POLYNÔMES

♦ ***Exercice 1.*** [○]
La valuation d'un polynôme P, notée $\mathrm{val}(P)$, est le degré du monôme (non nul) de plus petit degré dans P (avec la convention $\mathrm{val}(0) = +\infty$). Par exemple $\mathrm{val}(X^{1975} - X^{17}) = 17$.

Démontrer que, pour tous P, Q dans $K[X]$, on a

$$\mathrm{val}(P+Q) \geqslant \min\{\mathrm{val}(P)\,;\,\mathrm{val}(Q)\} \qquad \text{et} \qquad \mathrm{val}(PQ) = \mathrm{val}(P) + \mathrm{val}(Q).$$

Les deux résultats sont évidents si l'un des deux polynômes est nul. On suppose donc que P et Q sont non nuls.

On écrit P et Q sous la forme $P = \sum_{j=u}^{+\infty} a_j X^j$ et $Q = \sum_{j=v}^{+\infty} b_j X^j$ avec $u = \mathrm{val}(P)$, $v = \mathrm{val}(Q)$ et les suites (a_n) et (b_n) qui sont stationnaires à la valeur 0 à partir d'un certain rang.

Pour le produit, on a

$$PQ = \sum_{k=u+v}^{+\infty} \Bigg(\sum_{\substack{i+j=k \\ 0\leqslant i\leqslant n,\ 0\leqslant j\leqslant m}} a_i b_j \Bigg) X^k$$

et le coefficient de X^{u+v} vaut $a_u b_v \neq 0$, donc

$$\boxed{\mathrm{val}(PQ) = \mathrm{val}(P) + \mathrm{val}(Q).}$$

Pour la somme, on suppose (sans restreindre la généralité du propos) que $v \geqslant u$, d'où

$$P + Q = \sum_{j=u}^{v-1} a_j X^j + \sum_{j=v}^{+\infty} (a_j + b_j) X^j,$$

d'où

$$\boxed{\mathrm{val}(P+Q) \geqslant u = \min\{\mathrm{val}(P); \mathrm{val}(Q)\}.}$$

♦ ***Exercice 2.*** [○]
Soit K un corps dans lequel $2 \neq 0$.

1. Soit A un polynôme à coefficients dans K tel que $A(-X) = A(X)$. Démontrer que tous les monômes de A sont de degré pair.
2. Soit P un polynôme à coefficients dans K. Justifier l'existence et l'unicité d'un polynôme $\widehat{P}$ tel que $\widehat{P}(X^2) = P(X)P(-X)$. Que vaut le degré de $\widehat{P}$ par rapport au degré de P ?
3. Soient $P, Q \in K[X]$. Établir que $\widehat{PQ} = \widehat{P}\widehat{Q}$.

1. Soit $A = a_0 + a_1 X + \cdots + a_n X^n$. Comme $A(-X) = A(X)$, on a

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

ce qui donne, en vertu du principe d'identification des coefficients,

$$\forall k \in [\![0; n]\!]\,, \qquad a_k = (-1)^k a_k.$$

Cela implique que tous les coefficients d'indice impair sont nuls (car $2 \neq 0$), ce qui revient bien à dire que

$$\boxed{\text{tous les monômes de } A \text{ sont de degré pair.}}$$

2. Existence :
Posons $A = P(X)P(-X)$ de sorte que $A(-X) = A(X)$. La question 1 nous dit que A ne possède que des monômes pairs, c'est-à-dire qu'il existe $a_0, a_2, \dots, a_{2n} \in K$ tels que

$$A = a_0 + a_2X^2 + \cdots + a_{2n}X^{2n}.$$

En posant

$$\widehat{P} = a_0 + a_2X + \cdots + a_{2n}X^n,$$

on a alors

$$\widehat{P}(X^2) = P(X)P(-X),$$

ce qui démontre l'existence de $\widehat{P}$. En passant au degré, on voit que

$$2 \times \deg(\widehat{P}) = \deg(P) + \deg(P),$$

ce qui donne

$$\deg(\widehat{P}) = \deg(P),$$

puisque $2 \neq 0$.

Unicité :
Supposons l'existence d'un autre polynôme $\widetilde{P}$ tel que $\widetilde{P}(X^2) = P(X)P(-X)$. On a alors $\widehat{P}(X^2) = \widetilde{P}(X^2)$ et $\deg(\widehat{P}) = \deg(\widetilde{P})$. On écrit $\widehat{P} = a_0 + a_1X + \cdots + a_nX^n$ et $\widetilde{P} = b_0 + b_1X + \cdots + b_nX^n$. L'égalité $\widehat{P}(X^2) = \widetilde{P}(X^2)$ donne $a_0 + a_1X^2 + \cdots + a_nX^{2n} = b_0 + b_1X^2 + \cdots + b_nX^{2n}$, ce qui implique, par identification des coefficients, que $a_0 = b_0$, $a_1 = b_1$, …, $a_n = b_n$. Donc $\widetilde{P} = \widehat{P}$, ce qui démontre l'unicité.

En conclusion,

$$\boxed{\text{il existe un unique polynôme } \widehat{P} \text{ tel que } \widehat{P}(X^2) = P(X)P(-X) \text{ et } \deg(\widehat{P}) = \deg(P).}$$

3. On a

$$\widehat{PQ}(X^2) = (PQ)(X)(PQ)(-X) = P(X)P(-X)Q(X)Q(-X) = \widehat{P}(X^2)\widehat{Q}(X^2) = (\widehat{P}\widehat{Q})(X^2),$$

ce qui démontre, par unicité, que

$$\boxed{\widehat{PQ} = \widehat{P}\widehat{Q}.}$$

♦ ***Exercice 3.*** [○]
Soit $P \in \mathbb{R}[X]$ tel que $P(X^2) = (X^2+1)P(X)$.

1. Déterminer P à l'aide d'une identification des coefficients.
2. Retrouver l'expression de P en déterminant ses racines.

Notons n le degré de P. Le polynôme $P(X^2)$ est alors de degré $2n$ et le polynôme $(X^2+1)P(X)$ est de degré $n+2$. L'égalité $P(X^2) = (X^2+1)P(X)$ implique donc que $2n = n+2$, ce qui donne $n = 2$ ou $n = -\infty$. Donc

$$\boxed{\deg P \text{ vaut } -\infty \text{ ou } 2.}$$

1. Constatons tout d'abord que le polynôme nul satisfait bien la relation $P(X^2) = (X^2+1)P(X)$.
Si P n'est pas le polynôme nul, la question précédente nous dit que $P(X) = aX^2 + bX + c$ avec $a \neq 0$. L'égalité $P(X^2) = (X^2+1)P(X)$ est alors équivalente à

$$\begin{aligned}
& aX^4 + bX^2 + c = (X^2+1)(aX^2+bX+c) \\
\iff \quad & aX^4 + bX^2 + c = aX^4 + bX^3 + (c+a)X^2 + bX + c \\
\iff \quad & \begin{cases} a = a \\ 0 = b \\ b = a + c \\ 0 = b \\ c = c \end{cases} \qquad \text{par identification des coefficients} \\
\iff \quad & \begin{cases} a = \lambda \\ b = 0 \\ c = -\lambda \end{cases} \qquad (\lambda \in \mathbb{R}^*),
\end{aligned}$$

donc $P(X) = \lambda(X^2-1)$ avec $\lambda \in \mathbb{R}^*$.
En conclusion,

$$\boxed{P(X) = \lambda(X^2-1) \text{ avec } \lambda \in \mathbb{R}.}$$

2. Si P n'est pas le polynôme nul, il est de degré 2 donc on doit pouvoir lui trouver deux racines complexes.
En posant $X = 1$ dans la relation $P(X^2) = (X^2+1)P(X)$, on obtient $P(1) = 2P(1)$, ce qui donne $P(1) = 0$.
En posant $X = -1$ dans la relation $P(X^2) = (X^2+1)P(X)$, on obtient $P(1) = 2P(-1)$, ce qui donne $P(-1) = P(1)/2 = 0$. On peut aussi poser $X = i$ dans la relation $P(X^2) = (X^2+1)P(X)$, ce qui donne directement $P(-1) = 0$.
Comme -1 et 1 sont racines de P, on a $P(X) = \lambda(X+1)(X-1)$, ce qui donne

$$\boxed{P(X) = \lambda(X^2-1) \text{ avec } \lambda \in \mathbb{R}.}$$

♦ ***Exercice 4.*** [∘]
Soient K un corps de caractéristique nulle, $P \in K[X]$, $\alpha \in K$ et $m \in \mathbb{N}$. Écrire la division euclidienne de P par $(X-\alpha)^m$ à l'aide des polynômes $(X-\alpha)^k$ pour $k \in \mathbb{N}$.

La formule de Taylor dit que

$$P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k = \sum_{k=0}^{m-1} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k + (X-\alpha)^m \sum_{k=m}^{+\infty} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^{k-m}.$$

Or

$$\deg\Big(\sum_{k=0}^{m-1} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k\Big) \leqslant m = \deg\big((X-\alpha)^m\big),$$

donc la relation ci-dessus exprime que

le quotient et le reste de la division euclidienne de P par $(X-\alpha)^m$ sont respectivement $\displaystyle\sum_{k=m}^{+\infty} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^{k-m}$ et $\displaystyle\sum_{k=0}^{m-1} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k$.

♦ ***Exercice 5.*** [⋆]
Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$. On pose

$$P_n = \frac{X^n(bX-a)^n}{n!}.$$

Démontrer que, pour tout $\ell \in \mathbb{N}$, ${P_n}^{(\ell)}(0)$ est un entier relatif.

Le binôme de Newton donne

$$P_n = \sum_{k=0}^{n} \binom{n}{k} \frac{b^k(-a)^{n-k}}{n!} X^{n+k}$$

donc

$$P_n = \sum_{\ell=n}^{2n} \binom{n}{\ell-n} \frac{b^{\ell-n}(-a)^{2n-\ell}}{n!} X^\ell.$$

Par ailleurs, la formule de Taylor nous dit que

$$P_n = \sum_{\ell=0}^{2n} \frac{{P_n}^{(\ell)}(0)}{\ell!} X^\ell.$$

Par identification des coefficients, il s'ensuit que

$$\forall \ell \in \mathbb{N} \setminus [\![n; 2n]\!], \qquad {P_n}^{(\ell)}(0) = 0 \in \mathbb{Z}.$$

Par ailleurs, pour $\ell \in \{n, \dots, 2n\}$, on a

$$\forall \ell \in [\![n; 2n]\!], \qquad {P_n}^{(\ell)}(0) = \frac{\ell!}{n!}\binom{n}{\ell-n} b^{\ell-n}(-a)^{2n-\ell} \in \mathbb{Z}.$$

Donc

$$\boxed{\forall \ell \in \mathbb{N}, \qquad {P_n}^{(\ell)}(0) \in \mathbb{Z}.}$$

♦ ***Exercice 6.*** [○]
Soit $A(X) = X^7 - X - 1$ et $B(X) = X^5 + 1$. Démontrer que A et B sont premiers entre eux et trouver l'ensemble des couples $(U, V) \in K[X]^2$ tels que $AU + BV = 1$.

Appliquons l'algorithme d'Euclide

Quotients	Restes	Coefficients de Bézout	
	$X^7 - X - 1$	1	0
X^2	$X^5 + 1$	0	1
$-X^3 + X^2 - 1$	$-X^2 - X - 1$	1	$-X^2$
$X + 1$	$-X$	$X^3 - X^2 + 1$	$-X^5 + X^4 - X^2 + 1$
X	-1	$-X^4 + X^2 - X$	$X^6 - X^4 + X^3 - X - 1$
	0		

Cela prouve que

$$\boxed{A \wedge B = 1}$$

Par ailleurs, le couple

$$(U_0, V_0) = (X^4 - X^2 + X, -X^6 + X^4 - X^3 + X + 1)$$

est donc une solution particulière de l'équation $AU + BV = 1$.

En soustrayant les deux égalités $AU+BV = 1$ et $AU_0+BV_0 = 1$, on obtient $A(U-U_0)+B(V-V_0) = 0$, c'est-à-dire $A(U - U_0) = B(V_0 - V)$. En particulier, A divise $B(V_0 - V)$ et comme $\operatorname{pgcd}(A, B) = 1$, il s'ensuit, d'après le lemme de Gauß, que A divise $V_0 - V$. D'où l'existence d'un polynôme $K \in \mathbb{R}[X]$ tel que $V - V_0 = KA$.

En remplaçant dans l'équation $AU + BV = 1$, on trouve que $U = U_0 - KB$.

L'ensemble des solutions de $AU + BV = 1$ est donc

$$\boxed{\left\{\left(X^4 - X^2 + X - K(X^5 + 1), -X^6 + X^4 - X^3 + X + 1 + K(X^7 - X - 1)\right) : K \in \mathbb{R}[X]\right\}}.$$

♦ ***Exercice 7.*** [○]

1. Soit $a, b \in \mathbb{C}$ tels que $a \neq b$ et soit $P \in \mathbb{C}[X]$.
   a) Déterminer, en fonction de $P(a)$ et $P(b)$, le reste de la division de P par $(X-a)(X-b)$.
   b) Déterminer, en fonction de $P(a)$ et $P'(a)$, le reste de la division de P par $(X - a)^2$.
2. Calculer le reste de la division euclidienne de $(X - 1)^{n+2} + X^{2n+1}$ par $X^2 - X + 1$. Qu'en déduire ?

1. a) La division euclidienne de P par $(X-a)(X-b)$ donne $P = (X-a)(X-b)Q+R$ où $R = uX+v$ avec $u, v \in \mathbb{C}$. En substituant a à X puis b à X, on obtient $P(a) = ua + v$ et $P(b) = ub + v$. On en déduit que

$$u = \frac{P(a) - P(b)}{a - b} \qquad \text{et} \qquad v = \frac{aP(b) - bP(a)}{a - b},$$

c'est-à-dire

$$\boxed{R = \frac{P(a) - P(b)}{a - b}X + \frac{aP(b) - bP(a)}{a - b}\cdot}$$

b) La division euclidienne de P par $(X - a)^2$ donne $P = (X - a)^2Q + R$ où $R = uX + v$ avec $u, v \in \mathbb{C}$. En substituant a à X, on obtient $P(a) = ua + v$. En dérivant, on a $P' = 2(X - a)Q + (X - a)^2Q' + u$ et en substituant a à X, on obtient $P'(a) = u$. On en déduit que

$$u = P'(a) \qquad \text{et} \qquad v = P(a) - aP'(a),$$

c'est-à-dire

$$\boxed{R = P'(a)(X - a) + P(a).}$$

Remarque : On retrouve le résultat donné par la formule de Taylor.

2. On note R_n le reste de la division de $P_n = (X-1)^{n+2} + X^{2n+1}$ par $X^2 - X + 1 = (X+j)(X+j^2)$. D'après la question 1.a), on a

$$R_n = \frac{P_n(-j) - P_n(-j^2)}{j^2 - j} X + \frac{-jP_n(-j^2) + j^2 P_n(-j)}{j^2 - j}.$$

Or

$$P_n(-j) = (-j-1)^{n+2} + (-j)^{2n+1} = (j^2)^{n+2} - j^{2n+1} = j^{2n+1}(j^3 - 1) = 0$$

et

$$P_n(-j^2) = (-j^2-1)^{n+2} + (-j^2)^{2n+1} = j^{n+2} - j^{4n+2} = j^{n+2} - j^{3n} j^{n+2} = j^{n+2} - j^{n+2} = 0,$$

donc

$$R_n = 0,$$

ce qui signifie que

$$\boxed{X^2 - X + 1 \text{ divise } (X-1)^{n+2} + X^{2n+1}}$$

♦ ***Exercice 8.*** [⋆]
Soient $A, B \in \mathbb{C}[X]$ et $p \in \mathbb{N}^*$. Prouver que B divise A si et seulement si $B(X^p)$ divise $A(X^p)$.

Si B divise A, il est clair que $B(X^p)$ divise $A(X^p)$.

Réciproquement, supposons que $B(X^p)$ divise $A(X^p)$. La division euclidienne de A par B donne $A = BQ + R$ avec $\deg(R) < \deg(B)$. En composant par X^p, on obtient $A(X^p) = B(X^p)Q(X^p) + R(X^p)$. On constate que $\deg\big(R(X^p)\big) = \deg(R) \times p < \deg(B) \times p = \deg\big(B(X^p)\big)$, donc la relation $A(X^p) = B(X^p)Q(X^p) + R(X^p)$ est la division euclidienne de $A(X^p)$ par $B(X^p)$. Comme $B(X^p)$ divise $A(X^p)$, on sait que le reste de cette division euclidienne est nul, c'est-à-dire $R(X^p) = 0$. On a donc $\deg(R) \times p = -\infty$, c'est-à-dire $\deg(R) = -\infty$ ou encore $R = 0$. Cela donne $A = BQ$, ce qui démontre que B divise A.

En conclusion,

$$\boxed{B \text{ divise } A \text{ si, et seulement si, } B(X^p) \text{ divise } A(X^p).}$$

♦ ***Exercice 9.*** [⋆] (Algorithme de Hörner)
On veut calculer la valeur du polynôme $P = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$ en $\alpha \in K$. L'algorithme de Hörner consiste à effectuer ce calcul de la façon suivante :

$$P(\alpha) = a_0 + (a_1 + \cdots + (a_{n-2} + (a_{n-1} + a_n\alpha)\alpha)\alpha \cdots)\alpha)\alpha.$$

Pour cela, on écrit les coefficients du polynôme dans la première ligne d'un tableau à 2 lignes et $n+1$ colonnes, en partant du coefficient dominant pour aller vers le coefficient constant. La première case de la seconde ligne contient le même nombre que celle qui est juste au dessus d'elle, à savoir a_n. Ainsi pour le polynôme $P = -X^3 + 3X + 1$ et la valeur $\alpha = 4$, on part du tableau :

-1	0	3	1
-1			

On remplit alors les cases de la seconde ligne de proche en proche de la gauche vers la droite. Pour remplir la case C, on multiplie par α le nombre inscrit dans la case à gauche de C et on ajoute à ce résultat la valeur du coefficient situé au dessus de C ; on inscrit alors le nombre obtenu dans C. Dans notre exemple, on obtient

-1	0	3	1
-1	-4	-13	-51

Le dernier résultat de la seconde ligne est la valeur de $P(\alpha)$. Ici $P(4) = -51$.

1. Dénombrer les multiplications effectuées par l'algorithme naïf calculant toutes les puissances de α avant de les combiner linéairement. Faire de même avec l'algorithme de Hörner.
2. Expliquer comment on peut utiliser l'algorithme de Hörner pour effectuer la division euclidienne de P par $X - \alpha$.

   Vérifier que 2 est une racine de $P = 3X^4 - 2X^3 - 9X^2 + 5X - 6$ et factoriser P par $X - 2$.

1. L'algorithme de Hörner nécessite seulement n multiplications alors que l'algorithme naïf calculant toutes les puissances de α avant de les combiner linéairement en requiert $n(n+3)/2$.
2. La division euclidienne de P par $X-\alpha$ est de la forme $P=(X-\alpha)Q+P(\alpha)$. On constate, par identification, que les coefficients b_k de Q vérifient $b_{n-1}=a_n$ puis $q_{k-1}=\alpha q_k+a_k$ pour tout $k\in[\![1;n-1]\!]$, ce qui correspond aux coefficients du tableau de l'algorithme de Hörner. La dernière valeur donne le reste.

   On a

3	-2	-9	5	-6
3	4	-1	3	0

   donc

$$\boxed{3X^4-2X^3-9X^2+5X-6=(X-2)(3X^3+4X^2-X+3)}$$

♦ ***Exercice 10.*** [○]
Soient $A,B\in K[X]$. Démontrer que A et B sont premiers entre eux si, et seulement si, $A+B$ et AB le sont.

Supposons que $A+B$ et AB sont premiers entre eux. D'après Bézout, il existe alors $U,V\in K[X]$ tels que $U(A+B)+VAB=1$, c'est-à-dire $(U+VB)A+UB=1$, ce qui démontre que A et B sont premiers entre eux d'après le théorème de Bézout.

Récirpoquement, supposons que A et B sont premiers entre eux. Soit P un polynôme irréductible diviseur commun de $A+B$ et AB. L'indépendance divisorielle nous dit que P divise A ou P divise B. Traitons le cas où P divise A (par exemple). Comme P divise aussi $A+B$, il divise $(A+B)-A)=B$. Mézalors, P divisant A et B qui sont premiers entre eux, on en déduit que P est constant. Les seuls diviseurs communs de $A+B$ et AB étant les polynômes constants, on en déduit que $A+B$ et AB sont premiers entre eux.

En conclusion,

$$\boxed{A \text{ et } B \text{ sont premiers entre eux si, et seulement si, } A+B \text{ et } AB \text{ le sont.}}$$

♦ ***Exercice 11.*** [⋆]
Soient $n,m\in\mathbb{N}^*$.
1. Démontrer que le pgcd de X^n-1 et X^m-1 est $X^{n\wedge m}-1$.
2. On suppose que $n\wedge m=1$. Démontrer que $(X^n-1)(X^m-1)$ divise $(X-1)(X^{nm}-1)$.

1. Effectuons la division euclidienne de n par m, ce qui donne $n=mq+r$ où $0\leqslant r<m$. Alors

$$\begin{aligned}X^n-1 &= X^{mq+r}-1\\ &= X^{mq+r}-X^r+X^r-1\\ &= (X^{mq}-1)X^r+X^r-1\\ &= (X^m-1)(X^{m(q-1)}+\cdots+X^m+1)X^r+(X^r-1)\end{aligned}$$

   et, comme $\deg(X^r-1)=r<m=\deg(X^m-1)$, la relation ci-dessus est la division euclidienne de X^n-1 par X^m-1. Il s'ensuit que, si l'on note $\mathscr{D}(A)$ l'ensemble des diviseurs du polynôme A, on a

$$\mathscr{D}(X^n-1)\cap\mathscr{D}(X^m-1)=\mathscr{D}(X^m-1)\cap\mathscr{D}(X^r-1).$$

   En itérant ce raisonnement, on retrouve l'algorithme d'Euclide, ce qui donne au final

$$\mathscr{D}(X^n-1)\cap\mathscr{D}(X^m-1)=\mathscr{D}(X^{n\wedge m}-1).$$

   Donc

$$\boxed{(X^n-1)\wedge(X^m-1)=X^{n\wedge m}-1.}$$

2. Comme $(A\wedge B)(A\vee B)=AB$ lorsque A et B sont unitaires, on a

$$[(X^n-1)\wedge(X^m-1)]\times[(X^n-1)\vee(X^m-1)]=(X^n-1)(X^m-1).$$

Or $n \wedge m = 1$, donc, d'après la question précédente, on a

$$(X^n - 1) \wedge (X^m - 1) = X - 1.$$

Par ailleurs, comme $X^n - 1$ et $X^m - 1$ divisent $X^{nm} - 1$ d'après la formule de Bernoulli, on a

$$(X^n - 1) \vee (X^m - 1) \mid X^{nm} - 1.$$

Donc

$$\boxed{(X^n - 1)(X^m - 1) \text{ divise } (X - 1)(X^{nm} - 1).}$$

♦ ***Exercice 12.*** [○] (Un polynôme symétrique)
Soit $P = 2X^4 - 5X^3 + 4X^2 - 5X + 2$. Démontrer que l'équation $P(z) = 0$ (d'inconnue $z \in \mathbb{C}$) est équivalente à l'équation $P(z)/z^2 = 0$. En déduire les racines de P à l'aide du changement de variable $Z = z + 1/z$.

Constatons que 0 n'est pas une racine de P, ce qui permet d'effectuer le changement de variable $Z = z + 1/z$.

On a

$$Z^2 = z^2 + \frac{1}{z^2} + 2.$$

Alors

$$\begin{aligned}
P(z) = 0 &\iff 2z^4 - 5z^3 + 4z^2 - 5z + 2 = 0 \\
&\iff 2z^2 - 5z + 4 - 5\frac{1}{z} + 2\frac{1}{z^2} = 0 && \text{après division par } z^2 \text{ (licite car 0 n'est pas solution)} \\
&\iff 2\Big(z^2 + 2 + \frac{1}{z^2}\Big) - 5\Big(z + \frac{1}{z}\Big) = 0 \\
&\iff 2Z^2 - 5Z = 0 \\
&\iff Z = 0 \text{ ou } Z = \frac{5}{2}.
\end{aligned}$$

Or

$$z + \frac{1}{z} = 0 \iff z^2 = -1 \iff z = \pm i$$

et

$$z + \frac{1}{z} = \frac{5}{2} \iff 2z^2 - 5z + 2 = 0 \iff z = \frac{1}{2} \text{ ou } z = 2,$$

donc

$$\boxed{\text{les racines de } P \text{ sont } \frac{1}{2},\ 2,\ i \text{ et } -i.}$$

♦ ***Exercice 13.*** [○] (Racines évidentes)
Soit $P = n_d X^d + \cdots + n_1 X + n_0$ un polynôme de degré $d \geqslant 1$ à coefficients entiers.

1. Démontrer que si P admet un nombre entier a comme racine, alors nécessairement a divise n_0. Une telle racine est appelée racine évidente du polynôme P.
   Les polynômes $X^3 - X^2 - 109X - 11$ et $X^{10} + X^5 + 1$ ont-ils des racines évidentes ?
2. Généraliser le résultat précédent en indiquant ce que l'on peut dire des entiers a et b (avec $b \neq 0$ et $a \wedge b = 1$) lorsque P admet le nombre rationnel a/b comme racine.

1. On a $P(a) = 0$, c'est-à-dire $n_d a^d + \cdots + n_1 a = -n_0$, ce qui donne $a(-n_d a^{d-1} - \cdots - n_1) = n_0$. Cela démontre, par conséquent, que a divise n_0. Ainsi

$$\boxed{\text{si } P \text{ admet une racine } a \in \mathbb{Z}, \text{ alors } a \text{ divise } n_0.}$$

Si $X^3 - X^2 - 109X - 11$ admet une racine dans $\mathbb{Z}$, cette racine divise -11 donc peut valoir -11, -1, 1 ou 11. En essayant, on voit que

$$\boxed{-11 \text{ est bien racine du polynôme } X^3 - X^2 - 109X - 11.}$$

Si $X^{10} + X^5 + 1$ admet une racine dans $\mathbb{Z}$, cette racine divise 1 donc peut valoir -1 ou 1. Aucune de ces deux valeurs n'est racine de ce polynôme donc

$$\boxed{X^{10} + X^5 + 1 \text{ n'a pas de racine évidente.}}$$

2. On a $P(a/b)=0$, c'est-à-dire $n_d(a/b)^d+\cdots+n_1(a/b)+n_0=0$, ce qui donne $n_da^d+n_{d-1}a^{d-1}b+\cdots+n_1ab^{d-1}+n_0b^d=0$, d'où

$$a(-n_da^{d-1}-n_{d-1}a^{d-2}-\cdots-n_1b^{d-1})=n_0b^d \qquad \text{et} \qquad b(-n_{d-1}a^{d-1}-\cdots-n_1ab^{d-2}-n_0b^{a-1})=n_da^d.$$

Alors, on a

$$a \mid n_0b^d \qquad \text{et} \qquad b \mid n_da^d.$$

Comme $a\wedge b=1$, le lemme de Gauss nous dit que

$$a \mid n_0 \qquad \text{et} \qquad b \mid n_d.$$

Ainsi

si P admet une racine $a/b\in\mathbb{Q}$ avec $a\in\mathbb{Z}$, $b\in\mathbb{N}^*$ et $a/b=1$, alors a divise n_0 et b divise n_d.

♦ ***Exercice 14.*** [○] (Racine commune)

1. Démontrer que si deux polynômes A et B ont une racine en commun, celle-ci est aussi racine du reste de la division euclidienne de A par B.
2. Trouver une racine commune de $A=X^4+(-1+i)X^3+(-3+i)X^2+(-5-i)X+10+25i$ et $B=X^3+2X^2+(2-i)X-1-7i$.

1. Soit $\alpha\in\mathbb{C}$ une racine commune de A et B, c'est-à-dire $A(\alpha)=B(\alpha)=0$. En effectuant la division euclidienne de A par B, on obtient $A=BQ+R$ où R désigne le reste (avec donc $\deg R<\deg Q$). En substituant X par α, il vient $A(\alpha)=B(\alpha)Q(\alpha)+R(\alpha)$, c'est-à-dire $R(\alpha)=0$. Donc α est racine de R. Ainsi,

si A et B ont une racine en commun, celle-ci est aussi racine du reste de la division de A par B.

2. Si les polynômes A et B ont une racine α en commun dans $\mathbb{C}$, celle-ci est aussi racine du reste de la division euclidienne de A par B, d'après la question précédente. Or cette division donne

$$A(X)=B(X)\times(X-3+i)+(X^2+(1+i)X+5i),$$

donc α est nécessairement une racine de $R(X)=X^2+(1+i)X+5i$. Son discriminant vaut $\Delta=(1+i)^2-4\times1\times5i=-18i=18\,\mathrm{e}^{-i\pi/2}$ et les deux racines carrées de Δ sont $\delta=3\sqrt{2}\,\mathrm{e}^{-i\pi/4}=3(1-i)$ et $-\delta=-3(1-i)$. Les racines de R sont donc

$$\omega_1=\frac{-1-i+3(1-i)}{2}=1-2i \qquad \text{et} \qquad \omega_2=\frac{-1-i-3(1-i)}{2}=-2+i.$$

Or

$$B(1-2i)=(1-2i)^3+2(1-2i)^2+(2-i)(1-2i)-1-7i=-18-18i\neq0$$

et

$$A(-2+i)=B(-2+i)=\text{ calculs }=0,$$

donc

$-2+i$ est une racine commune de A et B.

♦ ***Exercice 15.*** [○]

Soit $n\in\mathbb{N}$. Démontrer que le polynôme $P_n=\sum_{k=0}^{n}\frac{1}{k!}X^k$ n'a que des racines simples.

Soit $\alpha\in\mathbb{C}$ une racine de P_n. Comme

$$P_n'(X)=\sum_{k=1}^{n}\frac{X^{k-1}}{(k-1)!}=\sum_{k=0}^{n-1}\frac{X^k}{k!}=P_n(X)-\frac{X^n}{n!},$$

on a

$$P_n'(\alpha)=P_n(\alpha)-\frac{\alpha^n}{n!}=-\frac{\alpha^n}{n!},$$

donc si on suppose que $P_n'(\alpha)=0$, on a $-\frac{\alpha^n}{n!}=0$, c'est-à-dire $\alpha=0$ ce qui est absurde puisque 0 n'est pas racine de P_n. Donc

le polynôme $P_n=\sum_{k=0}^{n}\frac{1}{k!}X^k$ n'a que des racines simples.

♦ ***Exercice 16.*** [○]

1. Soit $P \in K[X]$. Démontrer que si P et P' sont premiers entre eux, alors P n'admet que des racines simples dans K (c'est-à-dire $\forall \alpha \in K$, $\text{mult}(\alpha) \leqslant 1$).
2. Démontrer que la réciproque est vraie si $K = \mathbb{C}$ mais fausse si $K = \mathbb{R}$.

1. Par contraposition. Supposons que P admette une racine multiple α dans K. Alors $(X-\alpha)^2$ divise P, c'est-à-dire qu'il existe $Q \in K[X]$ tel que $P = (X-\alpha)^2 Q$. En dérivant, on obtient $P' = 2(X-\alpha)Q + (X-\alpha)^2 Q'$. Par conséquent, $X - \alpha$ divise P et P', ce qui démontre que P et P' ne sont pas premiers entre eux. En conclusion,

si P et P' sont premiers entre eux, alors P n'admet que des racines simples dans K.

2. Si $P \in \mathbb{C}[X]$ n'admet que des racines simples sur $\mathbb{C}$, alors P et P' n'ont pas de racines en commun, ce qui signifie qu'ils n'ont aucun facteur irréductible en commun dans leurs décompositions primaires, c'est-à-dire que P et P' sont premiers entre eux. Ainsi

dans $\mathbb{C}[X]$, P et P' sont premiers entre eux si, et seulement si, P n'a que des racines simples dans $\mathbb{C}$.

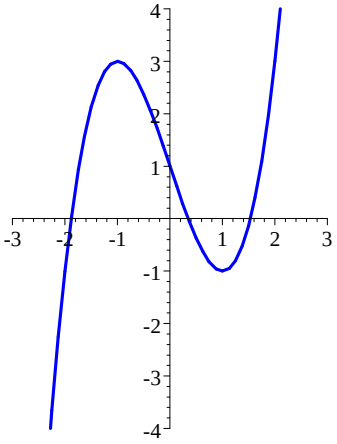
   Dans $\mathbb{R}[X]$, le polynôme $P = (X^2+1)^2$ n'admet que des racines simples : et pour cause, il n'admet aucune racine ! Mais $P = (X^2+1)^2$ et $P' = 4X(X^2+1)$ ne sont pas premiers entre eux puisque X^2+1 est un diviseur commun de P et P'. Donc

dans $\mathbb{R}[X]$, un polynôme peut n'admettre que des racines simples dans $\mathbb{R}$ et ne pas être, pour autant, premier avec son polynôme dérivé.

♦ ***Exercice 17.*** [○]

Démontrer que $P = X^3 - 3X + 1$ admet trois racines réelles.

Il suffit d'étudier
la fonction $x \longmapsto x^3 - 3x + 1$



♦ ***Exercice 18.*** [⋆]

Déterminer les polynômes complexes dont l'application polynomiale associée est surjective puis ceux dont l'application polynomiale associée est injective.

Dans la solution de cet exercice, on confond les notions de polynômes et de fonctions polynomiales.

1. Un polynôme constant n'est évidemment pas surjectif.

   Supposons maitenant que P est un polynôme complexe non constant. Alors pour tout $\omega \in \mathbb{C}$, le polynôme $P - \omega$ n'est pas contant et possède, à ce titre, au moins une racine d'après le théorème de d'Alembert–Gauß, c'est-à-dire qu'il existe $a \in \mathbb{C}$ tel que $P(a) - \omega = 0$ ou encore $P(a) = \omega$. Donc P est surjectif.

En conclusion,

toutes les applications polynomiales complexes non constantes sur des surjections de $\mathbb{C}$ sur $\mathbb{C}$.

2. Un polynôme constant n'est évidemment pas injectif.

   Un polynôme de degré 1 est injectif et même bijectif puisque la réciproque de $z \longmapsto az+b$ (où $a \neq 0$) est $z \longmapsto (z-b)/a$.

   Un polynôme P de degré $n \geqslant 2$ n'est pas injectif. En effet, comme P admet n racines d'après le théorème de d'Alembert–Gauß, le nombre 0 possède plusieurs antécédents par P sauf dans le cas où P est de la forme $P = a(X-\alpha)^n$ avec $a \in \mathbb{C}^*$ et $\alpha \in \mathbb{C}$. Mézalors, on a $P(\alpha+1) = P(\alpha + \mathrm{e}^{i2\pi/n})$, ce qui écarte l'injectivité également dans ce cas.

   En conclusion,

   les seules applications polynomiales complexes injectives sont celles de degré 1.

♦ ***Exercice 19.*** [○]
Soient $P, Q \in \mathbb{C}_3[X]$ tels que $P(0) = Q(0)$, $P'(0) = Q'(0)$, $P''(0) = Q''(0)$ et $P'''(0) = Q'''(0)$. Démontrer que $P = Q$ de deux manières.

1. D'après la règle sur le degré d'une somme, on a

$$\deg R \leqslant \max\{\deg P; \deg Q\} \leqslant 3.$$

   Par ailleurs, on a

$$\begin{aligned} R(0) &= P(0) - Q(0) = 0, \\ R'(0) &= P'(0) - Q'(0) = 0, \\ R''(0) &= P''(0) - Q''(0) = 0 \end{aligned}$$

   et

$$R'''(0) = P'''(0) - Q'''(0) = 0,$$

   ce qui démontre que 0 est racine de P de multiplicité au moins 4.

   Or seul le polynôme nul admet plus de racines (comptées avec multiplicités) que son degré, donc $R = 0$, c'est-à-dire

$$\boxed{P = Q.}$$

2. On a

$$\begin{aligned} P(X) &= \sum_{k=0}^{3} \frac{P^{(k)}(0)}{k!} X^k && \text{d'après Taylor pour } P \\ &= \sum_{k=0}^{3} \frac{Q^{(k)}(0)}{k!} X^k && \text{car } P(0) = Q(0),\ P'(0) = Q'(0), \\ & && P''(0) = Q''(0) \text{ et } P'''(0) = Q'''(0). \\ &= Q(X) && \text{d'après Taylor pour } Q, \end{aligned}$$

   donc

on retrouve que $P = Q$.

♦ ***Exercice 20.*** [⋆]
Démontrer qu'il n'existe pas de polynôme $P \in \mathbb{C}[X]$ tel que $\forall z \in \mathbb{C},\ P(z) = \overline{z}$.

Si un tel polynôme P existait, alors $P(X) - X$ admettrait tout nombre réel comme racine et serait donc le polynôme nul, ce qui forcerait $P(X) = X$ et donc aussi $\forall z \in \mathbb{C},\ \overline{z} = z$: absurde ! Donc

la conjugaison n'est pas une application polynomiale.

♦ ***Exercice 21.*** [○]
Démontrer qu'un corps fini n'est pas algébriquement clos.

Si K est fini, le polynôme $1+\prod_{k\in K}(X-k)$ n'a pas de racines. Donc

$$\boxed{\text{un corps fini n'est pas algébriquement clos.}}$$

♦ ***Exercice 22.*** [○]
Déterminer la factorisation, dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$ des polynômes

$$A=X^6+1, \qquad B=X^{10}+X^5+1 \qquad \text{et} \qquad C=X^{2n}-2(\cos\alpha)X^n+1.$$

On trouve

$$\boxed{X^6+1=(X-\mathrm{e}^{i\pi/6})(X-i)(X-\mathrm{e}^{i5\pi/6})(X-\mathrm{e}^{i7\pi/6})(X+i)(X-\mathrm{e}^{i11\pi/6})}$$

et

$$\boxed{X^6+1=\left(X^2+1\right)(X^2-\sqrt{3}X+1)(X^2+\sqrt{3}X+1).}$$

À finir.

♦ ***Exercice 23.*** [○]
Factoriser dans $\mathbb{R}[X]$ le polynôme

$$P_n=1+\frac{X}{1!}+\frac{X(X+1)}{2!}+\cdots+\frac{X(X+1)\cdots(X+n-1)}{n!}.$$

On a

$$P_0=1$$
$$P_1=1+X$$
$$P_2=1+X+\frac{X(X+1)}{2}=\frac{(X+1)(X+2)}{2}$$
$$P_3=1+X+\frac{X(X+1)}{2}+\frac{X(X+1)(X+2)}{6}=\frac{(X+1)(X+2)}{2}+\frac{X(X+1)(X+2)}{6}=\frac{(X+1)(X+2)(X+3)}{6}.$$

Une démonstration par récurrence (immédiate) nous permet alors de justifier que

$$\boxed{\forall n\in\mathbb{N}, \qquad P_n(X)=\frac{(X+1)\cdots(X+n)}{n!}.}$$

♦ ***Exercice 24.*** [⋆]
Soit $n\in\mathbb{N}^*$. Factoriser $1+X+X^2+\cdots+X^{n-1}$ et en déduire la valeur de $\prod_{k=1}^{n-1}\sin(k\pi/n)$.

Les racines de $1+X+X^2+\cdots+X^{n-1}$ sont les éléments de $\mathbb{U}_n\setminus\{1\}$, donc

$$1+X+X^2+\cdots+X^{n-1}=\prod_{k=1}^{n-1}(X-\mathrm{e}^{i2k\pi/n}).$$

En substituant 1 à X dans cette égalité polynomile, on obtient

$$\begin{aligned}
n &= \prod_{k=1}^{n-1}(1-\mathrm{e}^{i2k\pi/n}) \\
&= \prod_{k=1}^{n-1}\mathrm{e}^{ik\pi/n}(\mathrm{e}^{-ik\pi/n}-\mathrm{e}^{ik\pi/n}) \\
&= \prod_{k=1}^{n-1}\mathrm{e}^{ik\pi/n}\times\prod_{k=1}^{n-1}(-2i)\sin\frac{k\pi}{n} \\
&= \mathrm{e}^{i(1+2+\cdots+n-1)\pi/n}\times(-2i)^{n-1}\times\prod_{k=1}^{n-1}\sin\frac{k\pi}{n} \\
&= \mathrm{e}^{i(n-1)\pi/2}\times(-2i)^{n-1}\times\prod_{k=1}^{n-1}\sin\frac{k\pi}{n} \\
&= i^{n-1}\times(-2i)^{n-1}\times\prod_{k=1}^{n-1}\sin\frac{k\pi}{n} \\
&= 2^{n-1}\times\prod_{k=1}^{n-1}\sin\frac{k\pi}{n},
\end{aligned}$$

donc

$$\boxed{\prod_{k=1}^{n-1}\sin\frac{k\pi}{n}=\frac{n}{2^{n-1}}\cdot}$$

♦ ***Exercice 25.*** [○]
Soit $P\in K[X]$ un polynôme de degré 2 ou 3. Démontrer que P est irréductible si, et seulement si, il n'a pas de racine dans K. Est-ce encore vrai pour des polynômes de degré plus élevé ?

Un polynôme de degré 2 ou 3 est non irréductible si et seulement s'il possède un diviseur de degré 1. Comme tout polynôme $aX+b$ de degré 1 (c'est-à-dire $a\neq 0$) possède une racine dans K (qui est $-b/a$), on en déduit qu'un polynôme de degré 2 ou 3 est non irréductible si et seulement s'il possède une racine dans K. On a ainsi démontré que

un polynôme de degré 2 ou 3 est irréductible si, et seulement si, il n'a pas de racine dans K.

♦ ***Exercice 26.*** [⋆]
Soient $P,Q\in\mathbb{C}[X]$ tels que, pour tout $z\in\mathbb{C}$, $|P(z)|=|Q(z)|$. Démontrer qu'il existe $u\in\mathbb{U}$ tel que $Q=uP$.

Soit a une racine de P. Alors $|Q(a)|=|P(a)|=|0|=0$ donc $Q(a)=0$, ce qui signifie que a est une racine de Q. Il existe alors $P_1,Q_1\in\mathbb{C}[X]$ tels que $P=(X-a)P_1$ et $Q=(X-a)Q_1$. L'hypothèse $\forall z\in\mathbb{C},\ |P(z)|=|Q(z)|$ donne alors $\forall z\in\mathbb{C},\ |(z-a)P_1(z)|=|(z-a)Q_1(z)|$, c'est-à-dire $\forall z\in\mathbb{C}\setminus\{a\},\ |P_1(z)|=|Q_1(z)|$. Par continuité des applications $z\longmapsto|P_1(z)|$ et $z\longmapsto|Q_1(z)|$, on a $\forall z\in\mathbb{C},\ |P_1(z)|=|Q_1(z)|$. Si a est encore racine de P_1, on peut reprendre le même raisonnement. On en déduit, au final, que si a est une racine de P de multiplicité m, alors a est une racine de Q de multiplicité au moins m. En échangeant les rôles de P et Q, on en conclut que si a est une racine de P de multiplicité m, alors a est une racine de Q de multiplicité m.

Dès lors, P et Q ont la même décomposition primaire, au coefficient dominant près, ce qui signifie qu'il existe $u\in\mathbb{C}^*$ tel que $Q=uP$.

Si $P=Q=0$, on prend $u=1$ et tout va bien. Sinon, l'hypothèse $\forall z\in\mathbb{C},\ |P(z)|=|Q(z)|$ donne $\forall z\in\mathbb{C},\ |P(z)|=|u|\times|P(z)|$, ce qui implique que $|u|=1$.

En conclusion,

il existe $u\in\mathbb{U}$ tel que $Q=uP$.

♦ ***Exercice 27.*** [⋆]
Déterminer les nombres réels a, b, c pour qu'ils soient racines de $P(X) = X^3 + aX^2 + bX - c$.

Les nombres réels a, b, c sont racines du polynôme $P(X)$ si, et seulement si,

$$X^3 + aX^2 + bX - c = (X-a)(X-b)(X-c) = X^3 - (a+b+c)X^2 + (ab+bc+ac)X - abc,$$

ce qui donne, après identification des coefficients,

$$(S)\begin{cases} a+b+c = -a & (1) \\ ab+bc+ac = b & (2) \\ abc = c & (3) \end{cases}$$

On distingue alors deux cas :

- Premier cas : $c = 0$
  Dans ce cas, le système devient
  $$(S)\begin{cases} 2a+b = 0 & (1) \\ ab = b & (2) \end{cases}$$
  On distingue alors deux sous-cas :
  - Premier sous-cas : $b = 0$
    L'équation (1) nous dit alors que $a = 0$. On trouve donc $(a, b, c) = (0, 0, 0)$.
  - Second sous-cas : $b \neq 0$
    L'équation (2) nous dit alors que $a = 1$. En reportant dans (1), il vient $b = -2$. On trouve donc $(a, b, c) = (1, -2, 0)$.
- Second cas : $c \neq 0$
  On peut simplifier c dans l'équation (3). Alors
  $$(S) \iff \begin{cases} 2a+b+c = 0 & (1) \\ ab+bc+ac = b & (2) \\ ab = 1 & (3) \end{cases} \iff \begin{cases} 2a+b+c = 0 & (1) \\ 1+bc+ac = b & (2) \\ ab = 1 & (3) \end{cases}$$
  En multipliant l'équation (1) par b et l'équation (2) par b^2 tout en tenant compte de (3), on obtient le système « sans a » suivant :
  $$\begin{cases} 2+b^2+bc = 0 & (1') \\ b^2+b^3c+bc = b^3 & (2') \end{cases} \iff \begin{cases} -bc = b^2+2 & (1') \\ b^3-b^2-bc(b^2+1) = 0 & (2') \end{cases}$$
  En reportant l'expression de $-bc$ donnée par $(1')$ dans $(2')$, il vient
  $$\begin{aligned} & b^3 - b^2 + (b^2+2)(b^2+1) = 0 \\ \iff \quad & b^4 + b^3 + 2b^2 + 2 = 0 \\ \iff \quad & b^2(b^2+b+2) + 2 = 0 \\ \iff \quad & b^2\left(\left(b+\frac{1}{2}\right)^2 + \frac{7}{4}\right) + 2 = 0 \end{aligned}$$
  Il est clair que cette dernière équation n'a pas de solution (le membre de gauche est supérieur ou égal à 2). Par conséquent, il n'y a pas de solution dans ce cas

Finalement,

$$\boxed{(a, b, c) = (0, 0, 0) \qquad \text{ou} \qquad (a, b, c) = (1, -2, 0).}$$

♦ ***Exercice 28.*** [⋆] (Discriminant)

Soient $P = a_nX^n + \cdots + a_1X + a_0$ un polynôme à coefficients complexes de degré n (c'est-à-dire $a_n \neq 0$) et $\alpha_1, \alpha_2, \ldots, \alpha_n$ les n racines (éventuellement égales) de P dans $\mathbb{C}$. On appelle *discriminant de P* le nombre complexe Δ défini par

$$\Delta = {a_n}^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2.$$

1. Quel résultat liant le discriminant et les racines multiples peut-on énoncer ?
2. Calculer Δ dans le cas du polynôme $P = aX^2 + bX + c$.
3. Démontrer que $\Delta = (-1)^{n(n-1)/2} {a_n}^{n-2} \prod_{\ell=1}^{n} P'(\alpha_\ell)$.
4. Calculer Δ dans le cas du polynôme $P = X^3 + pX + q$.

1. Vue la définition du discriminant, on a

le discriminant d'un polynôme est nul si, et seulement si, le polynôme admet au moins une racine complexe multiple.

2. Soit $P = aX^2 + bX + c$. On note α et β les racines de P. On a

$$\begin{aligned} \Delta &= a^{2\times 2-2}(\alpha - \beta)^2 \\ &= a^2(\alpha^2 + \beta^2 - 2\alpha\beta) \\ &= a^2\big((\alpha+\beta)^2 - 4\alpha\beta\big) \\ &= a^2\Big(\Big(-\frac{b}{a}\Big)^2 - 4\frac{c}{a}\Big) \\ &= a^2\frac{b^2-4ac}{a^2}, \end{aligned}$$

donc

$$\boxed{\Delta = b^2 - 4ac.}$$

3. On a

$$P = a_n \prod_{k=1}^{n} (X - \alpha_k)$$

d'où

$$P' = a_n \sum_{k=1}^{n} \prod_{\substack{j=1 \\ j\neq k}}^{n} (X - \alpha_j),$$

ce qui donne, pour tout $\ell \in [\![1; n]\!]$,

$$P'(\alpha_\ell) = a_n \prod_{\substack{j=1 \\ j\neq \ell}}^{n} (\alpha_\ell - \alpha_j).$$

Il s'ensuit que

$$\prod_{\ell=1}^{n} P'(\alpha_\ell) = \prod_{\ell=1}^{n} a_n \prod_{\substack{j=1 \\ j\neq \ell}}^{n} (\alpha_\ell - \alpha_j) = {a_n}^n (-1)^{n(n-1)/2} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2$$

donc

$${a_n}^{n-2}(-1)^{n(n+1)/2} \prod_{\ell=1}^{n} P'(\alpha_\ell) = {a_n}^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2 = \Delta.$$

On a ainsi démontré que

$$\boxed{\Delta = (-1)^{n(n-1)/2} {a_n}^{n-2} \prod_{\ell=1}^{n} P'(\alpha_\ell).}$$

4. Soit $P = X^3 + pX + q$. On note α, β et γ les racines de P. Comme $P' = 3X^2 + p$, on a

$$\begin{aligned}\Delta &= (-1)^{3(3-1)/2} 1^{3-2} (3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p) \\ &= -p^3 - 3(\alpha^2 + \beta^2 + \gamma^2)p^2 - 9(\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2)p - 27(\alpha\beta\gamma)^2\end{aligned}$$

Or les expressions symétriques des racines donnent $\alpha + \beta + \gamma = 0$, $\alpha\beta + \beta\gamma + \gamma\alpha = p$ et $\alpha\beta\gamma = -q$. Il en découle que

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) = -2p$$

et

$$\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 = (\alpha\beta + \beta\gamma + \gamma\alpha)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma) = p^2.$$

Donc

$$\Delta = -p^3 - 3(-2p)p^2 - 9p^3 - 27q^2,$$

c'est-à-dire

$$\boxed{\Delta = -4p^3 - 27q^2.}$$

♦ ***Exercice 29.*** [⋆]
Soit $n \in \mathbb{N}^*$.

1. Exprimer de deux manières l'unique polynôme $L \in \mathbb{R}[X]$, de degré inférieur ou égal à $n-1$, pour lequel $L(k) = k^{n-1}$ pour tout $k \in [\![1; n]\!]$.
2. En déduire une expression simplifiée de $\displaystyle\sum_{k=0}^{n} \binom{n+1}{k} (-1)^{n-k} k^n$.

1. On a évidemment

$$\boxed{L = X^{n-1}.}$$

Par ailleurs, le résultat sur les polynômes de Lagrange nous dit que

$$\boxed{L = \sum_{k=1}^{n} k^{n-1} \prod_{\substack{j=1 \\ j\neq k}}^{n} \frac{X-j}{k-j}.}$$

2. On a

$$L(n+1) = (n+1)^{n-1}$$

et

$$\begin{aligned}L(n+1) &= \sum_{k=1}^{n} k^{n-1} \prod_{\substack{j=1 \\ j\neq k}}^{n} \frac{n+1-j}{k-j} \\ &= \sum_{k=1}^{n} k^{n-1} \Big(\frac{n}{k-1} \times \cdots \times \frac{n-k+2}{1} \times \frac{n-k}{-1} \times \cdots \times \frac{1}{-(n-k)} \Big) \\ &= \sum_{k=1}^{n} k^{n-1} (-1)^{n-k} \frac{n!}{(k-1)!(n-k+1)!} \\ &= \sum_{k=1}^{n} k^{n-1} (-1)^{n-k} \binom{n}{k-1} \\ &= \sum_{k=1}^{n} k^{n-1} (-1)^{n-k} \frac{k}{n+1} \binom{n+1}{k} \\ &= \frac{1}{n+1} \sum_{k=1}^{n} k^n (-1)^{n-k} \binom{n+1}{k},\end{aligned}$$

donc

$$\boxed{\sum_{k=0}^{n} \binom{n+1}{k} (-1)^{n-k} k^n = (n+1)^n.}$$

♦ ***Exercice 30.*** [○]
Soient K un corps fini et $f : K \longrightarrow K$ une application. Démontrer que f est polynomiale.

f est le polynome d'interpolation de Lagrange L telle que $\forall x \in K,\ L(x) = f(x)$, c'est-à-dire

$$\forall x \in K, \qquad f(x) = \sum_{k \in K} f(k) \prod_{j \in K \setminus \{k\}} \frac{t-j}{k-j}.$$

♦ ***Exercice 31.*** [○]
Soient $P \in \mathbb{Z}[X]$, $n \in \mathbb{Z}$ et $m = P(n)$. Démontrer que, pour tout $k \in \mathbb{Z}$, m divise $P(n+km)$.
En déduire qu'il n'existe pas de polynôme $P \in \mathbb{Z}[X]$ non constant tel que, pour tout $n \in \mathbb{N}$, $P(n)$ soit un nombre premier.

Posons $P = a_0 + a_1 X + \cdots + a_d X^d$. Pour tout $k \in \mathbb{Z}$ et tout $\ell \in \mathbb{N}$, on a

$$(n+km)^\ell = \sum_{j=0}^{\ell} \binom{\ell}{j} (km)^j n^{\ell-j} = n^\ell + km \sum_{j=1}^{\ell} \binom{\ell}{j} (km)^{j-1} n^{\ell-j} \equiv n^\ell \ \ [m],$$

donc, pour tout $k \in \mathbb{Z}$, on a

$$P(n+km) = \sum_{\ell=0}^{d} a_\ell (n+km)^\ell \equiv \sum_{\ell=0}^{d} a_\ell n^\ell \equiv P(n) \equiv 0 \ \ [m],$$

c'est-à-dire

pour tout $k \in \mathbb{Z}$, m divise $P(n+km)$.

Soit $P \in \mathbb{Z}[X]$ tel que, pour tout $n \in \mathbb{N}$, $P(n)$ soit un nombre premier. On pose $p = P(0)$. Alors, d'après le résultat ci-dessus, pour tout $k \in \mathbb{Z}$, on a $P(kp)$ est divisible par p. Comme $P(kp)$ est premier pour tout $k \in \mathbb{Z}$, on a nécessairement $P(kp) = p$ pour tout $k \in \mathbb{Z}$. Le polynôme P prend donc la valeur p sur une infinité de valeurs, ce qui signifie que P est constant à la valeur p. Ainsi,

il n'existe pas de polynôme $P \in \mathbb{Z}[X]$ non constant tel que, pour tout $n \in \mathbb{N}$, $P(n)$ soit un nombre premier.

♦ ***Exercice 32.*** [○]
Soit $P \in \mathbb{Z}[X]$ tel que $P(0)$ et $P(1)$ soient impairs. Prouver que P n'a pas de racine dans $\mathbb{Z}$.

Notons $P = a_0 + a_1 X + \cdots + a_n X^n$ avec a_0 et $a_0 + a_1 + \cdots + a_n$ impairs.
Si m est pair alors $P(m) = a_0 + a_1 m + \cdots + a_n m^n$ est impair donc $P(m) \neq 0$.
Si m est impair alors $P(m) = a_1(m-1) + \cdots + a_n(m^n - 1) + (a_0 + a_1 + \cdots + a_n)$ est impair donc $P(m) \neq 0$.
En conclusion,

P n'admet pas de racine dans $\mathbb{Z}$.

♦ ***Exercice 33.*** [★]
1. Soient $P, Q \in \mathbb{Q}[X]$ deux polynômes irréductibles non associés. Démontrer qu'ils n'ont pas de racine complexe en commun.
2. Soit P un polynôme irréductible de $\mathbb{Q}[X]$. Démontrer que P n'a pas de racine complexe multiple.
3. Démontrer que, pour tout $n \in \mathbb{N}^*$, le polynôme $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$. *Indication : factoriser.*

1. Comme $P, Q \in \mathbb{Q}[X]$ sont deux polynômes irréductibles distincts de $\mathbb{Q}[X]$, ils sont premiers entre eux. Il existe donc $U, V \in \mathbb{Q}[X]$ tel que $UP + VQ = 1$. Dès lors, si P et Q avaient une racine complexe en commun, celle-ci serait une racine de 1, ce qui est absurde ! Donc

P et Q n'ont pas de racine complexe en commun.

2. Raisonnons par l'absurde en supposant que P admet une racine multiple dans $\mathbb{C}$. Alors P et P' ne seraient pas premiers entre eux, autrement dit on aurait $P \wedge P' \neq 1$. Mais $P \wedge P'$ se calculant par l'algorithme d'Euclide, c'est un polynôme à coefficients dans $\mathbb{Q}$. Ainsi, P serait divisible par un polynôme non constant de $\mathbb{Q}[X]$, ce qui est absurde pour un polynôme irréductible. Donc

$$\boxed{P \text{ n'a pas de racine complexe multiple.}}$$

3. Soit $n \in \mathbb{N}^*$. Les racines de $P_n = X^n - 2$ sont les racines n-èmes de 2, c'est-à-dire les nombres complexes $2^{1/n}\,\mathrm{e}^{2ik\pi/n}$ où k décrit $[\![0; n-1]\!]$. La factorisation de P sur $\mathbb{C}$ prend donc l'allure suivante

$$P_n = \prod_{k=0}^{n-1} (X - 2^{1/n}\,\mathrm{e}^{2ik\pi/n}).$$

Raisonnons alors par l'absurde en supposant que $P_n = X^n - 2$ admet un diviseur $Q \in \mathbb{Q}[X]$ de degré $p \in [\![1; n-1]\!]$. La décomposition ci-dessus nous dit que, peu importe les facteurs irréductibles de la décomposition primaire de Q sur $\mathbb{C}$, le terme constant de Q est nécessairement de la forme $\pm 2^{p/n}$ avec $0 < p/n < n$. Or $2^{p/n} \notin \mathbb{Q}$ donc c'est absurde ! En conclusion,

$$\boxed{X^n - 2 \text{ est irréductible dans } \mathbb{Q}[X].}$$

Il y a donc dans $\mathbb{Q}[X]$ des polynômes irréductibles de degré arbitrairement élevé.

♦ ***Exercice 34.*** [⋆] (Polynôme conjugué)

Pour tout polynôme $P = a_0 + a_1 X + \cdots + a_n X^n$ à coefficients complexes, on définit le polynôme conjugué de P, noté $\overline{P}$, par la formule

$$\overline{P} = \overline{a_0} + \overline{a_1} X + \cdots + \overline{a_n} X^n.$$

1. Démontrer que $\forall z \in \mathbb{C}$, $\overline{P}(\overline{z}) = \overline{P(z)}$.
2. Soit P un polynôme à coefficients complexes tel que $\forall x \in \mathbb{R}$, $P(x) \in \mathbb{R}$. Démontrer que P est à coefficients réels.
3. Soit P un polynôme à coefficients complexes.

   On pose $R = P\overline{P}$. Démontrer que le polynôme R est à coefficients réels.

   En déduire qu'il est équivalent de dire que « tout polynôme à coefficients complexes non constant admet une racine complexe » (théorème de d'Alembert Gauß) et de dire que « tout polynôme à coefficients réels non constant admet une racine complexe ».

1. On utilise successivement que le conjugué d'une somme est la somme des conjugués et que le conjugué d'un produit est le produit des conjugués pour écrire que, pour tout $z \in \mathbb{C}$,

$$\overline{P(z)} = \overline{a_0 + a_1 z + \cdots + a_n z^n} = \overline{a_0} + \overline{a_1}\overline{z} + \cdots + \overline{a_n}\overline{z}^n = \overline{P}(\overline{z}),$$

donc

$$\boxed{\forall z \in \mathbb{C}, \qquad \overline{P(z)} = \overline{P}(\overline{z}).}$$

2. Pour tout nombre réel x, on a $P(x) = \overline{P(x)} = \overline{P}(\overline{x}) = \overline{P}(x)$ donc tout nombre réel est racine de $Q = P - \overline{P}$. Cela implique que Q est nul (puisqu'il admet une infinité de racines et que seul le polynôme sait faire cela). On en déduit que $P = \overline{P}$ et par identification des coefficients de P et $\overline{P}$, on obtient $\forall i \in [\![0; n]\!]$, $a_i = \overline{a_i}$, c'est-à-dire que

$$\boxed{\text{les coefficients de } P \text{ sont des nombres réels.}}$$

3. a) Pour obtenir le résultat souhaité, il suffit, d'après la question précédente, de justifier que $R(\mathbb{R}) \subset \mathbb{R}$. Or, pour tout nombre réel x, on a $R(x) = P(x)\overline{P}(x) = P(x)\overline{P}(\overline{x}) = P(x)\overline{P(x)} = |P(x)|^2 \in \mathbb{R}$, où l'on a utilisé l'égalité $\overline{x} = x$ et le résultat de la question 1. Donc

$$\boxed{\text{le polynôme } R \text{ est à coefficients réels.}}$$

   b) Si $R(z_0) = 0$ alors $P(z_0) = 0$ ou $\overline{P}(z_0) = 0$. Dans le premier cas, z_0 est racine de P et dans le deuxième cas, on peut écrire, en utilisant le résultat de la question 1 et l'égalité $\overline{\overline{P}} = P$, que $0 = \overline{0} = \overline{\overline{P}(z_0)} = \overline{\overline{P}}(\overline{z_0}) = P(\overline{z_0})$ d'où on tire que $\overline{z_0}$ est alors racine de P. Ainsi,

$$\boxed{\text{si } R(z) \text{ admet une racine } z_0 \in \mathbb{C} \text{ alors } P(z) \text{ admet } z_0 \text{ ou } \overline{z_0} \text{ comme racine.}}$$

c) Si « tout polynôme à coefficients complexes de degré $\geqslant 1$ admet une racine complexe » alors, comme $\mathbb{R} \subset \mathbb{C}$, on a, a fortiori, que « tout polynôme à coefficients réels de degré $\geqslant 1$ admet une racine complexe ».

Réciproquement, on considère un polynôme P à coefficients complexes de degré $\geqslant 1$ et l'on introduit le polynôme $R = P\overline{P}$. On sait alors que R est un polynôme à coefficients réels (on l'a montré en 2. a)) et que son degré est $\geqslant 1$ (car $\deg R = 2 \deg P$). Ainsi, par hypothèse, R admet une racine complexe z_0, ce qui signifie que $P(z_0) = 0$ ou $\overline{P}(z_0) = 0$. Dans le premier cas, z_0 est racine de P et dans le deuxième cas, on peut écrire, en utilisant le résultat de la question 1 et l'égalité $\overline{\overline{P}} = P$, que $0 = \overline{0} = \overline{\overline{P}(z_0)} = \overline{\overline{P}}(\overline{z_0}) = P(\overline{z_0})$ d'où on tire que $\overline{z_0}$ est alors racine de P.

En conclusion, on a

il est équivalent de dire que « tout polynôme à coefficients complexes non constant admet une racine complexe » (théorème de d'Alembert Gauß) et de dire que « tout polynôme à coefficients réels non constant admet une racine complexe ».