X-ENS Maths A 2019

Partie I

1. $I(\alpha)$ est le noyau du morphisme d'anneaux $f : \left| \begin{array}{ccc} \mathbb{Q}[X] & \longrightarrow & \mathbb{C} \\ P & \longmapsto & P(\alpha) \end{array} \right.$

(morphisme d'évaluation).

Donc $\boxed{I(\alpha) \text{ est un idéal de } \mathbb{Q}[X].}$

De plus, $I(\alpha) \neq \{0\}$ car α est algébrique.

---

2. Si $\alpha \in \mathbb{Q}$, $X - \alpha \in I(\alpha)$

Donc nécessairement, par unicité, $\Pi_\alpha = X - \alpha$ et α est de degré $\deg(X-\alpha) = 1$.

Si, réciproquement, α est de degré 1, on a Π_α de degré 1, unitaire avec α comme racine donc $\Pi_\alpha = X - \alpha \in \mathbb{Q}[X]$ donc $\alpha \in \mathbb{Q}$.

Finalement, $\boxed{\alpha \text{ de degré } 1 \iff \alpha \in \mathbb{Q}.}$

3- (a) Si $\Pi_\alpha = Q \times R$ avec $Q, R \in \mathbb{Q}[X]$,

Alors $Q(\alpha) = 0$ ou $R(\alpha) = 0$

donc $Q \in I(\alpha)$ ou $R \in I(\alpha)$

donc $\Pi_\alpha \mid Q$ ou $\Pi_\alpha \mid R$

et comme $Q \mid \Pi_\alpha$ et $R \mid \Pi_\alpha$

On a $\begin{cases} Q \in \mathbb{Q}^* \Pi_\alpha \\ R \text{ constant} \end{cases}$ ou $\begin{cases} R \in \mathbb{Q}^* \Pi_\alpha \\ Q \text{ constant} \end{cases}$

Donc $\boxed{\Pi_\alpha \text{ est irréductible.}}$

(b) $P \in \mathbb{Q}[X]$ unitaire et irréductible.

$z \in \mathbb{C}$ racine de P est bien algébrique.

Alors, par définition, $P \in I(z)$

donc $\Pi_z \mid P$. Comme Π_z et P sont tous deux unitaires et irréductible, $\boxed{P = \Pi_z}$

---

4 (a) $A, B \in \mathbb{Q}[X]$ avec une racine commune $z \in \mathbb{C}$

Alors z est racine de $A \wedge B$ donc

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

(Rappel : l'algorithme d'Euclide permet de voir que le pgcd est le même dans tout corps.)

(b) Supposons que Π_α ait une racine multiple $z \in \mathbb{C}$.

On a $\Pi_\alpha(z) = 0$ donc $\Pi_z \mid \Pi_\alpha$.

Comme Π_z et Π_α sont unitaires et irréductibles, $\Pi_z = \Pi_\alpha$.

Puis $\Pi_\alpha'(z) = 0$ et $\Pi_\alpha' \in \mathbb{Q}[X]$

donc $\Pi_z = \Pi_\alpha \mid \Pi_\alpha'$

Or $\deg \Pi_\alpha' < \deg \Pi_\alpha$ et $\Pi_\alpha \neq 0_{\mathbb{Q}[X]}$

ce qui est contradictoire.

Donc $\boxed{\text{les racines complexes de } \Pi_\alpha \text{ sont simples.}}$

---

5 (a) Soit $\alpha \in \mathbb{Q}$ entier algébrique : On a $P \in \mathbb{Z}[X] \setminus \{0\}$ unitaire tel que $P(\alpha) = 0$. On note $P = a_0 + a_1 X + \dots + a_{n-1} X^{n-1} + X^n$ avec $a_0, \dots, a_{n-1} \in \mathbb{Z}$. Alors $a_0 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1} + \alpha^n = 0$

En écrivant $\alpha = \frac{p}{q}$ avec $\begin{cases} p \wedge q = 1 \\ q > 0 \end{cases}$, on tire

$$a_0 q^n + a_1 p q^{n-1} + \dots + a_{n-1} p^{n-1} q + p^n = 0$$

Donc $q \mid p^n$ et $q \wedge p = 1$ et $q > 0$ donc $q = 1$.

Ainsi $\boxed{\alpha \in \mathbb{Z}.}$

(b) Soit $\alpha \in \mathbb{C}$ entier algébrique. __But__ : $\Pi_\alpha \in \mathbb{Z}[X]$.

On a $P \in \mathbb{Z}[X]$ unitaire tel que $P(\alpha) = 0$.

Alors $\Pi_\alpha \mid P$: On a $Q \in \mathbb{Q}[X]$ tel que $P = \Pi_\alpha \times Q$

Alors toute racine de Π_α est aussi racine de P donc est un entier algébrique.

Or les coefficients de Π_α sont des rationnels, $\pm$ somme de produits de ces racines (relation coefficients - racines, Π_α scindé dans $\mathbb{C}$) ils ces coefficients rationnels sont donc, avec le théorème admis, des entiers algébriques, et avec 5.a, ils sont entiers.

Ainsi, $\boxed{\Pi_\alpha \in \mathbb{Z}[X].}$

---

6. (a) $|\alpha| = 1$, $\deg \Pi_\alpha = 2$, α entier algébrique. Alors $\alpha \notin \mathbb{Q}$.

D'après la question précédente, $\Pi_\alpha \in \mathbb{Z}[X]$.

Mais comme $\Pi_\alpha \in \mathbb{R}[X]$, $\bar{\alpha}$ est aussi racine de Π_α donc

$$\Pi_\alpha = (X - \alpha)(X - \bar{\alpha}) = X^2 - 2\mathrm{Re}(\alpha) X + |\alpha|^2$$
$$= X^2 - 2\mathrm{Re}(\alpha) X + 1$$

avec $-2\mathrm{Re}(\alpha) \in \mathbb{Z}$ et $|\mathrm{Re}(\alpha)| < |\alpha| = 1$
strict car $\alpha \neq \bar{\alpha}$ vu 4.b donc $\mathrm{Im}\,\alpha =$

donc $-2\,\mathrm{Re}(\alpha) \in]\!]-2, 2[\![= \{-1, 0, 1\}$.

• Soit $\Pi_\alpha = X^2+1$ donc $X^4-1=(X^2-1)(X^2+1)\in I(\alpha)$
et $\alpha\in \mathbb{U}_4$.

• Soit $\Pi_\alpha = X^2+X+1$ donc $X^3-1=(X-1)(X^2+X+1)\in I(\alpha)$
et $\alpha\in\mathbb{U}_3$.

• Soit $\Pi_\alpha = X^2-X+1$ donc $X^6-1=(X^2-X+1)(X^4+X^3-X-1)$
$\in I(\alpha)$
et $\alpha \in \mathbb{U}_6$

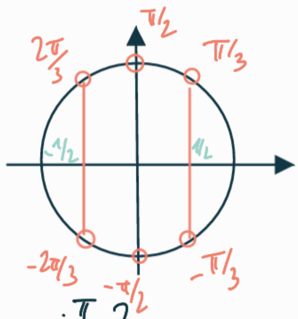
(Si cela ne saute pas aux yeux, on peut écrire

$$\alpha^2=\alpha-1 \quad \text{donc} \quad \alpha^6=(\alpha-1)^3 = \alpha^3-3\alpha^2+3\alpha-1$$
$$= (\alpha^2-\alpha)-3(\alpha-1)+3\alpha-1$$
$$= -1-3\alpha+3+3\alpha-1$$
$$= 1.$$

ou remarquer que $\alpha\in\{-j,-\bar{j}\}$)

Dans tous les cas, $\boxed{\alpha \text{ est une racine de l'unité.}}$

Autre argumentation possible: écrire $\alpha=e^{i\theta}$



alors $-2\mathrm{Re}(\alpha) = -2\cos\theta \in\{-1,0,1\}$

donc $\cos\theta\in\{-\frac{1}{2},0,\frac{1}{2}\}$

donc $\alpha\in\left\{e^{\frac{2i\pi}{3}}, e^{-\frac{2i\pi}{3}}, e^{\frac{i\pi}{3}}, e^{-\frac{i\pi}{3}}, e^{i\frac{\pi}{2}}, e^{-i\frac{\pi}{2}}\right\}$

donc $\boxed{\alpha \text{ racine de l'unité.}}$

---

6 (b) Soit $\alpha=\dfrac{3+4i}{5}$. Alors $|\alpha|^2=\dfrac{9+16}{25}=1$ donc $\boxed{\alpha\in\mathbb{U}.}$

$\alpha\notin\mathbb{Q}$ donc α n'est pas algébrique de degré 1

et $(X-\alpha)(X-\bar{\alpha}) = X^2-2\mathrm{Re}(\alpha)X+1 = X^2-\frac{6}{5}X+1 \in \mathbb{Q}[X]$ unitaire

donc $\Pi_\alpha = X^2-\frac{6}{5}X+1$ et $\boxed{\alpha \text{ algébrique de degré } 2.}$

Reste à montrer que $\boxed{\alpha \text{ n'est pas une racine de l'unité.}}$

Or, si c'était le cas, α annulerait $X^n - 1$ donc serait un entier algébrique et donc $\Pi_\alpha \in \mathbb{Z}[X]$ par 5.b ce qui est faux ici.

Partie 2 : C'est très classique (polynômes cyclotomiques)

7_ Soit $n \geq 1$. $X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right)$

Or $\forall d \in [\![1, n-1]\!]$, $\left(e^{\frac{2ik\pi}{n}}\right)^d \neq 1 \iff \forall d \in [\![1, n-1]\!]$, $\frac{2kd\pi}{n} \notin 2\pi\mathbb{Z}$

$\iff \forall d \in [\![1, n-1]\!]$, $kd \notin n\mathbb{Z}$

$\iff \forall d \in [\![1, n-1]\!]$, $kd \not\equiv 0 \, [n]$

$\iff k \wedge n = 1$

En effet, si $k \wedge n \neq 1$, $d = \frac{n}{k \wedge n} \in [\![1, n-1]\!]$ et $k \times d = k \vee n \equiv 0 \, [n]$

et si $k \wedge n = 1$, on a une relation de Bézout

$$ku + nv = 1 \quad \text{avec } u, v \in \mathbb{Z}$$

donc $ku \equiv 1 \, [n]$

et $\forall d \in [\![1, n-1]\!]$, $kd \times u \equiv d \, [n]$ $\not\equiv 0 \, [n]$ donc $kd \not\equiv 0 \, [n]$.

donc $\mathbb{P}_n = \left\{ e^{\frac{2ik\pi}{n}},\ k \wedge n = 1 \right\}$

Alors $\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}},\ k \in [\![0, n-1]\!] \right\}$

$$\underset{\substack{\text{on simplifie} \\ \text{la fraction } \frac{k}{n} \\ \text{de manière unique}}}{=} \bigsqcup_{d | n} \left\{ e^{\frac{2il\pi}{d}},\ l \wedge d = 1 \right\}$$

$$= \bigsqcup_{d | n} \mathbb{P}_d$$

Remarque : le dernier chapitre d'algèbre nous permettra de conclure plus rapidement (anneau $\mathbb{Z}/n\mathbb{Z}$ ou ordre d'un élément dans un groupe : $\mathbb{P}_d$ contient les éléments du groupe $(\mathbb{U}_n, \times)$ d'ordre d...)

donc $X^n - 1 = \prod_{z \in \mathbb{U}_n} (X - z) = \prod_{d | n} \prod_{z \in \mathbb{P}_d} (X - z)$

donc $\boxed{X^n - 1 = \prod_{d|n} \Phi_d}$.

8(a) p premier, $k \in \mathbb{N}^*$. D'après la question précédente,

$$X^{p^k} - 1 = \prod_{d|p^k} \Phi_d = \prod_{l=0}^{k} \Phi_{p^l}$$

$$= \Phi_{p^k} \times \prod_{l=0}^{k-1} \Phi_{p^l} = \Phi_{p^k} \prod_{d|p^{k-1}} \Phi_d$$

$$= \Phi_{p^k} \times \left(X^{p^{k-1}} - 1\right) \text{ toujours d'après 7.}$$

donc $\Phi_{p^k} = \dfrac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = \dfrac{1 - (X^{p^{k-1}})^p}{1 - X^{p^{k-1}}} = \sum_{l=0}^{p-1} \left(X^{p^{k-1}}\right)^l$ (somme géométrique)

donc $\boxed{\Phi_{p^k} = X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + \dots + X^{p^{k-1}} + 1}$

8.(b) $\boxed{\Phi_1 = X - 1}$ car $\mathbb{P}_1 = \{1\}$

Dans (a), on a en particulier $\Phi_p = X^{p-1} + \dots + X + 1$

$\boxed{\Phi_2 = \Phi_{2^1} = X + 1}$ d'après (a)

$\boxed{\Phi_3 = \Phi_{3^1} = X^2 + X + 1}$ d'après (a)

$\boxed{\Phi_4 = \Phi_{2^2} = X^2 + 1}$ d'après (a)

$\boxed{\Phi_5 = \Phi_{5^1} = X^4 + X^3 + X^2 + X + 1}$ d'après (a)

$$X^6 - 1 = \Phi_6 \times \Phi_3 \times \Phi_2 \times \Phi_1 \text{ d'après 7.}$$

$$= \Phi_6 \times (X^2 + X + 1)(X+1)(X-1) = \Phi_6 \times (X^3 - 1)(X+1)$$

donc $\Phi_6 = \dfrac{(X^3)^2 - 1^2}{(X^3-1)(X+1)} = \dfrac{X^3+1}{X+1} = \dfrac{X^3-(-1)^3}{X+1}$

avec $a^3-b^3=(a-b)(a^2+ab+b^2)$

donc $\boxed{\Phi_6 = X^2 - X + 1.}$

On aurait aussi pu voir que

$$\Phi_6 = \prod_{\substack{k\in[\![0,5]\!] \\ k\wedge 6=1}} \left(X - e^{\frac{2ik\pi}{6}}\right) = \left(X-e^{\frac{i\pi}{3}}\right)\left(X-e^{i\frac{5\pi}{3}}\right)$$
$$= \left(X-e^{\frac{i\pi}{3}}\right)\left(X-e^{-i\frac{\pi}{3}}\right) = X^2 - X + 1.$$

9(a) D'après 8. a, $\forall p$ premier, $\forall k\geq 1$, $\Phi_{p^k}(0) = 1$.

On sait aussi que $\Phi_1(0) = -1$.

On montre par récurrence (forte) $\forall n\geq 2$, $\mathcal{P}(n)$: « $\Phi_n(0)=1$ ».

C'est vrai au rang 2 et si on se donne $n\geq 3$ tel que c'est vrai jusqu'au rang $n-1$, alors, avec la question 7,

$$-1 = \prod_{d|n} \Phi_d(0) = \Phi_n(0) \times \underbrace{\prod_{\substack{d|n \\ 2\leq d\leq n-1}} \Phi_d(0)}_{=1 \text{ par HR}} \times \underbrace{\Phi_1(0)}_{=-1}$$

donc $\Phi_n(0)=1$ ce qui établit la récurrence.

Ainsi $\boxed{\Phi_n(0) = \begin{cases} -1 & \text{si } n=1 \\ 1 & \text{si } n\geq 2 \end{cases}}$

9.(b) On a $\Phi_1(1) = 0$ et pourtant p premier et $k\geq 1$

$\Phi_{p^k}(1) = p$ d'après 8. a.

Conjecturons une formule en fonction de la décomposition primaire de n :

Si $n = pq$ avec $p \neq q$ des nombres premiers, d'après la question 7 divisée par $X-1 = \Phi_1$,

$$n = 1^{n-1} + 1^{n-2} + \dots + 1^1 + 1 = \Phi_n(1) \times \underbrace{\Phi_p(1)}_{=p} \times \underbrace{\Phi_q(1)}_{=q}$$

donc $\Phi_n(1) = 1$.

Si $n = p^2 q$, de même, $n = \Phi_n(1) \times \Phi_{pq}(1) \times \Phi_{p^2}(1) \times \Phi_p(1) \times \Phi_q(1)$

$$= \Phi_n(1) \times 1 \times p^2 q$$

donc $\Phi_n(1) = 1$

Soit donc, pour $n \in \mathbb{N}$, $\mathcal{P}(n)$: « $\boxed{\Phi_n(1) = \begin{cases} 0 & \text{si } n = 1 \\ p & \text{si } n = p^k \text{ avec } p \text{ premier}, k \geq 1 \\ 1 & \text{sinon} \end{cases}}$ »

Par récurrence forte :

- L'initialisation a été vue pour $n = 1$ et n de la forme p^k
- Soit $n \geq 2$ tel que $\forall k \leq n-1$, $\mathcal{P}(k)$ vraie.

Soit n a un unique diviseur premier et $\mathcal{P}(n)$ est déjà vue

Soit $n = p_1^{k_1} \dots p_q^{k_q}$ où $p_1, \dots, p_q$ premiers 2 à 2 distincts et $k_1, \dots, k_q \in \mathbb{N}^*$.

Alors, toujours avec 7. simplifiée par $X-1$,

$$n = \Phi_n(1) \times \prod_{\substack{d \mid n \\ d \text{ a au moins} \\ 2 \text{ diviseurs} \\ \text{premiers} \\ \text{et } d \neq n}} \Phi_d(1) \times \prod_{i=1}^{q} \left(\prod_{l=1}^{k_i} \Phi_{p_i^l}(1) \right)$$

$$\underset{HR}{=} \Phi_n(1) \times 1 \times \underbrace{\prod_{i=1}^{q} \left(\underbrace{\prod_{l=1}^{k_i} p_i}_{= p_i^{k_i}} \right)}_{= n}$$

$$= n \, \Phi_n(1)$$

Donc $\Phi_n(1) = 1$, ce qui établit la récurrence.

---

10. Par récurrence forte : $\boxed{\forall n \in \mathbb{N}, \ \Phi_n \in \mathbb{Z}[X].}$

. Si $n = p^k$ où p premier et $k \in \mathbb{N}$, les questions précédentes donnent $\Phi_n \in \mathbb{Z}[X]$.

. Soit $n \geq 2$ tel que $\forall d \leq n-1$, $\Phi_d \in \mathbb{Z}[X]$.

Avec 7., $X^n - 1 = \Phi_n \times \underbrace{\prod_{\substack{d|n \\ d \neq n}} \Phi_d}_{= P \in \mathbb{Z}[X] \text{ par HR}}$

Écrivons $\Phi_n = X^q + a_{q-1} X^{q-1} + \dots + a_1 X + 1$ (avec 9.a)

et $P = X^{n-q} + b_{n-q-1} X^{n-q-1} + \dots + b_1 X - 1$ (avec 9.a)

où $b_1, \dots, b_{n-q-1} \in \mathbb{Z}$

Alors, si $k \in [\![1, n-1]\!]$, le coefficient de degré k de $X^n - 1 = \Phi_n \times P$ est

$$0 = \sum_{l=0}^{k} a_l b_{k-l} = b_k + a_1 b_{k-1} + \dots + a_{k-1} b_1 - a_k$$

donc $\forall k \in [\![1, n-1]\!]$, $a_k = \underbrace{b_k + a_1 b_{k-1} + \dots + a_{k-1} b_1}_{\in \mathbb{Z}}$

On obtient alors par récurrence finie que

$\forall k \in [\![1, n-1]\!]$, $a_k \in \mathbb{Z}$

donc $\boxed{\Phi_n \in \mathbb{Z}[X].}$

11 a) Comme $a_k z^k = (z_1 z)^k + \cdots + (z_n z)^k$

et comme $\forall j \in [\![1,n]\!]$, $R\left(\sum (z_j z)^k\right) = \dfrac{1}{|z_j|} = 1$,

$$R\left(\sum a_k z^k\right) \geqslant \min_{1 \leq j \leq n} \frac{1}{|z_j|} = 1$$

Donc $\boxed{\forall z \in \mathbb{C} \text{ tel que } |z| < 1, \sum a_k z^k \text{ converge.}}$

---

11. b) Soit $z \in \mathbb{C}^*$ tel que $|z| < 1$

Comme $\left|\frac{1}{z}\right| > 1$, $\frac{1}{z} \notin \{z_1, \dots, z_n\}$ donc $P\left(\frac{1}{z}\right) \neq 0$ et

$$\frac{P'\left(\frac{1}{z}\right)}{P\left(\frac{1}{z}\right)} = \sum_{i=1}^{n} \frac{1}{\frac{1}{z} - z_i} = \sum_{i=1}^{n} z \times \frac{1}{1 - z z_i}$$

$$= z \times \sum_{i=1}^{n} \sum_{k=0}^{+\infty} (z z_i)^k \quad \text{car } |z z_i| = |z||z_i| < 1$$

$$= z \sum_{k=0}^{+\infty} \left(\sum_{i=1}^{n} z_i^k\right) z^k$$

$$= z f(z)$$

donc $\boxed{P'\left(\frac{1}{z}\right) = z f(z) P\left(\frac{1}{z}\right).}$

---

11. c) $P \in \mathbb{Z}[X]$ donc $P' \in \mathbb{Z}[X]$

et $z^{n-1} P'\left(\frac{1}{z}\right) = z^n P\left(\frac{1}{z}\right) f(z)$

En écrivant $P = b_0 + b_1 X + \dots + b_{n-1} X^{n-1} + X^n$,
($b_n = 1$)

$$\sum_{k=1}^{n} k b_k z^{n-1-(k-1)} = \sum_{k=1}^{n} k b_k z^{n-k}$$
$$= \sum_{k=0}^{n} b_k z^{n-k} \times f(z)$$

Posons $c_k = \begin{cases} (n-k) b_{n-k} & \text{si } k \in [\![0, n-1]\!] \\ 0 & \text{sinon} \end{cases}$

$b'_k = \begin{cases} b_{n-k} & \text{si } k \in [\![0,n]\!] \\ 0 & \text{si } k \geq n+1 \end{cases}$

Alors $\displaystyle\sum_{k=0}^{+\infty} c_k z^k = \sum_{k=0}^{+\infty} b'_k z^k \times \sum_{k=0}^{+\infty} a_k z^k$

vrai pour tout $z \in \mathbb{C}^*$ tel que $|z| < 1$

[et aussi pour $z = 0$: $c_0 = n = 1 \times n = b'_0 \times a_0$ ce qui se retrouve aussi par continuité]

Donc les séries entières ont mêmes coefficients, et en reconnaissant un produit de Cauchy

$$\forall k \in \mathbb{N}, \underbrace{c_k}_{\in \mathbb{Z}} = \sum_{l=0}^{k} b'_l a_{k-l}$$
$$= \sum_{l=0}^{k} b_{n-l} a_{k-l} \quad \text{avec } b_p = 0 \text{ si } p \notin [\![0,n]\!]$$
$$= a_k + \sum_{l=0}^{k-1} a_l \underbrace{b_{n-k+l}}_{\in \mathbb{Z}}$$

ce qui permet, par récurrence finie, d'obtenir que pour tout $k \in \mathbb{N}$, $\boxed{a_k = c_k - \sum_{l=0}^{k-1} a_l b_{n-k+l} \in \mathbb{Z}.}$

Autre argument possible : les relations ci-dessus donnent $a_k \in \mathbb{Q}$ et par le théorème admis, les a_k sont des entiers algébrique, donc ils sont dans $\mathbb{Z}$ (s.a).

12. a) Comme $z_1, \dots, z_n \in \mathbb{U}$,

$\forall k \in \mathbb{N}, \ |a_k| \leq |z_1|^k + \dots + |z_n|^k = n$

donc $\forall k \in \mathbb{N}, \ a_k \in [\![-n, n]\!]$.

Donc pour tout $k \in \mathbb{N}$, $(a_k, a_{k+1}, \dots, a_{k+n})$ peut prendre un nombre fini de valeurs (au plus $(2n+1)^{n+1}$)

Donc, $\boxed{\text{nécessairement, on a } k < l \text{ tel que } (a_k, \dots, a_{k+n}) = (a_l, \dots, a_{l+n}).}$ (Principe des tiroirs)

---

12. b Soit $f : \left| \begin{array}{l} \mathbb{C}_n[X] \longrightarrow \mathbb{C} \\ F \longmapsto \sum_{i=1}^{n} F(z_i)(z_i^l - z_i^k) \end{array} \right.$

Alors f est linéaire et par définition de k et l,

$\forall i \in [\![0, n]\!], \ f(X^i) = \sum_{i=1}^{n} \left(z_i^{l+i} - z_i^{k+i} \right) = a_{l+i} - a_{k+i} = 0$

Donc f nulle sur la base $(1, \dots, X^n)$ de $\mathbb{C}_n[X]$

donc est nulle sur $\mathbb{C}_n[X]$.

$$\boxed{\forall F \in \mathbb{C}_n[X], \ \sum_{i=1}^{n} F(z_i)(z_i^k - z_i^l) = 0}$$

---

12. c Comme $P \in \mathbb{Q}[X]$, unitaire, irréductible dans $\mathbb{Q}[X]$, d'après 3. b, $P = \Pi_{z_i}$ pour tout $i \in [\![1, n]\!]$.

Puis, avec 4 b, $\boxed{\text{les } z_i \text{ sont 2 à 2 distincts.}}$

En appliquant b aux polynômes d'interpolation de Lagrange associés à $z_1, \dots, z_n$, on obtient

$\forall i \in [\![1, n]\!]$, $z_i^{\ell} - z_i^{k} = 0$ ie $\boxed{z_i^{\ell-k} = 1}$

donc $\boxed{z_i \in \mathbb{U}_{\ell-k} \text{ est une racine de } 1.}$

---

13 a – $z \in \mathbb{P}_n$, p premier, $p \nmid n$.

$F, G \in \mathbb{Z}[X]$. Par le binôme de Newton

$$(F+G)^p = \sum_{k=0}^{p} \binom{p}{k} F^k G^{p-k}$$

$$= F^p + G^p + \sum_{k=1}^{p-1} \binom{p}{k} F^k G^{p-k}.$$

Or $\forall k \in [\![1, p-1]\!]$, $p \mid \binom{p}{k}$ car $k\binom{p}{k} = p\binom{p-1}{k-1}$

donc $p \mid k\binom{p}{k}$ avec $p \wedge k = 1$

et on conclut avec le lemme de Gauß.

donc $\binom{p}{k} = p \times \alpha_{p,k}$ avec $\alpha_{p,k} \in \mathbb{Z}$.

Finalement, $\boxed{(F+G)^p = F^p + G^p + pH}$

où $H = \sum_{k=1}^{p-1} \alpha_{p,k} F^k G^{p-k} \in \mathbb{Z}[X]$

13.b Comme z racine de $X^n - 1$, il est un entier algébrique et donc, par 5.b, $\boxed{\Pi_z \in \mathbb{Z}[X]}$.

Notons $\Pi_z = \sum_{k=0}^{d} \alpha_k X^k$.

On peut étendre la formule de 13a par récurrence :

$$\left[\sum_{k=0}^{d} \alpha_k X^k\right]^p = \sum_{k=0}^{d} (\alpha_k X^k)^p + pH \quad \text{où } H \in \mathbb{Z}[X].$$

Donc $\Pi_z(X^p) - \Pi_z^p = \sum_{k=0}^{d} (\alpha_k - \alpha_k^p) X^{pk} + pH$.

Or $\forall k \in [\![0, d]\!]$, $\alpha_k^p \equiv \alpha_k\ (p)$ par petit théorème de Fermat

donc $\forall k \in [\![0, d]\!]$, $p \mid \alpha_k - \alpha_k^p$ et on a bien

$\boxed{F \in \mathbb{Z}[X] \text{ tel que } \Pi_z(X^p) - \Pi_z^p = pF.}$

13c - On a alors

$$\Pi_z(z^p) = (\underbrace{\Pi_z(z)}_{=0})^p + pF(z)$$

donc $\frac{\Pi_z(z^p)}{p} = F(z)$ est une somme de produit d'entiers qui sont des entiers algébriques et de puissances de z qui l'est aussi. D'après le théorème admis en préambule, $\boxed{\frac{\Pi_z(z^p)}{p} \text{ est un entier algébrique.}}$

14. a

$$\prod_{1\le i<j\le n} (z_i - z_j)^2 = \left[\prod_{1\le i<j\le n} (z_i - z_j)\right]^2$$

Or, si $i \in [\![1, n]\!]$, $P'(z_i) = n z_i^{n-1} \underset{z_i^n=1}{=} \dfrac{n}{z_i} = \sum_{k=1}^{n} \underbrace{\prod_{\substack{1\le j\le n\\ k\ne j}} (z_i - z_j)}_{=0 \text{ si } j=i}$

$$= \prod_{\substack{1\le j\le n\\ j\ne i}} (z_i - z_j)$$

Donc $\dfrac{n^n}{z_1 \cdots z_n} = \prod_{i=1}^{n} \prod_{\substack{1\le j\le n\\ j\ne i}} (z_i - z_j) = \prod_{\substack{1\le i,j\le n\\ i\ne j}} (z_i - z_j)$

$$= (-1)^{\frac{n(n-1)}{2}} \prod_{1\le i<j\le n} (z_i - z_j)^2$$

de plus, par les relations coefficients - racines ($X^n - 1$ scindé dans $\mathbb{C}$), $z_1 \cdots z_n = (-1)^n \times (-1) = (-1)^{n-1}$

Finalement, $\boxed{\prod_{1\le i<j\le n} (z_i - z_j)^2 = (-1)^{\frac{(n-1)(n-2)}{2}} n^n}$

---

14. b On suppose que $\Pi_z(z^p) \ne 0$.

Comme $\Pi_z \mid X^n - 1 = \prod_{i=1}^{n} (X - z_i)$, il est de la forme

$\Pi_z = \prod_{i=1}^{k} (X - z_i)$ (quitte à réordonner les racines)

et on peut supposer $z = z_1$ (racine de Π_z).

Alors $(z^p)^n = (z^n)^p = 1$ donc $z^p \in \{z_1, \dots, z_n\}$.

Comme $\Pi_z(z^p) \ne 0$, $z^p \notin \{z_1, \dots, z_k\}$.

On suppose, quitte à réordonner, que $\zeta^p = \zeta_{k+1}$.

Alors $\Pi_\zeta(\zeta^p) = \prod_{i=1}^{k} (\zeta_{k+1} - \zeta_i)$.

Puis $\dfrac{n^n}{\Pi_\zeta(\zeta^p)} \underset{qu. 14a}{=} \dfrac{(-1)^{\frac{(n-1)(n-2)}{2}} \prod_{1 \leq i < j \leq n} (\zeta_i - \zeta_j)^2}{\prod_{i=1}^{k} (\zeta_{k+1} - \zeta_i)}$ ces termes se simplifient dans

Avec le théorème du préambule, on en déduit que $\dfrac{n^n}{\Pi_\zeta(\zeta^p)} = u$ est un entier algébrique.

Mais alors $\dfrac{n^n}{p} = u \times \dfrac{\Pi_\zeta(\zeta^p)}{p}$ est un rationnel entier algébrique avec le théorème et 13.c.

Donc, d'après 5.a, $\dfrac{n^n}{p} \in \mathbb{Z}$ et $p \mid n^n$, donc $p \mid n$ car p est premier, ce qui est contradictoire.

Finalement, $\boxed{\Pi_\zeta(\zeta^p) = 0.}$

14.c Commençons par traiter le cas où $\zeta = e^{\frac{2i\pi}{n}}$ qui est bien racine de Φ_n (car $1 \wedge n = 1$.)

On a $\Pi_\zeta \mid \Phi_n$ car $\Phi_n \in \mathbb{Q}[X]$ (10.) et $\Phi_n(\zeta) = 0$.

et si $k \wedge n = 1$ alors $k = p_1^{\alpha_1} \cdots p_q^{\alpha_q}$ avec $p_1, \dots, p_q$ premiers distincts ne divisant pas n et $\alpha_1, \dots, \alpha_q \in \mathbb{N}^*$

D'après 14.b), z^{p_1} racine de Π_z.

Donc $\Pi_z = \Pi_{z^{p_1}}$ par 3.b)

donc $(z^{p_1})^{p_1} = z^{p_1^2}$ racine de Π_z (14b)

et en recommençant (récurrence),

$\forall \alpha_1 \in \mathbb{N}^*$, $z^{p_1^{\alpha_1}}$ est racine de $\Pi_z = \Pi_{z^{p_1^{\alpha_1}}}$

En appliquant le même raisonnement à $z^{p_1^{\alpha_1}}$ avec p_2,

on obtient de même

$\forall \alpha_2 \in \mathbb{N}^*$, $z^{p_2^{\alpha_2}}$ racine de $\Pi_z = \Pi_{z^{p_1^{\alpha_1} p_2^{\alpha_2}}}$

et par récurrence, tout z^k où $k \wedge n = 1$ est

racine de Π_z, ie tout élément de $\mathbb{P}_n$.

Finalement, $\boxed{\Pi_z = \Phi_n}$ (avec polynômes unitaires, $\Pi_z | \Phi_n$ et {racines de Φ_n} $\subset$ {racine de Π_z})

et, en particulier, Φ_n irréductible sur $\mathbb{Q}[X]$.