

DS

du 26/3/2025

Tout appareil connecté est interdit. Calculatrices interdites.

CORRECTION

EXERCICE 1: THÉORÈME DE WILSON

- ① Pour $n = 2$, $1 + (n - 1)! = 2$ est divisible par 2 et 2 est un nombre premier.
 Pour $n = 3$, $1 + (n - 1)! = 3$ est divisible par 3 et 3 est premier.
 Pour $n = 4$, $1 + (n - 1)! = 7$ n'est pas divisible par 4 et 4 n'est pas un nombre premier.
 Le théorème est vérifié pour $n = 2, 3, 4$.
 Dans la suite, on fixe $n > 4$.
- ② Soit $n > 4$ un entier non premier. Alors il existe $p, q \in \llbracket 2, n - 1 \rrbracket, n = pq$
- Si $p \neq q$, comme $(n - 1)! = \prod_{k=1}^{n-1} k$, on aura à un moment $k = p$ puis $k = q$, ainsi, $p \cdot q$ divise $(n - 1)!$.
 - Si $p = q$, comme $n \geq 3$, alors $p \neq 2$, et $n = p^2 \geq 3p > 2p$. Ainsi, dans le produit $(n - 1)!$ intervient une fois p lorsque $k = p$ et une deuxième fois lorsque $k = 2p$, donc $p^2 \mid (n - 1)!$.
- ③ Si n divise $(n - 1)! + 1$ alors $n^2 \mid 1$, d'après la question précédente, donc $n = \pm 1$. Absurde car $n \geq 4$.
- ④ Par contraposée, on a montré que si n divise $1 + (n - 1)!$, alors n est premier.
- ⑤ Soit $k, x \in \llbracket 1, n - 1 \rrbracket$. Par définition du reste r dans la division euclidienne de kx par n , on a $r \in \llbracket 0, n - 1 \rrbracket$. De plus, si $r = 0$, cela signifie que n divise kx . Or n est un nombre premier qui divise un produit, donc n divise soit x soit k , ce qui est impossible car $k, x \in \llbracket 1, n - 1 \rrbracket$. Donc $r \in \llbracket 1, n - 1 \rrbracket$.
- ⑥ Soit $k \in \llbracket 1, n - 1 \rrbracket$ et x, y deux entiers de $\llbracket 1, n - 1 \rrbracket$. On suppose que $\varphi_k(x) = \varphi_k(y)$. Alors cela signifie que n divise $kx - ky = k(x - y)$. Or n est un nombre premier, qui ne divise pas $k \in \llbracket 1, n - 1 \rrbracket$, donc n est premier avec k . D'après le lemme de Gauss, $n \mid (x - y)$. Or $x - y \in \llbracket -(n - 1), n - 1 \rrbracket$, et dans cet intervalle le seul multiple de n est 0. Donc $x = y$. Par définition, on a montré que L'application φ_k est injective.
- ⑦ (a) Soit $k \in \llbracket 1, n - 1 \rrbracket$. Ainsi, n ne divise pas k . Comme n est un nombre premier, n est premier avec k . D'après le théorème de Bézout, il existe $a_0, b_0 \in \mathbb{Z}$ tel que $a_0 n + b_0 k = 1$.
- (b) • **Analyse.** Soit (a, b) un autre couple solution. Alors $an + bk = a_0 n + b_0 k$. Donc $n(a - a_0) = k(b_0 - b)$. n divise le premier membre, donc il divise $k(b_0 - b)$. Or n est premier avec k , d'après le théorème de Gauss, $n \mid b_0 - b$. Il existe donc $c \in \mathbb{Z}$, tel que $b_0 - b = cn$. En remplaçant, on a $n(a - a_0) = ckn$ Donc $a = a_0 + ck$ et $b = b_0 - cn$.
- **Synthèse.** $n(a_0 + ck) + k(b_0 - cn) = a_0 n + b_0 k = 1$.
 L'ensemble des solutions de cette équation est $\{(a_0 + ck, b_0 - cn) \mid c \in \mathbb{Z}\}$.

- ③ Par équivalence, on a $b'k \equiv 1[n] \Leftrightarrow \exists a' \in \mathbb{Z}, b'k + a'n = 1 \Leftrightarrow \exists c \in \mathbb{Z}, b' = b_0 - cn$.

On effectue alors la division euclidienne de b_0 par n , soit, il existe $(q, r) \in \mathbb{Z} \times \llbracket 0, n-1 \rrbracket$, $b_0 = nq + r$. En prenant $c = q$, on obtient $rk \equiv 1[n]$ et $r \in \llbracket 0, n-1 \rrbracket$.

De plus, $r \neq 0$ car sinon, $rk = 0$.

On vient de montrer $\text{l'existence de } b' = r \in \llbracket 1, n-1 \rrbracket \text{ tel que } b'k \equiv 1[n]$.

- ⑧ Soit $k \in \llbracket 1, n-1 \rrbracket$. L'existence vient de la question précédente: comme $b'k \equiv 1[n]$, alors le reste de la division euclidienne de $b'k$ par n est 1, donc $\varphi_k(b') = 1$.

De plus, on a montré à la question ⑥ que φ_k est injective, d'où l'unicité de l'antécédent s'il existe.

Donc $\forall k \in \llbracket 1, n-1 \rrbracket, \exists ! k' \in \llbracket 1, n-1 \rrbracket, \varphi_k(k') = 1$.

- ⑨ • Supposons que $\varphi_k(k) = 1$, alors le reste de la division euclidienne de k^2 par n est 1, donc $n|k^2 - 1 = (k-1)(k+1)$.

Or n est un nombre premier qui divise un produit, donc n divise l'un des facteurs.

Si $n|k-1$, comme $k-1 \in \llbracket 0, n-2 \rrbracket$, on a $k-1 = 0$ donc $k = 1$.

Sinon, $n|k+1 \in \llbracket 2, n \rrbracket$, donc $k+1 = n$ soit $k = n-1$.

- On suppose que $k = 1$ ou $k = n-1$, alors

▷ si $k = 1$, on a $k^2 = 0 \cdot n + 1$ et $0 \leq 1 < n$ donc $\varphi_k(k) = 1$.

▷ si $k = (n-1)$, on a $k^2 = n \cdot (n-2) + 1$ et $0 \leq 1 < n$ donc $\varphi_k(k) = 1$.

Dans tous les cas, $\varphi_k(k) = 1$.

- ⑩ Soient $x, y \in \llbracket 2, n-2 \rrbracket$. On a

$$\varphi_x(y) = 1 \iff \exists q \in \mathbb{Z}, xy = nq + 1 \iff \varphi_y(x) = 1.$$

- ⑪ Soit k un entier dans $\llbracket 2, n-2 \rrbracket$, d'après la question précédente, $\varphi_k(k) \neq 1$, donc d'après la question ⑧, il existe un unique $k' \in \llbracket 1, n-1 \rrbracket$ différent de k tel que $\varphi_k(k') = 1$. Donc $kk' \equiv 1[n]$.

On prend le produit $2 \dots (n-2)$. On considère l'entier 2 et son $k'_2 \neq 2$ associé, et on les réunit devant. Dans le produit restant, on prend l'entier i_2 suivant, et on le réunit avec "son" $k'_{i_2} \neq i_2$ correspondant (et qui n'est ni 2, ni k'_2 ...). Et ainsi de suite.

Ainsi, le produit s'écrit $2 \dots (n-2) = k_1 k'_1 k_2 k'_2 \dots k_p k'_p$, et on regarde modulo n , pour obtenir

$$2 \dots (n-2) = k_1 k'_1 k_2 k'_2 \dots k_p k'_p = 1^p = 1[n].$$

- ⑫ On multiplie par $n-1$ et on additionne pour obtenir $(n-1)! + 1 \equiv n[n] \equiv 0[n]$, donc n divise $(n-1)! + 1$.

EXERCICE 2

- ① On applique le théorème de Bézout qui nous donne directement l'existence de ce couple, si X^n et $(1-X)^n$ sont premiers entre eux.

Pour vérifier cette dernière assertion, il suffit de voir que ces deux polynômes ont pour seule racine respective 0 et 1, et n'ont donc pas de racine commune.

- ② Si (P, Q) est solution alors le couple $(P + K \cdot X^n, Q - L \cdot (1-X)^n)$ est aussi solution, pour tous polynômes K et L .

Par division euclidienne par X^n , il existe un polynôme K et un polynôme P_0 de degré inférieur strictement à n , tels que $P = K \cdot X^n + P_0$. De cette manière, on obtient un couple de solutions (P_0, Q_0) , avec $\deg P_0 < n$. En passant aux degrés dans l'équation, on remarque que $\deg Q_0 = \deg P_0 < n$.

Pour l'unicité, soient P_1, P_2, Q_1, Q_2 de degrés strictement inférieurs à n tels que $(1-X)^n P_1(X) + X^n Q_1(X) = (1-X)^n P_2(X) + X^n Q_2(X)$. Alors, $(1-X)^n (P_1 - P_2) = X^n (Q_2 - Q_1)$. Or, X^n et $(1-X)^n$ sont premiers entre eux donc le lemme de Gauss entraîne que X^n divise le polynôme $P_1 - P_2$ de degré strictement inférieur à n . Ainsi, $P_1 = P_2$ et par suite $Q_1 = Q_2$.

- ③ En substituant $1-X$ à X dans l'identité précédente, on obtient $X^n P(1-X) + (1-X)^n Q(X) = 1$, $\deg P(1-X) < n$ et $\deg Q(X) < n$, donc l'unicité établie à la deuxième question donne $Q(X) = P(1-X)$.

- ④ D'après les questions précédentes, $(1-X)^n P(X) = -X^n P(1-X) + 1$ ce qui entraîne en dérivant,

$$(1-X)^{n-1}(-nP(X) + (1-X)P'(X)) = X^{n-1}(-nP(1-X) + XP'(1-X)).$$

En utilisant le lemme de Gauss, on obtient que $-nP(X) + (1-X)P'(X)$ est un multiple de X^{n-1} et que son degré est strictement inférieur à n . Il existe donc $\lambda \in \mathbb{R}$ tel que $(1-X)P'(X) - nP(X) = \lambda X^{n-1}$.

- ⑤ Replaçons P dans l'équation juste obtenue. Pour le terme de degré $n-1$, on obtient $(2n-1)p_{n-1} = -\lambda$

et pour les termes de degré $k \in \llbracket 0, n-2 \rrbracket$, $p_{k+1} = p_k \frac{n+k}{k+1}$.

- ⑥ On peut alors remarquer qu'en évaluant l'expression de l'énoncé en 0, on obtient que $p_0 = P(0) = 1$ puis en déduire pour tout $k \in \llbracket 1, n-1 \rrbracket$,

$$p_k = \prod_{j=0}^{k-1} \frac{n+j}{j+1} = \frac{(n+k-1)!}{k!(n-1)!} = \binom{n+k-1}{k}.$$

- ⑦ On peut montrer par vérification rapide que les solutions du système sont les polynômes

$$P_0(X+2)X^n + Q_0(X^2+1)(1-X)^n + X^n(1-X)^n.$$

EXERCICE 3

- ① On fait une étude de fonction: $A' = 3X^2 - 1$.

le tableau de variation de $\tilde{A}$ est:

x	$-\infty$	$-\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$+\infty$			
$\tilde{A}'(x)$		+	0	-	0	+	
$\tilde{A}(x)$	$-\infty$	$\nearrow$	< 0	$\searrow$	< 0	$\nearrow$	$+\infty$

D'après le tableau de variations, $\tilde{A}$ est strictement négative sur $]-\infty, \frac{1}{\sqrt{3}}]$.

Sur $[\frac{1}{\sqrt{3}}, +\infty[$, $\tilde{A}$ est continue, strictement croissante, et $\tilde{A}(\frac{1}{\sqrt{3}}) < 0$, $\lim_{x \rightarrow +\infty} \tilde{A}(x) = +\infty$. Par théorème de bijection, il existe un unique $\alpha \in [\frac{1}{\sqrt{3}}, +\infty[$ racine de A .

(de plus, $\tilde{A}(1) = 1 > 0$, donc $\alpha < 1$.)

- ② si $\alpha \in \mathbb{Q}$, il existerait deux entiers $p \in \mathbb{Z}, q \in \mathbb{N}$ premiers entre eux tels que $\alpha = \frac{p}{q}$. Alors, $p^3 - pq^2 = -q^3$. p divise le membre de gauche, donc il divise $-q^3$; or p est premier avec q , donc par théorème de Gauss (appliquée 3 fois), $p \mid -1$. donc $p = \pm 1$.

De même, $p^3 = q(-q^2 + pq)$ donc $q \mid 1$. Ainsi, $q = 1$. Les seules racines rationnelles possibles sont -1 et 1 qui ne conviennent pas.

Ainsi, $\alpha \notin \mathbb{Q}$.

- ③ Le polynôme A est de degré 3, sans racine dans $\mathbb{Q}$: il est donc irréductible dans $\mathbb{Q}[X]$ (si on pouvait le factoriser comme produit de deux polynômes PQ où $\deg(P) > 0$ et $\deg(Q) > 0$, alors on aurait $\deg(P) = 1$ ou $\deg(Q) = 1$, et P ou Q aurait une racine rationnelle, donc A aussi. contradiction).

Dans $\mathbb{R}$, A a une racine donc on peut le factoriser par $X - \alpha$: A n'est pas irréductible dans $\mathbb{R}$.

- ④ Soit β une des deux autres racines. Alors cette autre racine est complexe non réelle, et la troisième racine est donc $\bar{\beta}$.

Dans $\mathbb{C}$, le polynôme A est scindé, et d'après les relations coefficients racines:

$$\alpha + \beta + \bar{\beta} = \sigma_1 = 0, \text{ donc } \boxed{\operatorname{Re}(\beta) = \frac{-\alpha}{2}}.$$

$$\text{De même, } \alpha\beta\bar{\beta} = \sigma_3 = \frac{-(-1)}{1} = 1, \text{ donc } \boxed{|\beta|^2 = \frac{1}{\alpha}}.$$

- ⑤ En posant la division euclidienne de $P = X^5 + 2X^4 - 3X^3$ par $A = X^3 - X - 1$, on obtient:

$$\boxed{P = (X^2 + 2X - 2)A + 3X^2 - 2 \quad \text{et} \quad \deg(3X^2 - 2) < \deg(A) = 3}$$

- ⑥ EN regardant l'égalité précédente en $\alpha : x = 0 + 3\alpha^2 - 2$ car $\tilde{A}(\alpha) = 0$. Ainsi,

$$\boxed{\text{si } B = 3X^2 - 2 \in \mathbb{Q}_2[X], x = \tilde{B}(\alpha)}.$$

- ⑦ On pose $A_1 = \mathbb{Q}[\alpha] = \{\tilde{B}(\alpha) \mid B \in \mathbb{Q}[X]\}$

et $A_2 = \{\tilde{B}(\alpha) \mid B \in \mathbb{Q}_2[X]\}$.

• Clairement, $A_2 \subset A_1$

• Réciproque. Soit $x \in A_1$. Alors : $\exists B \in \mathbb{Q}[X], x = \tilde{B}(\alpha)$.

J'effectue la division euclidienne de B par A dans $\mathbb{Q}[X]$ et je note $B_1 \in \mathbb{Q}[X]$ le reste:

$\exists Q \in \mathbb{Q}[X], B = QA + B_1$ et $\deg(B_1) < 3$. En regardant en α qui annule A :

$x = \tilde{B}(\alpha) = \tilde{B}_1(\alpha)$ et $\deg(B_1) \leq 2$ donc $x \in A_2$.

CONCLUSION $\boxed{A_1 = A_2}$.

Comme α est racine de A , alors $\alpha^3 = \alpha + 1$

$$\text{Donc } x = \alpha^3(\alpha^2 + 2\alpha - 3) = (\alpha + 1)(\alpha^2 + 2\alpha - 3) = \alpha^3 + 3\alpha^2 - \alpha - 3 = \boxed{3\alpha^2 - 2}.$$

(On aurait aussi pu faire la division euclidienne de $X^5 + 2X^4 - 3X^3$ par A .

- ⑧ Soit $A = X^3 - X - 1$ et $B = X^2 + 2X$

$$A = (X - 2)B(X) + 3X - 1 \quad \text{Alors } 3X - 1 = A - (X - 2)B$$

$$B(X) = (\frac{1}{3}X + \frac{7}{9})(3X - 1) + \frac{7}{9} \quad \text{Alors } \frac{7}{9} = B - (\frac{1}{3})(X + \frac{7}{9})(3X - 1) = B - \frac{1}{9}(3X + 7)(A - (X - 2)B)$$

$$\text{Soit } 7 = 9B + (3X + 7)(X - 2)B - (3X + 7)A \text{ ou encore: } \boxed{1 = \frac{1}{7}(3X^2 + X - 5)B - \frac{1}{7}(3X + 7)A}$$

$$U = -\frac{1}{7}(3X + 7) \text{ et } V = \frac{1}{7}(3X^2 + X - 5) \text{ conviennent.}$$

- ⑨ Il suffit de regarder l'égalité précédente en α :

$$\tilde{A}(\alpha)\tilde{U}(\alpha) + \tilde{B}(\alpha)\tilde{V}(\alpha) = 1. \text{ Alors:}$$

$(\alpha^2 + \alpha)\tilde{V}(\alpha) = 1$. Comme $V \in \mathbb{Q}[X]$, alors $\tilde{V}(\alpha) \in \mathbb{Q}[\alpha]$. Ainsi y est inversible dans $\mathbb{Q}[\alpha]$ et son inverse est : $\tilde{V}(\alpha) = \frac{1}{\alpha^2 + \alpha}(3\alpha^2 + \alpha - 5)$.

- ⑩ Soit $\beta \in \mathbb{Q}[\alpha] \setminus \{0\}$. Alors il existe un polynôme $B \in \mathbb{Q}_2[X]$ tel que $\beta = \tilde{B}(\alpha)$. Comme A est un polynôme irréductible, et que $\deg(A|B) < 3$; alors A et B sont premiers entre eux.

D'après le théorème de Bézout, il existe $U, V \in \mathbb{Q}[X]$ tel que: $AU + BV = 1$.

En regardant en α , on obtient que $\tilde{V}(\alpha)\beta = 1$ et $\tilde{V}(\alpha) \in \mathbb{Q}[\alpha]$.

Conclusion: tout élément non nul de $\mathbb{Q}[\alpha]$ possède un inverse dans cet ensemble, qui a déjà une structure d'anneau commutatif, donc $\boxed{\mathbb{Q}[\alpha] \text{ est un corps.}}$

- ⑪ Soit φ un automorphisme de ce corps. On a admis: $\forall r \in \mathbb{Q}, \varphi(r) = r$.

Il reste à trouver l'image de α pour avoir l'image de tout $\mathbb{Q}[\alpha]$.

Or $\alpha^3 - \alpha - 1 = 0$. Ainsi

$\varphi(0) = 0 = \varphi(\alpha^3 - \alpha - 1) = \varphi(\alpha)^3 - \varphi(\alpha) - 1$. Donc $\varphi(\alpha)$ est une racine de A . De plus, elle est réelle car $\varphi : \mathbb{Q}[\alpha] \rightarrow \mathbb{Q}[\alpha] \subset \mathbb{R}$. Or A ne possède qu'une seule racine réelle, donc $\varphi(\alpha) = \alpha$.

Ainsi, pour tout polynôme $P \in \mathbb{Q}[X]$, comme φ est un automorphisme,

$\varphi(\tilde{P}(\alpha)) = \tilde{P}(\varphi(\alpha)) = \tilde{P}(\alpha)$. **Le seul automorphisme du corps $\mathbb{Q}[\alpha]$ est l'identité.**

EXERCICE 4

- ① **Solutions constantes.** Soit $P(X) = c \in \mathbb{C}$. L'équation $(\star)$ devient

$$c = c^2,$$

d'où $c = 0$ ou $c = 1$.

- ② **Unicité du coefficient dominant.** Soit $P \in \mathcal{E}$ de degré d et de coefficient dominant $\alpha \neq 0$. Le terme dominant de $P(X^2)$ est αX^{2d} , celui de $P(X+a)P(X+b)$ est $\alpha^2 X^{2d}$. On obtient $\alpha = \alpha^2$, donc $\alpha = 1$.

- ③ **Cas $a = b$.**

- (a) En comparant le nombre de racines distinctes de $P(X^2)$ et de $P(X+a)^2$, on montre que toute racine de P est nulle.
 (b) On en déduit que $P(X) = X^n$. L'équation impose alors $a = 0$. Ainsi :

$$\mathcal{E} = \begin{cases} \{X^n \mid n \geq 1\} & \text{si } a = 0, \\ \emptyset & \text{sinon.} \end{cases}$$

- ④ **Unicité à degré fixé.**

- (a) Un calcul direct donne $D(X^2) = R(X)$ et $\deg R = \deg P + \deg D$.
 (b) En comparant les degrés, on obtient $\deg D = \deg P$, ce qui impose $D = 0$. Donc $P = Q$.

- ⑤ Si $a, b \in \mathbb{R}$, alors $\overline{P}$ est aussi solution. Par unicité à degré fixé, $P = \overline{P}$, donc $P \in \mathbb{R}[X]$.

- ⑥ **Cas $a = 0, b = -1$.**

- (a) Par itération, α^{2^n} est racine pour tout n .
 (b) Cela impose $\alpha = 0$ ou $|\alpha| = 1$.
 (c) Le cas $\alpha = 0$ est impossible.
 (d) On obtient alors $|\alpha + 1| = 1$.
 (e) Les seules solutions sont les racines de $X^2 + X + 1$, donc

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

- (f) Ainsi

$$\mathcal{E} = \{(X^2 + X + 1)^n \mid n \geq 1\}.$$

- ⑦ La stabilité par produit découle directement de l'équation $(\star)$.

- ⑧ Résultat classique de factorisation de $A^n - B^n$.

- ⑨ Si $P^n \in \mathcal{E}$ et P est unitaire, alors $P \in \mathcal{E}$.

- ⑩ Les degrés étant des entiers, il existe un unique élément de degré minimal dans $\mathcal{E}$, noté M .

- 11) Tout $P \in \mathcal{E}$ vérifie $P^t = M^s$, d'où $P = M^n$.

$$\mathcal{E} = \{M^n \mid n \in \mathbb{N}^*\}$$