide.
[7] Dans $\mathbf{Z}$ donc.
[8] Cette fois dans $\mathbf{K}[X]$.

SOLUTION DE L'EXERCICE 34.11

1. Puisque P est unitaire et irréductible, et que $P \wedge Q \mid P$, on a $P \wedge Q = P$ ou $P \wedge Q = 1$.
Mais dans le premier cas, on aurait $P \mid Q$, et par irréductibilité de Q, P et Q seraient associés.
Étant tous deux unitaires, ils seraient égaux, ce qui n'est pas le cas.

Donc P et Q sont premiers entre eux.
Supposons par l'absurde qu'ils possèdent une racine complexe commune $\alpha \in \mathbf{C}$. Par Bézout, il existe $U, V \in \mathbf{Q}[X]$ tels que $PU + QV = 1$, et donc α est racine de 1, ce qui est absurde.

2. Si $\deg P = 1$, alors P a une seule racine complexe[9], qui est simple.
Supposons donc $\deg P \geqslant 2$.

[9] Et qui est même rationnelle.

Supposons par l'absurde que P possède une racine α de multiplicité supérieure ou égale à 2.
Alors α est racine à la fois de P et de P'.
Par ailleurs, $P \wedge P'$ est un diviseur de P, de degré inférieur ou égal à $\deg P' < \deg P$, et donc est égal à 1.
On conclut alors comme dans la question précédente.

SOLUTION DE L'EXERCICE 34.12

Pour $n = 1$, c'est évident.
Sinon, notons que les racines complexes de P_n sont les racines $n^{\text{èmes}}$ de 2, donc les complexes de la forme $e^{\frac{2ik\pi}{n}} \sqrt[n]{2}$, $k \in [\![0, n-1]\!]$.

Supposons par l'absurde que $P_n = QR$, avec Q, R non constants, qu'on peut supposer unitaires[10].

[10] Quitte à les multiplier par une constante.

Notons $A = \left\{k \in [\![0, n-1]\!] \mid Q\left(\sqrt[n]{2}e^{\frac{2ik\pi}{n}}\right) = 0\right\}$, de sorte que $Q = \prod_{k\in A}\left(X - \sqrt[n]{2}e^{\frac{2ik\pi}{n}}\right)$ dans $\mathbf{C}[X]$.

> **Remarque**
> On notera que les racines complexes de P_n étant simples, il en est de même de celles de Q.

Le coefficient constant q_0 de Q est donc $(-1)^p 2^{\frac{p}{n}} \prod_{k\in A} e^{\frac{2ik\pi}{n}}$, où $p = \deg Q = \mathrm{Card}(A)$.
Mais $q_0 \in \mathbf{Q}$, si bien que $|q_0| = 2^{\frac{p}{n}} \in \mathbf{Q}$.

Montrons que ceci n'est pas possible pour $1 < p < n$.
Supposons par l'absurde que $2^{\frac{p}{n}} = \frac{a}{b}$, avec $a \wedge b = 1$.
Alors $2^p = \frac{a^n}{b^n}$, et donc $b^n 2^p = a^n$. Donc $2 \mid a^n$, et par conséquent, $2 \wedge b^n = 1$.
Donc $p = v_2(a^n) = nv_2(a)$, ce qui n'est pas possible puisque $1 < p < n$.

Solution de l'exercice 34.13

Dans la suite, nous noterons $R = P - Q$, le but de l'exercice étant donc de prouver que $R = 0$.

1. Les deux polynômes $P \wedge P'$ et $(P-1) \wedge P'$ sont des diviseurs de P'.
Mais P et $P-1$ sont évidemment premiers entre eux[11], et donc $P \wedge P'$ et $(P-1) \wedge P'$ le sont aussi.
Puisque les deux divisent P', leur produit aussi.
Or, $\deg(P') = \deg(P) - 1$, et donc $\deg(P \wedge P') + \deg((P-1) \wedge P') \leqslant \deg(P') \leqslant \deg(P) - 1$.

[11] Par Bézout.

2. Quitte à échanger P et Q, supposons $\deg P \geqslant \deg Q$, de sorte que $\deg R \leqslant \deg P$.
Les racines de P sont donc racines de R. De même, les racines de $P-1$ sont des racines de R, et ces racines ne peuvent être racines de P.
La clé est alors de reconnaître que P étant scindé, $\deg(P) - \deg(P \wedge P')$ est le nombre de racines distinctes[12] de P. C'est en fait le résultat de l'exercice 34.4.

[12] Donc comptées sans multiplicités.

Et sur le même principe, puisque P' est aussi le polynôme dérivé de $P-1$,
$\deg(P-1) - \deg((P-1) \wedge P')$ est le nombre de racines distinctes de $P-1$.
Donc nous avons déjà un certain nombre de racines, au moins égal à

$$\deg(P) - \deg(P' \wedge P) + \underbrace{\deg(P-1)}_{=\deg P} - \deg((P-1) \wedge P') \geqslant 2\deg(P) - (\deg(P) - 1) \geqslant \deg(P) + 1 > \deg(R).$$

Et donc R possède strictement plus de racines que son degré, il est donc nul, de sorte que $P = Q$.

Solution de l'exercice 34.14

Soit $F = \frac{P}{Q} \in \mathbf{K}[X]$ une fraction rationnelle, sous forme irréductible, qui possède $\lambda \in \mathbf{K}$ à la fois comme pôle et comme zéro.
Alors λ est racine de P et de Q en même temps. Et donc P et Q sont tous deux divisibles par $X - \lambda$, ce qui contredit le fait qu'ils soient premiers entre eux.

Solution de l'exercice 34.15

Remarque *: le résultat de cet exercice a déjà été prouvé dans l'exercice 18.21.*

Nous savons déjà que si $P \in \mathbf{C}[X]$ possède pour racines $\lambda_1, \dots, \lambda_n$, de multiplicités respectives $m_1, \dots, m_n$, alors $\frac{P'}{P} = \sum_{i=1}^{n} \frac{m_i}{X - \lambda_i}$.

Mais par ailleurs, si $P' \mid P$, puisque $\deg P' = \deg P - 1$, il existe $\lambda, m \in \mathbf{C}$ tel que $\frac{P'}{P} = \frac{m}{X - \lambda}$.
Donc par unicité de la décomposition en éléments simples, λ est l'unique racine complexe de P, et m est en fait un entier, égal à la multiplicité de λ.
Et donc $P = \alpha(X - \lambda)^n$, avec α le coefficient dominant de P.

Inversement, tout polynôme de cette forme est tel que $P' \mid P$.

SOLUTION DE L'EXERCICE 34.16

Notons $F = \dfrac{P}{Q}$ la forme irréductible de F, de sorte que A soit l'ensemble des racines de Q.

Il s'agit alors de trouver les $a \in \mathbf{C}$ pour lesquels il existe $x \in \mathbf{C} \setminus A$ tel que $\dfrac{P(x)}{Q(x)} = a$.

Soit encore $P(x) - aQ(x) = 0$, c'est-à-dire tels que $P - aQ$ possède une racine dans $\mathbf{C} \setminus A$.

Notons tout de suite que si $P - aQ$ possède une racine dans $\mathbf{C}$, celle-ci ne peut pas être dans A.

En effet, un élément $z \in A$ est par définition[13] une racine de Q, et s'il est également racine de $P - aQ$, alors il est racine de P. Et donc P et Q sont tous deux divisibles par $X - z$, contredisant l'irréductibilité de F.

[13] D'un pôle.

Autrement dit

Un scalaire ne peut être à la fois un zéro et un pôle.

Donc il s'agit de déterminer pour quels $a \in \mathbf{C}$, $P - aQ$ possède une racine.

Mais par le théorème de d'Alembert-Gauss, tout polynôme non constant possède au moins une racine.

Or, $P - aQ$ n'est constant que si il existe $b \in \mathbf{C}$ tel que $P - aQ = b \Leftrightarrow P = aQ + b$.

Dans ce cas, $P - aQ$ n'a pas de racine, donc a n'a pas d'antécédent par F.

En revanche, pour $a' \neq a$, $P - a'Q$ n'est pas constant, et donc a' possède un antécédent par F.

Donc si $P = aQ + b$, alors $\operatorname{Im} F = \mathbf{C} \setminus \{a\}$.

Et si P n'est pas de la forme $aQ + b$, alors F est surjective.

Remarque

b ne peut pas être nul, faute de quoi $F = \dfrac{aQ}{Q} = a$ serait constante.

SOLUTION DE L'EXERCICE 34.17

Notons $R(X)$ la fraction rationnelle définie par $R(X) = \displaystyle\sum_{\omega \in \mathbf{U}_7} \frac{1}{X - \omega}$.

Il est alors classique que si $P(X) = \displaystyle\prod_{\omega \in \mathbf{U}_7} (X - \omega)$, alors $R(X) = \dfrac{P'(X)}{P(X)}$.

Et donc $R(3) = \dfrac{P'(2)}{P(2)}$.

Or, toutes les racines $7^{\text{èmes}}$ de l'unité vérifient $\omega^7 = 1$, et sont donc racines de $X^7 - 1$.

Ainsi, $X^7 - 1$ est divisible par P. Mais puisqu'il possède même degré que P, et même coefficient dominant, $X^7 - 1 = P$.

Et donc $P'(X) = 7X^6$, de sorte que

$$\sum_{\omega \in \mathbf{U}_7} \frac{1}{2 - \omega} = R(2) = \frac{P'(2)}{P(2)} = \frac{7 \times 2^6}{2^7 - 1} = \frac{448}{127}.$$

SOLUTION DE L'EXERCICE 34.18

Notons $F = \displaystyle\sum_{\omega \in \mathbf{U}_n} \frac{\omega^2}{X - \omega}$, et cherchons à exprimer F sous la forme $\dfrac{P}{Q}$.

Puisque F ne possède que les éléments de $\mathbf{U}_n$ comme pôles, tous simples, Q peut être pris sous la forme $Q = \displaystyle\prod_{\omega \in \mathbf{U}_n} (X - \omega) = X^n - 1$.

Les pôles étant simples, leur partie polaire est alors $\dfrac{P(\omega)}{Q'(\omega)(X - \omega)}$.

Par unicité de la partie polaire, on a donc $\dfrac{P(\omega)}{Q'(\omega)} = \omega^2 \Leftrightarrow P(\omega) = n\omega^{n-1}\omega^2 = n\omega^{n+1} = n\omega$.

Mais puisque $\deg F \leqslant -1$, et que $\deg Q = n$, $\deg P \leqslant n - 1$.

Donc $P(X) - nX$ possède n racines[14], et est de degré au plus $n - 1$: il est nul, et donc $P = nX$, de sorte que la fraction cherchée est $\dfrac{nX}{X^n - 1}$.

Et notons alors que cette fraction est bien irréductible.

Remarque

Si on veut vraiment la forme irréductible, peut être que le dénominateur ne sera qu'un diviseur de ce polynôme. Mais nous verrons cela en temps voulu.

[14] Nous avons prouvé ci-dessus que tous les $\omega \in \mathbf{U}_n$ en sont racine.

SOLUTION DE L'EXERCICE 34.19

1. Nous savons[15] que $\cos(nx) = \operatorname{Re}\left((\cos x + i \sin x)^n\right)$.
Mais en utilisant la formule du binôme, il vient

$$\cos(nx) = \operatorname{Re}\left(\sum_{k=0}^{n} \binom{n}{k} i^k (\sin x)^k (\cos x)^{n-k}\right).$$

[15] C'est la formule de Moivre.

Les termes réels sont ceux pour k pair, c'est-à-dire les $k = 2p$, avec $0 \leqslant p \leqslant \left\lfloor \frac{n}{2} \right\rfloor$.
Donc

$$\cos(nx) = \sum_{p=0}^{\lfloor n/2 \rfloor} \binom{n}{2p} (-1)^p \sin^{2p}(x)(\cos x)^{n-2p} = \sum_{p=0}^{\lfloor n/2 \rfloor} \binom{n}{2p} (-1)^p (1-\cos^2(x))^p (\cos x)^{n-2p}.$$

Donc le polynôme $P_n = \sum_{p=0}^{\lfloor n/2 \rfloor} \binom{n}{2p} (-1)^p (1-X^2)^p X^{n-2p}$ convient .

Prouvons que c'est le seul : si P et Q sont deux tels polynômes, la fonction cos ayant pour image $[-1,1]$, alors pour tout $x \in [-1,1]$, $P(x) = Q(x)$.
Donc $P - Q$ possède une infinité de racines, et donc est nul.

2. Les $x_k = \cos\left(\frac{\pi}{2n} + \frac{k\pi}{n}\right)$, avec $0 \leqslant k \leqslant n-1$ sont des racines de P_n, deux à deux distinctes car cos est injective sur $[0, \pi]$.

3. Puisque $\frac{1}{P_n}$ n'a que des pôles simples, on peut utiliser une formule vue en cours[16] :

[16] Celle qui donne la partie polaire d'un pôle simple.

$$\frac{1}{P_n} = \sum_{k=0}^{n-1} \frac{1}{P'(x_k)(X - x_k)}.$$

Mais en dérivant par rapport à θ la relation $P_n(\cos\theta) = \cos(n\theta)$, on obtient

$$-\sin(\theta) P_n'(\cos(\theta)) = -n\sin(n\theta).$$

En particulier, pour $\theta = \frac{\pi}{2n} + \frac{k\pi}{n}$, on a $\sin(n\theta) = \sin\left(\frac{\pi}{2} + k\pi\right) = (-1)^k$.
Et donc $P_n'(x_k) = \frac{(-1)^k n}{\sin\left(\frac{\pi}{2n} + \frac{k\pi}{n}\right)}$.
On en déduit que

$$\frac{1}{P_n} = \sum_{k=0}^{n-1} \frac{(-1)^k \sin\left(\frac{\pi}{2n} + \frac{k\pi}{n}\right)}{n(X - x_k)}.$$

Solution de l'exercice 34.20

1. Notons $\lambda_1, \dots, \lambda_n$ les racines éventuellement confondues[17] de P.

[17] En cas de racine multiple.

Alors pour $x \notin \{\lambda_1, \dots, \lambda_n\}$, $\frac{P'(x)}{P(x)} = \sum_{k=1}^{n} \frac{1}{x - x_k}$.
Et donc par dérivation de cette relation, pour $x \notin \{\lambda_1, \dots, \lambda_n\}$,
$\frac{P'(x)^2 - P(x)P''(x)}{P(x)^2} = \sum_{k=1}^{n} \frac{1}{(x-x_k)^2} \geqslant 0$, si bien que $P'(x)^2 - P(x)P''(x) \geqslant 0$.
Par continuité[18], cette relation reste évidemment valable en les λ_i.

[18] De P, P' et P''.'

2. Il est classique[19] que si $P \in \mathbf{R}[X]$ est scindé sur $\mathbf{R}$, alors P' l'est aussi, et donc pour tout $k \leqslant \deg P$, $P^{(k)}$ est scindé.

[19] Cela découle de Rolle.

Soit donc $k \in [\![1, n-1]\!]$. Alors en appliquant le résultat de la question précédente à $P^{(k-1)}$, et en évaluant en 0, il vient

$$(k!a_k)^2 - (k+1)!(k-1)!a_{k+1}a_{k-1} \geqslant 0.$$

Soit encore $ka_k^2 - (k+1)a_{k+1}a_{k-1} \geqslant 0 \Leftrightarrow k(a_k^2 - a_{k+1}a_{k-1}) \geqslant a_{k+1}a_{k-1}$.

Si $a_{k+1}a_{k-1} \leqslant 0$, l'inégalité demandée est triviale. Et sinon, il suffit de repartir de celle que nous venons de prouver en notant que $a_{k+1}a_{k-1} \geqslant 0$.

Solution de l'exercice 34.21

Pour $\theta \in \mathbf{R}$, $f(\theta) = \frac{1}{2}\sum_{k=0}^{n} \left(a_k\left(e^{ik\theta} + \frac{1}{e^{ik\theta}}\right) + \frac{b_k}{i}\left(e^{ik\theta} - \frac{1}{e^{ik\theta}}\right)\right)$.

Soit donc $F(X) = \frac{1}{2}\sum_{k=0}^{n}\left(a_k\left(X^k+\frac{1}{X^k}\right)+\frac{b_k}{i}\left(X^k-\frac{1}{X^k}\right)\right)$, de sorte que pour $\theta \in \mathbf{R}$, $f(\theta) = F(e^{i\theta})$.

On a alors $X^n F = \frac{1}{2}\sum_{k=0}^{n}\left[(a_k - ib_k)X^{n+k} + (a_k+ib_k)X^{n-k}\right] \in \mathbf{C}_{2n}[X]$.
Notons donc P ce polynôme.

▶ Si P n'est pas le polynôme nul, supposons par l'absurde que f s'annule au moins $2n+1$ fois sur $[0,2\pi[$, en $\theta_1,\dots,\theta_{2n+1}$.
Alors, la fonction $\theta \mapsto e^{i\theta}$ étant injective sur $[0,2\pi[$, F s'annule également $2n+1$ fois, en $e^{i\theta_1},\dots,e^{i\theta_{2n+1}}$.
Donc P possède $2n+1$ racines distinctes, ce qui est absurde puisque $\deg P \leqslant 2n$.

⚠ Attention !
Si on ne mentionne pas l'injectivité, rien ne justifie que les racines de P soient distinctes.
Donc il n'y a pas de contradiction.

▶ Si P est le polynôme nul, alors $F = 0$, et donc pour tout $\theta \in \mathbf{R}$, $f(\theta) = F(e^{i\theta}) = 0$, et donc f est la fonction nulle.

Remarque : il n'est pas beaucoup plus difficile de constater que P est nul si et seulement si $a_0 = a_1 = \cdots = a_n = b_1 = \cdots = b_n = 0$.
En revanche, le b_0 ne sert à rien, puisqu'il apparaît dans la somme multiplié par $\sin(0x) = 0$.

SOLUTION DE L'EXERCICE 34.22

Détails
Plusieurs arguments peuvent être invoqués ici, par exemple l'irréductibilité de X dans $\mathbf{C}[X]$, qui divise donc un produit si et seulement si il divise l'un des termes.
Ou encore le fait qu'un polynôme est divisible par X si et seulement si il s'annule en 0.

1. Si $F' = \frac{1}{X}$, alors $X(P'Q - PQ') = Q^2$, si bien que $X \mid Q^2$.
Mais alors $X \mid Q$.

2. Si $X^n \mid Q$, alors $X^{2n} \mid Q^2 = X(P'Q - PQ')$.
Donc $X^{2n-1} \mid P'Q - PQ'$. Et donc, puisque $2n-1 \geqslant n$, $X^n \mid P'Q - PQ'$.
Puisque par ailleurs, il est clair que $X^n \mid P'Q$, nécessairement $X^n \mid PQ'$.

Puisque nous avons supposé $n \geqslant 1$, $X \mid Q$, et P et Q étant premiers entre eux, $X \wedge P = 1$, si bien que $X^n \wedge P = 1$.
Et donc par le lemme de Gauss, $X^n \mid Q'$.

3. Il s'agit de prouver qu'une telle fraction F n'existe tout simplement pas. En effet, si $F = \frac{P}{Q}$ convient, nous avons prouvé dans la question 1) que nécessairement $X \mid Q$.
Notons alors $n \geqslant 1$ la multiplicité de 0 en tant que racine de Q. Alors la multiplicité de 0 en tant que racine de Q' est aussi supérieure ou égale à n. Donc la multiplicité de 0 en tant que racine de Q est supérieure ou égale à $n+1$, ce qui est absurde.
Donc une telle fraction rationnelle F n'existe pas.

SOLUTION DE L'EXERCICE 34.23

1. Puisque $A + B = C$, on a par dérivation $A' + B' = C'$, et donc $\frac{A'+B'}{A+B} = \frac{C'}{C}$. Soit encore

$$(A+B)\frac{C'}{C} = A' + B' = A\frac{A'}{A} + B\frac{B'}{B} \Leftrightarrow A\left(\frac{A'}{A} - \frac{C'}{C}\right) = B\left(\frac{C'}{C} - \frac{B'}{B}\right).$$

Les polynômes A, B, C sont uniquement supposés premiers entre eux dans leur ensemble, mais ils sont alors nécessairement premiers entre eux deux à deux.
En effet, si deux d'entre eux avaient un facteur irréductible commun[20], alors la relation $A + B = C$ montre que le facteur en question divise à la fois A, B et C.
Notons

$$A = \alpha\prod_{i=1}^{n_A}(X-a_i)^{\alpha_i},\ B = \beta\prod_{i=1}^{n_B}(X-b_i)^{\beta_i},\ C = \gamma\prod_{i=1}^{n_C}(X-c_i)^{\gamma_i}$$

les décompositions de A, B et C en produits de facteurs irréductibles, où les a_i (resp. b_i et c_i sont supposés deux à deux distincts).

Alors nous savons que les décompositions en éléments simples de $\frac{A'}{A}$, $\frac{B'}{B}$ et $\frac{C'}{C}$ sont les suivantes :

$$\frac{A'}{A} = \sum_{i=1}^{n_A}\frac{\alpha_i}{X-a_i},\ \frac{B'}{B} = \sum_{i=1}^{n_B}\frac{\beta_i}{X-b_i} \text{ et } \frac{C'}{C} = \sum_{i=1}^{n_C}\frac{\gamma_i}{X-c_i}.$$

[20] Qui rappelons-le, dans $\mathbf{C}[X]$ signifie une racine commune.

Un dénominateur commun à ces trois fractions est $D = \prod_{i=1}^{n_A}(X-a_i)\prod_{i=1}^{n_B}(X-b_i)\prod_{i=1}^{n_C}(X-c_i)$, qui est de degré $n_A+n_B+n_C$.
Il existe donc P et Q deux polynômes tels que $\frac{A'}{A}-\frac{C'}{C}=\frac{P}{D}$ et $\frac{C'}{C}-\frac{B'}{B}=\frac{Q}{D}$.
Puisque $\deg\left(\frac{A'}{A}-\frac{C'}{C}\right)$ est égal à -1, on a donc $\deg P = \deg D - 1$. Et de même pour $\deg Q$.
Mais alors l'égalité précédemment prouvée nous donne $AP = BQ$, et par le lemme de Gauss, A qui est premier avec B doit diviser Q, et de même, $B \mid P$.
Donc $\deg A \leqslant \deg D - 1$ et $\deg B \leqslant \deg D - 1$. Donc de même, $C \leqslant \deg D - 1$.
Donc $\max(\deg A, \deg B, \deg C) \leqslant \deg(D) - 1 < \deg D$.
Puisque $\deg D$ n'est rien d'autre que le m de l'énoncé, on a donc bien l'inégalité voulue.

2. Soient(P,Q,R) trois polynômes non nuls tels que $P^n+Q^n=R^n$, et soit D leur PGCD.
Il existe donc trois polynômes P_1, Q_1, R_1, premiers dans leur ensemble tels que $P = DP_1, Q = DQ_1$ et $R = DR_1$.

En divisant par D^n, on a donc $P_1^n + Q_1^n = R_1^n$.

Supposons R_1 constant, et notons $\zeta = e^{i\frac{\pi}{n}}$, qui est une racine $n^{\text{ème}}$ de -1.
Alors $P_1^n + Q_1^n = P_1^n - (\zeta Q)^n = \prod_{k=1}^{n}(P_1 - \zeta^k Q_1)$.
Alors pour tout $k \in [\![1,n]\!]$, $P_1 - \zeta^k Q_1$ est constant, ce qui signifie[21] que P_1 et Q_1 sont constants.
De même, si P_1 est constant, $P_1^n = R_1^n - Q_1^n = R_1^n + (\zeta Q_1)^n$, et alors le même argument prouve que Q_1 et R_1 sont constants.
Donc si l'un des trois polynômes P_1, Q_1, R_1 est constant, les trois le sont, et donc P, Q et R sont associés.

[21] Regarder les coefficients dominants.

Supposons P_1, Q_1, R_1 non constants, et appliquons alors le résultat de la question précédente :

$$\max(\deg P_1^n, \deg Q_1^n, \deg R_1^n) < m$$

où m est le nombre de racines distinctes de $(P_1Q_1R_1)^n$.
Or $(P_1Q_1R_1)^n$ a mêmes racines que $P_1Q_1R_1$.
Et les polynômes étant premiers entre eux, ils n"existe pas de racine commune à P_1, Q_1 et R_1.
De plus, il n'existe pas non plus de racine commune à deux d'entre eux, puisque si par exemple $\alpha \in \mathbf{C}$ est une racine de P_1 et R_1, alors $Q_1^n(\alpha) = R_1^n(\alpha) - P_1^n(\alpha) = 0$, ce qui est absurde.
Donc m est égal au nombre de racines de P_1, plus le nombre de racines de Q_1, plus le nombre de racines de Q_1.
En notant $r(P_1)$ le nombre de racines de P_1, on a donc prouvé que

$$r(P_1)+r(Q_1)+r(R_1) > \max(\deg P_1^n, \deg Q_1^n, \deg R_1^n) = n\max(\deg P_1, \deg Q_1, \deg R_1) \geqslant 3\max(\deg(P_1), \deg(Q_1), \deg(R_1)).$$

Puisqu'on a évidemment $\deg(P_1) \geqslant r(P_1)$, et de même pour Q_1 et R_1, il vient donc $\deg(P_1) + \deg(Q_1) + \deg(Q_1) > 3\max(\deg P_1, \deg Q_1, \deg R_1)$, ce qui est absurde.

Ainsi, si $P^n + Q^n = R^n$, alors P, Q et R sont associés.

Remarque *: il s'agit là d'une version polynomiale du théorème de Fermat qui affirme que pour $n \geqslant 3$, les seules solutions entières » de $a^n + b^n = c^n$ sont les solutions triviales*[22]
Ici, il y a davantage de solutions triviales, à savoir tous les triplets de la forme $(\alpha D, \beta D, \gamma D)$, avec $D \in \mathbf{C}[X]$ et α, β, γ des complexes tels que $\alpha^n + \beta^n = \gamma^n$.

[22] Avec $abc = 0$.