Agrégation externe 2019.

Autour du théorème de Fermat-Wiles.

$$x^n + y^n + z^n = 0$$

corrigé par:
SABIR ILYASS
2021.

Le problème présenté ici, est le sujet de l'algèbre du concours Agrégation externe 2019.

Le problème est long ! il est composé de 5 grands parties, pour arriver finalement à montrer le théorème de Fermat-Wiles pour certains nombres premiers (régulier).

Le problème est un excellent sujet formateur pour les futurs candidats de l'agrégation en maths, et peut-être aussi intéressant pour les étudiants de CPGE scientifiques.

La première partie consiste à montrer quelques résultats de la division euclidienne des polynômes à coefficients entiers, de montrer que l'anneau $\mathbb{Z}[\zeta]$ est euclidien pour $\zeta = \exp(2i\pi/3)$. Ensuite on introduit la notion de polynôme cyclotomique, un résultat fort des polynômes cyclotomiques, qu'ils sont à coefficients entiers, et irréductibles de $\mathbb{Q}[X]$. Ce que nous fournit un excellent exemple pour dire que pour tout entier $n \in \mathbb{N}$, il existe un polynôme de $\mathbb{Q}$[X] irréductible de $\mathbb{Q}[X]$. Ce qui n'est pas vrai pour $\mathbb{R}$[X], et encore pour $\mathbb{C}[X]$, en particulier alors que $\mathbb{Q}$ n'est pas algébriquement clos. D'autre part les questions 4.a, 4.b, et 4.c sert à introduire les matrices compagnon, un outil trop utiliser pour simplifier les démonstration (Comme la démonstration du théorème de Cayley-Hamilton par exemple !), aussi ici la présence des matrices compagnon est pour démontrer le résultat énoncé dans la question 4.e, qui sera utiliser plusieurs fois dans la suite du problème.

La deuxième partie est sur les nombres algébriques, un très bon résultat présenté dans la question 1.b sur la finitude des racines de l'unité inclus dans une extension fini de $\mathbb{Q}$, et donc le corps des nombres algébriques est de degré infini sur $\mathbb{Q}$. Vers la fin de la partie, on va montrer que l'ensemble des nombres entiers algébriques est un sous anneau de $\mathbb{C}$.

Passant à la troisième partie, qui consiste à étudier et caractériser quelques résultat sur $\mathbb{Z}[\zeta]$(qui seront utiliser après dans les partie 4 et 5), où $\zeta = \exp((2i\pi)/p)$, notamment sur les inversibles de l'anneau $\mathbb{Z}[\zeta]$.

La partie 4 a pour but de montrer le théorème de Fermat pour $n = 3$.

Et enfin dans la partie 5 traite le théorème de Fermat pour certains nombres premiers, et dans des cas particuliers.

En conclusion, Le théorème de Fermat (en anglais Last Fermat 's theorem) est énoncé (conjecturé) par le mathématicien français Pierre Fermat en 1637, et n'étais pas démontrer qu'en 1986, la démonstration est présentée par la première fois par le mathématicien britannique Andrew Wiles, la démonstration est basée sur plusieurs théories, comme la théorie de GALOIS, et encore des résultats de maths moderne, qui ne sont pas existé dans la 17 -ème siècle. Pour ce qui veut savoir la démonstration de ce théorème n'hésitez pas à cliquer sur le lien vers la fin de ce fichier, (la beauté du livre va vous attirer de lire le livre en entier).

Note: Pour la solution, c'est un travail personnel, qui m'a fallu près 8 heures pour répondre à toutes les questions !

Bon courage pour la suite . . .

Table des matières

N.B : Si vous trouvez des erreurs de Francais ou de mathématiques ou bien si vous avez des questions et/ou des suggestions, envoyez-moi un mail à **ilyasssabir7@gmail.com**

Définitions et rappels

— Soit A un anneau commutatif unitaire intègre dont on note 1_A l'élément unité.

— On rappelle que $u \in A$ est inversible s'il existe $u' \in A$ tel que $uu' = 1_A$. On note $A^\times$ l'ensemble des inversibles de A, qui **est un groupe multiplicatif**.

— Un élément x de A est dit **irréductible** si x n'est pas inversible et si pour tous $\alpha, \beta \in A$, $x = \alpha\beta$ implique $\alpha \in A^\times$ ou $\beta \in A^\times$.

— Deux éléments $x, y \in A$ sont dits associés s'il existe $u \in A^\times$ tel que $x = uy$. On note alors $x \sim y$.

— Soit I un idéal de A ; on dit que deux éléments $\alpha, \beta \in A$ sont congrus modulo I si $\alpha - \beta \in I$. On écrit alors $\alpha = \beta \pmod{I}$.

— Pour $x \in A$, on note $\langle x \rangle = xA$ l'idéal engendré par x. Un tel idéal est dit **principal**.

— Soient I, J deux idéaux de A. On dit que I divise J si $J \subseteq I$. Par ailleurs, on note IJ l'idéal produit de I et J, qui est l'ensemble des sommes finies $\sum_i x_i y_i$ avec $x_i \in I$ et $y_i \in J$.

— On rappelle qu'un nombre complexe α est dit algébrique (sur $\mathbb{Q}$) s'**il existe un polynôme non nul P de $\mathbb{Q}[X]$ tel que $P(\alpha) = 0$**.
Il existe alors un polynôme unitaire de plus petit degré annulant α, que l'on appelle **polynôme minimal de α** et que l'on note π_α. Les racines complexes de ce polynôme sont appelées les conjugués de α.

— On appelle entier algébrique tout nombre complexe qui est racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$.

— On rappelle une version du **lemme de Gauss**, que l'on pourra utiliser librement : soit $P \in \mathbb{Z}[X]$ tel que $P = P_1 P_2$ avec P_1 et P_2 des polynômes de $\mathbb{Q}[X]$. Alors il existe un rationnel $r \in \mathbb{Q}$, non-nul, tel que $rP_1 \in \mathbb{Z}[X]$ et $\frac{1}{r} P_2 \in \mathbb{Z}[X]$.

— On dit qu'un groupe abélien G est de **type fini** s'il existe une famille génératrice finie de G, c'est-à-dire un entier r et une famille $(a_1, \ldots, a_r)$ d'éléments de G tels que tout élément de G s'écrit comme une combinaison linéaire à coefficients entiers des $a_1, \ldots, a_r$.

Notations

— Pour un anneau A commutatif et un entier naturel non nul n, on note $\mathcal{M}_n(A)$ l'algèbre des matrices carrées $n \times n$ à coefficients dans A ; la matrice unité est notée I_n.

Si M est une matrice de $\mathcal{M}_n(A)$, on note χ_M son **polynôme caractéristique**, qui est le polynôme unitaire défini par

$$\chi_M = \det(XI_n - M)$$

et on note π_M son **polynôme minimal**.

— Pour un nombre premier p, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

— Pour tout entier algébrique α, on note $\mathbb{Z}[\alpha]$ l'anneau des éléments de la forme $P(\alpha)$ où P parcourt $\mathbb{Z}[X]$.

Dans le problème, les textes placés entre les symboles ✠✠...✠✠ précisent des notations et définitions qui sont utilisées dans la suite de l'énoncé

1 Exercices préliminaires

1. Soit $B \in \mathbb{Z}[X]$ un polynôme unitaire et $A \in \mathbb{Z}[X]$. Montrer qu'il existe $Q, R \in \mathbb{Z}[X]$ tels que $A = BQ + R$ avec $\deg R < \deg B$ ou $R = 0$.

Indication : On pourra faire une preuve par récurrence sur le degré de A.

2. **L'anneau $\mathbb{Z}[j]$.** On note $j = e^{\frac{2i\pi}{3}}$.

(a) Démontrer que j est un élément algébrique sur $\mathbb{Q}$ et préciser son polynôme minimal.

(b) Démontrer que $\mathbb{Z}[j] = \{a + bj, (a,b) \in \mathbb{Z}^2\}$.

Pour tout nombre complexe z, on pose $N(z) = z\bar{z} = |z|^2$.

(c) Démontrer que pour tout $z \in \mathbb{Z}[j]$, on a $N(z) \in \mathbb{N}$. En déduire que si $z \in \mathbb{Z}[j]$ est inversible, alors $N(z) = 1$, puis que $\mathbb{Z}[j]^\times$ possède 6 éléments que l'on précisera.

(d) Soient $x \in \mathbb{Z}[j]$ et $y \in \mathbb{Z}[j] \setminus \{0\}$. Déterminer un élément $q \in \mathbb{Z}[j]$ tel que $N\left(\frac{x}{y} - q\right) < 1$. En déduire que l'anneau $\mathbb{Z}[j]$ est euclidien.

3. Polynômes cyclotomiques.

Soit n un entier naturel non nul. On note Φ_n le $n-i$ème polynôme cyclotomique. On rappelle que si μ_n^* désigne l'ensemble des racines primitives $n-i$èmes de l'unité dans $\mathbb{C}$, ce polynôme est défini par

$$\Phi_n(X) = \prod_{\mu \in \mu_n^*} (X - \mu)$$

(a) Démontrer que

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

(b) En déduire que $\Phi_n(X) \in \mathbb{Z}[X]$.

(c) Soit p un nombre premier.
On note $\pi : \mathbb{Z} \to \mathbb{F}_p$ la surjection canonique. Le morphisme d'anneaux π s'étend, coefficient par coefficient, en un morphisme d'anneaux de $\mathbb{Z}[X]$ sur $\mathbb{F}_p[X]$, noté $\hat{\pi}$ (on ne demande pas de justifier ce point). Si Φ_p désigne le $p-i$ème polynôme cyclotomique, on rappelle que $\Phi_p = \sum_{k=0}^{p-1} X^k$.

i. Démontrer que $\hat{\pi}(X^p - 1) = (X - 1_{\mathbb{F}_p})^p$.

ii. Soient P et Q deux polynômes unitaires et non constants dans $\mathbb{Z}[X]$ tels que $X^p - 1 = PQ$. Démontrer que $P(1)$ et $Q(1)$ sont des entiers multiples de p.

iii. Retrouver ainsi que Φ_p est un polynôme irréductible de $\mathbb{Q}[X]$.

✠✠ De manière générale, Φ_n est irréductible pour tout $n \in N \setminus \{0\}$, résultat que l'on admet ici et que l'on pourra utiliser librement dans la suite. ✠✠

iv. Soit $\zeta = e^{\frac{2i\pi}{p}}$. Déterminer le polynôme minimal de ζ sur $\mathbb{Q}$ et en déduire le degré de l'extension de corps $\mathbb{Q}(\zeta)/\mathbb{Q}$.

4. MATRICES COMPAGNONS. Soit n un entier naturel non nul. Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme unitaire de $\mathbb{C}[X]$. On lui associe sa matrice compagnon C_P définie dans $\mathcal{M}_n(\mathbb{C})$ par

$$C_P = \begin{pmatrix} 0 & 0 & . & . & 0 & -a_0 \\ 1 & 0 & & & 0 & -a_1 \\ 0 & 1 & & & . & . \\ . & 0 & & & . & . \\ . & . & & & . & . \\ . & . & . & . & 0 & -a_{n-2} \\ 0 & 0 & 0 & 0 & 1 & -a_{n-1} \end{pmatrix}$$

On note $\mathcal{E} = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{C}^n$.

(a) Pour $k \in \{1, \ldots, n-1\}$, exprimer $C_P^k e_1$ dans la base $\mathcal{E}$. En déduire que pour tout polynôme $Q \in \mathbb{C}[X]$ non nul et de degré inférieur ou égal à $n-1$, la matrice $Q(C_P)$ est non nulle.
En déduire le degré du polynôme minimal de C_P .

(b) Exprimer $C_p^n e_1$ dans la base $\mathcal{E}$. En déduire que P est le polynôme minimal de C_P .

(c) En déduire le polynôme χ_{C_P} .

Soit $M \in \mathcal{M}_n(\mathbb{C})$ de polynôme caractéristique χ_M . Soient $\alpha_1, \ldots, \alpha_n$ les racines complexes de χ_M comptées avec leur multiplicité. Soit Q un polynôme de $\mathbb{C}[X]$.

(d) Démontrer que le polynôme caractéristique de la matrice $Q(M)$ est

$$\chi_{Q(M)} = \prod_{k=1}^{n} (X - Q(\alpha_k))$$

INDICATION : On pourra commencer par traiter le cas où M est triangulaire.

(e) Soit A un sous-anneau de $\mathbb{C}$. On suppose que le polynôme Q est dans $A[X]$. Soit $P \in A[X]$ un polynôme unitaire dont on note $\alpha_1, \ldots, \alpha_n$ les racines complexes comptées avec leur multiplicité.
Démontrer que $\prod_{k=1}^{n} (X - Q(\alpha_k))$ est un polynôme de $A[X]$.

2 Nombres algébriques

1. (a) On désigne par φ l'indicatrice d'Euler, qui à tout entier $n \in N \setminus \{0\}$ associe le nombre d'entiers non nuls inférieurs à n et premiers avec n. Justifier que pour tout entier $d \geqslant 1$, l'ensemble des entiers n tels que $\varphi(n) \leqslant d$ est fini.

(b) En déduire que si $\boldsymbol{K}/\mathbb{Q}$ est une extension finie de $\mathbb{Q}$, où $\boldsymbol{K}$ est un sous-corps de $\mathbb{C}$, alors $\boldsymbol{K}$ contient un nombre fini de racines de l'unité.

2. Soit $\alpha\in\mathbb{C}$ un nombre algébrique dont on rappelle que l'on a noté π_α son polynôme minimal. On note $\boldsymbol{K}=\mathbb{Q}(\alpha)$ le plus petit corps contenant α et $\mathbb{Q}$, et $d=[\boldsymbol{K}:\mathbb{Q}]$, le degré de l'extension de corps $\mathbb{Q}(\alpha)/\mathbb{Q}$.

(a) Montrer que π_α est un polynôme irréductible de $\mathbb{Q}[X]$ et que son degré est égal à d.

(b) Montrer que si σ est un morphisme de $\mathbb{Q}-$algèbre de $\boldsymbol{K}$ dans $\mathbb{C}$, $\sigma(\alpha)$ est une racine de π_α, c'est-à-dire un conjugué de α. En déduire qu'il y a exactement d tels morphismes de $\mathbb{Q}$-algèbre, que l'on notera $\sigma_k:\boldsymbol{K}\to\mathbb{C}, k\in\{1,\dots,d\}$.

3. Soit $\alpha\in\mathbb{C}$ un nombre algébrique et soit $\theta\in\boldsymbol{K}=\mathbb{Q}(\alpha)$. Comme dans la question précédente, les σ_k avec $k\in\{1,\dots,d\}$ désignent les morphismes de $\mathbb{Q}-$algèbre de $\mathbb{Q}(\alpha)$.

(a) Justifier que θ est un nombre algébrique.

On pose

$$P_\theta=\prod_{k=1}^{d}(X-\sigma_k(\theta))\in\mathbb{C}[X].$$

(b) Montrer que $P_\theta\in\mathbb{Q}[X]$.

(c) Justifier que π_θ divise P_θ, puis montrer que P_θ est une puissance de π_θ.

4. Montrer qu'un nombre algébrique α est un entier algébrique si et seulement si son polynôme minimal est à coefficients entiers.

5. Soit α un nombre complexe.

(a) Montrer que si α est un entier algébrique, alors le groupe additif G engendré par la partie $\{\alpha^n, n\in N\}$ est de type fini.

(b) Réciproquement, montrer que si G est de type fini alors α est un entier algébrique.
Indication : En notant $(g_1,\dots,g_n)$ une famille génératrice finie de G, on pourra considérer le déterminant du système obtenu en écrivant les éléments $\alpha g_i, i\in\{1,\dots,n\}$ comme combinaison linéaire des g_j .

6. En déduire que l'ensemble $\mathfrak{D}_\mathbb{C}$ des entiers algébriques de $\mathbb{C}$ est un sous-anneau de $\mathbb{C}$.
Indication : On pourra utiliser sans démonstration qu'un sous-groupe d'un groupe abélien de type fini est de type fini.

7. Montrer que $\mathfrak{D}_\mathbb{C}\cap\mathbb{Q}=\mathbb{Z}$.

✠✠ Dans la suite, on considère le corps $\boldsymbol{K}=\mathbb{Q}(\zeta)$ où $\zeta=e^{\frac{2i\pi}{p}}$ avec p premier impair, et on note $\mathfrak{D}_{\boldsymbol{K}}$ l'ensemble des entiers algébriques de $\boldsymbol{K}$. On pose $\lambda=1-\zeta$.

On définit la norme et la trace de tout élément $\theta \in \boldsymbol{K} = \mathbb{Q}(\zeta)$ par

$$N(\theta) = \prod_{k=1}^{p-1} \sigma_k(\theta)$$

et

$$\mathrm{Tr}(\theta) = \sum_{k=1}^{p-1} \sigma_k(\theta)$$

où les σ_k sont les morphismes de $\mathbb{Q}-$algèbre de $\mathbb{Q}(\zeta)$ définis dans la question 2 de cette partie.✠✠

3 Le corps $\mathbb{Q}(\zeta)$ et son anneau d'entiers

1. (a) Montrer que les morphismes de $\mathbb{Q}-$algèbre de $\mathbb{Q}(\zeta)$ sont les σ_k tels que $\sigma_k(\zeta) = \zeta^k$, avec $k \in \{1, ..., p-1\}$.

(b) i. Montrer que $N(\zeta) = 1$ et $\mathrm{Tr}(\zeta) = -1$.

ii. Montrer que $N(1-\zeta) = p$ et $N(1+\zeta) = 1$.

2. Montrer l'inclusion $\mathbb{Z}[\zeta] \subseteq \mathfrak{D}_{\boldsymbol{K}}$.

3. Soit $z \in \mathbb{Z}[\zeta]$.

(a) Montrer que $z \in Z[\zeta]^\times$ si et seulement si $N(z) \in \{-1, +1\}$.

(b) Montrer que si $N(z)$ est un nombre premier, alors z est irréductible.

4. Le but de cette question est de montrer que l'ensemble G des racines de l'unité contenues dans $\boldsymbol{K}$ est formé exactement des éléments de la forme $\pm\zeta^k$, $k \in \{0, \ldots, p-1\}$.

(a) Justifier que G est un groupe fini cyclique, dont on notera n le cardinal.

(b) Soit ω un générateur de G. Justifier que $2p \,|\, n$ et que $\mathbb{Q}(\zeta) = \mathbb{Q}(\omega)$.

(c) En déduire que $n = 2p$ et conclure.

5. On note $\langle\lambda\rangle = \lambda\mathbb{Z}[\zeta]$, l'idéal de $\mathbb{Z}[\zeta]$ engendré par λ.

(a) Montrer que $\langle\lambda\rangle \cap \mathbb{Z} = p\mathbb{Z}$.

(b) Montrer que pour tout $k \in \{1, \ldots, p-1\}$, on a

$$\frac{1-\zeta}{1-\zeta^k} \in Z[\zeta]^\times$$

et en déduire que

$$\lambda^{p-1}\mathbb{Z}[\zeta]=p\mathbb{Z}[\zeta].$$

(c) Soit ψ le morphisme d'anneaux de $\mathbb{Z}[X]$ dans $\mathbb{Z}[\zeta]/\langle\lambda\rangle$, qui à $P\in\mathbb{Z}[X]$ associe $P(\zeta)(\mathrm{mod}\,\langle\lambda\rangle)$. Déterminer l'image de ψ et montrer que $\ker\psi$ est l'ensemble des polynômes $P\in\mathbb{Z}[X]$ tels que $P(1)=0\,(\mathrm{mod}\,p\mathbb{Z})$.

(d) En déduire que $Z[\zeta]/\langle\lambda\rangle$ est isomorphe à $\mathbb{F}_p$.

(e) Que peut-on en déduire pour l'idéal $\langle\lambda\rangle$?

6. On détermine ici la structure de $\mathbb{Z}[\zeta]^\times$. Le but est de démontrer que les éléments de $\mathbb{Z}[\zeta]^\times$ sont les $\zeta^r\varepsilon$, où $r\in\mathbb{Z}$ et ε est un réel inversible de $\mathbb{Z}[\zeta]$.

Soit $u\in\mathbb{Z}[\zeta]^\times$.

(a) Soit $P=\sum_{k=0}^{d}a_kX^k\in\mathbb{Z}[X]$ un polynôme unitaire de degré d, dont on note $\alpha_1,\ldots,\alpha_d$ les racines complexes comptées avec leur multiplicité. On suppose que pour tout $k\in\{1,\ldots,d\}$, α_k est de module 1.

i. Montrer que pour tout $k\in\{0,\ldots,d\}$, on a $|a_k|\leqslant\binom{d}{k}$.

En déduire qu'il n'existe qu'un nombre fini d'entiers algébriques de degré d dont tous les conjugués sont de module 1.

ii. En déduire également que les racines de P sont des racines de l'unité.

Indication : On pourra considérer les polynômes $P_n=\prod_{k=1}^{d}(X-\alpha_k^n)$, $n\in\mathbb{N}$, dont on montrera qu'ils sont dans $\mathbb{Z}[X]$.

(b) Soit $P\in\mathbb{Z}[X]$ tel que $u=P(\zeta)$. Montrer que, pour tout $k\in\{1,\ldots,p-1\}$, $u_k=P(\zeta^k)$ est un conjugué de u, et que c'est un élément de $\mathbb{Z}[\zeta]^\times$.

(c) Justifier que $\frac{u_p}{u_{p-1}}$ est un entier algébrique dont tous les conjugués sont de module 1.

(d) En déduire qu'il existe $m\in\mathbb{Z}$ tel que $\frac{u_1}{u_{p-1}}=\pm\zeta^m$.

(e) i. Soit $\theta\in\mathbb{Z}[\zeta]$. Justifier qu'il existe un entier $a\in\mathbb{Z}$ tel que $\theta=a\,(\mathrm{mod}<\lambda>)$. En déduire que deux éléments conjugués de $\mathbb{Z}[\zeta]$ sont égaux modulo $<\lambda>$.

ii. Démontrer que $\frac{u_1}{u_{p-1}}=\zeta^m$.

(f) Justifier l'existence de $r\in\mathbb{Z}$ tel que $2r=m\,(\mathrm{mod}\,p\mathbb{Z})$. On pose $\varepsilon=\zeta^{-r}u$. Montrer que $\varepsilon\in\mathbb{R}$ et conclure.

7. Le but de ce qui suit est de montrer que $\mathfrak{D}_{\boldsymbol{K}}=\mathbb{Z}[\zeta]$.

(a) Montrer que pour tout $\theta \in \mathfrak{D}_{\boldsymbol{K}}$, on a $N(\theta) \in \mathbb{Z}$ et $\mathrm{Tr}(\theta) \in \mathbb{Z}$.

(b) Soit $\theta \in \boldsymbol{K} = \mathbb{Q}(\zeta)$ un entier algébrique. Il existe des rationnels $a_0, \ldots, a_{p-2}$ tels que

$$\theta = \sum_{k=0}^{p-2} a_k \zeta^k$$

i. Pour $k \in \{0, \ldots, p-2\}$, calculer $b_k = \mathrm{Tr}(\theta\zeta^{-k} - \theta\zeta)$ et justifier que $b_k \in \mathbb{Z}$.

ii. Montrer qu'il existe des entiers $c_0, c_1, \ldots, c_{p-2}$, que l'on exprimera en fonction des b_k, tels que

$$p\theta = \sum_{k=0}^{p-2} c_k \lambda^k$$

Justifier ensuite que pour tout $k \in \{0, \ldots, p-2\}$

$$b_k = \sum_{l=k}^{p-2} (-1)^l \binom{l}{k} c_l$$

iii. Montrer qu'il existe $\beta \in \mathbb{Z}[\zeta]$ tel que $p = \lambda^{p-1}\beta$. En déduire que $p \mid c_0$, puis que pour tout $k \in \{0, \ldots, p-2\}$, on a $p \mid c_k$. Conclure.

4 Le théorème de Fermat pour $p = 3$

On cherche à démontrer dans cette partie que l'équation

$$x^3 + y^3 + z^3 = 0 \tag{1}$$

n'a pas de solution entières non triviales, *i.e.*, telles que $xyz \neq 0$.

Soient x, y et z trois entiers relatifs tels que $x^3 + y^3 + z^3 = 0$.

1. On suppose que $3 \nmid xyz$. Montrer que x^3 vaut $+1$ ou $-1 \pmod 9$ et conclure à une impossibilité.
✠✠ On traite à présent le cas $3 \mid xyz$. Dans la suite de cette partie, on note $\lambda = 1 - j$ avec toujours $j = e^{\frac{2i\pi}{3}}$ et on suppose que les entiers x, y et z sont premiers entre eux dans $\mathbb{Z}[j]$ (et pas seulement dans $\mathbb{Z}$), cas auquel on peut se ramener en divisant par leur pgcd dans $\mathbb{Z}[j]$. ✠✠

2. Montrer que 3 et λ^2 sont associés dans $\mathbb{Z}[j]$, ce que l'on a noté $3 \sim \lambda^2$.

3. Soit $s \in \mathbb{Z}[j]$ tel que $s \neq 0 \pmod{\langle\lambda\rangle}$. Montrer qu'il existe $\varepsilon \in \{-1, +1\}$ tel que $s^3 = \varepsilon \pmod{\langle\lambda^4\rangle}$.
INDICATION : On pourra remarquer que tout élément $s \in \mathbb{Z}[j]$ est congru à $-1, 0$ ou $1 \pmod{\langle\lambda\rangle}$.

✠✠ Par symétrie des rôles de x, y et z, on peut supposer que $3 \mid z$ (et donc $3 \nmid x$, $3 \nmid y$ puisqu'ils sont premiers entre eux). En particulier, on a $\lambda \mid z$, $\lambda \nmid x$ et $\lambda \nmid y$ dans $\mathbb{Z}[j]$.
On note n la valuation en λ de z ; il existe donc $\mu \in \mathbb{Z}[j]$ premier avec λ tel que $z = \mu\lambda^n$, et par hypothèse $n \geqslant 1$. On a donc $x^3 + y^3 + \mu^3\lambda^{3n} = 0$.

La propriété suivante (qui pourra être utilisée sans plus de justification) est donc vérifiée :

$$(P_n)\,:\,\text{il existe}\,\alpha,\beta,\delta\in\mathbb{Z}[j]\,\text{et}\,\omega\in\mathbb{Z}[j]^\times\,\text{tels que}\begin{cases}\lambda\nmid\alpha\beta\delta\\ \alpha\ \text{ et }\ \beta\,\text{premiers entre eux}\\ \alpha^3+\beta^3+\omega\lambda^{3n}\delta^3=0\end{cases}$$

Nous allons montrer que si (P_n) est vérifiée, alors $n\geqslant 2$ et (P_{n-1}) est également vérifiée. ✠✠

4. Supposons (P_n) vérifiée pour un quadruplet $(\alpha,\beta,\delta,\omega)$. En considérant les valeurs de α^3, β^3 et $\omega\lambda^{3n}\delta^3\,(\mathrm{mod}\,\langle\lambda^4\rangle)$, montrer que $n\geqslant 2$.

5. Supposons (P_n) vérifiée pour un quadruplet $(\alpha,\beta,\delta,\omega)$. On montre dans cette question que (P_{n-1}) est également vérifiée.

(a) Montrer que

$$-\omega\lambda^{3n}\delta^3=(\alpha+\beta)(\alpha+j\beta)(\alpha+j^2\beta).$$

(b) En déduire que λ divise chacun des facteurs $\alpha+\beta,\alpha+j\beta$ et $\alpha+j^2\beta$.

(c) Démontrer que λ est un **pgcd** de $\alpha+\beta$ et $\alpha+j\beta$. En déduire que λ^2 divise exactement l'un des éléments $\alpha+\beta,\alpha+j\beta$ ou $\alpha+j^2\beta$.

Quitte à remplacer β par $j\beta$ ou $j^2\beta$, on peut supposer que λ^2 divise $\alpha+\beta$. Il existe donc des éléments κ_1, κ_2 et κ_3 de $\mathbb{Z}[j]$ tels que $\lambda\nmid\kappa_1\kappa_2\kappa_3$ et

$$\begin{cases}\alpha+\beta=\lambda^{3n-2}\kappa_1\\ \alpha+j\beta=\lambda\kappa_2\\ \alpha+j^2\beta=\lambda\kappa_3\end{cases}$$

(d) Montrer que $-\omega\delta^3=\kappa_1\kappa_2\kappa_3$ et en déduire qu'il existe des éléments γ_1,γ_2 et γ_3 de $\mathbb{Z}[j]$ tels que pour tout $l\in\{1,2,3\}$, $\kappa_l\sim\gamma_l^3$.

(e) Démontrer qu'il existe deux inversibles τ et τ' de $\mathbb{Z}[j]^\times$ tels que

$$\gamma_2^3+\tau\gamma_3^3+\tau'\lambda^{3(n-1)}\gamma_1^3=0.$$

(f) Montrer que si $\tau=\pm1$, alors (P_{n-1}) est vérifiée.

(g) Montrer que $\tau=\pm1\,(\mathrm{mod}\,\langle\lambda^3\rangle)$, puis que $\tau\notin\{j,-j,j^2,-j^2\}$.

6. Conclure que l'équation (1) n'a pas de solution (x,y,z) dans le cas $3\,|\,xyz$.

5 Le théorème de Fermat pour p régulier et $p\nmid xyz$

✠✠ On admet dans la suite que pour tout corps $\boldsymbol{K}$ de degré fini sur $\mathbb{Q}$, son anneau des entiers $\mathfrak{D}_{\boldsymbol{K}}$ vérifie la propriété suivante :

Tout idéal non nul de $\mathfrak{D}_{\boldsymbol{K}}$ s'écrit comme produit d'idéaux premiers, de manière unique à l'ordre près des facteurs.

Dans ce contexte, on dit que deux idéaux I et J sont premiers entre eux s'ils n'ont pas d'idéal premier en commun dans leur décomposition en produit d'idéaux premiers.

L'anneau $\mathbb{Z}[\zeta]$ qui est, d'après les résultats de la Partie 3, l'anneau des entiers de $\boldsymbol{K}=\mathbb{Q}(\zeta)$ vérifie donc cette propriété de factorisation de ses idéaux.

On suppose dans cette partie que $p>3$ est un nombre premier régulier, ce qui signifie que si I est un idéal de $\mathbb{Z}[\zeta]$ tel que I^p est principal, alors I est lui même principal. On rappelle que l'on a noté $\lambda=1-\zeta$ et que certaines propriétés de l'idéal $\langle\lambda\rangle$ ont été étudiées en Partie 3, question 5.

On démontre dans cette partie que l'équation

$$x^p+y^p+z^p=0 \tag{2}$$

n'admet pas de solutions entières non triviales dans le cas où $p\nmid xyz$.

Par l'absurde, on se donne trois entiers $x, y, z\in\mathbb{Z}$ deux à deux premiers entre eux dans $\mathbb{Z}$, tels que $p\nmid xyz$ et qui vérifient l'équation (2). ✠✠

1. Montrer l'égalité d'idéaux

$$\prod_{k=0}^{p-1}\langle x+\zeta^k y\rangle=\langle z^p\rangle$$

2. Soit deux entiers k et l tels que$0\leqslant k<l\leqslant p-1$. On montre dans cette question que les idéaux $\langle x+\zeta^k y\rangle$ et $\langle x+\zeta^l y\rangle$ de $\mathbb{Z}[\zeta]$ sont premiers entre eux. Par l'absurde, soit $\mathfrak{B}$ un idéal premier divisant $\langle x+\zeta^k y\rangle$ et $\langle x+\zeta^l y\rangle$.

(a) En considérant $\langle x+\zeta^l y\rangle-\langle x+\zeta^k y\rangle$, montrer que $\lambda y\in\mathfrak{B}$.

(b) Montrer que $y\notin\mathfrak{B}$, en déduire que $x+y\in\langle\lambda\rangle\cap\mathbb{Z}$ et conclure à une absurdité.

3. Justifier l'existence d'un idéal I tel que $\langle x+\zeta y\rangle=I^p$.

4. Montrer qu'il existe $r\in\mathbb{Z}$, ε réel inversible de $\mathbb{Z}[\zeta]$ et $\alpha\in\mathbb{Z}[\zeta]$ tels que $x+\zeta y=\zeta^r\varepsilon\alpha^p$.

5. Montrer qu'il existe $a\in\mathbb{Z}$ tel que $\alpha^p=a\,(\mathrm{mod}\,\langle p\rangle)$ (attention, ici $\langle p\rangle=p\mathbb{Z}[\zeta]$ et non $p\mathbb{Z}$) et en déduire que

$$x\zeta^{-r}+y\zeta^{1-r}-x\zeta^r-y\zeta^{r-1}=0\,(\mathrm{mod}\,\langle p\rangle).$$

6. Supposons que$r=0\,(\mathrm{mod}\,p\mathbb{Z})$. Montrer alors que $p\,|\,y$ dans $\mathbb{Z}$, ce qui est contraire à l'hypothèse.

On montrerait de même que l'on ne peut avoir $r=1\,(\mathrm{mod}\,p\mathbb{Z})$, ce que l'on admet.

7. D'après la question 5, il existe $\beta\in\mathbb{Z}[\zeta]$ tel que

$$x\zeta^{-r}+y\zeta^{1-r}-x\zeta^{r}-y\zeta^{r-1}=\beta p.$$

Montrer que deux des entiers $\pm r,\pm(1-r)$ sont égaux modulo p ; en déduire que $2r=1\,(\mathrm{mod}\,p\mathbb{Z})$.

8. Montrer que $\beta p\zeta^{r}=(x-y)\lambda$, puis que $x=y\,(\mathrm{mod}\,p\mathbb{Z})$.

9. Conclure à une absurdité.

SOLUTION

I Exercices préliminaires

1- Soit $B \in \mathbb{Z}[X]$ un polynôme unitaire, et $A \in \mathbb{Z}[X]$.
Montrons par récurrence sur $n = \deg(A)$ que:

$$\exists Q, R \in \mathbb{Z}[X] \text{ tels que } \begin{cases} A = B.Q + R \\ \deg(R) < \deg(B) \text{ ou } R = 0 \end{cases}$$

Remarquons tout d'abord, si $\deg(B) = 0$, on a alors $B = 1$, donc le résultat est trivial, puisque pour tout $A \in \mathbb{Z}[X]$, on a : $A = B \times A$.
On suppose dans la suite que $\deg(B) \geqslant 1$.
Pour $n = 0$, on a pour tout $A \in \mathbb{Z}[X]$, tel que $\deg(A) = 0$, on a

$$A = 0 \times B + A$$

Avec

$$\deg(A) = 0 < \deg(B)$$

Donc le résultat est vrai pour $n = 0$.
Soit $n \in \mathbb{N}$, supposons que le résultat est vrai pour $k = 0, 1, \ldots, n$ et montrons le pour $n+1$.
Soit $A \in \mathbb{Z}[X]$, tel que $\deg(A) = n+1$.
On peut écrire A comme:

$$A = XA_1 + a_0$$

Avec

$$\begin{cases} A_1 \in \mathbb{Z}[X] \\ a_0 = A(0) \in \mathbb{Z}[X] \end{cases}$$

On tire $\deg(A_1) = n$, donc d'après l'hypothèse de récurrence, on a l'existence de $Q_1, R_1 \in \mathbb{Z}[X]$ tel que :

$$\begin{cases} A_1 = BQ_1 + R_1 \\ \deg(R_1) < \deg(B) \end{cases}$$

On a alors

$$A = B(XQ_1) + XR_1 + a_0 \tag{3}$$

Or

$$\deg(XR_1) = 1 + \deg(R_1) \leqslant \deg(B) \tag{4}$$

Si $\deg(B) \geqslant \deg(A)$:
$\rightarrow$Si $\deg(B) > \deg(A)$:
On a

$$A = 0 \times B + A$$

Donc le résultat est vrai.
→Si $\deg(B)=\deg(A)$:
On note

$$A=\sum_{k=0}^{n+1}a_kX^k$$

Et

$$B=X^{n+1}+\sum_{k=0}^{n}b_kX^k$$

Avec $a_0,\dots,a_{n+1},b_0,\dots,b_n\in\mathbb{Z}$
On a

$$A-a_{n+1}B \;=\; \sum_{k=0}^{n}(a_k-a_{n+1}b_k)X^k$$

Donc

$$A \;=\; a_{n+1}B+\sum_{k=0}^{n}(a_k-a_{n+1}b_k)X^k$$

Avec $\deg\left(\sum\limits_{k=0}^{n}(a_k-a_{n+1}b_k)X^k\right)<n+1$. Donc par l'unicité de la division euclidienne, on a le résultat, puisque

$$\begin{cases} a_{n+1}\in\mathbb{Z}[X] \\ \sum\limits_{k=0}^{n}(a_k-a_{n+1}b_k)X^k\in\mathbb{Z}[X] \end{cases}$$

On suppose dans le suite que $\deg(B)<\deg(A)$.
D'après (2), on a

$$\begin{aligned}\deg(XR_1) &\leqslant \deg(B)\\ &< \deg(A)\\ &= n+1\end{aligned}$$

Donc $\deg(XR_1)\leqslant n$.
Si $R_1=0$, alors d'après (1), on a

$$A=B(XQ_1)+a_0$$

Avec $XQ_1\in\mathbb{Z}[X]$, et $a_0\in\mathbb{Z}[X]$. C'est fini !
Sinon ($R_1\neq 0$), on a

$$\deg(XR_1)\in[\![0,n]\!]$$

Par hypothèse de récurrence, on a l'existence de $Q_2,R_2\in\mathbb{Z}[X]$, tel que

$$\begin{cases} XR_1=BQ_2+R_2 \\ \deg(R_2)<\deg(B) \end{cases}$$

Donc via (1), on a

$$\begin{aligned} A &= B(XQ_1)+BQ_2+R_2+a_0 \\ &= B(XQ_1+Q_2)+R_2+a_0 \end{aligned}$$

Avec $XQ_1+Q_2\in\mathbb{Z}[X]$, $R_2+a_0\in\mathbb{Z}[X]$ et $\deg(R_2+a_0)<\deg(B)$.
D'où le résultat par récurrence.
Il ne reste que le cas où $\deg(A)\notin\mathbb{N}$, donc $\deg(A)=-\infty$, c'est-à-dire $A=0$.
On a

$$A=0\times B+0$$

Avec

$$\begin{cases} 0\in\mathbb{Z}[X] \\ \deg(0)=-\infty<\deg(B) \end{cases}$$

D'où le résultat.

2.a- On a

$$1+j+j^2=\frac{1-j^3}{1-j}=0$$

Donc $P(j)=0$, où $P=X^2+X+1\in\mathbb{Q}[X]$, et donc j est algébrique de $\mathbb{Q}$.

***Déterminons le polynôme minimal de j:**

Lemme 1.
Soient $\alpha\in\mathbb{C}$, et $P\in\mathbb{Q}[X]$ annulant α, alors $\pi_\alpha|P$.

Démonstration.
Puisque $\pi_\alpha\neq 0$, et $\mathbb{Q}[X]$ est euclidien (car $\mathbb{Q}$ est un corps), alors il existe $(Q,R)\in\mathbb{Q}[X]^2$ tel que:

$$\begin{cases} P=Q\pi_\alpha+R \\ \deg(R)<\deg(\pi_\alpha) \end{cases}$$

On a :

$$R(\alpha)=P(\alpha)-Q(\alpha)\pi_\alpha(\alpha)=0$$

Donc R annule α, de plus $\deg(R)<\deg(\pi_\alpha)$, et π_α est par définition est le polynôme non nul, unitaire, annulant α, et de **degré minimal**. Et puisque $\deg(R)<\deg(\pi_\alpha)$, alors forcément $R=0$.
D'où

$$\pi_\alpha|P$$ □

Montrons maintenant que $\pi_j=X^2+X+1$
Vu que $j^2+j+1=0$, alors $\pi_j|X^2+X+1$. Et donc pour conclure, il suffit de montrer que X^2+X+1 est irréductible sur $\mathbb{Q}[X]$.
On a le discriminant du trinôme X^2+X+1 est $-3<0$.
Donc X^2+X+1 est irréductible sur $\mathbb{R}[X]$.
Or $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, alors X^2+X+1 est irréductible aussi sur $\mathbb{Q}[X]$
Via la relation $\pi_j|X^2+X+1$. et X^2+X+1 est irréductible aussi sur $\mathbb{Q}[X]$, alors ou bien π_j est inversible ou bien π_j est associé à X^2+X+1.

Avec $\deg(\pi_j) \geqslant 1$, alors π_j et X^2+X+1 sont associés, de plus ils sont unitaires, donc ils sont égaux.

D'où

$$\pi_j = X^2+X+1$$

2.b- Montrons que

$$\mathbb{Z}[j] = \{a+bj; (a,b) \in \mathbb{Z}^2\}$$

Soit $(a,b) \in \mathbb{Z}^2$, on a $a+bj = P_{a,b}(j)$, avec $P_{a,b} = bX+a \in \mathbb{Z}[X]$, donc $a+bj \in \mathbb{Z}[j]$.

D'où

$$\{a+bj; (a,b) \in \mathbb{Z}^2\} \subseteq \mathbb{Z}[j]$$

Montrons maintenant que $\mathbb{Z}[j] \subseteq \{a+bj; (a,b) \in \mathbb{Z}^2\}$.

Soit $\alpha \in \mathbb{Z}[j]$, alors par définition il existe $P \in \mathbb{Z}[X]$ tel que $\alpha = P(j)$.

En utilisant la question 1 de cette partie, Puisque $X^2+X+1 \in \mathbb{Z}[X]$est unitaire, on a l'existence de $Q, R \in \mathbb{Z}[X]$ tel que :

$$\begin{cases} P = Q(X^2+X+1)+R \\ \deg(R) < \deg(X^2+X+1) = 2 \end{cases}$$

Donc

$$\alpha = P(j) = Q(j)(j^2+j+1)+R(j) = R(j)$$

Ecrivant $R = b_1 X + a_1 \in \mathbb{Z}[X]$, on a alors $\alpha = b_1 j + a_1 \in \{a+bj; (a,b) \in \mathbb{Z}^2\}$

D'où

$$\mathbb{Z}[j] \subseteq \{a+bj; (a,b) \in \mathbb{Z}^2\}$$

Finalement

$$\mathbb{Z}[j] = \{a+bj; (a,b) \in \mathbb{Z}^2\}$$

Si vous êtes intéressé, je vvous invite à montrer la généralisation suivante:

Généralisation 1.

Soit $n \in \mathbb{N}$ tel qu $n \geqslant 2$, notons $u_n = e^{\frac{2i\pi}{n}}$. On a

$$\mathbb{Z}[u_n] = \{a_0 + a_1 u_n + \cdots + a_{n-2} u_n^{n-2} / (a_0, a_1, \ldots, a_{n-2}) \in \mathbb{Z}^{n-1}\}$$

2.c- Soit $z \in \mathbb{Z}[j]$, on a l'existence de $(a,b) \in \mathbb{Z}^2$ tel que $z = a+jb$.

On a[1]

$$\begin{aligned} N(z) &= z\bar{z} \\ &= (a+jb)(a+\bar{j}b) \\ &= (a+jb)(a+j^2b) \qquad (5) \\ &= a^2+ab(j^2+j)+b^2 \\ &= a^2-ab+b^2 \qquad (6) \end{aligned}$$

1. (3): car $\bar{j} = j^2$ et (4): car $j^2+j = -1$.

Or

$$a^2+b^2 \geqslant 2|ab|$$

Donc

$$N(z) \geqslant 2|ab| - \text{ab} \geqslant 0$$

D'où $N(z) \in \mathbb{N}$.
Si $z \in \mathbb{Z}[j]$ est inversible dans $\mathbb{Z}[j]$, alors par définition il existe $z' \in \mathbb{Z}[j]$ tel que $z.z'=1$.
On a alors

$$N(z.z') = N(1) = 1.\bar{1} = 1$$

Et

$$N(z.z') = z.z'.\overline{z.z'} = z.\bar{z}.z'.\bar{z'} = N(z)N(z')$$

Donc $N(z)N(z')=1$ et $N(z), N(z') \in \mathbb{N}$, alors $N(z)=1$.
Déterminons les éléments de $\mathbb{Z}[j]^{\times}$.
On a $z=a+bj$, où $a,b \in \mathbb{Z}$. et $N(z)=1$, donc

$$a^2 - ab + b^2 = 1$$

Donc

$$ab+1 = a^2+b^2 \geqslant 2|ab|$$

Ainsi

$$(|ab| - ab) + |ab| \leqslant 1$$

Avec $|ab|-ab, |ab| \in \mathbb{N}$.
Alors

$$\left\{ \begin{array}{l} |ab|-ab=0 \\ |ab|=0 \end{array} \right. \text{ ou } \left\{ \begin{array}{l} |ab|-ab=0 \\ |ab|=1 \end{array} \right. \text{ ou } \left\{ \begin{array}{l} |ab|-ab=1 \\ |ab|=0 \end{array} \right.$$

Et $\left\{ \begin{array}{l} |ab|-ab=0 \\ |ab|=0 \end{array} \right.$ équivalent à $(a=0$ ou $b=0)$,
Si $a=0$, on a dans ce cas on a $1=N(z)=b^2$, donc $b=1$ ou $b=-1$.
D'où $z=j$ ou $z=-j$.
Si $b=0$, de même on a $a=1$ ou $a=-1$. et donc $z=1$ ou $z=-1$.

Et le système d'équations $\left\{ \begin{array}{l} |ab|-ab=0 \\ |ab|=1 \end{array} \right.$ «équivalent à $\left\{ \begin{array}{l} \text{ab}>0 \\ \text{ab}=1 \end{array} \right.$,
équivalent à $[(a=1 \text{ et } b=1) \text{ ou } (a=-1 \text{ et } b=-1)]$
Donc $z=1+j$ ou $z=-1-j$

Or $\left\{ \begin{array}{l} |ab|-ab=1 \\ |ab|=0 \end{array} \right.$ n'admet pas de solutions.

Ainsi

$$\mathbb{Z}[j]^\times \subseteq \{-1, 1, -j, j, -1-j, 1+j\}$$

Réciproquement, on a

$$\begin{aligned} (-1)^2 &= 1 \\ 1^2 &= 1 \\ -j(1+j) &= 1 \\ j(-1-j) &= 1 \end{aligned}$$

Donc par définition

$$\{-1, 1, -j, j, -1-j, 1+j\} \subseteq \mathbb{Z}[j]^\times$$

D'où

$$\mathbb{Z}[j]^\times = \{-1, 1, -j, j, -1-j, 1+j\} = \{-1, 1, -j, j, -j^2, j^2\}$$

2.d- Soit $x \in \mathbb{Z}[j]$ et $y \in \mathbb{Z}[j]\backslash\{0\}$. Cherchons $q \in \mathbb{Z}[X]$ tel que $N\left(\frac{x}{y} - q\right) < 1$.
Notons

$$x = a + jb \text{ et } y = c + jd$$

On a

$$\begin{aligned} \frac{x}{y} &= \frac{a+jb}{c+jd} \\ &= \frac{(a+jd)(c+j^2d)}{c^2-cd+d^2} \\ &= \frac{ac-ad+bd}{c^2-cd+d^2} + j\frac{bc-ad}{c^2-cd+d^2} \end{aligned}$$

Notons

$$\alpha = \frac{ac-ad+bd}{c^2-cd+d^2} \in \mathbb{Q} \text{ et } \beta = \frac{bc-ad}{c^2-cd+d^2} \in \mathbb{Q}$$

Lemme 2.
Soit $a \in \mathbb{R}$, alors il existe $t_a \in \mathbb{Z}$, tel que $|a - t_a| \leqslant \frac{1}{2}$

Démonstration.
On a si $a - \lfloor a \rfloor > \frac{1}{2}$, alors

$$(\lfloor a \rfloor + 1) - a = (\lfloor a \rfloor - a) + 1 < \frac{1}{2}$$

D'où le résultat. □

En particulier $\exists t_\alpha, t_\beta \in \mathbb{Z}$ tel que

$$\begin{cases} |\alpha - t_\alpha| \leqslant \frac{1}{2} \\ |\beta - t_\beta| \leqslant \frac{1}{2} \end{cases}$$

Notons $q = t_\alpha + jt\beta \in \mathbb{Z}[j]$, on a

$$\begin{aligned} N\left(\frac{x}{y} - q\right) &= N((\alpha - t_\alpha) + j(\beta - t_\beta)) \\ &= (\alpha - t_\alpha)^2 - (\alpha - t_\alpha)(\beta - t_\beta) + (\beta - t_\beta)^2 \\ &\leqslant \frac{3}{2}[(\alpha - t_\alpha)^2 + (\beta - t_\beta)^2] \\ &\leqslant \frac{3}{4} \\ &< 1 \end{aligned}$$

Doù le résultat.
Montrons que $\mathbb{Z}[j]$ est euclidien
Pour tout $x, y \in \mathbb{Z}[j]$ tel que $y \neq 0$, on a l'existence de $q \in \mathbb{Z}[j]$ tel que $N\left(\frac{x}{y} - q\right) < 1$
On a alors $x = yq + (x - qy)$ avec $N(x - qy) = N(y)N\left(\frac{x}{y} - q\right) < N(y)$
Et $x - qy \in \mathbb{Z}[j]$.
D'où l'application $N : \mathbb{Z}[j] \to \mathbb{R}$ vérifie pour tout $x, y \in \mathbb{Z}[j]$ tel que $y \neq 0$, $\exists (q, r) \in \mathbb{Z}[j]^2$ tel que

$$\begin{cases} x = q.y + r \\ N(r) < N(y) \end{cases}$$

D'où $\mathbb{Z}[j]$ est euclidien.

3- Les polynômes cyclotomiques

3.a- Montrons que

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Notons U_n l'ensemble des racines n-ième de l'unité. Montrons que

$$U_n = \bigsqcup_{d|n} \mu_d^\star$$

Soit $d \in \mathbb{N}$, tel que $d|n$, et soit $z \in \mu_d^\star$
On a z est une racine d-ième de l'unité donc $\exists k \in \mathbb{N}$, tel que $z = \exp\left(\frac{2i\pi k}{d}\right)$
On a alors

$$z^n = \exp\left(\frac{2i\pi kn}{d}\right) = \exp\left(2i\pi k \frac{n}{d}\right) = 1$$

Donc $z \in U_n$, ensuite $\mu_d^\star \subset U_n$, et ceci pour tout $d \in \mathbb{N}$, tel que $d|n$
Donc

$$\bigcup_{d|n} \mu_d^\star \subset U_n$$

Réciproquement, soit $z \in U_n$, alors il existe $k \in [\![0, n-1]\!]$, tel que $z = \exp\left(\frac{2ik\pi}{n}\right)$
Notons

$$k' = \frac{k}{n \wedge k} \text{ et } n' = \frac{n}{n \wedge k}$$

On a $n' \wedge k' = 1$, et

$$z = \exp\left(\frac{2ik'\pi}{n'}\right)$$

Avec $n'|n$, et $n' \wedge k' = 1$, alors $z \in \mu_{n'}^{\star} \subset \bigcup_{d|n} \mu_d^{\star}$.

Donc

$$U_n \subset \bigcup_{d|n} \mu_d^{\star}$$

Par suite

$$U_n = \bigcup_{d|n} \mu_d^{\star}$$

Il ne reste qu'à montrer que $\bigcup_{d|n} \mu_d^{\star}$ est disjoint.

Plus généralement, soit $k, l \in \mathbb{N}^{\star}$, tel que $k \neq l$, montrons que $\mu_k^{\star} \cap \mu_l^{\star} = \varnothing$

Par l'absurde, supposons que $\mu_k^{\star} \cap \mu_l^{\star} \neq \varnothing$, alors $\exists z \in \mu_k^{\star} \cap \mu_l^{\star}$

Donc

$$\exists k_1 \in [\![0, k-1]\!] \text{ tel que } z = \exp\left(\frac{2i\,k_1\pi}{k}\right) \text{ et } k_1 \wedge k = 1$$

et

$$\exists l_1 \in [\![0, l-1]\!] \text{ tel que } z = \exp\left(\frac{2i\,l_1\pi}{l}\right) \text{ et } l_1 \wedge l = 1$$

Par symétrie, on peut supposer que $k < l$. On a alors

$$\exp\left(\frac{2i\,k_1 l\pi}{k}\right) = \exp\left(\frac{2i\,l_1 l\pi}{l}\right) = \exp(2\mathrm{i}l_1\pi) = 1$$

Donc $\frac{k_1 l}{k} \in \mathbb{Z}$, donc $k|k_1 l$, avec $k_1 \wedge k = 1$, donc d'après le lemme de GAUSS, on en déduit que $k|l$, absurde! avec $k, l \in \mathbb{N}^{\star}$ et $k < l$.

D'où

$$\mu_k^{\star} \cap \mu_l^{\star} = \varnothing$$

Ainsi

$$\bigcup_{d|n} \mu_d^{\star} = \bigsqcup_{d|n} \mu_d^{\star}$$

Donc

$$U_n = \bigsqcup_{d|n} \mu_d^{\star}$$

A partir de ce résultat, on peut déduire que:

$$\begin{aligned} X^n - 1 &= \prod_{z \in U_n} (X - z) \\ &= \prod_{z \in \bigsqcup_{d|n} \mu_d^{\star}} (X - z) \\ &= \prod_{d|n} \left[\prod_{z \in \mu_d^{\star}} (X - z) \right] \\ &= \prod_{d|n} \Phi_d(X) \end{aligned}$$

3.b- En déduire que $\Phi_n(X) \in \mathbb{Z}[X]$,

Montrons le résultat par récurrence sur $n \in \mathbb{N}^\star$

Pour $n = 1$, on a $\Phi_1 = X - 1 \in \mathbb{Z}[X]$.

Soit $n \in \mathbb{N}^\star$, supposons que $\Phi_1, \Phi_2, \ldots, \Phi_n \in \mathbb{Z}[X]$, et montrons que $\Phi_{n+1} \in \mathbb{Z}[X]$.

On a d'après la question précédente

$$X^n - 1 = \Phi_{n+1} \prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d$$

Par hypothèse de récurrence, on a $\prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d \in \mathbb{Z}[X]$, de plus $\prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d$ est unitaire. En utilisant la question 1 de cette partie, il vient

$$\exists (Q, R) \in \mathbb{Z}[X]^2, X^{n+1} - 1 = Q \prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d + R$$

Et

$$\deg(R) < \deg\left(\prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d \right)$$

On a pour tout $\alpha \in \mathbb{C}$ racine de $\prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d$, on a

$$R(\alpha) = \alpha^{n+1} - 1 - Q(\alpha) \prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d(\alpha) = 0$$

Donc α est aussi racine de R.

Avec $\deg(R) < \deg\left(\prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d \right)$, donc forcément $R = 0$.

D'où

$$X^{n+1} - 1 = Q \prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d$$

Avec

$$\Phi_{n+1} = \frac{X^{n+1}}{\prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d} = Q \in \mathbb{Z}[X]$$

D'où le résultat par récurrence.

3.c- Soit p un nombre premier

3.c.i- On a pour

$$X^p - 1 - (X-1)^p = -\sum_{k=1}^{p-1} \binom{p}{k} X^k (-1)^{p-k} = \sum_{k=1}^{p-1} (-1)^k \binom{p}{k} X^k$$

On a pour tout $k \in [\![1, p-1]\!]$, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, donc

$$p! = k!(p-k)!\binom{p}{k}$$

Avec $\forall i \in [\![1,k]\!]$, $p \wedge i = 1$, donc $p \wedge k! = 1$, et $\forall i \in [\![1, p-k]\!]$, $p \wedge i = 1$, donc $p \wedge (p-k)! = 1$

Ainsi $p \wedge k!(p-k)! = 1$, avec $p | k!(p-k)!\binom{p}{k}$, donc d'après le lemme de GAUSS, on a

$$p | \binom{p}{k}$$

Ainsi

$$\pi\left((-1)^k \binom{p}{k} \right) = 0$$

D'où

$$\hat{\pi}(X^p - 1 - (X-1)^p) = \sum_{k=1}^{p-1} \pi\left((-1)^k \binom{p}{k} \right) X^k = 0$$

Donc

$$\hat{\pi}(X^p - 1) - \hat{\pi}((X-1)^p) = 0$$

D'où

$$\hat{\pi}(X^p - 1) = (X - 1_{F_p})^p$$

D'où le résultat.

3.c.ii- Soient P et Q deux polynômes unitaires non constants dans $\mathbb{Z}[X]$ tels que $X^p - 1 = PQ$.
Montrons que P divise $P(1)$ et $Q(1)$.
On a d'après la question précédente

$$\hat{\pi}(X^p - 1) = (X - 1_{F_p})^p$$

Donc

$$\hat{\pi}(P)\hat{\pi}(Q) = (X - 1_{F_p})^p$$

Puisque P et Q sont non constant, alors $\hat{\pi}(P)$ et $\hat{\pi}(Q)$ les aussi.
Par unicité de la décomposition en irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$, on en déduit l'existence de $k \in [\![1, p-1]\!]$ tel que

$$\begin{cases} \hat{\pi}(P) = (X - 1_{F_p})^k \\ \hat{\pi}(Q) = (X - 1_{F_p})^{p-k} \end{cases}$$

Donc

$$\begin{cases} \hat{\pi}(P)(1_{F_p}) = 0_{F_p} \\ \hat{\pi}(Q)(1_{F_p}) = 0_{F_p} \end{cases}$$

Ensuite

$$\begin{cases} \pi(P(1)) = 0 \\ \pi(Q(1)) = 0 \end{cases}$$

Donc $p|P(1)$ et $p|Q(1)$.

3.c.iii- Montrons que Φ_p est irréductible de $\mathbb{Q}[X]$.
Par l'absurde, supposons que Φ_p n'est pas irréductible de $\mathbb{Q}[X]$.
Alors ils existent $P, Q \subset \mathbb{Q}[X]$ tel que $\Phi_p = PQ$, et P, Q sont non-constants.
D'après le résultat admis, $\exists r \in \mathbb{Q}$, tel que

$$\begin{cases} rP \in \mathbb{Z}[X] \\ \frac{1}{r}Q \in \mathbb{Z}[X] \end{cases}$$

Notons $P_1 = rP$ et $Q_1 = \frac{1}{r}Q$. On a alors

$$\Phi_p = P_1 Q_1$$

Avec $P_1, Q_1 \in \mathbb{Z}[X]$ sont non-constants.
Notons

$$\begin{aligned} R_p(X) &= \Phi_p(X+1) \\ &= \sum_{k=0}^{p-1} (X+1)^k \\ &= \frac{(X+1)^p - 1}{X} \\ &= \sum_{k=1}^{p} \binom{p}{k} X^{k-1} \\ &= \sum_{k=0}^{p-1} \binom{p}{k+1} X^k \end{aligned}$$

Et notons $P_1 = \sum_{k=0}^{l} a_k X^k$ et $Q_1 = \sum_{k=0}^{m} b_k X^k$ où $l, k \geqslant 1$ et $a_0, \ldots, a_l, b_0, \ldots, b_m \in \mathbb{Z}$.
Or pour tout $k \in [\![0, p-2]\!], p|\binom{p}{k+1}$, donc dans $\mathbb{Z}/p\mathbb{Z}[X]$, on a

$$\hat{\pi}(R_p(X)) = X^{p-1}$$

Donc

$$\hat{\pi}(P_1 Q_1) = X^{p-1}$$

Ainsi

$$\hat{\pi}(P_1)\hat{\pi}(Q_1) = X^{p-1}$$

Par unicité de la décomposition en irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$, on a

$$\hat{\pi}(P_1) = \bar{a_l} X^l$$

Et

$$\hat{\pi}(Q_1) = \overline{b_m} X^m$$

Ainsi $\bar{a_0} = 0$ et $\bar{b_0} = 0$, donc $p|a_0$ et $p|b_0$, ainsi $p^2|a_0 b_0$
Or

$$a_0 b_0 = \binom{p}{1} = p$$

Alors $p^2|p$, absurde !
D'où Φ_p est irréductible.

3.c.iv- Soit $\zeta = e^{\frac{2i\pi}{p}}$.
On a ζ est une racine primitive de l'unité, donc $\Phi_p(\zeta) = 0$.
Donc

$$\pi_\zeta | \Phi_p$$

Or d'après la question précédente, on a Φ_p est irréductible, donc ou bien π_ζ est constant ou bien π_ζ est associé à Φ_p
Avec π_ζ est non constant, alors π_ζ et Φ_p sont associé, de plus ils sont unitaires, alors ils sont égaux.
D'où

$$\pi_\zeta = \Phi_p$$

On a

$$\mathbb{Q}(\zeta) = \{P(\zeta) \,/\, P \in \mathbb{Q}[X]\}$$

est un corps (facile à vérifier).
De plus, si $P \in \mathbb{Q}[X]$, on a par division euclidienne de P par Φ_p, on a l'existence de $Q, R \in \mathbb{Q}[X]^2$ tel que

$$P = Q\Phi_p + R \text{ et } \deg(R) < p$$

Notons $R = \sum_{k=0}^{p-1} a_k X^k$, on a

$$P(\zeta) = R(\zeta) = \sum_{k=0}^{p-1} a_k \zeta^k \in \text{vect}_{\mathbb{Q}}(1, \zeta, \ldots, \zeta^{p-1})$$

Donc

$$\mathbb{Q}(\zeta) \subset \text{vect}_{\mathbb{Q}}(1, \zeta, \ldots, \zeta^{p-1})$$

Réciproquement, pour tout $k \in [\![0, p-1]\!]$, on a $\zeta^k \in \mathbb{Q}(\zeta)$, avec $\mathbb{Q}(\zeta)$ est un $\mathbb{Q}$-espace vectoriel.
Alors

$$\text{vect}_{\mathbb{Q}}(1, \zeta, \ldots, \zeta^{p-1}) \subset \mathbb{Q}(\zeta)$$

D'où

$$\mathbb{Q}(\zeta) = \text{vect}_{\mathbb{Q}}(1, \zeta, \ldots, \zeta^{p-1})$$

Ainsi la famille $(1, \zeta, \ldots, \zeta^{p-1})$ est génératrice de $\mathbb{Q}(\zeta)$, montrons qu'elle est $\mathbb{Q}$-libre.

Pour cela, soient $a_0,\dots,a_{p-1}\in\mathbb{Q}$, tel que

$$\sum_{k=0}^{p-1}a_k\zeta^k=0$$

Donc $\sum_{k=0}^{p-1}a_kX^k\Big|_{X=\zeta}=0$, avec $\deg\left(\sum_{k=0}^{p-1}a_kX^k\right)\leqslant p-1<p$. donc par minimalité du degré de $\pi_\zeta=\Phi_p$, on a forcément $\sum_{k=0}^{p-1}a_kX^k=0$, par suite $a_0=\cdots=a_{p-1}=0$.

D'où $(1,\zeta,\dots,\zeta^{p-1})$ est $\mathbb{Q}-$libre.
Donc

$$[\mathbb{Q}(\zeta):\mathbb{Q}]=\dim_{\mathbb{Q}}(\mathbb{Q}(\zeta))=p$$

D'où l 'extension du corps $\mathbb{Q}(\zeta)/\mathbb{Q}$ est de degré p.

4- Matrice compagnons

4.a- Soit $k\in\{1,\dots,n-1\}$, Par récurrence fini sur k, on peut montrer facilement que

$$C_p^ke_1=e_{k+1}$$

Donc pour tout $Q\in\mathbb{C}[X]$ non nul de degré inférieur ou égal à $(n-1)$, si on note:

$$Q=\sum_{k=0}^{n-1}a_kX^k$$

On a

$$Q(C_p)e_1=\sum_{k=0}^{n-1}a_kC_p^ke_1=\sum_{k=0}^{n-1}a_ke_{k+1}\neq0$$

Car $(e_1,\dots,e_n)$ est $\mathbb{C}$-libre, et $(a_0,\dots,a_{n-1})$ sont non tous nuls.
Donc

$$Q(C_p)\neq0$$

En particulier, le degré du polynôme minimal π_{C_p} est supérieur ou égal à n.
Or

$$\deg(\pi_{C_p})\leqslant\deg(\chi_{C_p})=n$$

Avec χ_{C_p}: le polynôme caractéristique de C_p.

Donc

$$\deg(\pi_{C_p})=n$$

4.b- On a d'après la question précédente

$$C_p^{n-1}e_1=e_n$$

Donc

$$C_p^n e_1 = C_p e_n = \begin{pmatrix} -a_0 \\ -a_1 \\ . \\ . \\ . \\ -a_{n-1} \end{pmatrix} = -\sum_{k=0}^{n-1} a_k e_{k+1}$$

Donc

$$P(C_p) = C_p^n + \sum_{k=0}^{n-1} a_k C_p^k$$

Pour tout $j \in [\![2, n]\!]$, on a

$$\begin{aligned} P(C_p)e_j &= C_p^n e_j + \sum_{k=0}^{n-1} a_k C_p^k e_j \\ &= C_p^n (C_p^{j-1} e_1) + \sum_{k=0}^{n-1} a_k C_p^k (C_p^{j-1} e_1) \end{aligned}$$

L'égalité reste vrai aussi pour $j = 1$, donc pour tout $j \in [\![1, n]\!]$, on a

$$\begin{aligned} P(C_p)e_j &= C_p^{n+j-1} e_1 + \sum_{k=0}^{n-1} a_k C_p^{k+j-1} e_1 \\ &= C_p^{j-1} \left(C_p^n e_1 + \sum_{k=0}^{n-1} a_k C_p^k e_1 \right) \\ &= C_p^{j-1} \left(-\sum_{k=0}^{n-1} a_k e_k + \sum_{k=0}^{n-1} a_k e_k \right) \\ &= 0 \end{aligned}$$

Donc $e_j \in \mathrm{Ker}(P(C_p))$ et ceci pour tout $j \in [\![1, n]\!]$, donc $\mathrm{Ker}(P(C_p)) = \mathbb{C}^n$.
Alors

$$P(C_p) = 0$$

Ensuite

$$\pi_{C_p} | P$$

Avec $\deg(\pi_{C_p}) = \deg(P)$, et π_{C_p} et P sont unitaires, donc π_{C_p} et P sont égaux.

4.c- On a d'après le théorème de Cayley-Hamilton $\pi_{C_p} | \chi_{C_p}$, avec $\deg(\pi_{C_p}) = \deg(\chi_{C_p}) = n$
Donc π_{C_p} et χ_{C_p} sont associés, de plus ils sont unitaires, alors

$$\chi_{C_p} = \pi_{C_p} = P$$

4.d- Montrons que

$$\chi_{Q(M)} = \prod_{k=1}^{n} (X - Q(\alpha_k))$$

Puisque $\mathbb{C}$ est algébriquement clos, alors M est trigonalisable, donc $\exists P \in \mathrm{GL}_n(\mathbb{C})$ et $T \in T_{n,s}(\mathbb{C})$ tel que

$$M = PTP^{-1}$$

On a $\alpha_1, \ldots, \alpha_n$ sont les racines de χ_M, donc il existe une permutation $\sigma : \mathcal{S}_n \to \mathcal{S}_n$ tel que

$$T = \begin{pmatrix} \alpha_{\sigma(1)} & * & . & . & * \\ 0 & \alpha_{\sigma(2)} & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & \alpha_{\sigma(n)} \end{pmatrix}$$

On a pour tout $k \in \mathbb{N}$,

$$M^k = P \begin{pmatrix} \alpha_{\sigma(1)}^k & * & . & . & * \\ 0 & \alpha_{\sigma(2)}^k & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & \alpha_{\sigma(n)}^k \end{pmatrix} P^{-1}$$

Notons $Q = \sum_{k=0}^{l} a_k X^k$, on a alors

$$\begin{aligned} Q(M) &= \sum_{k=0}^{l} a_k P \begin{pmatrix} \alpha_{\sigma(1)}^k & * & . & . & * \\ 0 & \alpha_{\sigma(2)}^k & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & \alpha_{\sigma(n)}^k \end{pmatrix} P^{-1} \\ &= P \begin{pmatrix} \sum_{k=0}^{l} a_k \alpha_{\sigma(1)}^k & * & & & * \\ 0 & \sum_{k=0}^{l} a_k \alpha_{\sigma(2)}^k & . & . & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & 0 & * \\ 0 & 0 & 0 & 0 & \sum_{k=0}^{l} a_k \alpha_{\sigma(n)}^k \end{pmatrix} p^{-1} \\ &= P \begin{pmatrix} Q(\alpha_{\sigma(1)}) & * & . & . & * \\ 0 & Q(\alpha_{\sigma(2)}) & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & Q(\alpha_{\sigma(n)}) \end{pmatrix} P^{-1} \end{aligned}$$

Ainsi

$$\begin{aligned}
\chi_{Q(M)} &= \det(XI_n - M) \\
&= \det\left(P\begin{pmatrix} Q(\alpha_{\sigma(1)}) & * & . & . & * \\ 0 & Q(\alpha_{\sigma(2)}) & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & Q(\alpha_{\sigma(n)}) \end{pmatrix}P^{-1}\right) \\
&= \det\left(P\times P^{-1}\times\begin{pmatrix} Q(\alpha_{\sigma(1)}) & * & . & . & * \\ 0 & Q(\alpha_{\sigma(2)}) & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & Q(\alpha_{\sigma(n)}) \end{pmatrix}\right) \\
&= \det\begin{pmatrix} Q(\alpha_{\sigma(1)}) & * & . & . & * \\ 0 & Q(\alpha_{\sigma(2)}) & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & Q(\alpha_{\sigma(n)}) \end{pmatrix} \\
&= \prod_{k=1}^{n}(X - Q(\alpha_{\sigma(k)})) \\
&= \prod_{k=1}^{n}(X - Q(\alpha_k))
\end{aligned}$$

4.e- A est un sous-anneau de $\mathbb{C}$, et $Q \in A[X]$.
Soit $P \in A[X]$ unitaire dont $\alpha_1, \ldots, \alpha_n$ les racines complexes comptées avec leur multiplicité.
On a puisque $P \in A[X]$, alors $C_p \in \mathcal{M}_n(A)$, avec $\mathcal{M}_n(A)$ est un anneau, alors

$$\forall k \in \mathbb{N}, C_p^k \in \mathcal{M}_n(A)$$

Ensuite

$$\forall R \in A[X], R(C_p) \in \mathcal{M}_n(A)$$

En particulier

$$Q(C_p) \in \mathcal{M}_n(A)$$

Donc

$$XI_n - Q(C_p) \in \mathcal{M}_n(A)$$

Par définition de déterminant, et puisque A est un anneau, on en déduit que

$$\chi_{Q(C_p)} = \det(XI_n - Q(C_p)) \in A[X]$$

Or le polynôme caractéristique de C_p est P, dont les racines sont $\alpha_1, \ldots, \alpha_n$, alors d'après la question précédente, on a

$$\chi_{Q(C_p)} = \prod_{k=1}^{n} (X - Q(\alpha_k))$$

Enfin

$$\prod_{k=1}^{n} (X - Q(\alpha_k)) \in A[X]$$

II Nombres algébriques

1.a- On a $\varphi : \mathbb{N}^\star \to \mathbb{N}$ définie par :

$$\forall n \in \mathbb{N}^\star \; \varphi(n) = \text{card}\{k \in [\![1, n]\!], k \wedge n = 1\}$$

Soit $d \geqslant 1$ un entier, Montrons que

$$\{n \in \mathbb{N}^\star, \varphi(n) \leqslant d\} \text{ est fini}$$

On a pour tout $n \geqslant 2$, si on écrit

$$n = \prod_{j=1}^{r} p_{i_j}^{\alpha_{i_j}}$$

Où $i_1 < \ldots < i_r \in \mathbb{N}^\star$, $(p_i)_{i \in \mathbb{N}^\star}$ est la suite des nombres premiers et $\alpha_{i_1}, \ldots, \alpha_{i_r} \in \mathbb{N}^\star$
On a

$$\varphi(n) = n \prod_{j=1}^{r} \left(1 - \frac{1}{p_{i_j}}\right)$$

Or pour tout $i \in \mathbb{N}^\star$, on a $P_i \geqslant (i+1)$ (Car la suite $(p_i)_{i \in \mathbb{N}^\star}$ est une suite d'entiers strictement croissante avec $p_1 = 2$).
Donc

$$\begin{aligned} \varphi(n) &\geqslant n \prod_{j=1}^{r} \left(1 - \frac{1}{i_j + 1}\right) \\ &\geqslant n \prod_{j=1}^{i_r} \left(1 - \frac{1}{j+1}\right) \\ &= \frac{n}{i_r + 1} \end{aligned}$$

Avec

$$n = \prod_{j=1}^{r} p_{i_j}^{\alpha_{i_j}} \geqslant \prod_{j=1}^{r} p_{i_j}^{\alpha_{i_j}} \geqslant 2^{\alpha_{i_1} + \cdots + \alpha_{i_r}} \geqslant 2^{i_r}$$

Donc

$$i_r \leqslant \frac{\log(n)}{\log(2)}$$

Ainsi

$$\varphi(n) \geqslant \frac{n}{\frac{\log(n)}{\log(2)}+1} \underset{n\to+\infty}{\sim} \log(2)\frac{n}{\log(n)} \underset{n\to+\infty}{\to} +\infty$$

Donc $\exists N_0 \in \mathbb{N},\ \forall n \geqslant N_0\ \varphi(n) > d$.
D'où

$$\{n \in \mathbb{N}^\star, \varphi(n) \leqslant d\} \subseteq [\![1, N_0 - 1]\!]$$

On en déduit que $\{n \in \mathbb{N}^\star, \varphi(n) \leqslant d\}$ est fini.

1.b- Soit K un sous-corps de $\mathbb{C}$, tel que $K/\mathbb{Q}$ est une extension fini.
Montrons que K contient un nombre fini de racines de l'unité.
Soit u une racine de l'unité, donc par définition $\exists n \in \mathbb{N}^\star$, tel que $u^n = 1$.
Soit n_0 le plus petit des entiers non nuls tel que $u^{n_0} = 1$.
Alors u est une racine n_0-ième primitive de l'unité.
On a alors

$$\Phi_{n_0}(u) = 0$$

Avec Φ_{n_0} est irréductible sur $\mathbb{Q}[X]$, alors $\pi_\alpha = \Phi_{n_0}$.
Donc $\mathbb{Q}(u)/\mathbb{Q}$ est une extension fini de degré $=\deg(\Phi_{n_0}) = \varphi(n_0)$.
Donc

$$\varphi(n_0) \leqslant [K\colon \mathbb{Q}]$$

Ainsi

$$u \in \bigcup_{\substack{n_0 \in \mathbb{N}^\star \\ \varphi(n_0) \leqslant [K:\mathbb{Q}]}} \{\alpha \in \mathbb{C}/\alpha^{n_0} = 1\}$$

Or $\forall n_0 \in \mathbb{N}$, $\{\alpha \in \mathbb{C}/\alpha^{n_0} = 1\}$ est fini, et d'après la question précédente, on a l'ensemble

$$\{n_0 \in \mathbb{N}^\star/\varphi(n_0) \leqslant [K\colon \mathbb{Q}]\}$$

est fini.
D'où le résultat.

2.a- Montrons que π_α est irréductible de $\mathbb{Q}[X]$.
Soient $P, Q \in \mathbb{Q}[X]$, tel que $\pi_\alpha = PQ$.
On a $P(\alpha)Q(\alpha) = \pi_\alpha(\alpha) = 0$, donc $P(\alpha) = 0$ ou $Q(\alpha) = 0$.
Par symétrie, on suppose que $P(\alpha) = 0$. donc $\pi_\alpha | P$. car P est non nul (si c'est le cas, on aurra $\pi_\alpha = 0$ ce qui contredit le fait que $\deg(\pi_\alpha) \geqslant 1$).
Avec $\deg(P) \leqslant \deg(\pi_\alpha)$, donc forcément $\deg(P) = \deg(\pi_\alpha)$.
Ainsi P et π_α sont associés.
D'où π_α est irréductible de $\mathbb{Q}[X]$.

Notons $n=\deg(\pi_\alpha)$. Et soit $P\in\mathbb{Q}[X]$.Par division euclidienne de P par π_α, on a l'existence de $Q,R\in\mathbb{Q}[X]$ tel que

$$P=Q\pi_\alpha+R$$

Donc

$$P(\alpha)=Q(\alpha)\pi_\alpha(\alpha)+R(\alpha)=R(\alpha)\in \text{vect}_{\mathbb{Q}}(1,\alpha,\dots,\alpha^{n-1})$$

Ainsi

$$\mathbb{Q}(\alpha)=\{P(\alpha)\,/\,P\in\mathbb{Q}[X]\}\subset \text{vect}_{\mathbb{Q}}(1,\alpha,\dots,\alpha^{n-1})$$

En particulier, la famille $(1,\alpha,\dots,\alpha^{n-1})$ est génératrice de $\mathbb{Q}(\alpha)$.
Et si $a_0,\dots,a_{n-1}\in\mathbb{Q}$, tel que

$$\sum_{k=0}^{n-1}a_k\alpha^k=0$$

Alors $\pi_\alpha\Big|\sum_{k=0}^{n-1}a_kX^k$, avec $\deg(\pi_\alpha)=n$, alors $\sum_{k=0}^{n-1}a_kX^k=0$, ainsi $a_0=\cdots=a_{n-1}=0$
D'où la famille $(1,\alpha,\dots,\alpha^{n-1})$ est $\mathbb{Q}$-libre.
Par suite la famille $(1,\alpha,\dots,\alpha^{n-1})$ est une base de $\mathbb{Q}$-espace vectoriel $K=\mathbb{Q}(\alpha)$
Donc

$$d=[K:\mathbb{Q}]=\dim_{\mathbb{Q}}(K)=n$$

D'où

$$\deg(\pi_\alpha)=d$$

2.b- σ un morphisme de $\mathbb{Q}$-algébre de K dans $\mathbb{C}$.
Montrons que $\sigma(\alpha)$ est une racine de π_α.
Notons $\pi_\alpha=\sum_{k=0}^{d}a_kX^k$, on a $\pi_\alpha(\alpha)=0$, donc

$$\sum_{k=0}^{d}a_k\alpha^k=0$$

Ainsi

$$\sigma\left(\sum_{k=0}^{d}a_k\alpha^k\right)=0$$

Par suite

$$\sum_{k=0}^{d}a_k\sigma(\alpha)^k=0$$

D'où

$$\pi_\alpha(\sigma(\alpha))=0$$

D'où le résultat.

Montrons qu'il y a exactement d morphismes de $\mathbb{Q}$-algébre.

Lemme 3.

Soit $P \in \mathbb{Q}[X]$ irréductible, alors les racines complexes de P sont deux à deux distincts.

Démonstration.

Si P admet une racine double $\alpha \in \mathbb{C}$, alors α est aussi racine de P'

Donc on a $P \wedge P'$ est non constant dans $\mathbb{C}[X]$.

Or la division euclidienne est invariante par extension du corps, donc d'après l'algorithme d'EUCLIDE, $P \wedge P'$ reste non constant dans $\mathbb{Q}[X]$.

Or P est irréductible, donc $P \wedge P' = P$, en particulier $P' | P$.

Et puisque $\deg(P') = \deg(P) - 1 < \deg(P)$, alors $P' = 0$, donc P est constant, absurde!

D'où le résultat du lemme. □

On en déduit que π_α admet exactement d recines complexes, on les note par $\alpha_1, \ldots, \alpha_d$ avec $\alpha_1 = \alpha$.

Soient $\sigma, \tau : K \to \mathbb{C}$, deux morphismes d'algèbre tel que $\sigma(\alpha) = \tau(\alpha)$. Montrons que $\sigma = \tau$

Soit $x \in K = \mathbb{Q}(\alpha)$, alors il existe $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Q}[X]$, tel que $x = P(\alpha)$

On a alors

$$\begin{aligned} \sigma(x) &= \sigma\left(\sum_{k=0}^{n} a_k \alpha^k\right) \\ &= \sum_{k=0}^{n} a_k \sigma(\alpha)^k \\ &= \sum_{k=0}^{n} a_k \tau(\alpha)^k \\ &= \tau\left(\sum_{k=0}^{n} a_k \alpha^k\right) \\ &= \tau(x) \end{aligned}$$

Et ceci pour tout $x \in K$, donc $\sigma = \tau$, donc un morphisme d'algèbre $K \to \mathbb{C}$ est determiné par l'image de α. Avec cette image est une racine de π_α.

On en déduit qu'on ait exactement d morphismes de $\mathbb{Q}$-algèbre, $\sigma_k : K \to \mathbb{C}$, où $k \in \{1, 2, \ldots, d\}$.

3- Soit $\alpha \in \mathbb{C}$ un nombre algébrique, et $\theta \in K = \mathbb{Q}(\alpha)$

3.a- Justifiant que θ est un nombre algébrique.

On a $\mathbb{Q}(\theta)$ est un sous-algébre de $\mathbb{Q}(\alpha)$.

Or α est algébrique, alors l'extension du corps $\mathbb{Q}(\alpha)/\mathbb{Q}$ est fini, donc $\mathbb{Q}(\theta)/\mathbb{Q}$ est aussi fini, (Car $\mathbb{Q}(\theta)$ est un sous-algèbre de $\mathbb{Q}(\alpha)$).

D'où θ est un nombre algébrique.

3.b- Montrons que $P_\theta = \prod_{k=1}^{d} (X - \sigma_k(\theta)) \in \mathbb{Q}[X]$

Comme $\theta \in \mathbb{Q}(\alpha)$, alors $\exists R = \sum_{k=0}^{n} a_k X^k \in \mathbb{Q}[X]$ tel que $\theta = R(\alpha)$

On a pour tout $k \in [\![1, d]\!]$

$$\begin{aligned}\sigma_k(\theta) &= \sigma_k\left(\sum_{j=0}^{n} a_j \alpha^j\right) \\ &= \sum_{j=0}^{n} a_j \sigma_k(\alpha)^j \\ &= R(\sigma_k(\alpha))\end{aligned}$$

Donc

$$P_\theta = \prod_{k=1}^{d} (X - R(\sigma_k(\alpha)))$$

Or $\sigma_1(\alpha), \ldots, \sigma_d(\alpha)$ sont les racines de $\pi_\alpha \in \mathbb{Q}[X]$, et $R \in \mathbb{Q}[X]$.
Donc d'après la question **4.e** de la partie **I**, on a:

$$P_\theta = \prod_{k=1}^{d} (X - R(\sigma_k(\alpha))) \in \mathbb{Q}[X]$$

3.c- Justifiant que π_θ divise P_θ. avec la même notation précédente qu'on a utilisé à la question précédente: $\theta = \sum_{j=0}^{n} a_j \alpha^j$ où $a_0, \ldots, a_n \in \mathbb{Q}$.

On a

$$\begin{aligned}P_\theta(\theta) &= \prod_{k=1}^{d} (\theta - \sigma_k(\theta)) \\ &= \prod_{k=1}^{d} \left(\sum_{j=0}^{n} a_j \alpha^j - \sigma_k\left(\sum_{j=0}^{n} a_j \alpha^j\right)\right) \\ &= \prod_{k=1}^{d} \left(\sum_{j=0}^{n} a_j (\alpha^j - \sigma_k(\alpha)^j)\right)\end{aligned}$$

Or $\sigma_1(\alpha), \ldots, \sigma_d(\alpha)$ sont exactement les racines de π_α.
Donc

$$\exists k_0 \in [\![1, d]\!] \; \sigma_{k_0}(\alpha) = \alpha$$

On a alors

$$\begin{aligned}P_\theta(\theta) &= \left(\sum_{j=0}^{n} a_j (\alpha^j - \alpha^j)\right) \prod_{\substack{k=1 \\ k \neq k_0}}^{d} \left(\sum_{j=0}^{n} a_j (\alpha^j - \sigma_k(\alpha)^j)\right) \\ &= 0\end{aligned}$$

Avec $P_\theta \in \mathbb{Q}[X]$ (d'après la question précédente), alors via le lemme 1 on en déduit que $\pi_\theta | P_\theta$

Montrons maintenant que P_θ est une puissance de π_θ.

Notons

$$\mathcal{A}_\theta = \{k \in \mathbb{N} / \pi_\theta | P_\theta\}$$

On a d'après la première partie de cette question $1 \in \mathcal{A}_\theta$, donc $\mathcal{A}_\theta \neq \varnothing$. ainsi cette partie de $\mathbb{N}$ admet un plus grand élément notons $k_0 = \max(\mathcal{A}_\theta)$.

On a alors $\pi_\theta^{k_0} | P_\theta$ et $\pi_\theta^{k_0+1} \not| P_\theta$.

Donc il existe $Q \in \mathbb{Q}[X]$, tel que $P_\theta = Q\pi_\theta^{k_0}$

Avec $\pi_\theta \not| Q$ et π_θ est irréductible, alors $Q \wedge \pi_\theta = 1$.

Par suite via le théorème de BEZOUT[2], on a l'existence de $R, S \in \mathbb{Q}[X]$ tel que

$$R\pi_\theta + SQ = 1 \tag{7}$$

Par l'absurde, supposons que Q est non constant.

Alors d'après le théorème fondamental de l'algèbre, Q est scindé sur $\mathbb{C}$, de plus tout ces racines sont des racines de P_θ.

Notons $\pi_\theta = \sum_{j=0}^{l} \beta_j X^j$

On a les racines de P_θ sont $\sigma_1(\theta), \ldots, \sigma_d(\theta)$. Et pour tout $k \in [\![1, d]\!]$ on a

$$\begin{aligned}
\pi_\theta(\sigma_k(\theta)) &= \pi_\theta(\sigma_k(\theta)) \\
&= \sum_{j=0}^{l} \beta_j \sigma_k(\theta)^j \\
&= \sigma_k\left(\sum_{j=0}^{l} \beta_j \theta^j\right) \\
&= \sigma_k(\pi_\theta(\theta)) \\
&= \sigma_k(0) \\
&= 0
\end{aligned}$$

Soit γ un racine de Q, et puisque les recines de Q sont des racines de P_θ alors il existe $k_0 \in [\![1, d]\!]$ tel que

$$\gamma = \sigma_{k_0}(\theta)$$

via la relation (5) on a

$$1 = R(\sigma_{k_0}(\theta))\pi_\theta(\sigma_{k_0}(\theta)) + S(\sigma_{k_0}(\theta))\, Q(\sigma_{k_0}(\theta)) = 0$$

absurde !

D'où Q est constant, avec P_θ et π_θ sont unitaires alors $Q = 1$.

Par suite

$$P_\theta = \pi_\theta^{k_0}$$

2. Le théorème de BEZOUT est valable sur $\mathbb{Q}[X]$, car l'anneau $\mathbb{Q}[X]$ est euclidienne (car $\mathbb{Q}$ est un corps), donc $\mathbb{Q}[X]$ est un anneau de BEZOUT.

D'où le résultat.

4- Soit $\alpha \in \mathbb{C}$

$\Rightarrow$) Si α est un entier algébrique, alors par définition, il existe un polynôme unitaire, à coefficients entiers tel que $P(\alpha) = 0$

On a alors $\pi_\alpha | P$, donc $\exists Q \in \mathbb{Q}[X]$, tel que $P = \pi_\alpha Q$.

D'après le résultat admis, on a $\exists r \in \mathbb{Q}$ tel que $\begin{cases} r\pi_\alpha \in \mathbb{Z}[X] \\ \frac{1}{r}Q \in \mathbb{Z}[X] \end{cases}$

On a le coefficient dominant de $r\pi_\alpha$ est r, donc $r \in \mathbb{Z}$.

De même le coefficient dominant de $\frac{1}{r}Q$ est $\frac{1}{r}$, alors $\frac{1}{r} \in \mathbb{Z}$.

Ainsi $r \in \{-1, 1\}$, d'où $\pm\pi_\alpha \in \mathbb{Z}[X]$, donc $\pi_\alpha \in \mathbb{Z}[X]$.

$\Leftarrow$) Si $\pi_\alpha \in \mathbb{Z}[X]$,

puisque $\pi_\alpha(\alpha) = 0$, alors par définition α est un entier algébrique.

5.a- Si α est un entier algébrique, notons $d = \deg(\pi_\alpha)$

Soit $x \in \mathrm{gr}\{\alpha^n / n \in \mathbb{N}\}$, donc $\exists n_1, \ldots, n_r \in \mathbb{N}$, et $a_1, \ldots, a_r \in \mathbb{Z}$ tel que

$$x = a_1\alpha^{n_1} + \cdots + a_r\alpha^{n_r}$$

Notons

$$P = \sum_{k=1}^{r} a_k X^{n_k} \in \mathbb{Z}[X]$$

Via **la question 1 de la partie *I***, on a l'existence de $Q, R \in \mathbb{Z}[X]$ tel que

$$P = \pi_\alpha Q + R$$

Et $\deg(R) \leqslant d - 1$.

On a donc

$$x = P(\alpha) = \pi_\alpha(\alpha)Q(\alpha) + R(\alpha)$$

Donc x s'écrit comme combinaison linéaire à coefficients entiers de $1, \alpha, \ldots, \alpha^{d-1}$

D'où le groupe engendré par $\{\alpha^n / n \in \mathbb{N}\}$ est de type fini.

5.b- Réciproquement si G est de type fini,Montrons que α est un entier algébrique.

Soit $(g_1, \ldots, g_n)$ une famille génératrice fini de G.

Notons pour tout $i \in [\![1, n]\!]$

$$\alpha g_i = \sum_{k=1}^{n} a_{i,k} g_k$$

Où $a_{i,k} \in \mathbb{Z}$, $\forall i, k \in [\![1, n]\!]$

Notons $A = (a_{i,k})_{1 \leqslant i,k \leqslant n}$ et $X = \begin{pmatrix} g_1 \\ g_2 \\ . \\ . \\ . \\ g_n \end{pmatrix}$

On a alors

$$\alpha X = AX$$

Donc

$$(A - \alpha I_n)X = 0$$

En particulier

$$A - \alpha I_n \notin \mathrm{GL}_n(\mathbb{C})$$

D'où

$$\det(A - \alpha I_n) = 0$$

Ainsi

$$\sum_{\sigma \in \mathcal{S}_n} (-1)^{\varepsilon(\sigma)} \prod_{i=1}^{n} (a_{\sigma(i),i} - \alpha \delta_{\sigma(i),i}) = 0$$

Où $\varepsilon(\sigma) \in \{-1, 1\}$ est la signature de σ, $\forall \sigma \in \mathcal{S}_n$.
D'où

$$P(\alpha) = 0$$

Avec

$$P = \sum_{\sigma \in \mathcal{S}_n} (-1)^{\varepsilon(\sigma)} \prod_{i=1}^{n} (a_{\sigma(i),i} - X\delta_{\sigma(i),i}) \in \mathbb{Z}[X]$$

D'où α est un entier algébrique.

6- Montrons que $\mathcal{D}_{\mathbb{C}}$: l'ensemble des entiers algébriques de $\mathbb{C}$ est un sous-anneau de $\mathbb{C}$.
On a $0 \in \mathcal{D}_{\mathbb{C}}$ (car $\pi_0 = X \in \mathbb{Z}[X]$) donc $\mathcal{D}_{\mathbb{C}} \neq \varnothing$.
Soient $\alpha, \beta \in \mathcal{D}_{\mathbb{C}}$.
Les deuc groupes $G_\alpha := \mathrm{gr}\{\alpha^n / n \in \mathbb{N}\}$ et $G_\beta := \mathrm{gr}\{\beta^n / n \in \mathbb{N}\}$ sont de type fini.
Donc il existe une famille $(g_1, \ldots, g_n)$ (respectivement $(l_1, \ldots, l_m)$) génératrice de G_α (respectivement de G_β).
On a pour tout $i \in \mathbb{N}$, $\exists a_{i,1}, \ldots, a_{i,n} \in \mathbb{Z}$, tel que

$$\alpha^i = \sum_{k=1}^{n} a_{i,k} g_k$$

Et pour tout $i \in \mathbb{N}$, $\exists b_{i,1}, \ldots, b_{i,m} \in \mathbb{Z}$, tel que

$$\beta^i = \sum_{k=1}^{m} b_{i,k} l_k$$

Pour tout $x \in G_{\alpha\beta} := \mathrm{gr}\{(\alpha\beta)^n / n \in \mathbb{N}\}$, on a l'existence de $c_0, \ldots, c_r \in \mathbb{Z}$ tel que

$$x = \sum_{j=0}^{r} c_j (\alpha\beta)^j$$

On a alors

$$\begin{aligned} x &= \sum_{j=0}^{r} c_j \alpha^j \beta^j \\ &= \sum_{j=0}^{r} c_j \left(\sum_{k=1}^{n} a_{j,k} g_k \right) \left(\sum_{i=1}^{m} b_{j,i} l_i \right) \\ &= \sum_{j=0}^{r} \sum_{k=1}^{n} \sum_{i=1}^{m} c_j a_{j,k} b_{j,i} g_k l_i \\ &= \sum_{k=1}^{n} \sum_{i=1}^{m} \left(\sum_{j=0}^{r} c_j a_{j,k} b_{j,i} \right) g_k l_i \end{aligned}$$

Avec pour tout $k \in [\![1,n]\!]$ et $i \in [\![1,m]\!]$, $\sum_{j=0}^{r} c_j a_{j,k} b_{j,i} \in \mathbb{Z}$.

Donc la famille finie $(g_k l_i)_{\substack{1 \leqslant k \leqslant n \\ 1 \leqslant i \leqslant m}}$ est une famille génératrice de $G_{\alpha\beta}$.

D'après **les questions 5.*a* et 5.*b* de cette partie**, on déduit que $\alpha\beta \in \mathcal{D}_{\mathbb{C}}$.

Et pour tout $y \in G_{\alpha-\beta} := \text{gr}\{(\alpha-\beta)^n / n \in \mathbb{N}\}$, on a l'existence de $c_0; \ldots; c_r \in \mathbb{Z}$ tel que

$$y = \sum_{j=0}^{r} c_j (\alpha - \beta)^j$$

On a alors

$$\begin{aligned} y &= \sum_{j=0}^{r} c_j (\alpha - \beta)^j \\ &= \sum_{j=0}^{r} \sum_{k=0}^{j} \binom{j}{k} c_j (-1)^j \alpha^{j-k} \beta^k \\ &= \sum_{j=0}^{r} \sum_{k=0}^{j} \binom{j}{k} c_j (-1)^j \left(\sum_{i=1}^{n} a_{j-k,i}\, g_i \right) \left(\sum_{s=1}^{m} b_{k,s} l_s \right) \\ &= \sum_{j=0}^{r} \sum_{k=0}^{j} \sum_{i=1}^{n} \sum_{s=1}^{m} \binom{j}{k} c_j (-1)^j a_{j-k,i}\, b_{k,s} g_i l_s \\ &= \sum_{i=1}^{n} \sum_{s=1}^{m} \left(\sum_{j=0}^{r} \sum_{k=0}^{j} \binom{j}{k} c_j (-1)^j a_{j-k,i}\, b_{k,s} \right) g_i l_s \end{aligned}$$

Avec $\forall (i,s) \in [\![1,n]\!] \times [\![1,m]\!]$, on a $\sum_{j=0}^{r} \sum_{k=0}^{j} \binom{j}{k} c_j (-1)^j a_{j-k,i}\, b_{k,s} \in \mathbb{Z}$.

Alors la famille finie $(g_i l_s)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant s \leqslant m}}$ est génératrice de $G_{\alpha-\beta}$.

D'où d'après ce qui précède $\alpha - \beta \in \mathcal{D}_{\mathbb{C}}$.

Par suite $\mathcal{D}_{\mathbb{C}}$ est un sous anneau de $\mathbb{C}$.

7- Montrons que $\mathcal{D}_{\mathbb{C}} \cap \mathbb{Q} = \mathbb{Z}$.

Tout d'abord pour tout $z \in \mathbb{Z}$, on a $X - z \in \mathbb{Z}[X]$ annule z, donc $z \in \mathcal{D}_{\mathbb{C}}$, de plus $z \in \mathbb{Q}$.

Ainsi $z \in \mathcal{D}_{\mathbb{C}} \cap \mathbb{Q}$.
Par suite $\mathbb{Z} \subseteq \mathcal{D}_{\mathbb{C}} \cap \mathbb{Q}$.
Réciproquement pour tout $z \in \mathcal{D}_{\mathbb{C}} \cap \mathbb{Q}$.
On a $X - z \in \mathbb{Q}[X]$ annule z, donc $\pi_z | X - z$, avec $\deg(\pi_z) \geqslant 1$, alors $\pi_z = X - z$.
Or z est un entier algébrique, donc $\pi_z = X - z \in \mathbb{Z}[X]$.
On tire $z \in \mathbb{Z}$.
D'où $\mathcal{D}_{\mathbb{C}} \cap \mathbb{Q} \subseteq \mathbb{Z}$.
Enfin $\mathcal{D}_{\mathbb{C}} \cap \mathbb{Q} = \mathbb{Z}$

III Le corps $\mathbb{Q}(\zeta)$ et son anneau d'entiers

1.a- Montrons que les morphismes de $\mathbb{Q}$-algébre de $\mathbb{Q}(\zeta)$ sont les σ_k, tel que $\sigma_k(\zeta) = \zeta^k$, pour tout $k \in \{1, \ldots, p-1\}$.

On a p est premier, donc $\pi_\zeta = \Phi_p$. dont les racines sont $\zeta, \zeta^2, \ldots, \zeta^{p-1}$

Donc d'après les questions 2.a et 2.b de la partie $\mathbb{I}$, il y a exactement $(p-1)$ tels morphismes de $\mathbb{Q}$-algébre $\sigma_k : K = \mathbb{Q}(\zeta) \to \mathbb{C}$ tel que pour tout $k \in \{1, \ldots, p-1\}$ tel que $\sigma_k(\zeta)$ soit racine de Φ_p et $\sigma_1(\zeta), \ldots, \sigma_{p-1}(\zeta)$ sont deux à deux distincts.

Quitte à réordonner les $\sigma_1, \ldots, \sigma_{p-1}$. Alors les morphismes de $\mathbb{Q}$-algébre de $\mathbb{Q}(\zeta)$ sont les σ_k tel que $\sigma_k(\zeta) = \zeta^k$ pour tout $k \in \{1, 2, \ldots, p-1\}$.

1.b.i- On a

$$\begin{aligned} N(\zeta) &= \prod_{k=1}^{p-1} \sigma_k(\zeta) \\ &= \prod_{k=1}^{p-1} \zeta^k \\ &= \zeta^{p\frac{p-1}{2}} \\ &= \exp\left(2i\pi \frac{p-1}{2}\right) \end{aligned}$$

Avec p est impair, alors $\frac{p-1}{2} \in \mathbb{N}$, donc $N(\zeta) = 1$.
Et

$$\begin{aligned} \mathrm{Tr}(\zeta) &= \sum_{k=1}^{p-1} \sigma_k(\zeta) \\ &= \sum_{k=1}^{p-1} \zeta^k \\ &= \zeta \frac{1 - \zeta^{p-1}}{1 - \zeta} \\ &= \frac{\zeta - 1}{1 - \zeta} \\ &= -1 \end{aligned}$$

1.b.ii- Montrons que $N(1-\zeta)=p$ et $N(1+\zeta)=1$

Notons

$$\begin{aligned} P &= \Phi_p(X+1) \\ &= \sum_{k=0}^{p-1}(X+1)^k \\ &= \frac{(X+1)^p-1}{(X+1)-1} \\ &= \sum_{k=1}^{p}\binom{p}{k}X^{k-1} \\ &= \sum_{k=0}^{p-1}\binom{p}{k+1}X^k \end{aligned}$$

Avec

$$P=\prod_{k=1}^{p-1}(X-(\zeta^k-1))$$

Donc d'après les identités de Newton des polynômes symétriques, on a

$$(-1)^{p-1}\prod_{k=1}^{p-1}(\zeta^k-1)=\binom{p}{1}=p$$

Donc

$$\prod_{k=1}^{p-1}(1-\zeta^k)=p$$

Ainsi

$$\begin{aligned} N(1-\zeta) &= \prod_{k=1}^{p-1}(1-\sigma_k(\zeta)) \\ &= \prod_{k=1}^{p-1}(1-\zeta^k) \\ &= p \end{aligned}$$

Notons

$$Q=\Phi_p(X-1)$$

Et d'autre part

$$\begin{aligned} Q &= \sum_{k=0}^{p-1}(X-1)^k \\ &= \sum_{k=0}^{p-1}\sum_{i=0}^{k}\binom{k}{i}(-1)^{k-i}X^i \\ &= \sum_{i=0}^{p-1}\left[\sum_{k=i}^{p-1}\binom{k}{i}(-1)^{k-i}\right]X^i \end{aligned}$$

Avec $Q=\prod_{k=1}^{p-1}(X-(\zeta^k+1))$, donc d'après les identités de Newton, on a

$$\begin{aligned}(-1)^{p-1}\prod_{k=1}^{p-1}(\zeta^k+1) &= \sum_{k=0}^{p-1}\binom{k}{0}(-1)^k\\ &= \sum_{k=0}^{p-1}(-1)^k\\ &= 1\end{aligned}$$

Ainsi

$$\begin{aligned}N(1+\zeta) &= \prod_{k=1}^{p-1}(\zeta^k+1)\\ &= 1\end{aligned}$$

2- Montrons que $\mathbb{Z}[\zeta]\subseteq\mathcal{D}_K$

Soit $x\in\mathbb{Z}[\zeta]$,

Alors il existe $(a_0,\dots,a_n)\in\mathbb{Z}^{n+1}$, tel que $x=\sum_{k=0}^{n}a_k\zeta^k$

Tout d'abord, remarquons que $x\in\mathbb{Q}(\zeta)=K$

D'autre part, on a par division euclidienne de $P=\sum_{k=0}^{n}a_kX^k$ par π_ζ, et en utilisant la question I de la partie I, on a l'existence de $Q,R\in\mathbb{Z}[X]$ tel que

$$\begin{cases}P=Q\pi_\zeta+R\\ \deg(R)<\deg(\pi_\zeta)=\deg(\Phi_p)=p-1\end{cases}$$

Ecrivant $R=\sum_{k=0}^{p-2}r_kX^k$ où $r_0,\dots,r_{p-2}\in\mathbb{Z}$

On a alors

$$\begin{aligned}x &= P(\zeta)\\ &= P=Q(\zeta)\pi_\zeta(\zeta)+R(\zeta)\\ &= \sum_{k=0}^{p-2}r_k\zeta^k\end{aligned}$$

Or $\zeta\in\mathcal{D}_{\mathbb{C}}$ (car $\Phi_p\in\mathbb{Z}[X]$ annule ζ), et $\mathcal{D}_{\mathbb{C}}$ est un sous anneau de $\mathbb{C}$.

Alors

$$x=\sum_{k=0}^{p-2}r_k\zeta^k\in\mathcal{D}_{\mathbb{C}}$$

D'où

$$\mathbb{Z}[\zeta]\subseteq\mathcal{D}_{\mathbb{C}}$$

Ainsi

$$\mathbb{Z}[\zeta]\subseteq\mathcal{D}_{\mathbb{C}}\cap K=\mathcal{D}_K$$

D'où le résultat.

3- Soit $z \in \mathbb{Z}[\zeta]$

3.a- Montrons que

$$z \in \mathbb{Z}[\zeta]^{\times} \text{ si et seulement si } N(z) \in \{-1, 1\}$$

$\Rightarrow$)Si $z \in \mathbb{Z}[\zeta]^{\times}$,
Alors il existe $z' \in \mathbb{Z}[\zeta]$ tel que $z.z' = 1$

Lemme 4.
Soit $\theta \in \mathbb{Z}[\zeta]$, si θ est un entier algébrique, alors $N(\theta) \in \mathbb{Z}$

Démonstration.
On a θ est un entier algébrique, en particulier il est algébrique de $\mathbb{Q}$.
D'près **la question 3.b de la partie** $\mathbb{I}$, on a

$$P_\theta = \prod_{k=1}^{p-1} (X - \sigma_k(\theta)) \in \mathbb{Q}[X]$$

En particulier

$$N(\theta) = \prod_{k=1}^{p-1} \sigma_k(\theta) \in \mathbb{Q}$$

Ecrivant $\theta = P(\zeta)$, avec $P \in \mathbb{Z}[X]$,
On a alors

$$\begin{aligned} N(\theta) &= \prod_{k=1}^{p-1} \sigma_k(\theta) \\ &= \prod_{k=1}^{p-1} P(\zeta^k) \end{aligned}$$

Avec ζ est un entier algébrique, donc pour tout $k \in [\![1, p-1]\!]$ on a $P(\zeta^k)$ est un entier algébrique.
D'où

$$\prod_{k=1}^{p-1} P(\zeta^k) \in \mathcal{D}_{\mathbb{C}}$$

Ainsi

$$\prod_{k=1}^{p-1} P(\zeta^k) \in \mathcal{D}_{\mathbb{C}} \cap \mathbb{Q} = \mathbb{Z}$$

D'où

$$N(\theta) = \prod_{k=1}^{p-1} P(\zeta^k) \in \mathbb{Z}$$

□

Puisque $z.z' = 1$, alors

$$N(z.z') = N(1) = \prod_{k=1}^{p-1} \sigma_k(1) = 1$$

Or

$$\begin{aligned} N(z.z') &= \prod_{k=1}^{p-1}\sigma_k(z.z') \\ &= \prod_{k=1}^{p-1}\sigma_k(z)\sigma_k(z') \\ &= \left(\prod_{k=1}^{p-1}\sigma_k(z)\right)\left(\prod_{k=1}^{p-1}\sigma_k(z')\right) \\ &= N(z)N(z') \end{aligned}$$

Donc

$$N(z)N(z') = 1$$

Avec $N(z), N(z') \in \mathbb{Z}$, (d'après le lemme 4) donc $N(z) \in \{-1, 1\}$
$\Leftarrow$)Réciproquement si $N(z) \in \{-1, 1\}$
On a

$$\begin{aligned} N(z) &= \prod_{k=1}^{p-1}\sigma_k\left(\sum_{j=0}^{n} a_j\zeta^j\right) \\ &= \prod_{k=1}^{p-1}\left(\sum_{j=0}^{n} a_j\sigma_k(\zeta)^j\right) \\ &= \prod_{k=1}^{p-1}\left(\sum_{j=0}^{n} a_j\zeta^{jk}\right) \\ &= \prod_{k=1}^{p-1} P(\zeta^k) \end{aligned}$$

D'où $\prod_{k=1}^{p-1} P(\zeta^k) \in \{-1, 1\}$
Ainsi

$$z \times \prod_{k=2}^{p-1} P(\zeta^k) \in \{-1, 1\}$$

Avec $\prod_{k=2}^{p-1} P(\zeta^k) \in \mathbb{Z}[\zeta]$.
Donc $z \in \mathbb{Z}[\zeta]^{\times}$.

D'où l'équivalence.

3.b- Si $N(z)$ est un nombre premier.
Montrons que z est irréductible.
Soient $a, b \in \mathbb{Z}[\zeta]$ tel que $z = a.b$
On a alors

$$N(z) = N(ab) = N(a)N(b)$$

Via le lemme 4, on a $N(a), N(b) \in \mathbb{Z}$.
Or $N(z)$ est un nombre premier.
Alors $N(a) \in \{-1, 1\}$ ou $N(b) \in \{-1, 1\}$
Via la question précédente, on en déduit que $a \in \mathbb{Z}[\zeta]^\times$ ou $b \in \mathbb{Z}[\zeta]^\times$.
Ainsi z est irréductible de $\mathbb{Z}[\zeta]$

4.a- Justifions que G est un groupe fini cyclique.
Par définition, G est l'ensemble des racines de l'unité contenues dans K. avec K est un corps.
Alors $1 \in G$
Soit z, z' deux racines de l'unité inclus dans K, alors $z \times \frac{1}{z'}$ est une racine de l'unité inclus dans K (car K est un corps).
Ainsi $z \times \frac{1}{z'} \in G$
Donc G est un groupe.
Or $K/\mathbb{Q}$ est une extension finie, donc d'après la question 1.b de la partie 2 on a K contient un nombre fini de racines de l'unité.
Donc G est un groupe fini, notons $n = \#G$.
On a alors pour tout $z \in G$, $z^n = 1$.
Ainsi G est un sous groupe de $(\mathbb{U}_n, \times)$ qui est monogène, alors G est monogène aussi.
On en déduit que G est cyclique.
D'où le résultat.

4.b- Soit ω un générateur de G. Justifions que $2p \,|\, n$ et que $\mathbb{Q}(\zeta) = \mathbb{Q}(\omega)$.
On a $\omega \in G$, donc $|w| = 1$, et il existe $a_0, \ldots, a_{p-1} \in \mathbb{Q}$ tel que $\omega = \sum_{k=0}^{p-1} a_k \zeta^k$
On a alors

$$\begin{aligned}
\omega^p &= \left(\sum_{k=0}^{p-1} a_k \zeta^k\right)^p \\
&= \sum_{i_0+\cdots+i_{p-1}=p} \prod_{k=0}^{p-1} a_{i_k} \zeta^{i_k} \\
&= \sum_{i_0+\cdots+i_{p-1}=p} \prod_{k=0}^{p-1} a_{i_k} \zeta^{i_k} \\
&= \sum_{i_0+\cdots+i_{p-1}=p} \left(\prod_{k=0}^{p-1} a_{i_k}\right) \zeta^{i_0+\cdots+i_{p-1}} \\
&= \sum_{i_0+\cdots+i_{p-1}=p} \left(\prod_{k=0}^{p-1} a_{i_k}\right) \\
&\in \mathbb{R}
\end{aligned}$$

Donc $\omega^p \in \mathbb{R}$, et $|\omega^p| = 1$, donc $\omega^p = \pm 1$, donc $\omega^{2p} = 1$.
Ainsi $2p | n$
Montrons maintenant que $\mathbb{Q}(\omega) = \mathbb{Q}(\zeta)$.
On a $\omega \in \mathbb{Q}(\zeta)$, donc $\mathbb{Q}(\omega) \subset \mathbb{Q}(\zeta)$.
Or $\zeta \in G = <\omega>$, donc il existe $k \in \mathbb{N}$, tel que $\zeta = \omega^k \in \mathbb{Q}(\omega)$

Donc $\mathbb{Q}(\zeta)\subset\mathbb{Q}(\omega)$
Ainsi $\mathbb{Q}(\zeta)=\mathbb{Q}(\omega)$

4.c- Montrons que $2p=n$.

On a forcément $G=\mathbb{U}_n$, on va justifier dans un premier temps ce point là.
On a $\text{ord}(G)=n$, donc pour tout $g\in G$, on a $g^n=1$, donc $G\subset\mathbb{U}_n$,
Or $\text{card}(G)=\text{card}(\mathbb{U}_n)=n<+\infty$
D'où $G=\mathbb{U}_n$.
Avant d'attaquer la suite, on va montrer un lemme:

Lemme 5.
Soit $z\in\mathbb{C}$, on a alors

$$[\mathbb{Q}(z):\mathbb{Q}]=\deg(\pi_z)$$

Démonstration.
Soit $z\in\mathbb{C}$, on rappelle que π_z est irréductible de $\mathbb{Q}[X]$.
Soit $x\in\mathbb{Q}(z)$, alors on a l'existence de $a_0,\dots,a_r\in\mathbb{Q}$ tel que $x=\sum_{j=0}^{n}a_jz^j$. Par division euclidienne de $P=\sum_{j=0}^{n}a_jX^j$ par Φ_z, on a l'existence de $(Q,R)\in\mathbb{Q}[X]^2$ tel que $P=Q\pi_z+R$
Alors

$$x=P(z)=Q(z)\pi_z(z)+R(z)=R(z)=\text{vect}_{\mathbb{Q}}(1,z,\dots,z^{\deg(\pi_z)-1})$$

Ainsi $(1,z,\dots,z^{\deg(\pi_z)-1})$ est génératrice de $\mathbb{Q}-$espace vectoriel $\mathbb{Q}(z)$.
Montrons que cette famille est $\mathbb{Q}-$libre
Pour cela, considérons $b_0,\dots,b_{\deg(\pi_z)-1}\in\mathbb{Q}$, tel que $\sum_{k=0}^{\deg(\pi_z)-1}b_kz^k=0$
Alors $\pi_z\left|\sum_{k=0}^{\deg(\pi_z)-1}b_kz^k\right.$, ainsi $\deg(\pi_z)\leqslant\deg\left(\sum_{k=0}^{\deg(\pi_z)-1}b_kz^k\right)=\deg(\pi_z)-1$, absurde!
D'où $(1,z,\dots,z^{\deg(\pi_z)-1})$ est $\mathbb{Q}$-libre
Ensuite $(1,z,\dots,z^{\deg(\pi_z)-1})$ est une base de $\mathbb{Q}(z)$ comme étant un $\mathbb{Q}$ esppace vectoriel.
Ainsi

$$\begin{aligned}[\mathbb{Q}(z):\mathbb{Q}] &= \#\{1,z,\dots,z^{\deg(\pi_z)-1}\}\\ &= \deg(\pi_z)\end{aligned}$$

D'où le résultat.

□

On a ω est un générateur de G, donc ω est une racine primitive de n.
En utilisant le lemme précédent, on a

$$\begin{aligned}[\mathbb{Q}(\omega):\mathbb{Q}] &= \deg(\pi_\omega)\\ &= \deg(\Phi_n)\\ &= \varphi(n)\end{aligned}$$

Or d'après la questio, préédente on a $2p|n$, donc il existe $k\in\mathbb{N}^\star$ tel que $n=2kp$.
Si k s'écrit sous la forme $k=2^ap^b$, où $a,b\in\mathbb{N}$ non tous nuls.

On a alors

$$\begin{aligned}\varphi(n) &= \varphi(2^{a+1}p^{b+1})\\ &= 2^{a+1}p^{b+1}\left(1-\frac{1}{2}\right)\left(1-\frac{1}{p}\right)\\ &= 2^a p^b(p-1)\\ &\geqslant \min\left(2(p-1), p(p-1)\right)\\ &> p\end{aligned}$$

Donc

$$\begin{aligned}p &= [\mathbb{Q}(\zeta): Q]\\ &= [\mathbb{Q}(\omega): \mathbb{Q}]\\ &= \varphi(n)\\ &> p\end{aligned}$$

absurde!

Sinon si k est de la forme $k = 2^a p^b \prod_{i=1}^{l} p_i^{y_i}$, où les $a, b \in \mathbb{N}$ et $y_1, \ldots, y_l > 1$.et $p_1, \ldots, p_l \geqslant 3$
On a alors

$$\begin{aligned}p &= [\mathbb{Q}(\zeta): \mathbb{Q}]\\ &= [\mathbb{Q}(\omega): \mathbb{Q}]\\ &= \varphi(n)\\ &= \varphi\left(2^{a+1}p^{b+1}\prod_{i=1}^{l} p_i^{y_i}\right)\\ &= 2^{a+1}p^{b+1}\prod_{i=1}^{l} p_i^{y_i}\left(1-\frac{1}{2}\right)\left(1-\frac{1}{p}\right)\prod_{i=1}^{l}\left(1-\frac{1}{p_i}\right)\\ &= 2^a p^b \prod_{i=1}^{l} p_i^{y_i-1}(p_i-1)(p-1)\\ &\geqslant 2(p-1)\\ &> p\end{aligned}$$

absurde!
D'où $k = 1$, par suite $n = 2p$.
Ainsi

$$\begin{aligned}G &= \mathbb{U}_{2p}\\ &= \left\{\exp\left(\frac{2ik\pi}{2p}\right) / k \in [\![0, 2p-1]\!]\right\}\\ &= \{\pm\zeta^k / k \in [\![0, p-1]\!]\}\end{aligned}$$

D'où le résultat.

5.a- Montrons que

$$<\lambda>\cap\mathbb{Z}=p\mathbb{Z}$$

On a

$$<\lambda>=\lambda\mathbb{Z}[\zeta]$$

Avec $0=\lambda\times 0\in\lambda\mathbb{Z}[\zeta]=<\lambda>$
Donc $<\lambda>\neq\varnothing$.
De plus pour tout $x,y\in<\lambda>$, on a l'existence de $P,Q\in\mathbb{Z}[X]$ tel que $x=\lambda P(\zeta)$ et $y=\lambda Q(\zeta)$
Donc

$$x-y=x=\lambda(P-Q)(\zeta)\in\lambda\mathbb{Z}[\zeta]=<\lambda>$$

D'où $<\lambda>$ est un sous groupe de $\mathbb{C}$.
Avec $\mathbb{Z}$ est un sous groupe de $\mathbb{C}$, donc l'intersection $<\lambda>\cap\mathbb{Z}$ est un sous groupe de $\mathbb{C}$.
Avec $<\lambda>\cap\mathbb{Z}\subseteq\mathbb{Z}$, donc $<\lambda>\cap\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$.
Donc

$$\exists n\in\mathbb{N}\,\text{tel que}<\lambda>\cap\mathbb{Z}=n\mathbb{Z}$$

Or d'après la question b.ii de cette partie.
On a

$$\begin{aligned}p &= N(\lambda)\\ &= N(1-\zeta)\\ &= \prod_{k=1}^{p-1}\sigma_k(1-\zeta)\\ &= \prod_{k=1}^{p-1}(1-\zeta^k)\\ &= \lambda\prod_{k=2}^{p-1}(1-\zeta^k)\end{aligned}$$

Avec $\prod_{k=2}^{p-1}(1-\zeta^k)\in\mathbb{Z}[\zeta]$
Donc

$$p\in<\lambda>\cap\mathbb{Z}=n\mathbb{Z}$$

En particulier $n\neq 0$, de plus $p\in n\mathbb{Z}$.
Donc $\exists r\in\mathbb{N}$ tel que $p=nr$.
Puisque p est premier, alors $n=1$ ou $n=p$
Si $n=1$, donc $<\lambda>\cap\mathbb{Z}=\mathbb{Z}$
En particulier $1\in<\lambda>$
Donc

$$\exists x\in\mathbb{Z}[\zeta]\,1=\lambda x$$

D'où $\lambda \in \mathbb{Z}[\zeta]^\times$, absurde avec $N(\lambda) = p \notin \{-1, 1\}$.
Donc $n = p$.
En conclusion

$$<\lambda> \cap \mathbb{Z} = p\mathbb{Z}$$

5.b- Soit $K \in \{1, 2, \ldots, p-1\}$.
Montrons que

$$\frac{1-\zeta}{1-\zeta^k} \in \mathbb{Z}[\zeta]^\times$$

Méthode 1:
On a

$$\frac{1-\zeta^k}{1-\zeta} = \sum_{j=0}^{k-1} \zeta^j \in \mathbb{Z}[\zeta]$$

Et

$$\begin{aligned} N\left(\frac{1-\zeta^k}{1-\zeta}\right) &= N\left(\sum_{j=0}^{k-1} \zeta^j\right) \\ &= \prod_{l=1}^{p-1} \sigma_l\left(\sum_{j=0}^{k-1} \zeta^j\right) \\ &= \prod_{l=1}^{p-1}\left(\sum_{j=0}^{k-1} \sigma_l(\zeta)^j\right) \\ &= \prod_{l=1}^{p-1}\left(\sum_{j=0}^{k-1} \zeta^{jl}\right) \\ &= \prod_{l=1}^{p-1}\left(\frac{1-\zeta^{kl}}{1-\zeta^l}\right) \end{aligned}$$

Pour tout $k, l \in [\![1, p-1]\!]$, notons $r_{k,l}$ l'unique entier dans $[\![0, p-1]\!]$ qui représente le reste de la division euclidienne de kl par p.
On a

$$\forall k, l \in [\![1, p-1]\!], k \wedge p = 1 \text{ et } l \wedge p = 1$$

Donc $kl \wedge p = 1$, ainsi $r_{kl} \in [\![1, p-1]\!]$
Donc l'application $\begin{array}{ccc} [\![1, p-1]\!] & \to & [\![1, p-1]\!] \\ l & \longmapsto & r_{k,l} \end{array}$ est bien définie.
De plus, pour tout $l, l' \in [\![1, p-1]\!]$, si $r_{k,l} = r_{k,l'}$
Alors

$$k(l - l') \text{ est divisible par } p$$

Avec $p \wedge k = 1$, on en déduit via le lemme de GAUSS que

$$P \,|\, l - l'$$

Donc

$$\exists s \in \mathbb{Z} \text{ tel que } l - l' = s.p$$

Or

$$-(p-1) \leqslant l - l' \leqslant p-1$$

Donc

$$-\frac{p-1}{p} \leqslant s \leqslant \frac{p-1}{p}$$

Donc $s = 0$, par suite $l = l'$.
D'où l'application

$$\begin{array}{c} [\![1, p-1]\!] \to [\![1, p-1]\!] \\ l \longmapsto r_{k,l} \end{array} \text{ est injective, donc bijective}$$

D'où

$$\begin{aligned} \prod_{l=1}^{p-1}(1-\zeta^{kl}) &= \prod_{l=1}^{p-1}(1-\zeta^{r_{k,l}}) \\ &= \prod_{l=1}^{p-1}(1-\zeta^{l}) \end{aligned}$$

D'où

$$\begin{aligned} N\left(\frac{1-\zeta^k}{1-\zeta}\right) &= \frac{\prod_{l=1}^{p-1}(1-\zeta^l)}{\prod_{l=1}^{p-1}(1-\zeta^l)} \\ &= 1 \end{aligned}$$

Finalement

$$\frac{1-\zeta^k}{1-\zeta} \in \mathbb{Z}[\zeta]^\times$$

D'où

$$\frac{1-\zeta}{1-\zeta^k} = \frac{1}{\frac{1-\zeta^k}{1-\zeta}} \in \mathbb{Z}[\zeta]^\times$$

MÉTHODE 2: On a $p \wedge k = 1$, donc d'après le théorème de BEZOUT,

$$\exists n_0, m_0 \in \mathbb{Z} \text{ tel que } pn_0 + km_0 = 1$$

Donc

$$\forall \alpha \in \mathbb{Z}, p(n_0 - \alpha k) + k(m_0 + \alpha p) = 1$$

Avec $\lim_{\alpha \to +\infty} m_0 + \alpha p = +\infty$, alors $\exists \alpha_0 \in \mathbb{N}$ tel que $m_0 + \alpha_0 p > 0$

Pour ce $\alpha_0 \in \mathbb{N}$, on a

$$\begin{aligned}\frac{1-\zeta}{1-\zeta^k} &= \frac{1-\zeta^{1-p(n_0-\alpha_0 k)}}{1-\zeta^k} \\ &= \frac{1-(\zeta^k)^{m_0+\alpha_0 p}}{1-\zeta^k} \\ &= \sum_{j=0}^{m_0+\alpha_0 p-1} \zeta^{kj} \\ &\in \mathbb{Z}[\zeta]\end{aligned}$$

D'autre part

$$\begin{aligned}\frac{1}{\frac{1-\zeta}{1-\zeta^k}} &= \frac{1-\zeta^k}{1-\zeta} \\ &= \sum_{j=0}^{k-1} \zeta^j \\ &\in \mathbb{Z}[\zeta]\end{aligned}$$

Donc par définition,

$$\frac{1-\zeta}{1-\zeta^k} \in \mathbb{Z}[\zeta]^\times$$

Montrons que

$$\lambda^{p-1}\mathbb{Z}[\zeta] = p\mathbb{Z}[\zeta]$$

Soit $x \in p\mathbb{Z}[\zeta]$, donc $\exists P \in \mathbb{Z}[X]$ tel que $x = pP(\zeta)$
Donc

$$\begin{aligned}x &= N(1-\zeta)P(\zeta) \\ &= \prod_{k=1}^{p-1} \sigma_k(1-\zeta)P(\zeta) \\ &= \prod_{k=1}^{p-1} (1-\zeta^k)P(\zeta) \\ &= \prod_{k=1}^{p-1} \left[(1-\zeta)\left(\sum_{j=0}^{k-1}\zeta^j\right)\right] P(\zeta) \\ &= (1-\zeta)^{p-1}\left[\prod_{k=1}^{p-1}\left(\sum_{j=0}^{k-1}\zeta^j\right)\right] P(\zeta) \\ &\in \lambda^{p-1}\mathbb{Z}[\zeta]\end{aligned}$$

D'où

$$p\mathbb{Z}[\zeta] \subset \lambda^{p-1}\mathbb{Z}[\zeta]$$

Réciproquement on a

$$\begin{aligned}\lambda^{p-1} &= (1-\zeta)^{p-1}\\ &= \prod_{k=1}^{p-1}\left(\frac{1-\zeta}{1-\zeta^k}\right)\prod_{k=1}^{p-1}(1-\zeta^k)\\ &= N(1-\zeta)\prod_{k=1}^{p-1}\left(\frac{1-\zeta}{1-\zeta^k}\right)\\ &= p\prod_{k=1}^{p-1}\left(\frac{1-\zeta}{1-\zeta^k}\right)\end{aligned}$$

Avec $\frac{1-\zeta}{1-\zeta^k}\in\mathbb{Z}[\zeta]^\times$, pour tout $k\in[\![1,p-1]\!]$.

Donc

$$\prod_{k=1}^{p-1}\left(\frac{1-\zeta}{1-\zeta^k}\right)\in\mathbb{Z}[\zeta]^\times$$

D'où

$$\lambda^{p-1}\in p\mathbb{Z}[\zeta]$$

Ainsi

$$\lambda^{p-1}\mathbb{Z}[\zeta]\subset p\mathbb{Z}[\zeta]$$

Enfin

$$\lambda^{p-1}\mathbb{Z}[\zeta]=p\mathbb{Z}[\zeta]$$

5.c- Soit Ψ: le morphisme d'anneaux de $\mathbb{Z}[X]\to\mathbb{Z}[\zeta]/<\lambda>$.

Soit $P=\sum_{k=0}^{n}a_kX^k\in\mathbb{Z}[X]$.

On a pour tout $k\in[\![0,n]\!]$

$$\begin{aligned}\zeta^k &= (\zeta-1+1)^k\\ &= (1-\lambda)^k\\ &= \sum_{j=0}^{k}(-1)^j\binom{k}{j}\lambda^j\\ &= 1+\sum_{j=1}^{k}(-1)^j\binom{k}{j}\lambda^j\end{aligned}$$

Donc

$$\begin{aligned}P(\zeta) &= \sum_{k=0}^{n}a_k\zeta^k\\ &= \sum_{k=0}^{n}a_k\left(1+\sum_{j=1}^{k}(-1)^j\binom{k}{j}\lambda^j\right)\\ &= \sum_{k=0}^{n}a_k+\lambda\sum_{k=0}^{n}a_k\sum_{j=1}^{k}(-1)^j\binom{k}{j}\lambda^{j-1}\end{aligned}$$

Avec $\sum_{k=0}^{n} a_k \sum_{j=1}^{k} (-1)^j \binom{k}{j} \lambda^{j-1} \in \mathbb{Z}[\zeta]$

Donc

$$\sum_{k=0}^{n} a_k \sum_{j=1}^{k} (-1)^j \binom{k}{j} \lambda^{j-1} \in <\lambda>$$

Et donc

$$\begin{aligned} P(\zeta) &= \sum_{k=0}^{n} a_k \,(\mathrm{mod} <\lambda>) \\ &= P(1) \,(\mathrm{mod} <\lambda>) \end{aligned}$$

Par division euclidienne de $P(1)$ par p, on a l'existence de $q, r \in \mathbb{N}$ tel que

$$\begin{cases} P(1) = pq + r \\ r \in [\![0, p-1]\!] \end{cases}$$

Or $p \in p\mathbb{Z}[\zeta]$, donc $p \in \lambda^{p-1}\mathbb{Z}[\zeta]$.
Donc $\exists Q \in \mathbb{Z}[X]$ tel que $p = \lambda^{p-1} Q(\zeta)$.
Ainsi

$$\begin{aligned} p &= \lambda(1-\zeta)^{p-2} Q(\zeta) \\ &= \lambda[(1-X)^{p-2} Q]|_{X=\zeta} \\ &= 0 \,(\mathrm{mod} <\lambda>) \end{aligned}$$

Donc

$$P(1) = r \,(\mathrm{mod} <\lambda>)$$

Ainsi

$$\Psi(P) = r \,(\mathrm{mod} <\lambda>)$$

D'où

$$\Psi(P) = P(1) \,(\mathrm{mod}\, p\mathbb{Z})$$

Donc l'image de P par Ψ est le reste de la division euclidienne de $P(1)$ par p.
Soit $P \in \mathrm{Ker}(\Psi)$, alors d'après ce qui précéde, on a le reste de la division euclidienne de $P(1)$ par p est nul.
Donc

$$P(1) = 0 \,(\mathrm{mod}\, p\mathbb{Z})$$

Réciproquement si $P \in \mathbb{Z}[X]$, tel que $P(1) = 0 \,(\mathrm{mod}\, p\mathbb{Z})$
Alors d'après ce qui précède on a

$$\Psi(P) = 0 \,(\mathrm{mod}\, p\mathbb{Z}) = 0 \,(\mathrm{mod} <\lambda>)$$

D'où $P \in \mathrm{Ker}(\Psi)$

D'où le résultat.

5.d- On a d'après ce qui précède $\mathrm{Im}(\Psi)$ est isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$
Donc $\mathbb{Z}[\zeta]/<\lambda>$ est isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

5.e- Puisque $\mathbb{Z}[\zeta]/<\lambda>$ est isomorphe à $\mathbb{F}_p$, et p est un nombre premier
Alors l'idéal $<\lambda>$ est premier, comme étant un idéal de l'anneau $\mathbb{Z}[\zeta]$.

6.a- Soit $P = \sum_{k=0}^{d} a_k X^k$ un polynôme unitaire de degré d, dont on note $\alpha_1, \ldots, \alpha_d$ les racines complexes comptées avec leur multiplicité. On suppose que pour tout $k \in \{1, \ldots, d\}$, α_k est de module 1.

6.a.i- Soit $k \in [\![0, d]\!]$, montrons que

$$|a_k| \leqslant \binom{d}{k}$$

On a d'après les identités de Newton

$$a_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant d} \prod_{j=1}^{k} \alpha_{i_j}$$

Donc

$$\begin{aligned} |a_k| &\leqslant \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant d} \left| \prod_{j=1}^{k} \alpha_{i_j} \right| \\ &= \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant d} 1 \\ &= \binom{d}{k} \end{aligned}$$

Notons

$$\mathcal{E}_d = \{ z \in \mathcal{D}_{\mathbb{C}} / \deg(\pi_z) = d, \text{ et les conjugés de } z \text{ sont tous de module } 1 \}$$

Et

$$\mathcal{O}_d = \{ P \in \mathbb{Z}[X] / P \text{ de degré } d \text{ dont tous les racines sont de module } 1 \}$$

On a

$$\mathcal{E}_d \subset \bigcup_{P \in \mathcal{O}_d} P^{-1}(\{0\})$$

Or un polynôme de degré d admet au plus d racines distincts dans $\mathbb{C}$.
Donc pour tout $P \in \mathcal{O}_d$, ona

$$\#P^{-1}(\{0\}) \leqslant d$$

De plus

$$\mathcal{O}_d \subset \left\{ \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X] \,/\, \forall k \in [\![0,d]\!], a_k \leqslant \binom{d}{k} \right\}$$

Et la famille $\left\{ \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X] \,/\, \forall k \in [\![0,\ d]\!],\ a_k \leqslant \binom{d}{k} \right\}$ est en bijection avec $\left\{ (a_0,\ldots,a_d) \in \mathbb{Z}^d / \forall k \in [\![0,d]\!], a_k \leqslant \binom{d}{k} \right\}$

Avec $\left\{ (a_0,\ .\ .\ .\ ,\ a_d) \in \mathbb{Z}^d \,/\, \forall k \in [\![0,\ d]\!],\ a_k \leqslant \binom{d}{k} \right\}$ est fini, donc $\left\{ \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X] / \forall k \in [\![0,d]\!], a_k \leqslant \binom{d}{k} \right\}$ est fini aussi, ainsi $\mathcal{O}_d$ est fini.

Par suite

$$\begin{aligned}
\#\mathcal{E}_d &\leqslant \bigcup_{P \in \mathcal{O}_d} P^{-1}(\{0\}) \\
&\leqslant d \times \#\mathcal{O}_d \\
&\leqslant d \times \#\left\{ \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X] / \forall k \in [\![0,d]\!], a_k \leqslant \binom{d}{k} \right\} \\
&= d \prod_{k=0}^{d} \left(2\binom{d}{k} - 1 \right) \\
&< +\infty
\end{aligned}$$

D'où le résultat.

6.a.ii- On a $X^n \in \mathbb{Z}[X]$, et $P \in \mathbb{Z}[X]$ n polynôme unitaire de degré d, dont on note $\alpha_1,\ldots,\alpha_d$ les racines complexes comptées avec leur multiplicité. Et $\mathbb{Z}$ est un sous anneau de $\mathbb{C}$

Donc d'après la question 4.e de la partie I, on a pour tout $n \in \mathbb{N}$

$$P_n = \prod_{k=1}^{d} (X - \alpha_k^n) \in \mathbb{Z}[X]$$

Avec pour tout $(n,d) \in \mathbb{N} \times [\![1,d]\!]$ on a $|\alpha_k^n| = 1$, alors en utilisant les mêmes notations précédente, on a pour tout $k \in [\![1,d]\!]$

$$\forall n \in \mathbb{N}, \alpha_k^n \in \mathcal{E}_d$$

Avec $\mathcal{E}_d$ est fini, donc

$$\exists n_0, n_1 \in \mathbb{N}, \text{tel que } n_0 < n_1 \ \text{ et } \ \alpha_k^{n_0} = \alpha_k^{n_1}$$

Avec $\alpha_k \neq 0$, donc

$$\alpha_k^{n_1 - n_0} = 1$$

Donc α_k est un racine de l'unité

D'où le résultat.

6.b- Soit $P\in\mathbb{Z}[X]$ tel que $u=P(\zeta)$. Montrons que, pour tout $k\in\{1,\dots,p-1\}$, $u_k=P(\zeta^k)$ est un conjugué de u, et que c'est un élément de $\mathbb{Z}[\zeta]^\times$

On a avec les mêmes notations de la partie $\mathbb{I}$.

$$\begin{aligned}\prod_{k=1}^{p-1}(X-P(\zeta^k)) &= \prod_{k=1}^{p-1}(X-P(\sigma_k(\zeta)))\\ &= \prod_{k=1}^{p-1}(X-\sigma_k(P(\zeta)))\\ &= \prod_{k=1}^{p-1}(X-\sigma_k(u))\\ &= P_u\end{aligned}$$

D'après la question 3.c de la partie $\mathbb{I}$, on a P_u est une puissance de π_u
Donc pour tout $k\in\{1,\dots,p-1\}$, $u_k=P(\zeta^k)$ est un conjugué de u.
De plus $u=P(\zeta)\in\mathbb{Z}[\zeta]^\times$.
Donc d'après la question 3.a de cette partie, on a

$$N(u)\in\{-1,1\}$$

Donc pour tout $k\in\{1,2,\dots,p-1\}$ on a

$$\begin{aligned}u_k\prod_{\substack{j=1\\ j\neq k}}^{p-1}P(\zeta^j) &= \prod_{j=1}^{p-1}P(\zeta^j)\\ &= \prod_{j=1}^{p-1}\sigma_j(P(\zeta))\\ &= \prod_{j=1}^{p-1}\sigma_j(u)\\ &= N(u)\\ &\in \{-1,1\}\end{aligned}$$

Avec $\prod_{\substack{j=1\\ j\neq k}}^{p-1}P(\zeta^j)\in Z[\zeta]$, donc par définition

$$u_k\in\mathbb{Z}[\zeta]^\times$$

6.c- Justifions que $\frac{u_p}{u_{p-1}}$ est un entier algébrique dont tous les conjugués sont de module 1.

Soit $k \in [\![1, p-1]\!]$,
On a

$$u_{p-k} = P(\zeta^{p-k}) = P(\zeta^{-k}) = \overline{P(\zeta)} = \bar{u_k}$$

Donc $\left|\frac{u_k}{u_{p-k}}\right| = 1$
Or $\frac{u_1}{u_{p-1}} \in \mathbb{Z}[\zeta]^\times \subset \mathfrak{D}_K$, et ses conjugués sont

$$\begin{aligned}\sigma_k\left(\frac{u_1}{u_{p-1}}\right) &= \frac{\sigma_k(u_{k1})}{\sigma_k(u_{p-1})} \\ &= \frac{u_k}{P(\sigma_k(\zeta^{-1}))} \\ &= \frac{u_k}{u_{p-k}}\end{aligned}$$

D'où le résultat

6.d- En déduire qu'il existe $m \in \mathbb{Z}$ tel que $\frac{u_1}{u_{p-1}} = \pm\zeta^m$.
Via la question 6.a.ii, on a $\frac{u}{u_{p-1}}$ est une racine de l'unité de K.
Ainsi il existe $m \in \mathbb{Z}$ tel que $\frac{u}{u_{p-1}} = \pm\zeta^m$ (cf. question 4 de la partie 3)

6.e.i- Soit $\theta \in \mathbb{Z}[\zeta]$. Justifions qu'il existe un entier $a \in \mathbb{Z}$ tel que $\theta = a \,(\mathrm{mod} < \lambda >)$.
On a $\theta \in \mathbb{Z}[\zeta]$, donc il existe des entiers $a_0, \ldots, a_{p-2}$ tel que $\theta = \sum_{k=0}^{p-2} a_k\zeta^k$
Donc

$$\begin{aligned}\theta &= \sum_{k=0}^{p-2} a_k(\zeta^k - 1) + \sum_{k=0}^{p-2} a_k \\ &= \lambda \sum_{k=0}^{p-2} a_k \sum_{j=0}^{k-1} \zeta^j + \sum_{k=0}^{p-2} a_k \\ &= \sum_{k=0}^{p-2} a_k \,(\mathrm{mod} < \lambda >)\end{aligned}$$

On a alors $\theta = a \,(\mathrm{mod} < \lambda >)$, où $a = \sum_{k=0}^{p-2} a_k \in \mathbb{Z}$.

En déduire que deux éléments conjugués de $\mathbb{Z}[\zeta]$ sont égaux modulo $<\lambda>$.
Soit $\theta = \sum_{k=0}^{p-2} a_k\zeta^k \in \mathbb{Z}[\zeta]$, et $\sigma_j(\theta) = \sum_{k=0}^{p-2} a_k\zeta^{jk}$ un des conjugués de θ, où $k \in [\![0, p-1]\!]$.
On a

$$\begin{aligned}\theta - \sigma_j(\theta) &= \sum_{k=0}^{p-2} a_k(\zeta^k - \zeta^{jk}) \\ &= \lambda \sum_{k=0}^{p-2} a_k\zeta^k \sum_{l=0}^{jk-k-1} \zeta l \\ &= 0 \,(\mathrm{mod} < \lambda >)\end{aligned}$$

D'où le résultat.

6.e.ii- Montrons que $\frac{u_1}{u_{p-1}} = \zeta^m$

On a $\frac{u_1}{u_{p-1}} = \pm\zeta^m$, par l'absurde, si $\frac{u_1}{u_{p-1}} = -\zeta^m$

Alors

$$u = -\zeta^m u_{p-1} = -u_{p-1} (\mathrm{mod} < \lambda >)$$

De plus u et u_{p-1} sont conjugués, alors d'après la question précédente, on a

$$u = u_{p-1} (\mathrm{mod} < \lambda >)$$

Donc

$$2u = 0 \, (\mathrm{mod} < \lambda >)$$

Ainsi $2u \in < \lambda >$, avec $< \lambda >$ est premier.
Donc on a $2 \in < \lambda >$ ou $u \in < \lambda >$
Si $2 \in < \lambda >$, alors

$$N(\lambda) | N(2) = 2^{p-1}$$

Ainsi $p | 2^{p-1}$, absurde!
Donc $u \in < \lambda >$
Ainsi

$$p = N(\lambda) | N(u) = 1$$

Absurde!
D'où le résultat.

Remarque: On peut répondre directement à la question **6.e.ii** sans faire les questions **6.c, 6.d, 6.e.i**

Justifiant que $\frac{u_1}{u_{p-1}}$ est un entier algébrique dont tous les conjugués sont de module 1.

On a d'après la question précécente, on a

$$u_1, u_{p-1} \in \mathbb{Z}[\zeta]^\times$$

Donc

$$u_1, \frac{1}{u_{p-1}} \in \mathbb{Z}[\zeta]$$

D'après la question 2, on a $\mathbb{Z}[\zeta] \subseteq \mathcal{D}_K \subseteq D_{\mathbb{C}}$, avec $\mathcal{D}_{\mathbb{C}}$ est un anneau (la question 6 de la partie $\mathbb{I}$)
Alors

$$\frac{u_1}{u_{p-1}} = u_1 \times \frac{1}{u_{p-1}} \in \mathcal{D}_{\mathbb{C}}$$

Autrement dit, $\frac{u_1}{u_{p-1}}$ est un entier algébrique.

Il ne reste qu'à montrer que tous les conjugués de $\frac{u_1}{u_{p-1}}$ sont de module 1. En s'inspirant des questions 6.a.i et 6.a.ii de cette partie, il est préférable (vu que $\frac{u_1}{u_{p-1}}$ est un entier algébrique) de montrer que $\frac{u_1}{u_{p-1}}$ est un racine de l'unité.(au même temps on répond a la deuxième partie de cette question)

Notons

$$P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$$

On a d'après la formule multinôme

$$\begin{aligned}
u_{p-1}^p &= P(\zeta^{p-1})^p \\
&= P\left(\frac{1}{\zeta}\right)^p \\
&= \left(\sum_{k=0}^{n} a_k \zeta^{-k}\right)^p \\
&= \sum_{i_1+\cdots+i_n=p} \prod_{k=0}^{n} a_{i_k} \zeta^{-i_k} \\
&= \sum_{i_1+\cdots+i_n=p} \left(\prod_{k=0}^{n} a_{i_k}\right) \zeta^{-(i_1+\cdots+i_n)} \\
&= \sum_{i_1+\cdots+i_n=p} \left(\prod_{k=0}^{n} a_{i_k}\right) \zeta^{-p} \\
&= \sum_{i_1+\cdots+i_n=p} \left(\prod_{k=0}^{n} a_{i_k}\right) \\
&= \sum_{i_1+\cdots+i_n=p} \left(\prod_{k=0}^{n} a_{i_k}\right) \zeta^{p} \\
&= \sum_{i_1+\cdots+i_n=p} \left(\prod_{k=0}^{n} a_{i_k}\right) \zeta^{i_1+\cdots+i_n} \\
&= \sum_{i_1+\cdots+i_n=p} \prod_{k=0}^{n} a_{i_k} \zeta^{i_k} \\
&= \left(\sum_{k=0}^{n} a_k \zeta^{k}\right)^p \\
&= P(\zeta)^p \\
&= u_1^p
\end{aligned}$$

Donc

$$\left(\frac{u_1}{u_{p-1}}\right)^p = 1$$

Donc

$$\exists m \in \mathbb{Z}, \frac{u_1}{u_{p-1}} = \zeta^m$$

D'où le résultat.

6.f- Justifions l'existence de $r \in \mathbb{Z}$ tel que $2r = m \,(\mathrm{mod}\, p\mathbb{Z})$.
On a d'aprè le théorème de FERMAT:

$$2^{p-1} = 1 (\mathrm{mod}\, p\mathbb{Z})$$

Donc pour $r = m2^{p-1}$, on a $r = m \,(\mathrm{mod}\, p\mathbb{Z})$.
On pose $\varepsilon = \zeta^{-r} u$. Montrons que $\varepsilon \in \mathbb{R}$ et conclure.
On a[3]

$$\begin{aligned} \bar{\varepsilon} &= \zeta^r \bar{u} \\ &= \zeta^r u_{p-1} \\ &= \zeta^r (\zeta^{-m} u) \\ &= \zeta^r (\zeta^{-2r} u) \\ &= \zeta^{-r} u \\ &= \varepsilon \end{aligned}$$

D'où $\varepsilon \in \mathbb{R}$.
Avec $u, \zeta^{-r} \in \mathbb{Z}[\zeta]^\times$, alors $\varepsilon \in \mathbb{Z}[\zeta]^\times$. ainsi $u = \zeta^r \varepsilon$, où ε est un réel dans $\mathbb{Z}[\zeta]^\times$
CONCULSION: pour tout $u \in \mathbb{Z}[\zeta]^\times$, on a l'existence de $r \in \mathbb{Z}$, et ε un réel inversible de $\mathbb{Z}[\zeta]$ tel que

$$u = \zeta^r \varepsilon$$

7- Le but de ce qui suit est de montrer que $\mathcal{D}_K = \mathbb{Z}[\zeta]$.

7.a- Soit $\theta \in \mathcal{D}_K$, Montrons que

$$N(\theta) \in \mathbb{Z} \text{ et } \mathrm{Tr}(\theta) \in \mathbb{Z}$$

Puisque $\theta \in K = \mathbb{Q}(\zeta)$, alors il existe $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Q}[X]$, tel que $\theta = P(\zeta)$
On a alors

$$P_\theta = \prod_{k=1}^{p-1} (X - \sigma_k(\theta)) \in \mathbb{Q}[X]$$

En particulier

$$N(\theta) = \prod_{k=1}^{p-1} \sigma_k(\theta) \in \mathbb{Q}$$

De plus

$$N(\theta) = \prod_{k=1}^{p-1} P(\zeta^k)$$

Et $\zeta \in \mathcal{D}_K$, $P \in \mathbb{Q}[X]$, et $\mathcal{D}_K$ est un sous anneau de $\mathbb{C}$, alors $N(\theta) = \prod_{k=1}^{p-1} P(\zeta^k) \in \mathcal{D}_K$

3. C'est facile à vérifier que $\overline{u_{p-1}} = u$.

Par suite

$$N(\theta) \in \mathcal{D}_K \cap \mathbb{Q} = \mathbb{Z}$$

Et On a

$$\begin{aligned}
\mathrm{Tr}(\theta) &= \sum_{k=1}^{p-1} \sigma_k(\theta) \\
&= \sum_{k=1}^{p-1} \sigma_k(P(\zeta)) \\
&= \sum_{k=1}^{p-1} P(\sigma_k(\zeta)) \\
&= \sum_{k=1}^{p-1} P(\zeta^k) \\
&= \sum_{k=1}^{p-1} \sum_{j=0}^{n} a_j \zeta^{jk} \\
&= \sum_{j=0}^{n} a_j \left(\sum_{k=1}^{p-1} \zeta^{jk} \right) \\
&= \sum_{j=0}^{n} a_j \zeta^j \frac{1-\zeta^{j(p-1)}}{1-\zeta^j} \\
&= \sum_{j=0}^{n} a_j \frac{\zeta^j - 1}{1-\zeta^j} \\
&= -\sum_{j=0}^{n} a_j \\
&\in \mathbb{Q}
\end{aligned}$$

De plus $\zeta \in \mathcal{D}_K$, $P \in \mathbb{Q}[X]$, et $\mathcal{D}_K$ est un sous anneau de $\mathbb{C}$, alors $\mathrm{Tr}(\theta) = \sum_{k=1}^{p-1} P(\zeta^k) \in \mathcal{D}_K$

Par suite

$$\mathrm{Tr}(\theta) \in \mathcal{D}_K \cap \mathbb{Q} = \mathbb{Z}$$

D'où le résultat.

7.b.i- Soit $k \in [\![0, p-2]\!]$, on a

$$\begin{aligned}
b_k &= \mathrm{Tr}(\theta\zeta^{-k} - \theta\zeta) \\
&= \sum_{j=1}^{p-1} \sigma_j(\theta\zeta^{-k} - \theta\zeta) \\
&= \sum_{j=1}^{p-1} (\sigma_j(\theta)\sigma_j(\zeta)^{-k} - \sigma_j(\theta)\sigma_j(\zeta))
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{j=1}^{p-1}\left(\sigma_j\left(\sum_{l=0}^{p-2}a_l\zeta^l\right)\zeta^{-jk}-\sigma_j\left(\sum_{l=0}^{p-2}a_l\zeta^l\right)\zeta^j\right)\\
&= \sum_{j=1}^{p-1}\sum_{l=0}^{p-2}a_l(\zeta^{jl-jk}-\zeta^{jl-j})\\
&= \sum_{l=0}^{p-2}a_l\left(\sum_{j=1}^{p-1}(\zeta^{l-k})^j\right)-\sum_{l=0}^{p-2}a_l\left(\sum_{j=1}^{p-1}(\zeta^{l-1})^j\right)\\
&= \sum_{\substack{l=0\\l\neq k}}^{p-2}a_l\left(\sum_{j=1}^{p-1}(\zeta^{l-k})^j-\sum_{j=1}^{p-1}(\zeta^{l-1})^j\right)+a_k\left(p-1-\sum_{j=1}^{p-1}(\zeta^{l-1})^j\right)\\
&= \sum_{\substack{l=0\\l\neq k}}^{p-2}a_l\left(\sum_{j=1}^{p-1}(\zeta^{l-k})^j-\sum_{j=1}^{p-1}(\zeta^{l-1})^j\right)+a_k\left(p-1-\zeta^{l-1}\frac{1-\zeta^{(l-1)(p-1)}}{1-\zeta^{l-1}}\right)\\
&= \sum_{\substack{l=0\\l\neq k}}^{p-2}a_l\left[\zeta^{l-k}\frac{1-\zeta^{(l-k)(p-1)}}{1-\zeta^{l-k}}-\zeta^{l-1}\frac{1-\zeta^{(l-1)(p-1)}}{1-\zeta^{l-1}}\right]+pa_k\\
&= \sum_{\substack{l=0\\l\neq k}}^{p-2}a_l[-1-(-1)]+pa_k\\
&= pa_k
\end{aligned}
$$

De plus $\theta\zeta^{-k}-\theta\zeta\in\mathcal{D}_K$, donc d'après la question précédente, $b_k=\mathrm{Tr}(\theta\zeta^{-k}-\theta\zeta)\in\mathbb{Z}$.

7.b.ii- Montrons qu'il existe des entiers $c_0,\dots,c_{p-2}$. que l'on exprimera en onction des b_k tels que $p\theta=\sum_{k=0}^{p-2}c_k\lambda^k$,

On a

$$
\begin{aligned}
p\theta &= \sum_{k=0}^{p-2}pa_k(1-\lambda)^k\\
&= \sum_{k=0}^{p-2}\sum_{j=0}^{k}b_k(-1)^j\binom{k}{j}\lambda^j\\
&= \sum_{j=0}^{p-2}\sum_{k=j}^{p-2}b_k(-1)^j\binom{k}{j}\lambda^j
\end{aligned}
$$

On pose pour tout $k\in[\![0,p-2]\!]$, $c_k=\sum_{j=k}^{p-2}b_j(-1)^k\binom{j}{k}\in\mathbb{Z}$, on a alors $p\theta=\sum_{k=0}^{p-2}c_k\lambda^k$, CQFD.

Montrons que

$$\forall k\in[\![0,p-2]\!],\ b_k=\sum_{l=k}^{p-2}(-1)^l\binom{l}{k}c_l$$

On a

$$\begin{aligned}\sum_{k=0}^{p-2} b_k\zeta^k &= p\sum_{k=0}^{p-2} a_k\zeta^k \\ &= p\theta \\ &= \sum_{k=0}^{p-2} c_k\lambda^k \\ &= \sum_{k=0}^{p-2} c_k(1-\zeta)^k \\ &= \sum_{k=0}^{p-2}\sum_{j=0}^{k} c_k(-1)^j\binom{k}{j}\zeta^j \\ &= \sum_{k=0}^{p-2}\sum_{l=k}^{p-2} c_l(-1)^l\binom{l}{k}\zeta^k\end{aligned}$$

Avec $(1,\zeta,\ldots,\zeta^{p-2})$ est $\mathbb{Q}$-libre, alors

$$\forall k\in[\![0,p-2]\!], b_k = \sum_{l=k}^{p-2} c_l(-1)^l\binom{l}{k}$$

D'où le résultat

7.b.iii- On a d'après la question 1.b.ii de cette partie

$$\begin{aligned}p &= N(1-\zeta) \\ &= \prod_{k=1}^{p-1}\sigma_k(1-\zeta) \\ &= \prod_{k=1}^{p-1}(1-\zeta^k) \\ &= \prod_{k=1}^{p-1}\left[(1-\zeta)\sum_{j=0}^{k-1}\zeta^j\right] \\ &= (1-\zeta)^{p-1}\prod_{k=1}^{p-1}\left(\sum_{j=0}^{k-1}\zeta^j\right) \\ &= \lambda^{p-1}\prod_{k=1}^{p-1}\left(\sum_{j=0}^{k-1}\zeta^j\right)\end{aligned}$$

Avec $\beta = \prod_{k=1}^{p-1}\left(\sum_{j=0}^{k-1}\zeta^j\right)\in\mathbb{Z}[\zeta]$.

Montrons maintenant que $p|c_0$, on a

$$\begin{aligned} c_0 &= p\theta - \sum_{k=1}^{p-2} c_k \lambda^k \\ &= \beta\lambda^{p-1} - \lambda \sum_{k=1}^{p-2} c_k \lambda^{k-1} \end{aligned}$$

Donc

$$\begin{aligned} c_0^{p-1} &= N(c_0) \\ &= N\left(\lambda\left(\beta\lambda^{p-2} - \sum_{k=1}^{p-2} c_k \lambda^{k-1} \right) \right) \\ &= N(\lambda) N\left(\beta\lambda^{p-2} - \sum_{k=1}^{p-2} c_k \lambda^{k-1} \right) \\ &= pN\left(\beta\lambda^{p-2} - \sum_{k=1}^{p-2} c_k \lambda^{k-1} \right) \end{aligned}$$

Avec $N\left(\beta\lambda^{p-2} - \sum_{k=1}^{p-2} c_k \lambda^{k-1} \right) \in \mathbb{Z}$, donc $p|c_0^{p-1}$, avec p est premier alors $p|c_0$.

Passant maintenant à montrer que $p|c_k$ pour tout $k \in [\![0, p-2]\!]$,
Montrons ce résultat pas récurrence fini sur $k \in [\![0, p-2]\!]$
Pour $k = 0$, déjà fait !
Soit $k \in [\![0, p-3]\!]$, supposons que le résultat est vrai pour $1, 2, \ldots, k$ et montrons le pour $k+1$.
On a

$$c_{k+1}\lambda^{k+1} = p\left(\theta - \sum_{l=0}^{k} \frac{c_l}{p} \lambda^l \right) - \lambda^{k+2} \sum_{l=k+2}^{p-2} c_l \lambda^{l-k-2}$$

Avec pour tout $l \in [\![1, p-2]\!]$

$$\begin{aligned} c_{k+1}p^{k+1} &= c_{k+1} N(\lambda^{k+1}) \\ &= N(c_{k+1}\lambda^{k+1}) \\ &= N\left(\beta\lambda^{p+1}\left(\theta - \sum_{l=0}^{k} \frac{c_l}{p} \lambda^l \right) - \lambda^{k+2} \sum_{l=k+2}^{p-2} c_l \lambda^{l-k-2} \right) \\ &= N\left(\lambda^{k+2}\left[\beta\lambda^{p-k-1}\left(\theta - \sum_{l=0}^{k} \frac{c_l}{p} \lambda^l \right) - \sum_{l=k+2}^{p-2} c_l \lambda^{l-k-2} \right] \right) \\ &= N(\lambda^{k+2}) N\left(\left[\beta\lambda^{p-k-1}\left(\theta - \sum_{l=0}^{k} \frac{c_l}{p} \lambda^l \right) - \sum_{l=k+2}^{p-2} c_l \lambda^{l-k-2} \right] \right) \\ &= p^{k+2} N\left(\left[\beta\lambda^{p-k-1}\left(\theta - \sum_{l=0}^{k} \frac{c_l}{p} \lambda^l \right) - \sum_{l=k+2}^{p-2} c_l \lambda^{l-k-2} \right] \right) \end{aligned}$$

Donc

$$c_{k+1} = pN\left(\left[\beta\lambda^{p-k-1}\left(\theta - \sum_{l=0}^{k}\frac{c_l}{p}\lambda^l\right) - \sum_{l=k+2}^{p-2} c_l\lambda^{l-k-2}\right]\right)$$

Donc $p|c_{k+1}$
D'où le résultat.

IV Le théorème de Fermat pour $p=3$

1- On a $3\nmid xyz$, en particulier $3\nmid x$, donc $x\equiv 1[3]$ ou $x\equiv -1[3]$
Si $x\equiv 1[3]$,
On a

$$(x-1)^3 = x^3 + 3(x-x^2) - 1$$

Avec $9|(x-1)^3$ et $9|3(x-x^2)$, donc

$$x^3 \equiv 1[9]$$

De même si $x\equiv -1[3]$, on a

$$(x+1)^3 = x^3 + 3(x^2+x) + 1$$

Avec $9|(x-1)^3$ et $9|3(x^2+x)$, donc

$$x^3 \equiv -1[9]$$

Donc de même, on a

$$y^3\equiv 1[9] \text{ ou } y^3\equiv -1[9]$$

Et

$$z^3\equiv 1[9] \text{ ou } z^3\equiv -1[9]$$

Avec

$$x^3 = -(y^3+z^3)$$

Donc modulo 3 on aurra

$$1\equiv -2[9] \text{ ou } 1\equiv 0[9] \text{ ou } 1\equiv 2[9] \text{ ou } -1\equiv -2[9] \text{ ou } -1\equiv 0[9] \text{ ou } 1\equiv 2[9]$$

absurde !

2- On a

$$\begin{aligned}\lambda^2 &= (1-j)^2\\ &= 1-2j+j^2\\ &= (1+j+j^2)-3j\\ &= -3j\end{aligned}$$

D'après **la question 2.c de la partie *I***, on a $-j \in \mathbb{Z}[j]^\times$
Donc

$$3 \sim \lambda^2$$

3- . Soit $s \in \mathbb{Z}[j]$ tel que $s \neq 0 \,(\text{mod} < \lambda >)$. Montrons qu'il existe $\varepsilon \in \{-1, +1\}$ tel que $s^3 = \varepsilon \,(\text{mod} < \lambda >)$.

Suivant l'indication, montrons qu'il existe $\varepsilon \in \{-1, 1\}$ tel que $s = \varepsilon (\text{mod} < \lambda >)$
On a d'après la question précédente: $\lambda^2 \sim 3$ dans $\mathbb{Z}[j]$.
On a l'existence de $a, b \in \mathbb{Z}$ tel que $s = a + jb$
Donc

$$s = a - 2b + 3jb = a - 2b \,(\text{mod} < \lambda >) = \varepsilon \,(\text{mod} < \lambda >)$$

Où $\varepsilon \in \{-1, 0, 1\}$ est obtenu a partir de la division euclidienne de $a - 2b$ par 3.
Puisque $s \neq 0 \,(\text{mod} < \lambda >)$, On a alors $\varepsilon \in \{-1, 1\}$.
On a alors l'existence de $\chi \in \mathbb{Z}[j]$ tel que : $s - \varepsilon = \chi\lambda$.
Donc

$$\begin{aligned} s^3 - \varepsilon &= s^3 - \varepsilon^3 \\ &= (s-\varepsilon)^3 + 3\varepsilon s^2 - 3s \\ &= \chi^3\lambda^3 + 3\varepsilon s(s-\chi) \\ &= \chi^3\lambda^3 - j^2\lambda^2\varepsilon(\chi\lambda + \varepsilon)\chi\lambda \\ &= \chi^3\lambda^3 - j^2\lambda^3\varepsilon(\chi\lambda + \varepsilon)\chi \\ &= \chi\lambda^3(\chi^2 - j^2\varepsilon(\chi\lambda + \varepsilon)) \\ &= \chi\lambda^3(\chi^2 - j^2\varepsilon\chi\lambda - j^2) \end{aligned}$$

D'après ce qui précède, on a l'existence de $\varepsilon' \in \{-1, 1\}$ tel que $\chi = \varepsilon' \,(\text{mod}\,(<\lambda>))$

Ainsi, on a modulo $<\lambda>$

$$\begin{aligned} \chi^2 - j^2\varepsilon\chi\lambda - j^2 &= \varepsilon'^2 - j^2\varepsilon\chi\lambda - j^2 (\text{mod} < \lambda >) \\ &= \lambda[(1+j) - j^2\varepsilon\chi] (\text{mod} < \lambda >) \\ &= 0 \,(\text{mod} < \lambda >) \end{aligned}$$

Ainsi, il existe $\mu \in \mathbb{Z}[j]$ tel que $\chi^2 - j^2\varepsilon\chi\lambda - j^2 = \mu\lambda$
Par suite

$$\begin{aligned} s^3 - \varepsilon &= \chi\mu\lambda^4 \\ &= 0 \,(\text{mod} < \lambda^4 >) \end{aligned}$$

D'où le résultat.

4- Supposons que (P_n) est vérifiée pour un quadruplet $(\alpha, \beta, \delta, \omega)$.

Montrons que $n \geqslant 2$.
On a

$$z = \mu\lambda^n$$

Donc

$$\alpha^3 + \beta^3 + \omega\delta^3\lambda^{3n} = 0$$

Et on a

$$\lambda \nmid \alpha\beta\delta$$

Donc $\lambda \nmid \alpha$, $\lambda \nmid \beta$ et $\lambda \nmid \delta$,
Ainsi $\alpha \neq 0 \,(\mathrm{mod} < \lambda >)$ et $\beta \neq 0 \,(\mathrm{mod} < \lambda >)$ et $\delta \neq 0 \,(\mathrm{mod} < \lambda >)$
En utilisant la question 3 de cette partie, on a l'existence de $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{-1, 1\}$
tel que

$$\begin{cases} \alpha^3 = \varepsilon_1 (\mathrm{mod} < \lambda^4 >) \\ \beta^3 = \varepsilon_1 (\mathrm{mod} < \lambda^4 >) \\ \delta^3 = \varepsilon_1 (\mathrm{mod} < \lambda^4 >) \end{cases}$$

Donc

$$\begin{aligned} \omega\delta^3\lambda^{3n} &= -(\alpha^3 + \beta^3) \\ &= -(\varepsilon_1 + \varepsilon_2) \pmod{< \lambda^4 >} \end{aligned}$$

Avec $\alpha \wedge \beta = 1$, alors $\varepsilon_1 \neq \varepsilon_2$, avec $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$, alors $\varepsilon_1 + \varepsilon_2 = 0$.
Par suite

$$\omega\delta^3\lambda^{3n} = 0 \pmod{< \lambda^4 >}$$

Autrement dit

$$\lambda^4 | \omega\delta^3\lambda^{3n} \tag{8}$$

Avec $\omega \in \mathbb{Z}[j]^\times$, donc $\exists u = a + jb \in \mathbb{Z}[j]^\times$ tel que $\omega(a + jb) = 1$
Donc

$$(a + b).\omega - (b\omega)\lambda = 1$$

Donc d'après le théorème de BEZOUT, on a $\lambda \wedge \omega = 1$, donc $\lambda^4 \wedge \omega = 1$
Et donc d'après la relation (6), et via le lemme de GAUSS, on a

$$\lambda^4 | \delta^3\lambda^{3n} \tag{9}$$

D'autre part on a

$$\delta^3 = \varepsilon_1 (\mathrm{mod} < \lambda^4 >)$$

Donc $\exists t \in \mathbb{Z}[j]$ tel que $\delta^3 = \varepsilon_1 + t\lambda^4$,
Ainsi

$$\varepsilon_1\delta^3 - (\varepsilon_1 t)\lambda^4 = 1$$

Donc via le théorème de BEZOUT, on a $\delta^3 \wedge \lambda^4 = 1$.
Le lemme da GAUSS et la relation (7) assure que

$$\lambda^4 | \lambda^{3n}$$

Avec λ est non inversible, alors $3n \geqslant 4$, avec $n \in \mathbb{N}$, alors $n \geqslant 2$.
D'où le résulltat.

5.a- On a

$$-\omega\delta^3\lambda^{3n} = \alpha^3 + \beta^3$$

Avec $\lambda \nmid \alpha\beta\delta$, en particulier $\beta \neq 0$.
On a alors

$$\begin{aligned} -\omega\delta^3\lambda^{3n} &= \alpha^3 + \beta^3 \\ &= (-\beta)^3\left[\left(\frac{\alpha}{-\beta}\right)^3 - 1^3\right] \end{aligned}$$

Avec

$$X^3 - 1 = (X-1)(X-j)(X-j^2)$$

(Car les racines cubiques de l'unité sont exactement $(1, j, j^2)$).
Alors

$$\begin{aligned} -\omega\delta^3\lambda^{3n} &= \alpha^3 + \beta^3 \\ &= (-\beta)^3\left[\left(\frac{\alpha}{-\beta}\right)^3 - 1^3\right] \\ &= (-\beta)^3\left(\frac{\alpha}{-\beta} - 1\right)\left(\frac{\alpha}{-\beta} - j\right)\left(\frac{\alpha}{-\beta} - j^2\right) \\ &= (\alpha+\beta)(\alpha+j\beta)(\alpha+j^2\beta) \end{aligned}$$

D'où le résultat.

REMARQUE: On peut commencer par développer le terme à droite, et on a

$$\begin{aligned} (\alpha+\beta)(\alpha+j\beta)(\alpha+j^2\beta) &= \alpha^3 + j^2\alpha^2\beta - j^2\alpha^2\beta - j\alpha\beta^2 + j\alpha\beta^2 + \beta^3 \\ &= \alpha^3 + \beta^3 \\ &= -\omega\delta^3\lambda^{3n} \end{aligned}$$

5.b- On a d'après la question précédente $\lambda | (\alpha+\beta)(\alpha+j\beta)(\alpha+j^2\beta)$
Avec $N(\lambda) = 3$ qui est un nombre premier, alors d'après la question 3.b de la partie 3. on a λ est irréductible.
Donc $\lambda | \alpha+\beta$ ou $\lambda | \alpha+j\beta$ ou $\lambda | \alpha+j^2\beta$

Donc $\exists i_0 \in \{0,1,2\}$ tel que $\lambda | \alpha + j^{i_0}\beta$
Soit $k \in \{0,1,2\}$, on a

$$\begin{aligned} \alpha + j^k\beta &= \alpha + j^{i_0}\beta + \left(j^k - j^{i_0}\right)\beta \\ &= \alpha + j^{i_0}\beta + \varepsilon_{k,i_0} j^{\min(k,i_0)}(j^{\max(k,i_0)} - 1)\beta \end{aligned}$$

Avec

$$\varepsilon_{k,i_0} = \operatorname{sgn}(k - i_0) \in \{-1, 0, 1\}$$

Donc

$$\begin{aligned} \alpha + j^k\beta &= \alpha + j^{i_0}\beta + \varepsilon_{k,i_0} j^{\min(k,i_0)}(j-1)\beta\left(\sum_{l=0}^{\max(k,i_0)-1} j^l\right) \\ &= \alpha + j^{i_0}\beta - \lambda\varepsilon_{k,i_0} j^{\min(k,i_0)}\beta\left(\sum_{l=0}^{\max(k,i_0)-1} j^l\right) \end{aligned}$$

Avec

$$\lambda \Big| \alpha + j^{i_0}\beta \text{ et } \lambda | \lambda\varepsilon_{k,i_0} j^{\min(k,i_0)}\beta\left(\sum_{l=0}^{\max(k,i_0)-1} j^l\right)$$

Alors

$$\lambda | \alpha + j^{i_0}\beta - \lambda\varepsilon_{k,i_0} j^{\min(k,i_0)}\beta\left(\sum_{l=0}^{\max(k,i_0)-1} j^l\right) = \alpha + j^k\beta$$

Et ça pour $k = 0, 1, 2$.
D'où

$$\lambda | \alpha + \beta \text{ et } \lambda | \alpha + j\beta \text{ et } \lambda | \alpha + j^2\beta$$

5.c- Montrons que λ est un **pgcd** de $\alpha + \beta$ et $\alpha + j\beta$.
Notons d un pgcd de $\alpha + \beta$ et $\alpha + j\beta$.
on a alors d'après la question précédente $\lambda | \alpha + \beta$ et $\lambda | \alpha + j\beta$,
En particulier

$$\lambda | d$$

Et

$$d | \lambda\beta = (\alpha + \beta) - (\alpha + j\beta)$$

Alors

$$d | \lambda$$

Ainsi d et λ sont associés, d'où λ est un **pgcd** de $\alpha + \beta$ et $\alpha + j\beta$

De la même manière, on peut montrer facilemet que λ est aussi un pgcd de $\alpha + \beta$ et $\alpha + j^2\beta$ (respectivement de $\alpha + j\beta$ et $\alpha + j^2\beta$).

Notons

$$\begin{cases} \alpha+\beta=\lambda^{m_1}r_1 \\ \alpha+j\beta=\lambda^{m_2}r_2 \\ \alpha+j^2\beta=\lambda^{m_3}r_3 \end{cases}$$

Avec $\lambda\nmid r_1$, $\lambda\nmid r_2$ et $\lambda\nmid r_3$. et $m_1,m_2,m_3\geqslant 1$ des entiers qui représentent respectivement la valuation λ-adique de $\alpha+\beta$, $\alpha+j\beta$ et $\alpha+j^2\beta$.

D'après ce qui précède on a

$$\begin{cases} \min(m_1,m_2)=1 \\ \min(m_2,m_3)=1 \\ \min(m_3,m_1)=1 \end{cases}$$

Donc forcément deux des entiers m_1,m_2,m_3 est inférieur ou égal à 1.

Par symétrie (il suffit de remplacer β par $j\beta$ ou $j^2\beta$), on peut supposer que $m_1,m_2\leqslant 1$

Or $m_1,m_2\geqslant 1$, alors $m_1=m_2=1$.

Avec $\lambda^4|-\omega\delta^3\lambda^{3n}=(\alpha+\beta)(\alpha+j\beta)(\alpha+j^2\beta)=\lambda^{m_1+m_2+m_3}r_1r_2r_3$

Avec $\lambda\nmid r_1$ et $\lambda\nmid r_2$ et $\lambda\nmid r_3$ et λ est irréductible, alors $\lambda\wedge r_1r_2r_3=1$.

Par suite $m_1+m_2+m_3\geqslant 4$.

Donc $m_3\geqslant 2$.

D'où λ^2 divise $\alpha+j^2\beta$.

D'où le résultat.

5.d- On a

$$\begin{aligned} -\omega\delta^3\lambda^{3n} &= (\alpha+\beta)(\alpha+j\beta)(\alpha+j^2\beta) \\ &= \lambda^{3n}\kappa_1\kappa_2\kappa_3 \end{aligned}$$

Avec $\lambda\neq 0$, alors

$$-\omega\delta^3 = \kappa_1\kappa_2\kappa_3$$

Montrons l'existence de $\gamma_l\in\mathbb{Z}[j]$ tel que $\kappa_l\sim\gamma_l^3$ pour tout $l\in\{1,2,3\}$

Soit $l\in\{1,2,3\}$, on a $\mathbb{Z}[j]$ est un anneau principal, alors il existe $p_{1,l},\ldots,p_{m_l,l}\in\mathbb{Z}[j]$ des irréductibles deux à deux distincts, et $\eta_{1,l},\ldots,\eta_{lm_l,l}\in\mathbb{N}^\star$ et $\omega_l\in\mathbb{Z}[j]^\times$ tel que

$$\kappa_l=\omega_l\prod_{s=1}^{m_l}p_{s,l}^{\eta_{s,l}},\text{pour tout } l\in\{1,2,3\}$$

Via la question précédente, on a λ est un pgcd de $\alpha+\beta$ et $\alpha+j\beta$ (respectivement de $\alpha+j\beta$ et $\alpha+j^2\beta$; $\alpha+j^2\beta$ et $\alpha+\beta$)

Donc κ_1 et κ_2 (respectivement κ_2 et κ_3; κ_3 et κ_1) sont premier entre eux.

Ainsi $p_{1,1},\ldots,p_{m_1,1},p_{1,2},\ldots,p_{m_2,2},p_{1,3},\ldots,p_{m_3,3}$ sont deux à deux distincts.

Et on a

$$\begin{aligned} -\omega\delta^3 &= \kappa_1\kappa_2\kappa_3 \\ &= \prod_{l=1}^{3}\left(\omega_l\prod_{s=1}^{m_l}p_{s,l}^{\eta_{s,l}}\right) \\ &= \omega_1\omega_2\omega_3\prod_{l=1}^{3}\prod_{s=1}^{m_l}p_{s,l}^{\eta_{s,l}} \end{aligned}$$

Notons $\delta=\vartheta\prod_{s=1}^{m}p_s^{\tau_s}$ la décomposition en produit d'irréductibles de δ.
Avec $\vartheta\in\mathbb{Z}[j]^\times$, et $p_1,\dots,p_m$ des irréductibles deux à deux distincts et $\tau_1,\dots,\tau_m\in\mathbb{N}^\star$
On a alors

$$-\omega\vartheta^3\prod_{s=1}^{m}p_s^{3\tau_s}=\omega_1\omega_2\omega_3\prod_{l=1}^{3}\prod_{s=1}^{m_l}p_{s,l}^{\eta_{s,l}}$$

Par l'unicité de la décomposition en facteurs irréductibles, on a forcément

$$3\,\text{divise}\,\eta_{s,l}\,\text{pour tout}\,l\in\{1,2,3\}\ \text{ et }\ s\in[\![1,m_l]\!]$$

Notons pour tout $l\in\{1,2,3\}$ et $s\in[\![1,m_l]\!]$

$$\varsigma_{s,l}=\frac{\eta_{s,l}}{3}\in\mathbb{N}^\star$$

On a alors pour tout $l\in\{1,2,3\}$.

$$\kappa_l=\omega_l\left(\prod_{s=1}^{m_l}p_{s,l}^{\varsigma_{s,l}}\right)^3$$

Donc pour tout $l\in\{1,2,3\}$, on a

$$\kappa_l\sim\gamma_l^3$$

Avec

$$\gamma_l^3=\prod_{s=1}^{m_l}p_{s,l}^{\varsigma_{s,l}}$$

D'où le résultat.

5.e- Montrons qu'il existe deux inversibles τ et τ' de $\mathbb{Z}[j]^\times$ tel que

$$\gamma_2^3+\tau\gamma_3^3+\tau'\lambda^{3(n-1)}\gamma_1^3=0$$

Essayant de détailler la question, tout en profitant des résultats obtenus précédemment.

Puisque pour tout $l\in\{1,2,3\}$, on a $\kappa_l\sim\gamma_l^3$, donc il existe $a_l\in\mathbb{Z}[j]^\times$ tel que: $\kappa_l=a_l\,\gamma_l^3$.
Ainsi

$$\begin{cases}\alpha+\beta=\lambda^{3n-2}a_1\,\gamma_1^3\\ \alpha+j\beta=\lambda a_2\,\gamma_2^3\\ \alpha+j^2\beta=\lambda a_3\,\gamma_3^3\end{cases}$$

Il vient à trouver un triplet $(a,b,c)\in\mathbb{Z}[j]^\times\times\mathbb{Z}[j]^\times\times\mathbb{Z}[j]^\times$, tel que $a\gamma_2^3+b\gamma_3^3+c\lambda^{3(n-1)}\gamma_1^3=0$.
Ceci est équivalent à trouver $(a,b,c)\in\mathbb{Z}[j]^\times\times\mathbb{Z}[j]^\times\times\mathbb{Z}[j]^\times$, tel que

$$a(\alpha+\beta)+b(\alpha+j\beta)+c(\alpha+j^2\beta)=0$$

Il suffit alors de trouver $(a,b,c)\in\mathbb{Z}[j]^\times\times\mathbb{Z}[j]^\times\times\mathbb{Z}[j]^\times$, tel que

$$\begin{cases}a+b+c=0\\ a+jb+j^2c=0\end{cases}\tag{10}$$

Le triplet $(a,b,c)=(j^2,1,j)$ convient.
Ainsi

$$\lambda a_2\gamma_2^3+\lambda j\, a_3\gamma_3^3+j^2a_1\lambda^{\,3n-2}\gamma_1^3=0$$

Par suite

$$\gamma_2^3+ja_2^{-1}\,a_3\gamma_3^3+j^2a_2^{-1}a_1\lambda^{\,3(n-1)}\gamma_1^3=0$$

D'où le résultat pour $\tau=ja_2^{-1}\,a_3$, et $\tau'=j^2a_2^{-1}a_1$.

5.f- Si $\tau=\pm1$, montrons que (P_{n-1}) est vérifiée
On a

$$\gamma_2^3+(\tau\gamma_3)^3+\lambda^{3(n-1)}\gamma_1^3=0$$

Avec $\lambda\nmid\omega\delta^3=\kappa_1\kappa_2\kappa_3$,et $\kappa_l\sim\gamma_l^3$, pour $l\in\{1,2,3\}$, donc $\lambda\nmid(\gamma_1\gamma_2\gamma_3)^3$
Or λ est irréductible dans $\mathbb{Z}[j]$, car $N(\lambda)=3$ est premier.
Donc $\lambda\nmid\gamma_1\gamma_2\gamma_3$.
De plus, on a

$$\begin{cases}\alpha+j\beta=\lambda\kappa_2\\ \alpha+j^2\beta=\lambda\kappa_3\end{cases}$$

Donc

$$\lambda\alpha=(\alpha+j^2\beta)-j(\alpha+j\beta)=\lambda\kappa_3-j\lambda\kappa_2$$

Ainsi

$$\alpha=\kappa_3-j\kappa_2$$

De même, on trouve

$$\beta=j^2(\kappa_2-\kappa_3)$$

Soit d un PGCD de κ_2 et κ_3, alors d divise à la fois $\kappa_3-j\kappa_2=\alpha$ et $j^2(\kappa_2-\kappa_3)=\beta$
Donc d est un PGCD de α et β.
Or α et β sont premier entre eux, alors d est inversible.
Par suite κ_2 et κ_3 sont premiers entre eux.
D'après ce qui précéde, $(\kappa_1,\kappa_2,\kappa_3)$ vérifie (P_{n-1}).
D'où le résultat.

5.g- Montrons que $\tau=\pm1\,(\mathrm{mod}\,\langle\lambda^3\rangle)$.
On a d'après la question 5.e de cette partie:

$$\gamma_2^3+\tau\gamma_3^3+\lambda^{3(n-1)}\gamma_1^3=0 \tag{11}$$

Avec $n\geqslant2$, alors modulo $\langle\lambda^3\rangle$ on a

$$\gamma_2^3+\tau\gamma_3^3=0\,(\mathrm{mod}\,\langle\lambda^3\rangle)$$

Avec $\lambda\nmid\gamma_2,\gamma_3$, alors via la qustion 3 de cette partie, on a l'existence de $\varepsilon_2,\varepsilon_3\in\{-1,1\}$ tel que

$$\begin{cases}\gamma_2^3=\varepsilon_2\,(\mathrm{mod}\,\langle\lambda^4\rangle)\\ \gamma_3^3=\varepsilon_3\,(\mathrm{mod}\,\langle\lambda^4\rangle)\end{cases}$$

En particulier

$$\begin{cases}\gamma_2^3=\varepsilon_2\,(\mathrm{mod}\,\langle\lambda^4\rangle)\\ \gamma_3^3=\varepsilon_3\,(\mathrm{mod}\,\langle\lambda^4\rangle)\end{cases}$$

Ainsi l'équation (11) donne:

$$\varepsilon_2+\varepsilon_3\tau=0\,(\mathrm{mod}\,\langle\lambda^3\rangle)$$

D'où

$$\tau=\pm1\,(\mathrm{mod}\,\langle\lambda^3\rangle)$$

On peut facilement montrer que $-j,j,-j^2,j^2$ ne sont pas congrus à $\pm1\ (\mathrm{mod}\,\langle\lambda^3\rangle)$.
Ainsi $\tau\notin\{j,-j,j^2,-j^2\}$.

6- D'après tout ce qu'on vu dans cette partie, on a $j\in\mathbb{Z}[j]^\times=\{1,-1,j,-j,j^2,-j^2\}$
Or d'après la question précédente on a montré que $\tau\notin\{j,-j,j^2,-j^2\}$
D'où $\tau=\pm1$.
Et via la question 5.f, on en déduit que (P_{n-1}) est vérifiée.
Ainsi si (P_n) est vérifiée, alors $n\geqslant2$, et (P_{n-1}) est cérifiée
Par principe de récurrence, on a (P_1) est vérifiée et $1\geqslant2$, absurde!
D'où l'équation (1) n'a pas de solution $(x,y,z)\in\mathbb{Z}_\star^3$ dans le cas $3|xyz$.

V Le théorème de Fermat pour p régulier et $p\nmid xyz$

1- Montrons que

$$\prod_{k=0}^{p-1}\langle x+\zeta^k y\rangle=\langle z^p\rangle$$

Par définition, on a

$$\prod_{k=0}^{p-1}\langle x+\zeta^k y\rangle=\left\{\sum_{i\in J}\prod_{k=0}^{p-1}x_{k,i}/\,J\,\text{est un ensemble fini, et pour tout}\,(i,k)\in J\times[\![0,p-1]\!]\,x_{k,i}\in\langle x+\zeta^k y\rangle\right\}$$

Soit $t\in\prod_{k=0}^{p-1}\langle x+\zeta^k y\rangle$, on a alors l'existence d'un ensemble fini J, et $(x_{i,k})_{(i,k)\in J\times[\![0,p-1]\!]}$ tel que

$$t=\sum_{i\in J}\prod_{k=0}^{p-1}x_{k,i}$$

Et pour tout $(i,k)\in J\times[\![0,p-1]\!]\,x_{k,i}\in\langle x+\zeta^k y\rangle$, on a $x_{k,i}\in\langle x+\zeta^k y\rangle$
Donc pour tout $(i,k)\in J\times[\![0,p-1]\!]$, il existe $a_{k,i}\in\mathbb{Z}[\zeta]$ tel que $x_{k,i}=(x+\zeta^k y)a_{k,i}$

On a alors

$$\begin{aligned} t &= \sum_{i\in J}\prod_{k=0}^{p-1}[(x+\zeta^k y)a_{k,i}] \\ &= \sum_{i\in J}\prod_{k=0}^{p-1}(x+\zeta^k y)\prod_{k=0}^{p-1}a_{k,i} \\ &= \prod_{k=0}^{p-1}(x+\zeta^k y)\sum_{i\in J}\prod_{k=0}^{p-1}a_{k,i} \end{aligned}$$

Avec $x, y \neq 0$, on a alors

$$\begin{aligned} \prod_{k=0}^{p-1}(x+\zeta^k y) &= (-y)^p\prod_{k=0}^{p-1}\left(\frac{x}{-y}-\zeta^k\right) \\ &= (-y)^p\left(\left(\frac{x}{-y}\right)^p-1\right) \\ &= x^p+y^p \\ &= -z^p \end{aligned}$$

Donc

$$\begin{aligned} t &= -z^p\sum_{i\in J}\prod_{k=0}^{p-1}a_{k,i} \\ &\in \langle z^p\rangle \end{aligned}$$

D'où

$$\prod_{k=0}^{p-1}\langle x+\zeta^k y\rangle \subset \langle z^p\rangle$$

Réciproquement, soit $u\in\langle z^p\rangle$, alors il existe $u'\in\mathbb{Z}[\zeta]$, tel que $u=z^pu'$, on a alors

$$\begin{aligned} u &= u'z^p \\ &= -u'(x^p+y^p) \\ &= -u'\prod_{k=0}^{p-1}(x+\zeta^k y) \\ &\in \prod_{k=0}^{p-1}\langle x+\zeta^k y\rangle \end{aligned}$$

D'où

$$\langle z^p\rangle \subset \prod_{k=0}^{p-1}\langle x+\zeta^k y\rangle$$

Par suite

$$\prod_{k=0}^{p-1}\langle x+\zeta^k y\rangle = \langle z^p\rangle$$

2.a- Montrons que $\hat{}\lambda y\in\mathfrak{B}$.

On a

$$\begin{aligned}(x+\zeta^l y)-(x+\zeta^k y) &= \zeta^k(\zeta^{l-k}-1)y\\ &= \zeta^k(\zeta-1)\frac{1-\zeta^{l-k}}{1-\zeta}y\\ &= -\lambda y\zeta^k\frac{1-\zeta^{l-k}}{1-\zeta}\end{aligned}$$

Donc

$$\lambda y=-\frac{1}{\zeta^k}\times\frac{1-\zeta}{1-\zeta^{l-k}}[(x+\zeta^l y)-(x+\zeta^k y)]$$

Avec $l-k\in[\![1,p-1]\!]$, et en utilisant la question 5.b de la partie 3, on a

$$\frac{1-\zeta}{1-\zeta^{l-k}}\in\mathbb{Z}[\zeta]^\times$$

Et on a $N(\zeta^k)=1$. donc via la question 3.b de la partie 3, on a $\zeta^k\in\mathbb{Z}[\zeta]^\times$, donc $\frac{1}{\zeta^k}\in\mathbb{Z}[\zeta]^\times$.
Par suite

$$\frac{1}{\zeta^k}\times\frac{1-\zeta}{1-\zeta^{l-k}}\in\mathbb{Z}[\zeta]^\times$$

Donc

$$\lambda y\in\langle x+\zeta^l y\rangle\cap\langle x+\zeta^k y\rangle$$

2.b- Montrons que $y\notin\mathfrak{B}$,
On a $\mathfrak{B}$ est premier, on a $\lambda\in\mathfrak{B}$ ou $y\in\mathfrak{B}$.
Par l'absurde, supposons que $y\in\mathfrak{B}$.
D'après la question 1 de cette partie, on a $\mathfrak{B}$ divise $<z^p>$.
En particulier, $z\in\mathfrak{B}$.
Or y et z sont premiers entre eux, donc d'après le théorème de Bézout, on a l'existence de $(u,v)\in\mathbb{Z}^2$ tel que

$$uy+vz=1$$

Ainsi, $1\in\mathfrak{B}$, absurde!

Montrons que $x+y\in\langle\lambda\rangle\cap\mathbb{Z}$
On a $y\notin\mathfrak{B}$, et $\mathfrak{B}$ est premier, alors $\lambda\in\mathfrak{B}$, donc $<\lambda>\subset\mathfrak{B}$
Or $<\lambda>$ est premier (d'après la question 5 de la partie 3).
Or pour toit $k\in[\![0,p-1]\!]$

$$\zeta^k-1=\lambda\sum_{j=0}^{k-1}\zeta^j=0(\mathrm{mod}<\lambda>)$$

Ainsi

$$\zeta^k=1\,(\mathrm{mod}<\lambda>)$$

Par suite

$$x+y=x+\zeta^k y\,(\mathrm{mod}<\lambda>)$$

Par définition de $\mathfrak{B}$,

$$x+\zeta^k y=0\,(\mathrm{mod}<\lambda>)$$

Donc

$$x+y=0\,(\mathrm{mod}<\lambda>)$$

Ainsi $x+y\in\mathbb{Z}\cap<\lambda>=p\mathbb{Z}$

Par suite

$$p|z^p=-(x^p+y^p)=-(x+y)\sum_{k=0}^{p-1}x^k y^{p-1-k}$$

Avec p est premier, alors $p|z$, absurde avec $p|xyz$.
D'où le résultat souhaité.

3- Justifiant qu'il existe un idéal I tel que $<x+\zeta y>=I^p$
On a d'après la question 1,

$$\prod_{k=0}^{p-1}\langle x+\zeta^k y\rangle=\langle z^p\rangle$$

Comme les idéaux $<x+\zeta^k y>$ sont 2 à 2 premiers entre eux (via la question 2.a), et d'après le résultat énoncé, il y a unicité de la décomposition des idéaux en idéaux premiers dans $\mathbb{Z}[\zeta]$.

Or pour tout $k\in[\![0,p-1]\!]\langle x+\zeta^k y\rangle$ est une puissance p-ième d'un idéal, c'est en particulier vrai pour $<x+\zeta y>$.

4- Montrons qu'il existe $r\in\mathbb{Z}$, ε réel inversible de $\mathbb{Z}[\zeta]$ et $\alpha\in\mathbb{Z}[\zeta]$ tels que $x+\zeta y=\zeta^r\varepsilon\alpha^p$.
Comme $I^p=<x+\zeta y>$ est principal,et p est régulier.
Alors I est principal
Ainsi il existe $\alpha\in\mathbb{Z}[\zeta]$ tel que $<x+\zeta y>=<\alpha^p>$
En particulier il existe $\omega\in\mathbb{Z}[\zeta]^\times$ tel que $x+\zeta y=u\alpha^p$
Or d'après la question 6 de la partie 3, on peut écrire u sous la forme $u=\zeta^r\varepsilon$, avec $r\in\mathbb{Z}$, $\varepsilon\in\mathbb{Z}[\zeta]^\times\cap\mathbb{R}$.
D'où le résultat.

5- Montrons l'existence de $a\in\mathbb{Z}$ tel que $\alpha^p=a\,(\mathrm{mod}\,\langle p\rangle)$
Ecrivant $\alpha=a+\zeta b$, où $a,b\in\mathbb{Z}$
On a

$$\begin{aligned}\alpha^p &= (c+\zeta b)^p\\ &= \sum_{k=0}^{p}\binom{p}{k}\zeta^k b^k c^{p-k}\end{aligned}$$

Avec $p\left|\binom{p}{k}\right.$, pour tout $k\in[\![1,p-1]\!]$, alors

$$\alpha^p=c^p+b^p\,(\mathrm{mod}\,\langle p\rangle)$$

D'où le résultat. (on pose $a=c^p+b^p\in\mathbb{Z}$)
Montrons maintenant que

$$x\zeta^{-r}+y\zeta^{1-r}-x\zeta^r-y\zeta^{r-1}=0\,(\mathrm{mod}\,\langle p\rangle)$$

On a

$$\begin{aligned} x\zeta^{-r} + y\zeta^{1-r} - x\zeta^{r} - y\zeta^{r-1} &= (\zeta^{-r} - \zeta^{r})(x + \zeta y) \\ &= (\zeta^{-r} - \zeta^{r})\zeta^{r}\varepsilon\alpha^{p} \\ &= (1 - \zeta^{2r})\varepsilon\alpha^{p} \\ &= (1 - \zeta^{2r})\varepsilon a \,(\mathrm{mod}\,\langle p\rangle) \end{aligned}$$

Notons r_0 le reste de la division euclidienne de $2r$ par p.
On a alors $r_0 \in [\![0, p-1]\!]$, et

$$x\zeta^{-r} + y\zeta^{1-r} - x\zeta^{r} - y\zeta^{r-1} = (1 - \zeta^{2r_0})\varepsilon a \,(\mathrm{mod}\,\langle p\rangle)$$

Or

$$\begin{aligned} (1 - \zeta^{2r_0}) \prod_{\substack{k=1 \\ k\neq r_0}}^{p-1} (1 - \zeta^{k}) &= \prod_{k=1}^{p-1} (1 - \zeta^{k}) \\ &= N(1 - \zeta) \\ &= N(\lambda) \\ &= p \end{aligned}$$

Donc

$$(1 - \zeta^{2r_0})(1 - \zeta)^{p-1} = p \prod_{\substack{k=1 \\ k\neq r_0}}^{p-1} \frac{(1 - \zeta)}{(1 - \zeta^{k})}$$

Ainsi

$$\begin{aligned} 1 - \zeta^{2r_0} &= p \prod_{\substack{k=1 \\ k\neq r_0}}^{p-1} \frac{(1 - \zeta)}{(1 - \zeta^{k})} - (1 - \zeta^{2r_0})[(1 - \zeta)^{p-1} - 1] \\ &= p \prod_{\substack{k=1 \\ k\neq r_0}}^{p-1} \frac{(1 - \zeta)}{(1 - \zeta^{k})} - (1 - \zeta^{2r_0}) \sum_{j=1}^{p-1} \binom{p-1}{j} \zeta^{j} \\ &= p \prod_{\substack{k=1 \\ k\neq r_0}}^{p-1} \frac{(1 - \zeta)}{(1 - \zeta^{k})} - (1 - \zeta^{2r_0}) \sum_{j=1}^{\frac{p-1}{2}} \left[\binom{p-1}{2j-1} + \binom{p-1}{2j} \zeta \right] \zeta^{2j-1} \\ &= p \prod_{\substack{k=1 \\ k\neq r_0}}^{p-1} \frac{(1 - \zeta)}{(1 - \zeta^{k})} - (1 - \zeta^{2r_0}) \sum_{j=1}^{\frac{p-1}{2}} \left[\binom{p}{2j} - \lambda \binom{p-1}{2j} \right] \zeta^{j} \\ &= p \prod_{\substack{k=1 \\ k\neq r_0}}^{p-1} \frac{(1 - \zeta)}{(1 - \zeta^{k})} - (1 - \zeta^{2r_0}) \sum_{j=1}^{\frac{p-1}{2}} \binom{p}{2j} + \lambda(1 - \zeta^{2r_0}) \sum_{j=1}^{\frac{p-1}{2}} \binom{p-1}{2j} \zeta^{j} \end{aligned}$$

Avec $p|\binom{p}{2j}, \forall j \in \left[\!\left[1, \frac{p-1}{2}\right]\!\right]$, donc $p\prod_{\substack{k=1\\k\neq r_0}}^{p-1}\frac{(1-\zeta)}{(1-\zeta^k)} - (1-\zeta^{2r_0})\sum_{j=1}^{\frac{p-1}{2}}\binom{p}{2j} \in p\mathbb{Z}[\zeta]$

De plus

$$\begin{aligned}\lambda^p &= (1-\zeta)^p \\ &= \sum_{k=0}^{p}\binom{p}{k}\zeta^k \\ &= \sum_{k=1}^{p-1}\binom{p}{k}\zeta^k\end{aligned}$$

Or $p|\binom{p}{k}, \forall k \in [\![1, p-1]\!]$, donc $p|\lambda^p$

Avec p est irréductible dans $\mathbb{Z} \subset \mathbb{Z}[\zeta]$, donc p est irréductible dans $\mathbb{Z}[\zeta]$, ainsi $p|\lambda$

Par suite

$$\lambda(1-\zeta^{2r_0})\sum_{j=1}^{\frac{p-1}{2}}\binom{p-1}{2j}\zeta^j \in p\mathbb{Z}[\zeta]$$

D'où

$$(1-\zeta^{2r_0}) \in p\mathbb{Z}[\zeta]$$

Finalement

$$x\zeta^{-r} + y\zeta^{1-r} - x\zeta^r - y\zeta^{r-1} = 0 (\mathrm{mod} < p >)$$

6- Supposons que $r = 0\,(\mathrm{mod}\, p\mathbb{Z})$, Montrons que $p|y$ dans $\mathbb{Z}$.

On a d'après la question précédente

$$x\zeta^{-r} + y\zeta^{1-r} - x\zeta^r - y\zeta^{r-1} = 0\,(\mathrm{mod}\,\langle p\rangle)$$

Et $r = 0\,(\mathrm{mod}\, p\mathbb{Z})$, donc $\zeta^r = 1$, donc

$$y(\zeta^1 - \zeta^{-1}) = 0\,(\mathrm{mod}\,\langle p\rangle)$$

Donc il existe $t \in \mathbb{Z}[\zeta]$, tel que $y(\zeta^1 - \zeta^{p-1}) = pt$

On a alors[4]

$$\begin{aligned}N(y(\zeta^1 - \zeta^{p-1})) &= N(y\zeta^{p-1}(\zeta+1)(\zeta-1)) \\ &= N(y)N(\zeta^{p-1})N(\zeta-1)N(\zeta+1) \\ &= -py^{p-1}\end{aligned}$$

Dautre part

$$\begin{aligned}N(y(\zeta^1 - \zeta^{p-1})) &= N(pt) \\ &= p^{p-1}N(t)\end{aligned}$$

4. Car $\zeta^{p-1} \in \mathbb{Z}[\zeta]^\times$, alors $N(\zeta^{p-1}) = 1$, et d'après la partie 3 on a $N(1-\zeta) = p$ et $N(1+\zeta) = 1$

Donc

$$p^{p-2}N(t) = -y^{p-1}$$

Avec $N(t) \in \mathbb{Z}$ (voir le lemme 4)
Donc $p|y^p$, avec p est premier, alors $p|y$.
« On montrerait de même que l'on ne peut avoir $r = 1 \,(\mathrm{mod}\, p\mathbb{Z})$, ce que l'on admet. »

7- D'après la question 5, il existe $\beta \in \mathbb{Z}[\zeta]$ tel que

$$x\zeta^{-r} + y\zeta^{1-r} - x\zeta^{r} - y\zeta^{r-1} = \beta p$$

Montrons que deux des entiers $\pm r$, $\pm(1-r)$ sont égaux modulo p.
Par l'absurde, supposons qu'aucun des $\pm r$,$\pm(1-r)$ n'était égal modulo p.
On a

$$\beta = \frac{x}{p}\zeta^{-r} + \frac{y}{p}\zeta^{1-r} - \frac{x}{p}\zeta^{r} - \frac{y}{p}\zeta^{r-1}$$

Or $(1, \zeta, \ldots, \zeta^{p-2})$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\zeta)$, et $\beta \in \mathbb{Z}[\zeta]$.
Alors $\frac{x}{p} \in \mathbb{Z}$, ainsi $p|x$, absurde
D'où le résultat
Donc $\pm r = \pm(1-r) \,(\mathrm{mod}\, p\mathbb{Z})$, et ceci n'est possible que pour $r = (1-r) (\mathrm{mod}\, p\mathbb{Z})$
Ainsi $2r = 1 \,(\mathrm{mod}\, p\mathbb{Z})$

8- Montrons que $\beta p\zeta^r = (x-y)\lambda$
D'après la question précédente on a $2r = 1 \,(\mathrm{mod}\, p\mathbb{Z})$, alors

$$\begin{aligned} \beta p\zeta^r &= (x\zeta^{-r} + y\zeta^{1-r} - x\zeta^{r} - y\zeta^{r-1})\zeta^r \\ &= x + \zeta y - x\zeta^{2r} - y\zeta^{2r-1} \\ &= x + \zeta y - x\zeta - y \\ &= (x-y)(1-\zeta) \\ &= (x-y)\lambda \end{aligned}$$

Alors

$$N(\beta p\zeta^r) = N((x-y)\lambda) = N(\lambda)N(x-y) = p\,(x-y)^{p-1}$$

Avec

$$\begin{aligned} N(\beta p\zeta^r) &= N(\beta)N(p)N(\zeta^r) \\ &= p^{p-1}N(\beta) \end{aligned}$$

Donc

$$(x-y)^{p-1} = p^{p-2}N(\beta)$$

Avec $N(\beta) \in \mathbb{Z}$, alors $p|(x-y)^{p-2}$, avec p est premier, alors p divise $x-y$.
D'où

$$x = y \,(\text{mod}\, p\mathbb{Z})$$

9- On a d'après la question précédente

$$x = y \,(\text{mod}\, p\mathbb{Z})$$

Par symétrie, on trouve $z = y \,(\text{mod}\, p\mathbb{Z})$

Alors

$$\begin{cases} x^p = y^p \,(\text{mod}\, p\mathbb{Z}) \\ z^p = y^p \,(\text{mod}\, p\mathbb{Z}) \end{cases}$$

Ainsi

$$3x^p = x^p + y^p + z^p (\text{mod}\, p\mathbb{Z}) = 0 \,(\text{mod}\, p\mathbb{Z})$$

Alors $p|3x^p$, avec $p > 3$, donc $p|x^p$, d'où $p|x$ absurde avec $p \nmid xyz$.

Pour aller plus loin...

Pour qui est intéressé par la preuve du théorème de Wiles-Fermat (connus aussi par le dernier théorème de Fermat) je vous conseille de lire complétement le joli livre **«THE PROOF OF FERMAT'S LAST THEOREM »** de **Nigel Boston**, en cliquant sur le lien suivant:

https://people.math.wisc.edu/~boston/869.pdf