Mathématiques spéciales

Corrigé de la feuille d'exercices n°10

1. Exercices basiques

Exercice 1.

1. Le polynôme $X^4 + X^2 + 1$ est-il irréductible dans $\mathbb{R}[X]$? dans $\mathbb{C}[X]$?
2. La relation $\mathcal{R}$ définie sur $\mathbb{R}[X]$ par $A\mathcal{R}B$ si et seulement A divise B est-elle une relation d'ordre ?

Correction.

1. Les irréductibles de $\mathbb{R}[X]$ sont de degré 1 ou 2, les irréductibles de $\mathbb{C}[X]$ sont de degré 1. Le polynôme $X^4 + X^2 + 1$ n'est donc irréductible ni dans $\mathbb{R}[X]$, ni dans $\mathbb{C}[X]$.
2. On peut vérifier que la relation $\mathcal{R}$ est transitive et réflexive. En revanche, elle n'est pas anti-symétrique. Prenons par exemple $A = X$ et $B = 2X$. Alors A divise B, B divise A, et pourtant A est différent de B.

Exercice 2.

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

Correction.

Si $P = Q^2$ est le carré d'un polynôme, alors Q est nécessairement de degré 2, et son coefficient dominant est égal à 1. On peut donc écrire $Q(X) = X^2 + cX + d$. On a alors

$$Q^2(X) = X^4 + 2cX^3 + (2d + c^2)X^2 + 2cdX + d^2.$$

Par identification, on doit avoir $2c = 2a$, $2d + c^2 = b$, $2cd = 2$ et $d^2 = 1$. On trouve donc $c = a$ et $d = \pm 1$. Si $d = 1$, alors $c = 1$, et donc $a = 1$ et $b = 3$. Si $d = -1$, alors $c = -1$, $a = -1$ et $b = -1$. Les deux solutions sont donc

$$\begin{aligned} P_1(X) &= X^4 + 2X^3 + 3X^2 + 2X + 1 = (X^2 + X + 1)^2 \\ P_2(X) &= X^4 - 2X^3 - X^2 + 2X + 1 = (X^2 - X - 1)^2. \end{aligned}$$

Exercice 3.

Résoudre les équations suivantes, où l'inconnue est un polynôme P de $\mathbb{R}[X]$:

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

Correction.

1. Le polynôme nul est évidemment solution. Sinon, si P est solution, alors on a
$$2\deg(P) = \deg(P) + 2$$
ce qui prouve que $\deg(P)$ doit être égal à 2. Maintenant, si $P(X) = aX^2 + bX + c$, alors
$$\begin{aligned} P(X^2) &= aX^4 + bX^2 + c \\ (X^2+1)P(X) &= aX^4 + bX^3 + (a+c)X^2 + bX + c. \end{aligned}$$
On en déduit que $b = 0$, puis que $a + c = 0$. Les solutions sont donc les polynômes qui s'écrivent $P(X) = a(X^2 - 1)$, $a \in \mathbb{R}$.
2. Là encore, le polynôme nul est solution, et c'est la seule solution constante. Par ailleurs, si P est une solution non constante, alors son degré vérifie l'équation
$$2(\deg(P) - 1) = \deg(P)$$
ce qui entraîne que $\deg(P) = 2$. Maintenant, si $P(X) = aX^2 + bX + c$, alors
$$\begin{aligned} P'^2 &= (2aX + b)^2 = 4a^2X^2 + 4abX + b^2 \\ 4P &= 4aX^2 + 4bX + 4c. \end{aligned}$$
Ceci entraîne $a^2 = a$, donc $a = 1$ (le polynôme est de degré 2, $a \neq 0$), puis $c = b^2/4$. Les polynômes solutions sont donc le polynôme nul et les polynômes $P(X) = X^2 + bX + b^2/4$, avec $b \in \mathbb{R}$.
3. Si P est une solution qui n'est pas le polynôme nul, alors le degré de $P \circ P$ vaut $\deg(P)^2$, et donc on a l'équation
$$\deg(P)^2 = \deg(P).$$
et donc $\deg(P) = 1$ ou $\deg(P) = 0$. Maintenant, si $P(X) = aX + b$, alors
$$\begin{aligned} P \circ P(X) &= a(aX + b) + b = a^2X + (ab + b) \\ P(X) &= aX + b. \end{aligned}$$
On doit donc avoir $a^2 = a$, soit $a = 1$ ou $a = 0$, et $ab = 0$. Si $a = 1$, alors $b = 0$ et si $a = 0$, alors b peut être quelconque dans $\mathbb{R}$. Finalement, on trouve que les solutions sont les polynômes constants et le polynôme $P(X) = X$.

Exercice 4.

Calculer le quotient et le reste de la division euclidienne de

1. $X^4 + 5X^3 + 12X^2 + 19X - 7$ par $X^2 + 3X - 1$;
2. $X^4 - 4X^3 - 9X^2 + 27X + 38$ par $X^2 - X - 7$;
3. $X^5 - X^2 + 2$ par $X^2 + 1$.

Correction.

On trouve les résultats suivants :

1. Le quotient est $X^2 + 2X + 7$, le reste est nul ;

2. Le quotient est $X^2 - 3X - 5$, le reste est $X + 3$;
3. Le quotient est $X^3 - X - 1$, le reste est $X + 3$.

Exercice 5.

Soit $P \in \mathbb{K}[X]$, soit $a \in \mathbb{K}$ et soit R le reste de la division euclidienne de P par $(X - a)^2$. Exprimer R en fonction de $P(a)$ et de $P'(a)$.

Correction.

R est de degré au plus 1 et s'écrit donc $R(X) = \alpha X + \beta$. Évaluons la relation

$$P(X) = (X - a)^2 Q(X) + \alpha X + \beta$$

au point a. On trouve $P(a) = a\alpha + \beta$. Dérivons maintenant la relation précédente :

$$P'(X) = 2(X - a)Q(X) + (X - a)^2 Q'(X) + \alpha.$$

On évalue à nouveau en a et on trouve que

$$\alpha = P'(a).$$

En revenant à la première équation, on en déduit que $\beta = P(a) - aP'(a)$.

Exercice 6.

Donner une condition nécessaire et suffisante sur $(\lambda, \mu) \in \mathbb{C}^2$ pour que $X^2 + 2$ divise $X^4 + X^3 + \lambda X^2 + \mu X + 2$.

Correction.

On réalise la division euclidienne de $X^4 + X^3 + \lambda X^2 + \mu X + 2$ par $X^2 + 2$, et on trouve :

$$X^4 + X^3 + \lambda X^2 + \mu X + 2 = (X^2 + 2)(X^2 + X + (\lambda - 2)) + (\mu - 2)X + 6 - 2\lambda.$$

Le polynôme $X^2 + 2$ divise donc $X^4 + X^3 + \lambda X^2 + \mu X + 2$ si et seulement si le reste est nul, donc si et seulement si $\mu = 2$ et $\lambda = 3$. Une autre possibilité est de remarquer que les racines de $X^2 + 2$ sont $\sqrt{2}i$ et $-\sqrt{2}i$, et donc que la décomposition en produits d'irréductibles de $X^2 + 2$ est $(X - 2i)(X + 2i)$. Pour que $X^4 + X^3 + \lambda X^2 + \mu X + 2$ soit divisible par $X^2 + 2$, il faut et il suffit que $\sqrt{2}i$ et $-\sqrt{2}i$ soient racines de $X^4 + X^3 + \lambda X^2 + \mu X + 2$. On évalue ce polynôme en $\sqrt{2}i$ et $-\sqrt{2}i$ et on trouve un système linéaire que doit vérifier le couple (λ, μ). On trouve bien sûr la même solution.

Exercice 7.

Le but de cet exercice est de déterminer

$$E = \{P \in \mathbb{R}[X];\ P(X^2) = (X^3+1)P(X)\}.$$

1. Démontrer que le polynôme nul ainsi que le polynôme $X^3 - 1$ sont solutions du problème.
2. Analyse du problème. Soit $P \in E$ non nul.
   (a) Montrer que P est de degré 3.
   (b) Démontrer que $P(1) = 0$, puis que $P'(0) = P''(0) = 0$ (on pourra penser à dériver la relation $P(X^2) = (X^3+1)P(X)$).
   (c) En effectuant la division euclidienne de P par $X^3 - 1$, démontrer qu'il existe $\lambda \in \mathbb{R}$ tel que $P(X) = \lambda X^3 - 1$.
3. Synthèse du problème : en déduire l'ensemble E.

Correction.

1. Il est clair que $0 = (X^3+1)0$ et donc le polynôme nul est solution. Pour $P(X) = X^3 - 1$, on a $P(X^2) = X^6 - 1$ et $(X^3+1)P(X) = (X^3+1)(X^3-1) = X^6 - 1$. Ce polynôme est aussi solution.
2. (a) Notons n le degré de P. Alors $P(X^2)$ est de degré $2n$ et $(X^3+1)P(X)$ est de degré $n+3$. Le degré n vérifie donc l'équation $2n = n+3$, soit $n = 3$.
   (b) En évaluant la relation en $X = 1$, on a $P(1^2) = P(1) = 0$. Dérivons maintenant l'équation $P(X^2) = (X^3+1)P(X)$. On trouve
   $$2XP'(X^2) = 3X^2P(X) + (X^3+1)P'(X).$$
   Si on évalue en $X = 0$, on trouve $P'(0) = 0$. Dérivons une second fois cette équation. On trouve
   $$2P'(X^2) + 4X^2P''(X^2) = 6XP(X) + 6X^2P'(X) + (X^3+1)P''(X).$$
   On évalue cette équation en $X = 0$ et on trouve, tenant compte du fait que l'on sait déjà que $P'(0) = 0$, $P''(0) = 0$.
   (c) Effectuons la division euclidienne de P par $X^3 - 1$. On peut écrire
   $$P(X) = Q(X)(X^3 - 1) + R(X)$$
   où $\deg(R) \leq 2$ et donc $R(X)$ s'écrit $R(X) = aX^2 + bX + c$. De plus, en considérant le degré, Q ne peut être qu'un polynôme constant, et donc $Q(X) = \lambda$ avec $\lambda \in \mathbb{R}$. Il reste à montrer que $a = b = c = 0$. Puisque $P(1) = 0$, on a $a + b + c = 0$. De plus, dérivons $P(X) = \lambda(X^3 - 1) + (aX^2 + bX + c)$. On obtient
   $$P'(X) = 3\lambda X^2 + (2aX + b).$$
   Puisque $P'(0) = 0$, on a $b = 0$. On dérive une seconde fois la relation, on obtient
   $$P''(X) = 6\lambda X + 2a$$
   et puisque $P''(0) = 0$, on a $a = 0$ et finalement également $c = 0$.
3. La question précédente nous dit que si $P \in E$, alors ou bien P est nul ou bien $P(X) = \lambda(X^3 - 1)$ pour un certain $\lambda \in \mathbb{R}^*$. Réciproquement, d'après la première question, le polynôme nul et les polynômes $\lambda(X^3 - 1)$, $\lambda \in \mathbb{R}^*$ sont éléments de E. Finalement, on peut conclure que $E = \{\lambda(X^3 - 1);\ \lambda \in \mathbb{R}\}$.

Exercice 8.

Déterminer les pgcd suivants :

1. $P(X) = X^4 - 3X^3 + X^2 + 4$ et $Q(X) = X^3 - 3X^2 + 3X - 2$;
2. $P(X) = X^5 - X^4 + 2X^3 - 2X^2 + 2X - 1$ et $Q(X) = X^5 - X^4 + 2X^2 - 2X + 1$;
3. $P(X) = X^n - 1$ et $Q(X) = (X-1)^n$, $n \geq 1$.

Correction.

1. On applique l'algorithme d'Euclide. Le dernier reste non-nul donne un pgcd des deux polynômes. On a successivement :

$$\begin{aligned} X^4 - 3X^3 + X^2 + 4 &= (X^3 - 3X^2 + 3X - 2)X + (-2X^2 + 2X + 4) \\ X^3 - 3X^2 + 3X - 2 &= (-2X^2 + 2X + 4)\left(\frac{-X}{2} + 1\right) + 3X - 6 \\ (-2X^2 + 2X + 4) &= (3X - 6) \times \left(\frac{-2X}{3} - \frac{2}{3}\right). \end{aligned}$$

   Un pgcd est donc $3X - 6$ (ou $X - 2$).

2. On répète le même procédé :

$$\begin{aligned} X^5 - X^4 + 2X^3 - 2X^2 + 2X - 1 &= (X^5 - X^4 + 2X^2 - 2X + 1)1 + 2X^3 - 4X^2 + 4X - 2 \\ X^5 - X^4 + 2X^2 - 2X + 1 &= (2X^3 - 4X^2 + 4X - 2)((X^2)/2 + X/2) + X^2 - X + 1 \\ 2X^3 - 4X^2 + 4X - 2 &= (X^2 - X + 1)(2X - 2) + 0 \end{aligned}$$

   Un pgcd des deux polynômes est donc $X^2 - X + 1$.

3. Les diviseurs non-constants de Q sont les polynômes du type $c(X-1)^p$, avec $1 \leq p \leq n$. Parmi ces diviseurs, seuls ceux de la forme $c(X-1)$ divisent aussi P (par exemple, car 1 est racine simple et non double de P, ou bien parce qu'on sait comment décomposer P en produits d'irréductibles...). Ainsi, $P \wedge Q = X - 1$.

Exercice 9.

Trouver deux polynômes U et V de $\mathbb{R}[X]$ tels que $AU + BV = 1$, où $A(X) = X^7 - X - 1$ et $B(X) = X^5 - 1$.

Correction.

On utilise l'algorithme d'Euclide. On a

$$\begin{aligned} X^7 - X - 1 &= (X^5 - 1)X^2 + X^2 - X - 1 \\ X^5 - 1 &= (X^2 - X - 1)(X^3 + X^2 + 2X + 3) + 5X + 2 \\ X^2 - X - 1 &= (5X + 2)(X/5 - 7/25) - 11/25. \end{aligned}$$

On remonte ensuite les calculs. On va partir plutôt de

$$11 = -25(X^2 - X - 1) + (5X - 7)(5X + 2)$$

pour éviter de trainer des fractions. On trouve alors successivement :

$$\begin{aligned} 11 &= -25(X^2-X-1)+(5X-7)\big((X^5-1)-(X^2-X-1)(X^3+X^2+2X+3)\big) \\ &= (-5X^4+2X^3-3X^2-X-4)(X^2-X-1)+(5X-7)(X^5-1) \\ &= (-5X^4+2X^3-3X^2-X-4)(X^7-X-1)+(5X^6-2X^5+3X^4+X^3+4X^2+5X-7)(X^5-1). \end{aligned}$$

Il suffit de diviser par 11 pour obtenir les polynômes U et V.

Exercice 10.

Décomposer en produits d'irréductibles de $\mathbb{R}[X]$ les polynômes suivants :

1. X^4+1 **2.** X^8-1 **3.** $(X^2-X+1)^2+1$

Correction.

1. On commence par chercher les racines complexes pour factoriser dans $\mathbb{C}[X]$, puis on regroupe les racines complexes conjuguées.

$$\begin{aligned} X^4+1 &= (X-e^{i\pi/4})(X-e^{3i\pi/4})(X-e^{5i\pi/4})(X-e^{7i\pi/4}) \\ &= \big((X-e^{i\pi/4})(X-e^{7i\pi/4})\big)\big((X-e^{3i\pi/4})(X-e^{5i\pi/4})\big) \\ &= (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1). \end{aligned}$$

   Les deux polynômes de degré 2 que l'on obtient n'ont pas de racines réelles, ils sont donc irréductibles dans $\mathbb{R}[X]$.

2. On commence par utiliser une identité remarquable, puis la réponse à la question précédente :

$$\begin{aligned} X^8-1 &= (X^4-1)(X^4+1) \\ &= (X^2-1)(X^2+1)(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1) \\ &= (X-1)(X+1)(X^2+1)(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1). \end{aligned}$$

3. On commence par factoriser le polynôme dans $\mathbb{C}[X]$ en remarquant qu'il s'agit alors d'une différence de deux carrés :

$$(X^2-X+1)^2+1=(X^2-X+1)^2-i^2=(X^2-X+1-i)(X^2-X+1+i).$$

   On factorise alors chacun des polynômes de degré 2 dans $\mathbb{C}$, par exemple en calculant leur discriminant ou en remarquant que i (resp. $-i$) sont des racines évidentes. On trouve :

$$(X^2-X+1)^2+1=(X+i)(X-1-i)(X-i)(X-1+i).$$

   En regroupant les termes conjugués, on trouve finalement :

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

Exercice 11.

On considère le polynôme $P(X) = 2X^3 - X^2 - X - 3$.

1. Déterminer une racine rationnelle de P.
2. En déduire la factorisation de P en produit d'irréductibles de $\mathbb{C}[X]$.

Correction.

1. On va chercher une racine sous la forme p/q, avec $p \wedge q = 1$ et $q \geq 1$. L'équation s'écrit
$$2\frac{p^3}{q^3} - \frac{p^2}{q^2} - \frac{p}{q} - 3 = 0.$$
On multiplie tout par q^3 et on trouve
$$2p^3 - p^2q - pq^2 - 3q^3 = 0.$$
Puisque $q| - p^2q - pq^2 - 3q^3$ et que $q \wedge p = 1$, on en déduit que $q|2$, et donc que $q = 1$ ou 2. De même, puisque $p|2p^3 - p^2q - pq^2$ et que $p \wedge q = 1$, on trouve que $p|3$, ce qui donne $p \in \{-3, -1, 1, 3\}$. On trouve ensuite facilement à partir de ces informations que $3/2$ est racine de P.
2. Puisque $3/2$ est racine de P, on va factoriser le polynôme par $X - 3/2$, ou plutôt par $2X - 3$. On trouve
$$2X^3 - X^2 - X - 3 = (2X - 3)(X^2 + X + 1).$$
Reste à factoriser $X^2 + X + 1$ sur $\mathbb{C}$. Ses racines sont $\frac{-1 \pm i\sqrt{3}}{2}$. On en déduit que
$$P(X) = (2X - 3)\left(X - \frac{-1 + i\sqrt{3}}{2}\right)\left(X - \frac{-1 - i\sqrt{3}}{2}\right).$$

Exercice 12.

Soit P le polynôme $X^4 - 6X^3 + 9X^2 + 9$.

1. Décomposer $X^4 - 6X^3 + 9X^2$ en produit de facteurs irréductibles dans $\mathbb{R}[X]$.
2. En déduire une décomposition de P en produit de facteurs irréductibles dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$.

Correction.

1. On écrit simplement
$$X^4 - 6X^3 + 9X^2 = X^2(X^2 - 6X + 9) = X^2(X - 3)^2.$$
2. L'astuce(?) est d'écrire $9 = -(3i)^2$, et de reconnaitre une différence de deux carrés. Donc

on a :

$$\begin{aligned} X^4 - 6X^3 + 9X^2 + 9 &= \big(X(X-3)\big)^2 - (3i)^2 \\ &= \big(X(X-3) - 3i\big)\big(X(X-3) + 3i\big) \\ &= (X^2 - 3X - 3i)(X^2 - 3X + 3i). \end{aligned}$$

On factorise chacun de ces deux polynômes. Le discriminant du premier est $9 + 12i = (\sqrt{3}(2+i))^2$. Ses racines sont $\alpha_1 = \frac{3}{2} + \sqrt{3} + \frac{i\sqrt{3}}{2}$ et $\alpha_2 = \frac{3}{2} - \sqrt{3} - \frac{i\sqrt{3}}{2}$. Le discriminant du second est $9 - 12i = (\sqrt{3}(2-i))^2$, et ses racines sont $\beta_1 = \frac{3}{2} + \sqrt{3} - \frac{i\sqrt{3}}{2}$ et $\beta_2 = \frac{3}{2} - \sqrt{3} + \frac{i\sqrt{3}}{2}$. La décomposition de P en produit d'irréductibles de $\mathbb{C}[X]$ est donc

$$(X - \alpha_1)(X - \alpha_2)(X - \beta_1)(X - \beta_2).$$

Pour obtenir la décomposition en produit d'irréductibles de $\mathbb{R}[X]$, on regroupe les racines complexes conjuguées, à savoir α_1 et β_1 d'une part et α_2 et β_2 d'autre part. On trouve

$$P = \big(X^2 - (2\sqrt{3} + 3)X + 3\sqrt{3} + 6\big)\big(X^2 + (2\sqrt{3} - 3)X - 3\sqrt{3} + 6\big).$$

Exercice 13.

Décomposer en produits d'irréductibles de $\mathbb{C}[X]$ le polynôme $P(X) = X^9 + X^6 + X^3 + 1$.

Correction.

On va commencer par décomposer $Q(X) = X^3 + X^2 + X + 1$, dont -1 est racine évidente. On en déduit

$$Q(X) = (X + 1)(X^2 + 1) = (X + 1)(X - i)(X + i).$$

On a $P(X) = Q(X^3)$ et il s'agit maintenant de trouver les racines 3-ièmes de 1, i et $-i$. On en déduit que

$$\begin{aligned} P(X) &= (X + 1)(X - e^{i\pi/3})(X - e^{-i\pi/3})(X - e^{i\pi/2})(X - e^{-i5\pi/6})(X - e^{-i\pi/6}) \\ &\quad (X - e^{-i\pi/2})(X - e^{i5\pi/6})(X - e^{i\pi/6}). \end{aligned}$$

Exercice 14.

Soit $A \in \mathcal{M}_n(\mathbb{R})$. On note $C = \{M \in \mathcal{M}_n(\mathbb{R});\ AM = MA\}$. Montrer que C est une algèbre.

Correction.

Il suffit de démontrer que C est une sous-algèbre de $\mathcal{M}_n(\mathbb{R})$, c'est-à-dire à la fois un sous-anneau et un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$. Remarquons que la matrice nulle 0 et I_n sont membres de C. De plus, pour tous $M, N \in A$ et tout $\lambda \in \mathbb{R}$, alors on vérifie facilement que

1. $MN \in A$;
2. $\lambda M \in A$;
3. $M - N \in A$.

C'est bien que A est une algèbre.

Exercice 15.

Pour $a, b, c \in \mathbb{R}$, on note

$$M(a,b,c) = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}$$

et $E = \{M(a,b,c);\ a,b,c \in \mathbb{R}\}$. Démontrer que E une algèbre, et en donner une base en tant qu'espace vectoriel.

Correction.

On va prouver que E est une sous-algèbre de $\mathcal{M}_3(\mathbb{R})$. Pour cela, notons

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Alors il est clair que $E = \text{vect}(I_3, A, B)$ et que la famille (I_3, A, B) est libre. On en déduit que E est un sous-espace vectoriel de $\mathcal{M}_3(\mathbb{R})$ de dimension 3. De plus, un calcul rapide montre que

$$M(a,b,c)M(a',b',c') = M(aa\ +bc\ +cb\ , ab\ +a\ b+cc\ , ac\ +a\ c+bb\ ).$$

E est stable par produit matriciel, et c'est une sous-algèbre de $\mathcal{M}_3(\mathbb{R})$.

2. Exercices d'entraînement

Exercice 16.

Quel est le reste de la division euclidienne de $(X+1)^n - X^n - 1$ par

1. $X^2 - 3X + 2$ **2.** $X^2 + X + 1$ **3.** $X^2 - 2X + 1$?

Correction.

1. La méthode pour ce type d'exercice est toujours la même. On commence par écrire *a priori* le résultat de la division euclidienne, par exemple pour le premier polynôme :

$$(X+1)^n - X^n - 1 = Q(X)(X^2 - 3X + 2) + aX + b,$$

où a et b sont deux réels. On évalue ensuite la relation en les racines du diviseur, qui sont ici 1 et 2. On trouve alors

$$\begin{cases} 2^n - 2 &= a + b \\ 3^n - 2^n - 1 &= 2a + b. \end{cases}$$

Et finalement on résoud le système pour trouver a et b, qui sont ici égaux à :

$$\begin{cases} a &= 3^n - 2^{n+1} + 1 \\ b &= -3^n + 2^{n+1} + 2^n - 3. \end{cases}$$

2. On écrit la même chose,

$$(X+1)^n - X^n - 1 = Q(X)(X^2 + X + 1) + aX + b,$$

et on utilise cette fois que les racines de $X^2 + X + 1$ sont j et j^2. Il suffit ici en réalité d'utiliser l'évaluation en j, sachant que tout nombre complexe s'écrit de façon unique sous la forme $x + jy$, avec $x, y \in \mathbb{R}$. On trouve :

$$(1+j)^n - j^n - 1 = Q(j) \times 0 + aj + b.$$

On distingue ensuite suivant la valeur de n modulo 3, utilisant que

$$(1+j)^n - j^n - 1 = (-1)^n j^{2n} - j^n - 1.$$

— Si $n \equiv 0$ [3], alors $j^{2n} = j^n = 1$, et donc on a

$$(-1)^n - 2 = aj + b$$

de sorte que le reste est $(-1)^n - 2$.
— Si $n \equiv 1$ [3], alors $j^n = j$ et donc $j^{2n} = j^2 = -1 - j$, $j^n = j$, ce qui donne

$$\big((-1)^{n+1} - 1\big)j + \big((-1)^{n+1} - 1\big) = aj + b.$$

Le reste est donc $\big((-1)^{n+1} - 1\big)(X + 1)$.
— Si $n \equiv 2$ [3], alors $j^{2n} = j$ et $j^n = j^2 = -1 - j$. On trouve

$$\big((-1)^n + 1\big)j = aj + b.$$

Le reste est alors $\big((-1)^n + 1\big)X$.

3. On recommence en écrivant

$$(X+1)^n - X^n - 1 = Q(X)(X^2 - 2X + 1) + aX + b,$$

et en remarquant que $X^2 - 2X + 1$ a pour racine double 1. Si on évalue en 1, on obtient une seule relation, à savoir

$$2^n - 2 = a + b.$$

Pour obtenir une seconde relation, il faut dériver la relation issue de la division euclidienne et l'évaluer à nouveau en 1 (c'est toujours cette méthode qui fonctionne pour une racine double). On trouve :

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

ce qui donne la relation

$$n2^{n-1} - n = a.$$

On retrouve alors sans problèmes b, qui est égal à :

$$b = (2 - n)2^{n-1} + n - 2.$$

Exercice 17.

Démontrer que

1. $X^{n+1}\cos\big((n-1)\theta\big) - X^n\cos(n\theta) - X\cos\theta + 1$ est divisible par $X^2 - 2X\cos\theta + 1$;
2. $nX^{n+1} - (n+1)X^n + 1$ est divisible par $(X-1)^2$.

Correction.

1. Pour prouver que $X^2 - 2X\cos\theta + 1$ divise $X^{n+1}\cos\big((n-1)\theta\big) - X^n\cos(n\theta) - X\cos\theta + 1$, il suffit de prouver que ce dernier polynôme s'annule en les deux racines (complexes) de $X^2 - 2X\cos\theta + 1$, à savoir $e^{i\theta}$ et $e^{-i\theta}$. Il suffit de prouver le résultat pour $e^{i\theta}$ car, le polynôme étant réel, si z est racine, son conjugué $\bar{z}$ est racine. On trouve

$$\begin{gathered} e^{i(n+1)\theta}\cos\big((n-1)\theta\big) - e^{in\theta}\cos(n\theta) - e^{i\theta}\cos\theta + 1 = \\ \Big(\cos\big((n+1)\theta\big)\cos\big((n-1)\theta\big) - \cos^2(n\theta) - \cos^2\theta + 1\Big) + \\ i\Big(\sin\big((n+1)\theta\big)\cos\big((n-1)\theta\big) - \sin(n\theta)\cos(n\theta) - \sin\theta\cos\theta\Big). \end{gathered}$$

   Le reste n'est plus qu'une affaire de formules de trigonométrie :

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

   En faisant les bonnes sommes et différences des relations précédentes, on trouve bien que

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

2. C'est fois, on a affaire à une racine d'ordre 2, et il suffit de prouver que 1 est racine de $P(X) = nX^{n+1} - (n+1)X^n + 1$ et de $P'(X) = n(n+1)X^n - n(n+1)X^{n-1}$, ce qui est évident... Pour justifier cela, on peut faire appel à la partie du cours consacrée aux racines, ou partir de la division euclidienne

$$nX^{n+1} - (n+1)X^n + 1 = Q(X)(X-1)^2 + aX + b.$$

   Faire $X = 1$ dans la relation précédente donne $a + b = 0$. De plus, si on dérive la relation précédente et qu'on fait à nouveau $X = 1$, on obtient $a = 0$.

Exercice 18.

Soient $A, B, P \in \mathbb{K}[X]$ avec P non-constant. On suppose que $A \circ P | B \circ P$. Démontrer que $A | B$.

Correction.

On écrit la division euclidienne de B par A, $B = AQ + R$ avec $\deg(R) < \deg(A)$. On compose alors par P, et on obtient $B \circ P = (A \circ P) \times (Q \circ P) + R \circ P$. Or, le polynôme $A \circ P$ a pour degré $\deg(A) \times \deg(P)$. Le polynôme $R \circ P$ a pour degré $\deg(R) \times \deg(P)$. On en déduit que $\deg(R \circ P) < \deg(A \circ P)$ et donc que $B \circ P = (A \circ P) \times (Q \circ P) + R \circ P$ est la division euclidienne de $B \circ P$ par $A \circ P$. Mais on sait que $A \circ P | B \circ P$ et donc on en déduit que $R \circ P$ est égal à 0. Ceci n'est possible que si $R = 0$, et donc $A|B$.

Exercice 19.

Déterminer les polynômes $P \in \mathbb{R}_3[X]$ tels que $(X-1)^2$ divise $P(X)+1$ et $(X+1)^2$ divise $P(X)-1$.

Correction.

On commence par remarquer que les polynômes $(X-1)^2$ et $(X+1)^2$ sont premiers entre eux, une relation de Bezout entre eux étant obtenue par la formule

$$\left(\frac{X}{4} + \frac{1}{2}\right)(X-1)^2 + \left(\frac{-X}{4} + \frac{1}{2}\right)(X+1)^2 = 1.$$

On doit résoudre le système de "congruence" suivant :

$$\begin{cases} P(X) & \equiv & -1 \ [(X-1)^2] \\ P(X) & \equiv & 1 \ [(X+1)^2] \end{cases}$$

La première équation donne $P(X) = -1 + U(X)(X-1)^2$, et, en reportant dans la deuxième équation, on trouve

$$U(X)(X-1)^2 \equiv 2 \ [(X+1)^2].$$

On multiplie alors les deux membres par $(X/4 + 1/2)$, qui est tel que $(X/4+1/2)(X-1)^2 \equiv 1 \ [(X+1)^2]$. On en déduit

$$U(X) \equiv (X/2+1) \ [(X+1)^2] \implies U(X) = (X/2+1) + V(X)(X+1)^2.$$

Les solutions du système de congruence sont donc les polynômes de la forme

$$P(X) = -1 + (X/2+1)(X-1)^2 + V(X)(X-1)^2(X+1)^2,$$

où V est un polynôme quelconque. La seule solution dans $\mathbb{R}_3[X]$ est

$$P(X) = \frac{X^3}{2} - \frac{3X}{2}.$$

Exercice 20.

Dans cet exercice, on souhaite déterminer toutes les racines de polynômes de degré 3 ou 4 connaissant des informations sur ces racines.

1. Soit $P(X) = X^3 - 8X^2 + 23X - 28$. Déterminer les racines de P sachant que la somme de deux des racines est égale à la troisième.

2. Soit $Q(X) = X^4 + 12X - 5$. On note x_1, x_2, x_3, x_4 les racines de Q. On sait que $x_1 + x_2 = 2$.
   (a) Déterminer la valeur de x_1x_2, x_3x_4 et $x_3 + x_4$.
   (b) En déduire les valeurs des racines.

Correction.

1. Notons x_1, x_2 et x_3 les trois racines, avec par exemple $x_3 = x_1 + x_2$. Alors les relations coefficients/racine nous disent que $x_1+x_2+x_3 = 8$. En particulier, on trouve $x_3 = 4$, et donc P se factorise en $P(X) = (X-4)Q(X)$. La division euclidienne donne $Q(X) = X^2-4X+7$, dont les racines sont $2 + i\sqrt{3}$ et $2 - i\sqrt{3}$.
2. (a) On va utiliser les relations coefficients/racines. Pour cela, on développe

$$(X - x_1)(X - x_2)(X - x_3)(X - x_4) =$$

$$X^4 - (x_1 + x_2 + x_3 + x_4)X^3 + (x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4)X^2 -$$

$$(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4)X + x_1x_2x_3x_4.$$

On sait que

$$\sigma_1 = x_1 + x_2 + x_3 + x_4 = 0 \implies x_3 + x_4 = -2.$$

De plus,

$$\sigma_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = 0.$$

On peut réécrire ceci en

$$x_1x_2 + x_3x_4 + (x_1 + x_2)(x_3 + x_4) = 0$$

soit

$$x_1x_2 + x_3x_4 = 4.$$

On a également

$$\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = -12.$$

Ceci donne

$$x_1x_2(x_3 + x_4) + x_3x_4(x_1 + x_2) = -12 \implies x_1x_2 - x_3x_4 = 6.$$

Ceci suffit à déterminer $x_1x_2 = 5$ et $x_3x_4 = -1$.

   (b) De $x_1 + x_2 = 2$ et $x_1x_2 = 5$, on tire que x_1 et x_2 sont les racines de $X^2 - 2X + 5$, ie $1 \pm 2i$. De même, x_3 et x_4 sont les racines de $X^2 + 2X - 1$, ie $-1 \pm \sqrt{2}$.

Exercice 21.

Soit P un polynôme de $\mathbb{R}[X]$ de degré n ayant n racines réelles distinctes.

1. Démontrer que toutes les racines de P' sont réelles.
2. En déduire que le polynôme $P^2 + 1$ n'admet que des racines simples.
3. Reprendre les questions si l'on suppose simplement que toutes les racines de P sont réelles.

Correction.

1. Soient $\alpha_1 < \cdots < \alpha_n$ les racines de P. Alors, la fonction polynômiale $x \mapsto P(x)$ est continue et dérivable sur chaque $[\alpha_i, \alpha_{i+1}]$ et s'annule aux bornes de cet intervalle. Par le théorème de Rolle, on en déduit l'existence de $\beta_i \in]\alpha_i, \alpha_{i+1}[$ tel que $P'(\beta_i) = 0$. Les réels $\beta_1, \ldots, \beta_{n-1}$ sont alors distincts et sont des zéros de P'. Comme P' est de degré $n-1$, on a trouvé toutes les racines de P'.
2. On commence par remarquer que les racines de P^2+1 sont nécessairement complexes, ce polynôme étant supérieur ou égal à 1 sur $\mathbb{R}$. De plus, sa dérivée est $2PP'$, dont les racines sont toutes réelles par hypothèse et d'après le résultat de la question précédente. Ainsi, P^2+1 et son polynôme dérivé n'ont pas de racines communes. Toutes les racines de P^2+1 sont donc simples.
3. Il suffit de prouver que toutes les racines de P' sont réelles, et on obtiendra par le même raisonnement le résultat de la question 2. Il faut cette fois tenir compte de l'ordre de multiplicité des racines. Ainsi, notons $\alpha_1, \ldots, \alpha_p$ les racines de P, α_i étant de multiplicité m_i. On sait que $m_1 + \cdots + m_p = n$. Chaque α_i reste racine de P', de multiplicité $m_i - 1$ (avec l'abus de langage qu'une racine de multiplicité 0 n'est plus une racine...). De plus, le théorème de Rolle nous donne des nouvelles racines $\beta_1, \ldots, \beta_{p-1}$, avec $\beta_i \in]\alpha_i, \alpha_{i+1}[$. La somme des multiplicités des racines de P' que l'on a trouvé est donc :

$$\sum_{i=1}^{p}(m_i - 1) + (p-1) = n - p + p - 1 = n - 1.$$

Puisque P' est de degré $n-1$, on a trouvé toutes les racines de P' qui sont donc réelles.

Exercice 22.

Soit P un polynôme de $\mathbb{C}_n[X]$. Soient $\alpha_1, \ldots, \alpha_n$ les racines de P, d'images respectives dans le plan complexe $A_1, \ldots, A_n$. Soient $\beta_1, \ldots, \beta_{n-1}$ les racines de P', d'images respectives dans le plan complexe $B_1, \ldots, B_{n-1}$.

1. Montrer que les familles de points $(A_1, \ldots, A_n)$ et $(B_1, \ldots, B_{n-1})$ ont même isobarycentre.
2. Quelle est l'image dans la plan complexe de la racine de $P^{(n-1)}$?

Correction.

1. On peut toujours supposer que P est unitaire. On l'écrit donc $P(X) = X^n + a_{n-1}X^{n-1} + \ldots$. Les relations coefficients/racines donnent

$$-a_{n-1} = \alpha_1 + \cdots + \alpha_n.$$

P' s'écrit $P'(X) = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots$. Les relations coefficients/racines donnent cette fois

$$\frac{-(n-1)a_{n-1}}{n} = \beta_1 + \cdots + \beta_{n-1}.$$

Mettant ensemble ces deux équations, on voit facilement que

$$\frac{\alpha_1 + \cdots + \alpha_n}{n} = \frac{\beta_1 + \cdots + \beta_{n-1}}{n-1},$$

ce qui est la relation désirée.

2. Par récurrence, P, P', P'', $\dots$, $P^{(n-1)}$ sont tels que la famille de leurs racines respectives ont même isobarycentre. En particulier, $P^{(n-1)}$ n'a qu'une seule racine qui est l'isobarycentre des racines de P.

Exercice 23.

Soit P le polynôme $X^4 - 6X^3 + 9X^2 + 9$.

1. Décomposer $X^4 - 6X^3 + 9X^2$ en produit de facteurs irréductibles dans $\mathbb{R}[X]$.
2. En déduire une décomposition de P en produit de facteurs irréductibles dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$.

Correction.

1. On écrit simplement
$$X^4 - 6X^3 + 9X^2 = X^2(X^2 - 6X + 9) = X^2(X-3)^2.$$
2. L'astuce(?) est d'écrire $9 = -(3i)^2$, et de reconnaitre une différence de deux carrés. Donc on a :
$$\begin{aligned} X^4 - 6X^3 + 9X^2 + 9 &= \big(X(X-3)\big)^2 - (3i)^2 \\ &= \big(X(X-3) - 3i\big)\big(X(X-3) + 3i\big) \\ &= (X^2 - 3X - 3i)(X^2 - 3X + 3i). \end{aligned}$$
On factorise chacun de ces deux polynômes. Le discriminant du premier est $9 + 12i = (\sqrt{3}(2+i))^2$. Ses racines sont $\alpha_1 = \frac{3}{2} + \sqrt{3} + \frac{i\sqrt{3}}{2}$ et $\alpha_2 = \frac{3}{2} - \sqrt{3} - \frac{i\sqrt{3}}{2}$. Le discriminant du second est $9 - 12i = (\sqrt{3}(2-i))^2$, et ses racines sont $\beta_1 = \frac{3}{2} + \sqrt{3} - \frac{i\sqrt{3}}{2}$ et $\beta_2 = \frac{3}{2} - \sqrt{3} + \frac{i\sqrt{3}}{2}$. La décomposition de P en produit d'irréductibles de $\mathbb{C}[X]$ est donc
$$(X - \alpha_1)(X - \alpha_2)(X - \beta_1)(X - \beta_2).$$
Pour obtenir la décomposition en produit d'irréductibles de $\mathbb{R}[X]$, on regroupe les racines complexes conjuguées, à savoir α_1 et β_1 d'une part et α_2 et β_2 d'autre part. On trouve
$$P = \big(X^2 - (2\sqrt{3} + 3)X + 3\sqrt{3} + 6\big)\big(X^2 + (2\sqrt{3} - 3)X - 3\sqrt{3} + 6\big).$$

Exercice 24.

On considère les deux polynômes suivants :
$$P(X) = X^3 - 9X^2 + 26X - 24 \text{ et } Q(X) = X^3 - 7X^2 + 7X + 15.$$
Décomposer ces deux polynômes en produits d'irréductibles de $\mathbb{R}[X]$, sachant qu'ils ont une racine commune.

Correction.

Si a est une racine commune de P et Q, alors $X-a$ divise le pgcd de P et de Q. On commence donc par chercher ce pgcd, par exemple en appliquant l'algorithme d'Euclide. Ici, on a

$$\begin{aligned} X^3-9X^2+26X-24 &= X^3-7X^2+7X+15+(-2X^2+19X-39) \\ X^3-7X^2+7X+15 &= (-2X^2+19X-39)(-X/2-5/4)+(45X/4-135/4) \\ -2X^2+19X-39 &= (45X/4-135/4)(-8X/45+52/45) \end{aligned}$$

Le pgcd de P et Q est donc $45X/4-135/4$, ou encore $X-3$. On divise alors P et Q par $X-3$, et on trouve :

$$P(X)=(X-3)(X^2-6X+8) \text{ et } Q(X)=(X-3)(X^2-4X-5).$$

On factorise encore chacun des polynômes de degré 2 pour trouver finalement :

$$P(X)=(X-3)(X-2)(X-4) \text{ et } Q(X)=(X+1)(X-3)(X-5).$$

On aurait aussi pu factoriser ces polynômes en cherchant des racines évidentes de chacun...

Exercice 25.

1. Rappeler la décomposition en produits d'irréductibles de X^n-1.
2. En déduire la décomposition en produits d'irréductibles de $1+X+\cdots+X^{n-1}$.
3. Calculer $\prod_{k=1}^{n-1}\sin\left(\frac{k\pi}{n}\right)$.
4. Pour $\theta\in\mathbb{R}$, calculer $\prod_{k=0}^{n-1}\sin\left(\frac{k\pi}{n}+\theta\right)$.

Correction.

1. Les racines de ce polynôme sont les racines n-ièmes de l'unité. On en déduit que
$$X^n-1=\prod_{k=0}^{n-1}\left(X-e^{\frac{2ik\pi}{n}}\right).$$
2. On a $(1+X+\cdots+X^{n-1})(X-1)=X^n-1$. On en déduit que
$$1+X+\cdots+X^{n-1}=\prod_{k=1}^{n-1}\left(X-e^{\frac{2ik\pi}{n}}\right).$$
3. On va évaluer la factorisation précédente en 1. On trouve
$$n=\prod_{k=1}^{n-1}\left(1-e^{\frac{2ik\pi}{n}}\right).$$
Or,
$$1-e^{\frac{2ik\pi}{n}}=-2ie^{\frac{ik\pi}{n}}\sin\left(\frac{k\pi}{n}\right)=2(-1)e^{\frac{i\pi}{2}}e^{\frac{ik\pi}{n}}\sin\left(\frac{k\pi}{n}\right).$$

On effectue le produit et on trouve :

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

On en déduit que

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

4. La méthode est parfaitement similaire, mais cette fois on part de la factorisation de X^n-1 que l'on évalue en -2θ. On trouve d'une part

$$e^{-2ni\theta}-1=(-2i)e^{-in\theta}\sin(n\theta)$$

et d'autre part

$$\begin{aligned}\prod_{k=0}^{n-1}\left(e^{-2i\theta}-e^{\frac{2ik\pi}{n}}\right) &= \prod_{k=0}^{n-1}(-2i)e^{\frac{ik\pi}{n}-\theta}\sin\left(\frac{k\pi}{n}+\theta\right)\\ &= (-2i)2^{n-1}\prod_{k=0}^{n-1}\sin\left(\frac{k\pi}{n}+\theta\right).\end{aligned}$$

On conclut finalement que

$$\prod_{k=0}^{n-1}\sin\left(\frac{k\pi}{n}+\theta\right)=\frac{\sin(n\theta)}{2^{n-1}}.$$

3. Exercices d'approfondissement

Exercice 26.

Déterminer les couples (A,B) de polynômes non nuls de $\mathbb{R}[X]$ tels que le quotient et le reste dans la division euclidienne de A par B et dans la division euclidienne de B par A soient identiques.

Correction.

Procédons par analyse-synthèse. Supposons donc que la propriété est vraie. Il existe alors un polynôme Q et un polynôme R avec $\deg(R)<\min(\deg(A),\deg(B))$ tel que $A=BQ+R$ et $B=AQ+R$. Mais alors, on a aussi

$$\begin{aligned}A=(AQ+R)Q+R=AQ^2+RQ+R &\iff A(1-Q^2)-R(1+Q)=0\\ &\iff A(Q+1)(1-Q)-R(1+Q)=0\\ &\iff (Q+1)\big(A(1-Q)-R\big)=0.\end{aligned}$$

Si le produit de deux polynômes est nul, c'est que l'un de ces deux polynômes est nul. Ainsi, on

a ou bien $1+Q=0$ ou bien $A(1-Q)-R=0$. On distingue donc deux cas

— Si $Q=-1$, alors $A=-B+R$ et $B=-A+R$. Autrement dit, il existe deux polynômes $P,R\in\mathbb{R}[X]$ avec $\deg(R)<\deg(P)$ tels que $A=P+R$ et $B=-P+R$.

— Si $Q\neq -1$, alors $A(1-Q)-R=0$. Pour des considérations de degré (rappelons que $\deg(R)<\deg(A)$), ceci n'est possible que si $Q=1$ et $R=0$. On obtient alors le cas trivial $A=B$.

Passons à la synthèse. Supposons que $A=B$ ou qu'il existe un couple de polynômes (P,R) de $\mathbb{R}[X]$ avec $\deg(R)<\deg(P)$ tels que $A=P+R$ et $B=-P+R$. Alors les divisions euclidiennes de A par B et de B par A ont bien même quotient et même reste. On a donc démontré que l'ensemble des couples solutions est

$$\mathcal{S}=\{(P,P);\ P\in\mathbb{R}[X]\}\cup\{(P+R,-P+R);\ P,R\in\mathbb{R}[X],\ \deg(R)<\deg(P)\}.$$

Exercice 27.

Soient n, p deux entiers naturels non nuls et soit $P(X)=\sum_{k=0}^{n}a_kX^k$ un polynôme de $\mathbb{C}[X]$. Pour chaque $k\in\{0,\dots,n\}$, on note r_k le reste de la division euclidienne de k par p. Démontrer que le reste de la division euclidienne de P par X^p-1 est le polynôme $R(X)=\sum_{k=0}^{n}a_kX^{r_k}$.

Correction.

On va démontrer que X^p-1 divise $P-R$. En effet, le degré de R est inférieur strict à p, et R sera bien le reste dans la division euclidienne de P par X^p-1. On écrit alors que

$$P-R=\sum_{k=0}^{n}a_k(X^k-X^{r_k}),$$

et il suffit de prouver que X^p-1 divise chaque $X^k-X^{r_k}$. Écrivons alors $k=mp+r_k$, d'où l'on tire

$$X^k-X^{r_k}=X^{r_k}(X^{mp}-1)=X^{r_k}(X^p-1)(1+X^p+\cdots+X^{(m-1)p}).$$

X^p-1 divise bien $P-R$!

Exercice 28.

Soient $n,m\geq 1$. Déterminer le pgcd de X^n-1 et X^m-1.

Correction.

Une idée possible est d'appliquer l'algorithme d'Euclide pour calculer le pgcd de ces deux polynômes. On suppose par exemple $n>m$, et on écrit $n=mq+r$, avec $0\leq r<m$. Alors on a :

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

Le point crucial est que $X^{mp}-1$ est divisible par X^m-1. En effet,

$$X^{mp}-1=(X^m-1)(X^{m(p-1)}+X^{m\left((p-1)-1\right)}+\cdots+X^m+1).$$

Ainsi, $\text{pgcd}(X^n-1, X^m-1) = \text{pgcd}(X^m-1, X^r-1)$. Mais puisque $\text{pgcd}(n,m) = \text{pgcd}(m,r)$, on en déduit finalement que

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

Exercice 29.

1. Soit $P \in \mathbb{R}[X]$ vérifiant $P(X^2) = P(X-1)P(X+1)$.
   (a) Démontrer que si z est racine de P, il existe une racine de P de module supérieur strict à z.
   (b) En déduire les polynômes $P \in \mathbb{R}[X]$ solutions.
2. Soit $P \in \mathbb{R}[X]\backslash\{0\}$ vérifiant $P(X^2) = P(X)P(X-1)$.
   (a) Démontrer que si z est racine de P, alors $z = j$ ou $z = j^2$.
   (b) En déduire les polynômes $P \in \mathbb{R}[X]$ solution.

Correction.

1. (a) Soit z une racine de P. L'équation vérifiée par P s'écrit aussi $P\big((X+1)^2\big) = P(X)P(X+2)$, et donc $(z+1)^2$ est aussi racine de P. De même, $(z-1)^2$ est aussi racine de P. On va prouver qu'au moins un des deux nombres complexes $(z+1)^2$ ou $(z-1)^2$ est de module supérieur strict à z. En effet, $(z+1)^2 - (z-1)^2 = 4z$, et donc

   $$4|z| \leq |z+1|^2 + |z-1|^2.$$

   Ainsi, l'un de ces deux nombres complexes est de module supérieur ou égal à $2|z|$. Si $|z| \neq 0$, le résultat est prouvé. Sinon, si $z = 0$, le résultat est trivial.

   (b) Si P admet une racine (complexe), alors il en admet d'après la question précédente une infinité. C'est donc le polynôme nul. Les polynômes qui sont solutions de l'équation ne peuvent donc être que des polynômes constants, et les seuls polynômes constants solutions sont les polynômes $P(X) = 0$ et $P(X) = 1$.

2. (a) En raisonnant comme dans le premier cas, on voit que si z est racine de P, alors z^2 et $(z+1)^2$ sont aussi des racines de P. Par récurrence, z^{2n} et $(z+1)^{2n}$ seront racines pour tout entier n. Puisque le polynôme n'admet qu'un nombre fini de racines, les suites $(z^{2n})_n$ et $\big((z+1)^{2n}\big)_n$ ne peuvent prendre qu'un nombre fini de valeurs. Le premier point nous dit qu'on a nécessairement $z = 0$ ou $|z| = 1$. On note Γ_1 cet ensemble. Le second point nous dit que $z = -1$ ou $|z+1| = 1$, ensemble que l'on note Γ_2. Il est facile de vérifier (par exemple, en dessinant ses ensembles), que les points d'intersection de Γ_1 et Γ_2 sont $0, -1, j$ et j^2. Mais si $z = 0$ est racine, alors $(z+1)^2 = 1$ est aussi racine, ce qui n'est pas possible. De même, si $z = -1$ est racine, alors $(z+1)^2 = 0$ est racine, ce qui n'est pas (plus) possible. Donc les seules racines de P sont j et j^2.

   (b) Puisque P est à coefficients réels, j et j^2, qui sont des complexes conjugués, doivent être des racines de même multiplicité. On doit donc avoir $P(X) = \lambda(X-j)^n(X-j^2)^n = \lambda(X^2+X+1)^n$. Par identification des coefficients dominants, on trouve $\lambda = 1$. Réciproquement, on vérifie facilement que les polynômes $P(X) = (X^2+X+1)^n$ sont solutions de l'équation.

Exercice 30.

Soit, pour $n \geq 0$, $P_n(X) = \sum_{k=0}^{n} \frac{X^k}{k!}$.

1. Démontrer que P_n admet n racines simples complexes.
2. Démontrer que, si n est impair, une et une seule de ces racines est réelle, et que si n est pair, aucune des racines n'est réelle.

Correction.

1. Il suffit de prouver que P_n et P_n' n'ont pas de racines communes. Mais $P_n' = P_{n-1}$ et donc, $P_n(X) = P_n'(X) + \frac{X^n}{n!}$. Ainsi, si $P_n'(a) = 0$, alors $P_n(a) = \frac{a^n}{n!}$, et ceci ne peut être nul que si $a = 0$. Reste à voir que $P_n(0)$ n'est jamais nul. Mais c'est clair car $P_n(0) = 1$.
2. On va prouver par récurrence la proposition suivante :
   $\mathcal{P}_n$:
   — si n est pair, alors P_n n'admet pas de racines réelles ;
   — si n est impair, alors P_n admet une seule racine réelle a_n. De plus, $P_n(x) < 0$ pour $x < a_n$ et $P_n(x) > 0$ pour $x > a_n$.

Exercice 31.

1. Déterminer tous les polynômes $P \in \mathbb{C}[X]$ tels que $P(\mathbb{C}) \subset \mathbb{R}$.
2. Déterminer tous les polynômes $P \in \mathbb{C}[X]$ tels que $P(\mathbb{R}) \subset \mathbb{R}$.
3. Soit $P \in \mathbb{C}[X]$. Démontrer que $P(\mathbb{Q}) \subset \mathbb{Q}$ si et seulement si $P \in \mathbb{Q}[X]$.

Correction.

1. Il est clair que si $P(X) = a$, avec $a \in \mathbb{R}$, alors P est solution. Si P n'est pas constant, alors le polynôme $Q(X) = P(X) - i$ n'est pas constant lui aussi. D'après le théorème de d'Alembert-Gauss, il s'annule. En particulier, il existe $z \in \mathbb{C}$ tel que $P(z) = i$, et donc on n'a pas $P(\mathbb{C}) \subset \mathbb{R}$. Ainsi, les polynômes solutions sont les polynômes constants, avec une constante réelle.
2. Les polynômes à coefficients réels sont bien entendu solutions. De plus, si $x \in \mathbb{R}$, alors puisque $P(x) \in \mathbb{R}$, on a
$$P(x) = \overline{P(x)} = \overline{P}(x).$$
Ainsi, le polynôme $P - \overline{P}$ admet une infinité de racine. Ce ne peut être que le polynôme nul. Mais les coefficients de $P - \overline{P}$ sont ($2i$-fois) les parties imaginaires des coefficients de P. Ainsi, tous les coefficients de P ont une partie imaginaire nulle. C'est bien que P est un élément de $\mathbb{R}[X]$.
3. Il est clair que si $P \in \mathbb{Q}[X]$, alors $P(\mathbb{Q}) \subset \mathbb{Q}$. Réciproquement soit $P \in \mathbb{C}[X]$ tel que $P(\mathbb{Q}) \subset \mathbb{Q}$. Soit d le degré de P et oit $(L_0, \ldots, L_d)$ la famille des polynômes de Lagrange associée aux entiers $(0, \ldots, d)$. Alors la formule donnant ces polynômes nous dit qu'ils sont à coefficients dans $\mathbb{Q}$. De plus, on a
$$P(X) = \sum_{k=0}^{d} P(k) L_k(X).$$
P est bien à coefficients dans $\mathbb{Q}$.

Exercice 32.

On note

$$\mathcal{S} = \{P \in \mathbb{R}[X];\ \exists P_1, P_2 \in \mathbb{R}[X];\ P = P_1^2 + P_2^2\}.$$

1. Montrer que $\mathcal{S}$ est stable par produit. On pourra considérer l'application $\phi : \mathbb{C}[X] \to \mathbb{R}[X]$, $P \mapsto P\bar{P}$.
2. Soit $P \in \mathbb{R}[X]$ tel que $P(x) \geq 0$ pour tout $x \in \mathbb{R}$. Montrer qu'il existe $A, B \in \mathbb{R}[X]$ tels que $P = A^2 + B^2$.

Correction.

1. Cela suit directement de l'identité suivante, très simple à vérifier (mais moins à trouver !) :

$$(P_1^2 + P_2^2)(Q_1^2 + Q_2^2) = (P_1Q_2 + P_2Q_2)^2 + (P_1Q_1 - P_2Q_1)^2.$$

On peut la retrouver grâce à l'indication. En effet, si $P = P_1 + iP_2$ et $Q = Q_1 + iQ_2$, alors

$$\phi(P)\phi(Q) = \phi(PQ)$$

et les deux membres de l'égalité correspondent à l'égalité écrite ci-dessus.

2. Décomposons P en produits de facteurs irréductibles :

$$P(X) = \lambda \prod_{i=1}^{m} (X - a_i)^{m_i} \prod_{j=1}^{p} (X^2 + \alpha_j X + \beta_j)$$

où chaque polynôme $X^2 + \alpha_j X + \beta_j$ est de discriminant négatif. Puis P est toujours positif, il est clair que $\lambda \geq 0$ et que chaque m_i est pair (sinon P changerait de signe au voisinage de a_i et donc ne pourrait pas être positif partout). D'après la question précédente, il suffit de vérifier que chaque terme intervenant dans la décomposition précédente est une somme de deux carrés. Écrivant $\lambda = \mu^2$, on obtient $\lambda = \mu^2 + 0^2$. D'autre part, posons $m_i = 2n_i$ et $A_i = (X - a_i)^{n_i}$. Alors $(X - a_i)^{m_i} = A_i^2 + 0^2$. Reste à traiter les polynômes du type $X^2 - \alpha X + \beta$, de discriminant négatif. L'idée est d'utiliser la forme canonique de ces polynômes. En effet, on a

$$X^2 + \alpha X + \beta = \left(X + \frac{\alpha}{2}\right)^2 + \frac{4\beta - \alpha^2}{4}.$$

Puisque le discriminant est négatif, on peut poser

$$\gamma = \sqrt{\frac{4\beta - \alpha^2}{4}}$$

et on a alors

$$X^2 + \alpha X + \beta = \left(X + \frac{\alpha}{2}\right)^2 + \gamma^2.$$

Ce terme est aussi somme de deux carrés.

Exercice 33.

On dit qu'un polynôme $P \in \mathbb{C}[X]$ de degré n est réciproque s'il s'écrit $P = a_n X^n + \cdots + a_0$ avec $a_k = a_{n-k}$ pour tout k dans $\{0, \ldots, n\}$.

1. Soit $P \in \mathbb{C}[X]$ de degré n. Démontrer que P est réciproque si et seulement si $P(X) = X^n P\left(\frac{1}{X}\right)$.
2. Montrer qu'un produit de polynômes réciproques est réciproque.
3. On suppose que P et Q sont réciproques et que $Q|P$. Démontrer que $\frac{P}{Q}$ est réciproque.
4. Soit $P \in \mathbb{C}[X]$ un polynôme réciproque.
   a. Démontrer que si α est une racine de P, alors $\alpha \neq 0$ et α^{-1} est une racine de P.
   d. Démontrer que si 1 est une racine de P, alors sa multiplicité est supérieure ou égale à 2.
   c. Démontrer que si le degré de P est impair, alors -1 est racine de P.
   d. Démontrer que si P est de degré pair et si -1 est une racine de P, alors sa multiplicité est supérieure ou égale à 2.
5. Démontrer que tout polynôme réciproque de $\mathbb{C}[X]$ de degré $2n$ se factorise en

$$P = a_{2n}(X^2 + b_1 X + 1)\dots(X^2 + b_n X + 1).$$

   Que peut-on dire si le degré de P est impair ?

Correction.

1. Soit $P = a_n X^n + \cdots + a_0$, alors

$$X^n P\left(\frac{1}{X}\right) = a_0 X^n + \cdots + a_n.$$

   Ainsi, si P est réciproque, on a bien $X^n P(1/X) = P(X)$. Réciproquement, si $X^n P(1/X) = P(X)$, alors on a nécessairement $a_0 = a_n$, $a_1 = a_{n-1}$, etc... Donc P est réciproque.
2. Soient P et Q réciproques, de degrés respectifs n et m. Alors

$$X^n P(1/X) = P(X) \text{ et } X^m Q(1/X) = Q(X).$$

   On en déduit que

$$X^{n+m}(PQ)(1/X) = X^n P(1/X) X^m Q(1/X) = P(X)Q(X) = (PQ)(X).$$

   Ainsi, d'après la question précédente, PQ est réciproque.
3. Le raisonnement est complètement identique, en utilisant le quotient au lieu du produit !
4. (a) Puisque P est réciproque, $a_0 = a_n \neq 0$ et donc $P(0) = a_0 \neq 0$. D'autre part, si α est racine de P, alors la relation $P(\alpha) = \alpha^n P(\alpha^{-1})$ prouve que α^{-1} est aussi racine de P.
   (b) Dérivons la relation de la première question. On trouve, pour tout $x \neq 0$,

$$P'(x) = nx^{n-1}P(1/x) - x^{n-2}P'(1/x).$$

   On évalue en 1, et on trouve

$$P'(1) = -P'(1)$$

   et donc $P'(1) = 0$. On en déduit que 1 est racine au moins double.
   (c) On utilise encore le résultat de la première question, et on remarque que $P(-1) = -P(-1)$ puisque le degré de P est impair. Donc $P(-1) = 0$.

(d) On raisonne exactement comme deux questions plus haut.

5. On va procéder par récurrence sur n, le cas $n = 1$ étant trivial. Supposons donc que le résultat a été démontré pour tout polynôme réciproque de degré $2n$, et prouvons-le pour un polynôme réciproque P de degré $2n + 2$. Soit α une racine de P. Alors, on sait que $\alpha \neq 0$ et que α^{-1} est aussi racine de P. Si $\alpha \neq 1, -1$, $\alpha^{-1} \neq \alpha$ et on peut factoriser P par $(X-\alpha)(X-\alpha^{-1})$. Or, il est facile de vérifier que $(X-\alpha)(X-\alpha^{-1})$ s'écrit $(X^2+b_{n+1}X+1)$. D'autre part, si $\alpha = 1$ ou $\alpha = -1$, alors α est racine de multiplicité au moins deux, et on peut factoriser par $(X-\alpha)^2$. Un tel polynôme s'écrit encore $(X^2+b_{n+1}X+1)$. Donc, dans tous les cas, en notant $Q = X^2 + b_{n+1}X + 1$, on a $Q|P$ et P, Q réciproques. On en déduit que $\frac{P}{Q}$ est réciproque, de degré $2n$, donc par l'hypothèse de récurrence s'écrit

$$\frac{P}{Q} = a_{2n+2}(X^2 + b_1X + 1)\dots(X^2 + b_nX + 1).$$

On remultiplie par Q, et on a bien prouvé que le résultat est vrai au rang $n+1$. Si maintenant P est réciproque de degré impair $2n + 1$, alors -1 est racine de P et P se factorise par le polynôme réciproque $Q = X + 1$. Donc $\frac{P}{Q}$ est réciproque de degré pair $2n$, donc s'écrit $a_{2n+1}(X^2 + b_1X + 1)\dots(X^2 + b_nX + 1)$. Ainsi, tout polynôme réciproque de degré impair $2n + 1$ se factorise en

$$P = a_{2n+1}(X + 1)(X^2 + b_1X + 1)\dots(X^2 + b_nX + 1).$$

Exercice 34.

Soit A une algèbre commutative intègre de dimension finie $n \geq 2$ sur $\mathbb{R}$. On identifie $\mathbb{R}$ avec $\mathbb{R}.1$, où 1 est l'élément neutre de A pour la multiplication.

1. Démontrer que tout $a \in A$ non-nul est inversible.
2. Soit $a \in A$ et non dans $\mathbb{R} = \text{vect}(1)$. Prouver que la famille $(1, a)$ est libre, tandis que la famille $(1, a, a^2)$ est liée.
3. En déduire l'existence de $i \in \text{vect}(1, a)$ tel que $i^2 = -1$.
4. En déduire que $\dim(A) = 2$.
5. En déduire que A est isomorphe à $\mathbb{C}$.

Correction.

1. Soit $a \in A\backslash\{0\}$. Alors $\phi : A \to A,\ x \mapsto ax$ est une application linéaire si l'on voit A comme un $\mathbb{R}$-espace vectoriel. Elle est injective, car A est intègre et donc son noyau est réduit à $\{0\}$. Comme A est de dimension finie, l'application est bijective. Il existe $x \in A$ tel que $ax = 1$, ce qui prouve que a est inversible.
2. 1 et a sont non-nuls et $a \notin \text{vect}(1)$. Donc $(1, a)$ est libre. Maintenant, puisque A est de dimension finie n, la famille $(1, a, a^2, \dots, a^n)$ qui est constituée par $n+1$ vecteurs est liée. Il existe un polynôme $P \in \mathbb{R}_n[X]$ tel que $P(a) = 0$. On factorise P en produit d'irréductibles, $P = P_1 \cdots P_r$. Alors
$$P_1(a) \cdots P_r(a) = 0.$$
Puisque A est intègre, il existe un k tel que $P_k(a) = 0$. Mais P_k est de degré au plus 2, et il ne peut pas être de degré 1 puisque $(1, a)$ est libre. Donc P_k est de degré 2 et $(1, a, a^2)$ est

liée.

3. Soient α, β tels $a^2 + \alpha a + \beta = 0$, avec $\Delta = \alpha^2 - 4\beta < 0$ (conséquence de la question précédente). On a alors
$$\left(a + \frac{\alpha}{2}\right)^2 = \frac{\alpha^2 - 4\beta}{4}$$
ce qui entraîne
$$\left(\frac{2a + \alpha}{\sqrt{4\beta - \alpha^2}}\right)^2 = -1.$$
On a trouvé notre i !
4. Si $\dim(A) > 2$, on pourrait trouver b tel que la famille $(1, a, b)$ soit libre. Comme à la question précédente, on trouverait $j \in \text{vect}(1, b)$ tel que $j^2 = -1$. Mais alors,
$$(i - j)(i + j) = 0$$
et par intégrité de A, un des deux facteurs doit être nul. Dans un cas comme dans l'autre, cela implique $j \in \text{vect}(1, a)$ et donc $b \in \text{vect}(1, a)$, puisque qu'on peut aussi dire que $b \in \text{vect}(1, j)$. C'est une contradiction, et donc la dimension de A est deux.
5. L'isomorphisme est donné par $1_A \mapsto 1_{\mathbb{C}}$ et $i_A \mapsto i_{\mathbb{C}}$, dont on vérifie facilement que c'est un morphisme d'algèbre.