Etude de l'équation de Fermat pour les premiers réguliers

Philippe Caldero

12 octobre 2020

Résumé : On expose ici les idées du problème de mathématiques générales de l'agrégation externe de 2019. Au programme : la belle utilisation de l'unicité de la décomposition en idéaux premiers dans les anneaux d'entiers de corps de nombres, au service d'un théorème préparatoire sur l'équation de Fermat $x^p + y^p + z^p = 0$ quand p est un nombre premier dit « régulier ».

1 Prérequis

Les prérequis demandés dans ce qui suit dépassent d'une tête ceux exigés par l'agrégation et ses standards.

Parmi les éléments bien connus des agrégatifs, on aura besoin des nombres premiers, qui constituent un ensemble infini, et l'indicatrice d'Euler qui calcule le nombre $\varphi(n)$ des entiers de 1 à n premiers avec n :

$$\varphi(n) = n \prod_{p \in \mathcal{P}_n} \left(1 - \frac{1}{p}\right),$$

où $\mathcal{P}_n$ désigne l'ensemble des nombres premiers qui divisent n. Chose sans doute moins classique, l'ensemble $\mathcal{P}_n$ voit son cardinal majoré par $\log_2(n)$, puisque, bien évidemment, $2^{|\mathcal{P}_n|} \leq n$. En séparant $\mathcal{P}_n$ en $p = 2$ (éventuellement) et $p \geq 3$, on en déduit une minoration grossière de $\varphi(n)$:

$$\varphi(n) \geq n \times (1 - \frac{1}{2}) \times (1 - \frac{1}{3})^{|\mathcal{P}_n|} \geq \frac{n 2^{\log_2(n)}}{2 \times 3^{\log_2(n)}} = \frac{n^2}{2n^{\log_2(3)}} = \frac{n^{2-\log_2(3)}}{2},$$

ce qui implique que $\varphi(n)$ tend vers l'infini avec n.

On utilisera également avec bonheur le théorème de Kronecker qui stipule qu'un polynôme unitaire de $\mathbb{Z}[X]$ n'ayant que des racines complexes de norme inférieure à 1 ne peut avoir pour racines que 0 ou des racines de l'unité. Ce théorème est rarement ignoré des agrégatifs vu le nombre de fois qu'il a été choisi comme développement, voir [**?**].

A ce sujet, on rappelle aussi que pour tout entier naturel n le polynôme cyclotomique ϕ_n, c'est-à-dire le polynôme minimal sur $\mathbb{Q}$, d'une racine primitive n-ième de l'unité, est

irréductible. Il est dans $\mathbb{Z}[X]$, irréductible également sur $\mathbb{Z}$, et de degré $\varphi(n)$. On se servira surtout du cas où $n = p$ premier $\phi_p = X^{p-1} + \cdots + X + 1$.

Parmi les objets *borderline* du programme d'agrégation figure la théorie des corps, et donc des extensions de corps. Une fois passées les jolies applications du théorème de la base télescopique se dresse devant nous la théorie de Galois, que les étudiants préfèrent en général éviter, ayant suffisamment de soucis avec le reste du programme pour se consacrer à cette théorie splendide, certes, mais chronophage. On peut tout de même, sans trop s'impliquer, l'utiliser comme ligne directrice dans des cas particuliers bien connus. On commence par l'extension $\mathbb{R} \subset \mathbb{C}$, de degré 2, dont chacun sait qu'elle est gouvernée par l'automophisme bar, puisque $\overline{z} = z$ pour un z de $\mathbb{C}$ implique que z est dans le corps de base $\mathbb{R}$. Ce *théorème de descente* propre à la théorie de Galois se retrouve dans les extensions (finies) de corps finis, $\mathbb{F}_p \subset \mathbb{F}_{p^n}$, avec p premier, puisque l'on sait qu'un élément de $\mathbb{F}_{p^n}$ est dans $\mathbb{F}_p$ si et seulement s'il est stable par le morphisme $z \mapsto z^p$ de Frobenius.

Dans le texte qui suit, on aura besoin des extensions cyclotomiques de $\mathbb{Q}$: ce sont les extensions $\mathbb{Q} \subset \mathbb{Q}(\zeta)$, où ζ est une racine p-ième de l'unité, avec p premier. Nul besoin de théorie de Galois pour prouver facilement qu'il existe, pour tout $1 \leq k \leq p-1$, un automorphisme σ_k du corps $\mathbb{Q}(\zeta) = \mathbb{Q}[\zeta] \simeq \mathbb{Z}[X]/(\phi_p)$ tel que $P(\zeta)$, $P \in \mathbb{Z}[X]$, est envoyé sur $P(\zeta^k)$. L'ensemble de ces automorphismes constitue un groupe pour la loi $\circ$ isomorphe au groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ et tout $z \in \mathbb{Q}(\zeta)$ est dans $\mathbb{Q}$ si et seulement s'il est stable par les σ_k (et donc, juste par un générateur puisqu'on sait que $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique), voir [**?**, Exercice XIII-E.33].

On utilisera également la notion d'élément entier sur l'anneau $\mathbb{Z}$. Un élément de $\mathbb{C}$ est dit entier algébrique sur $\mathbb{Z}$, ou juste entier algébrique, s'il est racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$. On peut montrer[1] que la somme et le produit de deux entiers algébriques est encore entier algébrique, voir [**?**], c'est-à-dire que l'ensemble des entiers algébriques de $\mathbb{C}$ forme un anneau. Comme $\mathbb{Z}$ est factoriel, on voit facilement à l'aide du lemme de Gauss que l'anneau des entiers algébriques de $\mathbb{Q}$ est $\mathbb{Z}$ lui-même.

Aux confins de ces résultats sur la théorie des corps et l'intégralité, on trouve que la trace $\mathrm{tr}(z) := \sum_{k=1}^{p-1} \sigma_k(z)$ et la norme $N(z) := \prod_{k=1}^{p-1} \sigma_k(z)$ d'un élément z d'une extension $\mathbb{Q}(\zeta)$ de $\mathbb{Q}$ sont des entiers. En effet, par théorème de descente, ce sont des éléments de $\mathbb{Q}$ et par intégralité, ils sont dans $\mathbb{Z}$.

On arrive maintenant à ce qui sort totalement du programme de l'agrégation, mais qui, toutefois, reste facile à admettre tant cela généralise des résultats bien ingurgités. Les "petites" équations diophantiennes comme on peut les voir, notamment dans [**?**], citons par exemple certaines équations de Mordell, de Fermat pour n petit, ou le "problème des canards", jouent sur la factorialité de certains anneaux quadratiques, comme $\mathbb{Z}[i]$, $\mathbb{Z}[j]$, $\mathbb{Z}[i\sqrt{2}]$. Or, les exemples d'anneaux factoriels dans ce monde-là sont plutôt rares. Pire : il est difficile dans ce contexte de plonger un anneau intègre dans un anneau factoriel raisonnable. En revanche, les anneaux d'entiers de corps de nombres vérifient une propriété très analogue à la factorialité : à condition de remplacer la notion de nombre, resp. nombre premier, par la notion d'idéaux, resp. d'idéaux premiers, et la divisibilité par l'inclusion, selon le principe *diviser, c'est contenir*, on obtient l'unicité de la décomposition d'un idéal en produit d'idéaux premiers (à permutation près). C'est même finalement un peu plus

1. Une méthode exotique utilise le résultant.

joli que la factorialité des nombres, puisqu'on n'a pas à gérer les unités !

Si ζ est une racine p-ième de l'unité, alors, comme on va le voir dans le théorème 3.1, $\mathbb{Z}[\zeta]$ est l'anneau des entiers de $\mathbb{Q}(\zeta)$. On dira que le nombre premier p est régulier[2] si tout idéal I de $\mathbb{Z}[\zeta]$ est principal si et seulement si I^p est principal. Si l'on sait que le groupe abélien des idéaux (pour le produit) quotienté par le sous-groupe des idéaux principaux, est un groupe fini $\mathrm{Cl}(\mathbb{Q}(\zeta))$ (appelé groupe des classes d'idéaux du corps de nombres), alors, on comprend que p régulier revient à dire que p ne divise pas $|\mathrm{Cl}(\mathbb{Q}(\zeta))|$.

Voilà, ces quelques pages pourront intéresser ceux qui sont curieux de voir comment les idéaux ont remplacé les nombres de façon idéale et comment l'arithmétique s'est déployée autour de l'équation de Fermat, à tel point que l'on est en droit de se demander si on n'a pas tous été fermatés.

2 Les unités de $\mathbb{Z}[\zeta]$

2.1 Critère par la norme

Soit p un nombre premier impair. Comme ζ vérifie $X^p - 1 = 0$, c'est un entier algébrique et donc, $\mathbb{Z}[\zeta]$ est constitué d'entiers algébriques. On montrera plus tard qu'il s'agit exactement de l'anneau des entiers algébriques de $\mathbb{Q}(\zeta)$. En attendant, nous allons, comme il se doit dans les études d'anneaux, commencer par en étudier les unités, *i.e.* les inversibles.

Lemme 2.1. *Pour tout z de $\mathbb{Z}[\zeta]$, z est inversible dans $\mathbb{Z}[\zeta]$ si et seulement si $N(z) = \pm 1$.*

Démonstration. Comme z est dans $\mathbb{Z}[\zeta]$, il s'agit d'un entier algébrique et donc sa norme est dans $\mathbb{Z}$. S'il est inversible dans $\mathbb{Z}[\zeta]$, on peut écrire $zz' = 1$, avec $z' \in \mathbb{Z}[\zeta]$ et en prenant la norme qui est multiplicative, on voit que $N(z)N(z') = 1$, et donc, $N(z) = \pm 1$. Inversement, si $N(z) = \pm 1$, $z' := N(z) \prod_{\sigma \neq \mathrm{Id}} \sigma_k(z) \in \mathbb{Z}[\zeta]$ vérifie $zz' = N(z)N(z) = 1$.

2.2 Calculs de normes et traces

Il est temps de regarder de plus près les normes et traces d'éléments de $\mathbb{Z}[\zeta]$, nommément : ζ^k, $\lambda := 1 - \zeta$, $1 - \zeta^k$, $\lambda^k = (1 - \zeta)^k$. Voici un formulaire qui sera utile par la suite. On note N et tr respectivement la norme et la trace.

On a bien sur, $\mathrm{tr}(1) = p - 1$ et $N(1) = 1$, car 1 est stable par tous les σ_k, $1 \leq k \leq p - 1$.

$$N(\zeta^k) = 1,\ \mathrm{tr}(\zeta^k) = -1,\ 1 \leq k \leq p - 1.$$

On peut le faire par le calcul, mais cela provient surtout du fait que les conjugués de ζ, c'est-à-dire les ζ^k, $1 \leq k \leq p - 1$, sont les racines du polynôme unitaire irréductible $\phi_p = X^{p-1} + X^{p-2} + \cdots + 1$, donc la trace est la somme des racines et la norme est le produit des racines. On trouve bien $\mathrm{tr}(\zeta^k) = -1$ et $N(\zeta^k) = (-1)^{p-1} = 1$, d'après les relations coefficients racines.

$$N(1 - \zeta) = p,\ \mathrm{tr}(1 - \zeta) = p,\ N(1 + \zeta) = 1.$$

2. Notion introduite par Enrst Kummer en 1847.

Pour les normes, cela provient du fait que $1-\zeta$, resp. $1+\zeta$, est racine du polynôme de degré pair $\phi_p(1-X)$, resp. $\phi_p(X-1)$, dont l'évaluation en 0 est $\phi_p(1)=p$, resp. $\phi_p(-1)=1$. Pour la trace, on utilise juste sa linéarité.

$$N(1-\zeta^k)=p,\ \mathrm{tr}(\lambda^k)=p,\ 1\leq k\leq p-1.$$

Comme $1-\zeta^k$ est conjugué à $1-\zeta$, la première formule découle de $N(1-\zeta)=p$. La dernière formule s'obtient en utilisant le binôme de Newton $(1-\zeta)^k=1-\binom{k}{1}\zeta+\binom{k}{2}\zeta^2+\cdots+(-1)^k\binom{k}{k}\zeta^k$, en prenant la trace, et en remarquant que

$$-1+\binom{k}{1}-\binom{k}{2}+\cdots-(-1)^k\binom{k}{k}=-(1-1)^k=0$$

2.3 Les racines de l'unité dans $\mathbb{Z}[\zeta]$

Proposition 2.2. *L'ensemble des racines de l'unité de $\mathbb{Z}[\zeta]$ forme un sous-groupe G du groupe multiplicatif $\mathbb{Z}[\zeta]^*$ des unités de $\mathbb{Z}[\zeta]$. Ce groupe est fini, cyclique, d'ordre $2p$, engendré par la racine primitive $2p$-ième de l'unité $(-\zeta)$.*

Démonstration. Comme -1 est d'ordre 2 et ζ est d'ordre p impair, $-\zeta$ est d'ordre $2p$; il s'agit bien d'une racine primitive $2p$-ième de l'unité. De plus, G est clairement un groupe et donc $2p$ divise l'ordre de G, à condition que celui-ci soit fini !

Montrons que ce groupe est fini. Soit $\omega\in G$, ω est une racine de l'unité d'ordre, disons, m. On a $\mathbb{Q}\subset\mathbb{Q}(\omega)\subset\mathbb{Q}(\zeta)$, et donc

$$\varphi(m)=[\mathbb{Q}(\omega):\mathbb{Q}]\text{ divise }[\mathbb{Q}(\zeta):\mathbb{Q}]=\varphi(p)=p-1.$$

Ainsi, $\varphi(m)$ est borné par $p-1$ et donc m est borné (vu dans la section des prérequis) et G est inclus dans la réunion des racines m-ièmes de l'unité pour $1\leq m\leq p-1$; G est donc fini. Comme G est un sous-groupe fini d'un corps, on sait qu'il est cyclique engendré par ω d'ordre, disons, n et l'on sait d'après ce qui précède, que $2p$ divise n. On sait de plus, d'après ce qui précède, que $\varphi(n)$ divise $p-1=\varphi(2p)$. Montrons alors que $n=2p$, ce qui achèvera la preuve.

Ecrivons donc $n=2^kp^lm$ avec m premier avec $2p$, ce qui donne

$$\varphi(n)=\varphi(2^kp^l)\varphi(m)=(p-1)2^{k-1}p^{l-1}\varphi(m),$$

et donc $\varphi(n)$ ne peut diviser $p-1$ que si $k=l=1$ et $\varphi(m)=1$, c'est-à-dire $m=1$ compte tenu du fait que m est impair. Conclusion, $n=2p$.

2.4 L'idéal maximal (λ)

Proposition 2.3. *On rappelle que $\lambda=1-\zeta$. On a les assertions suivantes :*

(i) les idéaux (λ^{p-1}) et (p) de $\mathbb{Z}[\zeta]$ sont égaux,

(ii) $(\lambda)\cap\mathbb{Z}=p\mathbb{Z}$,

(iii) on a un isomorphisme d'anneaux $\mathbb{Z}[\zeta]/(\lambda)\simeq\mathbb{F}_p$,

(iv) l'idéal (λ) de $\mathbb{Z}[\zeta]$ est un idéal maximal (donc premier),

(v) tout élément de $\mathbb{Z}[\zeta]$ peut s'écrire sous la forme $a + \lambda\beta$, avec $0 \leq a \leq p-1$ et $\beta \in \mathbb{Z}[\zeta]$.

Démonstration. Montrons (i). Pour cela, on pose $\omega_k := \frac{1-\zeta^k}{1-\zeta}$, $1 \leq k \leq p-1$, qui est bien dans $\mathbb{Z}[\zeta]$ par la formule de la série géométrique. On a $N(\omega_k) = \frac{N(1-\zeta^k)}{N(1-\zeta)} = 1$, et donc ω_k est un inversible de $\mathbb{Z}[\zeta]$ par le lemme 2.1. On en déduit que $\prod_{k=1}^{p-1} \omega_k$ est également inversible, or il vaut

$$\prod_{k=1}^{p-1} \omega_k = \frac{\prod_{k=1}^{p-1}(1-\zeta^k)}{\lambda^{p-1}} = \frac{N(1-\zeta)}{\lambda^{p-1}} = \frac{p}{\lambda^{p-1}}.$$

Montrons l'assertion (ii). Comme (λ) est un idéal de $\mathbb{Z}[\zeta]$ ne contenant pas 1, puisque $N(\lambda) > 1$, $(\lambda) \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$ ne contenant pas 1. Or, il contient p, puisque $(p) = (\lambda^{p-1}) \subset (\lambda)$, par (i). L'assertion résulte du fait que $p\mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$ car p est premier.

Pour l'assertion (iii), considérons le morphisme $\psi : \mathbb{Z}[X] \to \mathbb{Z}[\zeta]/(\lambda)$ qui envoie P sur la classe $P(\zeta) + (\lambda)$. Ce morphisme est clairement surjectif et nous allons montrer que son noyau est donné par $\mathrm{Ker}(\psi) = \{P \in \mathbb{Z}[X],\ P(1) \in p\mathbb{Z}\}$.

Pour l'inclusion directe, soit P dans $\mathrm{Ker}(\psi)$, alors $P(\zeta) = \lambda Q(\zeta)$, avec $\deg(Q) < \deg(\phi_p) = p-1$. Par la formule de Taylor polynomiale

$$P(1) = P(\zeta + \lambda) = P(\zeta) + \lambda P'(\zeta) + \cdots + \frac{1}{p!}\lambda^p P^{(p)}(\zeta) \in (\lambda).$$

On a donc bien $P(1) \in (\lambda) \cap \mathbb{Z} = p\mathbb{Z}$ par (ii).

Pour l'inclusion inverse, on suppose $P(1) \in p\mathbb{Z}$, et donc $P(1) \in (\lambda^{p-1}) \subset (\lambda)$. Encore une fois, on applique la formule de Taylor polynomiale pour trouver

$$P(\zeta) = P(1-\lambda) = P(1) - \lambda P'(1) + \cdots - \frac{1}{p!}\lambda^p P^{(p)}(1) \in (\lambda),$$

et ainsi, $P \in \mathrm{Ker}(\psi)$. D'où l'égalité.

Or, $\{P \in \mathbb{Z}[X],\ P(1) \in p\mathbb{Z}\}$ est exactement le noyau du morphisme surjectif $\psi' : \mathbb{Z}[X] \to \mathbb{F}_p$ qui envoie P sur $P(1)$ modulo p. Il en résulte que

$$\mathbb{Z}[\zeta]/(\lambda) \simeq \mathbb{Z}[X]/\mathrm{Ker}\psi = \mathbb{Z}[X]/\mathrm{Ker}(\psi') \simeq \mathbb{F}_p.$$

L'idéal (λ) est donc maximal, donc premier, puisque le quotient est un corps. D'où (iv).

Encore une fois, comme 1 n'est pas dans (λ), sa classe $\overline{1}$ est non nulle, et comme le groupe additif $\mathbb{Z}[\zeta]$ est d'ordre premier p, $\overline{1}$ est d'ordre p. Donc, tous les $\overline{a}$, $0 \leq a \leq p-1$, sont des classes deux à deux distinctes qui constituent l'ensemble $\mathbb{Z}[\zeta]/(\lambda)$, ce qui prouve (v).

2.5 Expression des unités de $\mathbb{Z}[\zeta]$

Proposition 2.4. *Tout élément inversible de $\mathbb{Z}[\zeta]$ peut s'écrire sous la forme $u = \zeta^r \varepsilon$ avec $r \in \mathbb{N}$ et ε un réel inversible de $\mathbb{Z}[\zeta]$.*

Démonstration. Soit u inversible dans $\mathbb{Z}[\zeta]$, avec $uu' = 1$, ce qui implique $\sigma_k(u)\sigma_k(u') = 1$ pour tout k, et donc tous les conjugués $u_k := \sigma_k(u)$ sont également inversibles. De plus, si P est un polynôme de $\mathbb{Z}[X]$ tel que $u = P(\zeta)$, il vient que $u_k = \sigma_k(u) = P(\zeta^k)$, et en particulier en prenant le conjugué complexe, on obtient

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

Soit donc $v_k = \sigma_k\left(\frac{u}{\overline{u}}\right) = \frac{u_k}{u_{p-k}}$. Les v_k sont des complexes conjugués de module 1 dans $\mathbb{Z}[\zeta]$. Il en résulte que le polynôme $P = \prod_{k=1}^{p}(X - v_k)$ est unitaire, à coefficients dans $\mathbb{Z}[\zeta]$, stables par les σ_k, donc dans $\mathbb{Z}$ (voir prérequis). Comme P n'a que des racines de module 1, le théorème de Kronecker assure que ses racines sont des racines de l'unité. Par la proposition 2.2, les v_k sont des racines $2p$-ièmes de l'unité. En particulier, $\frac{u}{\overline{u}} = e\zeta^m$, avec $e = \pm 1$.

Par la proposition 2.3, $u = a + \lambda Q(\zeta)$, pour $1 \leq a \leq p-1$, et pour un polynôme $Q \in \mathbb{Z}[X]$. De plus, a est non nul car $N(u)$ est inversible et $N(\lambda)$ ne l'est pas. Donc, $\overline{u} = a + \overline{\lambda}Q(\overline{\zeta}) = a - \zeta^{-1}\lambda Q(\overline{\zeta})$. Comme $\zeta = 1 - \lambda$, on en déduit que $\zeta^m = 1$ modulo (λ),

$$u = e\zeta^m \overline{u} = ea \mod (\lambda).$$

Par identification $ea = a$ et donc $e = 1$ car a est non nul.

On en déduit que $\frac{u}{\overline{u}} = \zeta^m$. Soit a et b deux entiers tels que la relation de Bezout $2a + bp = 1$ est vérifiée (rendu possible car p est impair), alors $\zeta^m = \zeta^{m(2a+bp)} = \zeta^{2am}$. Posons donc $\varepsilon = \zeta^{-am}u$. Il vient alors

$$\overline{\varepsilon} = \zeta^{am}\overline{u} = \zeta^{am}\zeta^{-m}u = \zeta^{am}\zeta^{-2am}u = \varepsilon.$$

Il résulte que ε est réel, et il suffit de poser $r = am$ pour conclure la proposition.

3 L'anneau des entiers de $\mathbb{Q}(\zeta)$

Théorème 3.1. *L'anneau des entiers de $\mathbb{Q}(\zeta)$ est $\mathbb{Z}[\zeta]$.*

Démonstration. On a déjà vu que tout élément de $\mathbb{Z}[\zeta]$ est un entier algébrique. Il reste à montrer la réciproque. Soit donc θ dans $\mathbb{Q}(\zeta)$, supposons θ entier algébrique et écrivons-le sous la forme $\theta = \sum_{k=0}^{p-2} a_k\zeta^k$, avec $a_k \in \mathbb{Q}$. Le but est donc de montrer que les a_k sont entiers.

Posons pour tout k de 0 à $p-2$, $b_k := \mathrm{tr}(\theta\zeta^{-k} - \theta\zeta)$. On trouve

$$b_k = \mathrm{tr}\left(\sum_{s=0}^{p-2} a_s\zeta^{s-k} - a_s\zeta^{s+1}\right) = a_k(p-1) - \sum_{s\neq k} a_s - \sum_{s=0}^{p-2}(-a_s) = (p-1)a_k + a_k = pa_k.$$

Comme b_k est la trace d'un entier algébrique, b_k est un entier. Il reste à montrer que p divise tous les b_k.

Notons tout d'abord que l'on peut écrire

$$p\theta = \sum_{k=0}^{p-2} b_k \zeta^k = \sum_{k=0}^{p-2} b_k (1-\lambda)^k = \sum_{k=0}^{p-2} c_k \lambda^k,$$

où $(c_k)_k$ est défini en fonction de $(b_k)_k$ selon l'automorphisme de $\mathbb{Z}[X]$ qui envoie P sur $P(1-X)$ (et donc, $(c_k)_k$ est une suite à valeurs dans $\mathbb{Z}$) ; comme il envoie bijectivement $p\mathbb{Z}[X]$ sur $p\mathbb{Z}[X]$, montrer que p divise tous les b_k revient à montrer qu'il divise tous les c_k.

En prenant la trace dans l'égalité $p\theta = \sum_{k=0}^{p-2} c_k \lambda^k$, on obtient $p\,\mathrm{tr}(\theta) = (p-1)c_0 + p\sum_{k=1}^{p-2} c_k$, ce qui prouve que p divise c_0 puisque $\mathrm{tr}(\theta)$ est un entier. Soit $c_0 = pc_0'$.

Ecrivons maintenant l'égalité $p\theta = pc_0' + \sum_{k=1}^{p-2} c_k \lambda^k$, puis, en écrivant $p \in (\lambda^{p-1})$ par la proposition 2.3 (i), on considère l'égalité précédente modulo (λ^2), afin d'obtenir $\lambda c_1 = \lambda^2 \beta$, avec $\beta \in \mathbb{Z}[\zeta]$. Il en résulte que c_0 est divisible par λ et donc $c_0 \in (\lambda) \cap \mathbb{Z} = p\mathbb{Z}$. On montre ensuite par récurrence que tous les c_k sont dans $p\mathbb{Z}$ et on achève ainsi la preuve.

4 p-régulier et l'équation de Fermat

Théorème 4.1. *Soit $p > 3$ un nombre premier régulier, x, y, z trois entiers deux à deux premiers entre eux tels que $x^p + y^p + z^p = 0$, alors p divise xyz.*

Démonstration. On suppose par l'absurde[3] que x, y, z trois entiers deux à deux premiers entre eux tels que $x^p + y^p + z^p = 0$, et p ne divisant pas xyz.

On fixe $0 \leq k < l \leq p-1$, et on va montrer dans un premier temps que les idéaux $(x + \zeta^k y)$ et $(x + \zeta^l y)$ sont premiers entre eux. Par l'absurde, soit J un idéal premier les contenant tous les deux. Alors, en soustrayant, on obtient $x + \zeta^k y - x - \zeta^l y \in J$ et donc, $y(\zeta^k - \zeta^l) \in J$. En rappelant la preuve de la proposition 2.3 (i), on a $1 - \zeta^{l-k} = \lambda\beta$, avec β inversible, il vient que $\lambda y \zeta^k \beta \in J$ et donc, $\lambda y \in J$.

Si par l'absurde, y est dans J, alors $x \in J$, et donc $z^p \in J$, et $z \in J$ puisque J est un idéal premier. Donc, x, y, z sont tous trois dans $J \cap \mathbb{Z}$ qui est un idéal (strict : ni nul, forcément, ni $\mathbb{Z}$ sinon J contiendrait 1) de $\mathbb{Z}$, donc, de la forme $n\mathbb{Z}$. Ceci contredit le fait que les trois entiers sont premiers entre eux.

Donc, $y \notin J$, ce qui implique $\lambda \in J$ puisque J est premier. On a donc $(\lambda) \subset J$, et on obtient l'égalité des deux idéaux, par maximalité de (λ). Or,

$$x + y = x + \zeta^k y + (1 - \zeta^k) y = (x + \zeta^k y) + \lambda\gamma y \in J = (\lambda)$$

Résultat des courses : $x + y \in (\lambda) \cap \mathbb{Z} = p\mathbb{Z}$.

Réduisons l'égalité $x^p + y^p + z^p = 0$ modulo p, ce qui donne à l'aide du Frobenius $x + y + z = 0$ et donc $z = 0$. Donc p divise z, absurde par hypothèse.

3. Mettez les compteurs à zéro, ce n'est que le début qu'une longue suite d'absurdités. Welcome in Absurdland !

Il résulte que les idéaux $(x+\zeta^k y)$ et $(x+\zeta^l y)$ sont premiers entre eux[4]. Comme le produit des idéaux est égal à :

$$\prod_{k=0}^{p-1}(x+\zeta^k y) = (\prod_{k=0}^{p-1}(x+\zeta^k y)) = (x^p+y^p) = (z^p) = (z)^p,$$

et comme les idéaux du membre de gauche sont deux à deux premiers entre eux, il vient, en décomposant tous les idéaux en idéaux premiers, que les idéaux du membre de gauche sont tous les puissances p-ièmes d'idéaux. En particulier, il existe un idéal I tel que $(x+\zeta y) = I^p$.

Comme p est régulier, le fait que I^p soit principal implique que I est principal, disons $I = (\alpha)$, avec $\alpha \in \mathbb{Z}[\zeta]$. Ceci implique $(x+\zeta y) = (\alpha^p)$, et donc que $x+\zeta y$ et α^p sont égaux modulo un inversible. Par la proposition 2.4, on peut trouver un réel ε inversible de $\mathbb{Z}[\zeta]$ et un entier r tels que $x+\zeta y = \zeta^r \varepsilon \alpha^p$.

Il reste encore un dernier coup de collier pour atteindre une dernière absurdité.

Posons $\alpha = \sum_{k=0}^{p-2} a_k \zeta^k$, avec $a_k \in \mathbb{Z}$. Dans $\mathbb{Z}[\zeta]/(p)$, on a $\overline{\alpha}^p = \left(\sum_{k=0}^{p-2} a_k \overline{\zeta}^k\right)^p = \sum_{k=0}^{p-2} a_k^p \overline{\zeta}^{kp} = \sum_{k=0}^{p-2} a_k^p =: a$, avec $a \in \mathbb{Z}$. On en déduit que modulo (p)

$$x + y\zeta - x\zeta^{2r} - y\zeta^{2r-1} = \zeta^r \varepsilon \alpha^p - \zeta^r \varepsilon \overline{\alpha}^p = \zeta^r \varepsilon (a-a) = 0.$$

On voit que $r = 0$ est impossible, sinon, on aurait $y(1-\zeta^2) = p\beta$, avec $\beta \in \mathbb{Z}[\zeta]$. En prenant la norme, on aurait que p^{p-1} divise $y^{p-1}p$, donc p divise y contrairement aux hypothèses. De même $r \neq 1$.

Si $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ sont deux à deux distincts, ils sont $\mathbb{Z}$-libres, donc x et y seraient multiples de p, contrairement à l'hypothèse. On en déduit que modulo p, $r = 0$ ou 1, mais ceci est impossible, la seule possibilité qu'il reste est $2r = 1$ modulo p.

Conclusion, $x + y\zeta - x\zeta - y$ est dans l'idéal (p), ce qui peut s'écrire $\lambda(x-y) \in (p)$. En utilisant une dernière fois la norme, il vient que p^{p-1} divise $N(\lambda)(x-y)^{p-1} = p(x-y)^{p-1}$.

Ainsi, $x = y$ modulo p et de même on montrerait que $y = z$ modulo p. L'équation de Fermat donne alors $3z^p = 0$ modulo p et, comme $p > 3$, z est un multiple de p, ce qui achève la preuve dans une absurdité finale.

Remarque 4.2. Quels sont les p réguliers au fait ? Tout d'abord, le premier nombre premier irrégulier est 37, et la liste se prolonge avec 59, 67, etc... Plus généralement, on montre qu'un nombre premier p est régulier s'il ne divise pas les numérateurs des nombres de Bernoulli B_2, B_4,..., B_{p-3}. Si l'on en croit Wikipedia, on ne sait toujours pas si l'ensemble des nombres premiers est régulier.

4. J'en vois qui suivent plus là !

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'ÉDUCATION
NATIONALE

EAE MAT 1

SESSION 2019

AGREGATION
CONCOURS EXTERNE

Section : MATHÉMATIQUES

COMPOSITION DE MATHÉMATIQUES GÉNÉRALES

Durée : 6 heures

L'usage de tout ouvrage de référence, de tout dictionnaire et de tout matériel électronique (y compris la calculatrice) est rigoureusement interdit.

Si vous repérez ce qui vous semble être une erreur d'énoncé, vous devez le signaler très lisiblement sur votre copie, en proposer la correction et poursuivre l'épreuve en conséquence. De même, si cela vous conduit à formuler une ou plusieurs hypothèses, vous devez la (ou les) mentionner explicitement.

NB : Conformément au principe d'anonymat, votre copie ne doit comporter aucun signe distinctif, tel que nom, signature, origine, etc. Si le travail qui vous est demandé consiste notamment en la rédaction d'un projet ou d'une note, vous devrez impérativement vous abstenir de la signer ou de l'identifier.

Tournez la page S.V.P.

INFORMATION AUX CANDIDATS

Vous trouverez ci-après les codes nécessaires vous permettant de compléter les rubriques figurant en en-tête de votre copie.

Ces codes doivent être reportés sur chacune des copies que vous remettrez.

Concours	Section/option	Epreuve	Matière
EAE	1300A	101	0376

Les calculatrices, téléphones, tablettes, ordinateurs, montres connectées et tous appareils électroniques de communication ou de stockage, ainsi que les documents sont interdits.

La qualité de la rédaction sera un facteur important d'appréciation des copies. On invite donc les candidats à produire des raisonnements clairs, complets et concis.

Les candidats peuvent utiliser les résultats énoncés dans les questions ou parties précédentes, en veillant dans ce cas à préciser la référence du résultat utilisé.

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 $\mathbf{Q}$) s'il existe un polynôme non nul P de $\mathbf{Q}[X]$ 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 $\mathbf{Z}$.

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

— 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 $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$.

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

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

I Exercices préliminaires

1. Soit $B \in \mathbf{Z}[X]$ un polynôme unitaire et $A \in \mathbf{Z}[X]$. Montrer qu'il existe $Q, R \in \mathbf{Z}[X]$ 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 $\mathbf{Z}[j]$.** On note $j = e^{\frac{2i\pi}{3}}$.
   (a) Démontrer que j est un élément algébrique sur $\mathbf{Q}$ et préciser son polynôme minimal.
   (b) Démontrer que $\mathbf{Z}[j] = \{a + bj,\ (a, b) \in \mathbf{Z}^2\}$.
   Pour tout nombre complexe z, on pose $\mathrm{N}(z) = z\overline{z} = |z|^2$.
   (c) Démontrer que pour tout $z \in \mathbf{Z}[j]$, on a $\mathrm{N}(z) \in \mathbf{N}$. En déduire que si $z \in \mathbf{Z}[j]$ est inversible, alors $N(z) = 1$, puis que $\mathbf{Z}[j]^\times$ possède 6 éléments que l'on précisera.
   (d) Soient $x \in \mathbf{Z}[j]$ et $y \in \mathbf{Z}[j] \setminus \{0\}$. Déterminer un élément $q \in \mathbf{Z}[j]$ tel que $\mathrm{N}\left(\frac{x}{y} - q\right) < 1$.
   En déduire que l'anneau $\mathbf{Z}[j]$ est euclidien.
3. **Polynômes cyclotomiques**. Soit n un entier naturel non nul. On note Φ_n le n-ième polynôme cyclotomique. On rappelle que si μ_n^* désigne l'ensemble des racines primitives n-ièmes de l'unité dans $\mathbf{C}$, 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 $\Phi_n(X) \in \mathbf{Z}[X]$.
   (c) Soit p un nombre premier. On note $\pi : \mathbf{Z} \longrightarrow \mathbf{F}_p$ la surjection canonique. Le morphisme d'anneaux π s'étend, coefficient par coefficient, en un morphisme d'anneaux de $\mathbf{Z}[X]$ sur $\mathbf{F}_p[X]$, noté $\widehat{\pi}$ (on ne demande pas de justifier ce point). Si Φ_p désigne le p-ième polynôme cyclotomique, on rappelle que $\Phi_p = \sum_{k=0}^{p-1} X^k$.
      i. Démontrer que $\widehat{\pi}(X^p - 1) = (X - 1_{\mathbf{F}_p})^p$.
      ii. Soient P et Q deux polynômes unitaires et non constants dans $\mathbf{Z}[X]$ 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 $\mathbf{Q}[X]$.

      ☛*De manière générale, Φ_n est irréductible pour tout $n \in \boldsymbol{N} \setminus \{0\}$, 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 $\mathbf{Q}$ et en déduire le degré de l'extension de corps $\mathbf{Q}(\zeta)/\mathbf{Q}$.

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 $\mathbf{C}[X]$. On lui associe sa *matrice compagnon* C_P définie dans $\mathcal{M}_n(\mathbf{C})$ par

$$\mathrm{C}_P = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}.$$

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

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

(b) Exprimer $\mathrm{C}_P^n e_1$ 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 $M \in \mathcal{M}_n(\mathbf{C})$ 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 $\mathbf{C}[X]$.

(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 $\mathbf{C}$. 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 $A[X]$.

II Nombres algébriques

1. (a) On désigne par φ l'indicatrice d'Euler, qui à tout entier $n \in \mathbf{N} \setminus \{0\}$ 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 $\mathbf{K}/\mathbf{Q}$ est une extension finie de $\mathbf{Q}$, où $\mathbf{K}$ est un sous-corps de $\mathbf{C}$, alors $\mathbf{K}$ contient un nombre fini de racines de l'unité.

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

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

(b) Montrer que si σ est un morphisme de $\mathbf{Q}$-algèbre de $\mathbf{K}$ dans $\mathbf{C}$, $\sigma(\alpha)$ 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 $\mathbf{Q}$-algèbre, que l'on notera $\sigma_k : \mathbf{K} \to \mathbf{C}$, $k \in \{1, \ldots, d\}$.

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

(a) Justifier que θ est un nombre algébrique.

Tournez la page S.V.P.

On pose

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

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

(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 $\{\alpha^n,\ n \in \mathbf{N}\}$ est de type fini.

(b) Réciproquement, montrer que si G est de type fini alors α est un entier algébrique.

Indication : En notant $(g_1, \ldots, g_n)$ une famille génératrice finie de G, on pourra considérer le déterminant du système obtenu en écrivant les éléments αg_i, $i \in \{1, \ldots, n\}$ comme combinaison linéaire des g_j.

6. En déduire que l'ensemble $\mathfrak{O}_\mathbf{C}$ des entiers algébriques de $\mathbf{C}$ est un sous-anneau de $\mathbf{C}$.

Indication : On pourra utiliser sans démonstration qu'un sous-groupe d'un groupe abélien de type fini est de type fini.

7. Montrer que $\mathfrak{O}_\mathbf{C} \cap \mathbf{Q} = \mathbf{Z}$.

☛*Dans la suite, on considère le corps $\boldsymbol{K} = \boldsymbol{Q}(\zeta)$ où $\zeta = e^{\frac{2i\pi}{p}}$ avec p premier impair, et on note $\mathfrak{O}_{\boldsymbol{K}}$ l'ensemble des entiers algébriques de $\boldsymbol{K}$. On pose $\lambda = 1 - \zeta$.*
On définit la norme *et la* trace *de tout élément $\theta \in \boldsymbol{K} = \boldsymbol{Q}(\zeta)$ par*

$$\mathrm{N}(\theta) = \prod_{k=1}^{p-1} \sigma_k(\theta) \ \textit{et}\ \mathrm{Tr}(\theta) = \sum_{k=1}^{p-1} \sigma_k(\theta),$$

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

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

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

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

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

2. Montrer l'inclusion $\mathbf{Z}[\zeta] \subseteq \mathfrak{O}_\mathbf{K}$.

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

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

(b) Montrer que si $\mathrm{N}(z)$ 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 $\mathbf{K}$ 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 $2p \mid n$ et que $\mathbf{Q}(\zeta) = \mathbf{Q}(\omega)$.

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

5. On note $\langle\lambda\rangle = \lambda\mathbf{Z}[\zeta]$, l'idéal de $\mathbf{Z}[\zeta]$ engendré par λ.
   (a) Montrer que $\langle\lambda\rangle \cap \mathbf{Z} = p\mathbf{Z}$.
   (b) Montrer que pour tout $k \in \{1, \ldots, p-1\}$, on a $\dfrac{1-\zeta}{1-\zeta^k} \in \mathbf{Z}[\zeta]^\times$ et en déduire que
   $$\lambda^{p-1}\mathbf{Z}[\zeta] = p\mathbf{Z}[\zeta].$$
   (c) Soit ψ le morphisme d'anneaux de $\mathbf{Z}[X]$ dans $\mathbf{Z}[\zeta]/\langle\lambda\rangle$, qui à $P \in \mathbf{Z}[X]$ associe $P(\zeta)$ (mod $\langle\lambda\rangle$). Déterminer l'image de ψ et montrer que $\ker\psi$ est l'ensemble des polynômes $P \in \mathbf{Z}[X]$ tels que $P(1) = 0 \pmod{p\mathbf{Z}}$.
   (d) En déduire que $\mathbf{Z}[\zeta]/\langle\lambda\rangle$ est isomorphe à $\mathbf{F}_p$.
   (e) Que peut-on en déduire pour l'idéal $\langle\lambda\rangle$?
6. On détermine ici la structure de $\mathbf{Z}[\zeta]^\times$. Le but est de démontrer que les éléments de $\mathbf{Z}[\zeta]^\times$ sont les $\zeta^r\varepsilon$, où $r \in \mathbf{Z}$ et ε est un réel inversible de $\mathbf{Z}[\zeta]$.
   Soit $u \in \mathbf{Z}[\zeta]^\times$.
   (a) Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbf{Z}[X]$ 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 $P_n = \prod_{k=1}^{d}(X - \alpha_k^n)$, $n \in \boldsymbol{N}$, *dont on montrera qu'ils sont dans* $\boldsymbol{Z}[X]$.
   (b) Soit $P \in \mathbf{Z}[X]$ 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 $\mathbf{Z}[\zeta]^\times$.
   (c) Justifier que $\dfrac{u_1}{u_{p-1}}$ est un entier algébrique dont tous les conjugués sont de module 1.
   (d) En déduire qu'il existe $m \in \mathbf{Z}$ tel que $\dfrac{u_1}{u_{p-1}} = \pm\zeta^m$.
   (e) i. Soit $\theta \in \mathbf{Z}[\zeta]$. Justifier qu'il existe un entier $a \in \mathbf{Z}$ tel que $\theta = a \pmod{\langle\lambda\rangle}$. En déduire que deux éléments conjugués de $\mathbf{Z}[\zeta]$ sont égaux modulo $\langle\lambda\rangle$.
      ii. Démontrer que $\dfrac{u_1}{u_{p-1}} = \zeta^m$.
   (f) Justifier l'existence de $r \in \mathbf{Z}$ tel que $2r = m \pmod{p\mathbf{Z}}$. On pose $\varepsilon = \zeta^{-r}u$. Montrer que $\varepsilon \in \mathbf{R}$ et conclure.
7. Le but de ce qui suit est de montrer que $\mathfrak{O}_\mathbf{K} = \mathbf{Z}[\zeta]$.
   (a) Montrer que pour tout $\theta \in \mathfrak{O}_\mathbf{K}$, on a $\mathrm{N}(\theta) \in \mathbf{Z}$ et $\mathrm{Tr}(\theta) \in \mathbf{Z}$.
   (b) Soit $\theta \in \mathbf{K} = \mathbf{Q}(\zeta)$ 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 $b_k \in \mathbf{Z}$.

Tournez la page S.V.P.

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 $k \in \{0, \ldots, p-2\}$

$$b_k = \sum_{\ell=k}^{p-2} (-1)^\ell \binom{\ell}{k} c_\ell.$$

iii. Montrer qu'il existe $\beta \in \mathbf{Z}[\zeta]$ 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.

IV 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 $\boldsymbol{Z}[j]$ (et pas seulement dans $\boldsymbol{Z}$), cas auquel on peut se ramener en divisant par leur* `pgcd` *dans $\boldsymbol{Z}[j]$.* ☚

2. Montrer que 3 et λ^2 sont associés dans $\mathbf{Z}[j]$, ce que l'on a noté $3 \sim \lambda^2$.
3. Soit $s \in \mathbf{Z}[j]$ 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 $s \in \boldsymbol{Z}[j]$ 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 $\boldsymbol{Z}[j]$.*
On note n la valuation en λ de z ; il existe donc $\mu \in \boldsymbol{Z}[j]$ 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 :

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

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 $\omega\lambda^{3n}\delta^3 \pmod{\langle\lambda^4\rangle}$, 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 $\boldsymbol{Z}[j]$ 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 $\mathbf{Z}[j]$ tels que pour tout $\ell\in\{1,2,3\}$, $\kappa_\ell\sim\gamma_\ell^3$.

(e) Démontrer qu'il existe deux inversibles τ et τ' de $\mathbf{Z}[j]^\times$ 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 $\tau=\pm1\pmod{\langle\lambda^3\rangle}$, 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 $3\mid xyz$.

V 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 $\boldsymbol{Q}$, son anneau des entiers $\mathfrak{O}_{\boldsymbol{K}}$ vérifie la propriété suivante : tout idéal non nul de $\mathfrak{O}_{\boldsymbol{K}}$ 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 $\boldsymbol{Z}[\zeta]$ qui est, d'après les résultats de la Partie **III**, l'anneau des entiers de $\boldsymbol{K}=\boldsymbol{Q}(\zeta)$ 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 $\boldsymbol{Z}[\zeta]$ 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 **III**, 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 $x,y,z\in\boldsymbol{Z}$ deux à deux premiers entre eux dans $\boldsymbol{Z}$, 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 $0\leqslant k<\ell\leqslant p-1$. On montre dans cette question que les idéaux $\langle x+\zeta^k y\rangle$ et $\langle x+\zeta^\ell y\rangle$ de $\mathbf{Z}[\zeta]$ sont premiers entre eux. Par l'absurde, soit $\mathfrak{P}$ un idéal premier divisant $\langle x+\zeta^k y\rangle$ et $\langle x+\zeta^\ell y\rangle$.

(a) En considérant $(x+\zeta^\ell y)-(x+\zeta^k y)$, montrer que $\lambda y\in\mathfrak{P}$.

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

Tournez la page S.V.P.

3. Justifier l'existence d'un idéal I tel que $\langle x+\zeta y\rangle = I^p$.
4. Montrer qu'il existe $r \in \mathbf{Z}$, ε réel inversible de $\mathbf{Z}[\zeta]$ et $\alpha \in \mathbf{Z}[\zeta]$ tels que $x+\zeta y = \zeta^r \varepsilon \alpha^p$.
5. Montrer qu'il existe $a \in \mathbf{Z}$ tel que $\alpha^p = a \pmod{\langle p\rangle}$ (attention, ici $\langle p\rangle = p\mathbf{Z}[\zeta]$ et non $p\mathbf{Z}$) et en déduire que
$$x\zeta^{-r} + y\zeta^{1-r} - x\zeta^r - y\zeta^{r-1} = 0 \pmod{\langle p\rangle}.$$
6. Supposons que $r = 0 \pmod{p\mathbf{Z}}$. Montrer alors que $p \mid y$ dans $\mathbf{Z}$, ce qui est contraire à l'hypothèse.

On montrerait de même que l'on ne peut avoir $r = 1 \pmod{p\mathbf{Z}}$, ce que l'on admet.

7. D'après la question 5, il existe $\beta \in \mathbf{Z}[\zeta]$ 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 $2r = 1 \pmod{p\mathbf{Z}}$.
8. Montrer que $\beta p\zeta^r = (x-y)\lambda$, puis que $x = y \pmod{p\mathbf{Z}}$.
9. Conclure à une absurdité.

Chapitre 3

Épreuve écrite de mathématiques générales

Le sujet est disponible à l'URL http://www.devenirenseignant.gouv.fr/cid137747/sujets-rapports-des-jurys-agregation-2019.html ou sur le site agreg.org.

3.1 Commentaires sur l'épreuve écrite de mathématiques générales

Rétrospective historique

Le grand théorème de Fermat s'énonce ainsi en termes modernes : si n est un entier naturel supérieur ou égal à 3, il n'existe pas de solutions entières non triviales à l'équation

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

Cet énoncé apparaît dans une lettre de Fermat publiée en 1670. On voit facilement que si le théorème est prouvé pour un entier n, il l'est aussi pour tous les multiples de n, donc il suffit d'examiner le cas où n est premier impair, et le cas où $n = 4$. Gauss, après Euler, s'est intéressé au cas $n = 3$ en travaillant dans l'anneau $\mathbf{Z}[j]$ où $j = e^{2i\pi/3}$. La factorialité de cet anneau est un point crucial de la preuve. D'une manière générale, pour un nombre premier p et des entiers x, y et z, l'écriture

$$x^p + y^p = \prod_{k=0}^{p-1}(x + \zeta_p^k y) = z^p \tag{3.1}$$

où $\zeta_p = e^{2i\pi/p}$ suggère de travailler dans l'anneau $\mathbf{Z}[\zeta_p]$. Cependant, à la différence du cas $p = 3$, cet anneau n'est en général pas factoriel ($p = 23$ étant le plus petit nombre premier pour lequel $\mathbf{Z}[\zeta_p]$ n'est pas factoriel). Kummer s'en est rendu compte dans les années 1840 et a été conduit à introduire la notion de « nombre idéal », ancêtre de la notion moderne d'idéal. En réécrivant l'égalité (3.1) en termes d'idéaux :

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

et en démontrant que les idéaux $\langle x + \zeta_p^k y\rangle$ sont premiers entre eux, le fait que l'anneau des entiers d'un corps de nombres est un anneau de Dedekind assure que les idéaux $\langle x + \zeta_p^k y\rangle$ sont de la forme I_k^p, puissances p-ièmes d'idéaux. Lorsque p est un nombre premier *régulier*, c'est-à-dire tels que p ne divise pas le nombre de classes du corps cyclotomique $\mathbf{Q}(\zeta_p)$, alors les idéaux I_k sont principaux, ce qui, en connaisant la structure des unités de l'anneau $\mathbf{Z}[\zeta_p]$, permet de conclure.

Kummer démontre ainsi le théorème de Fermat pour les nombres premiers réguliers en 1847. On ne sait toujours pas s'il y a une infinité de tels nombres premiers. Pour (beaucoup) plus de détails sur les aspects historiques, voir [F1].

Description du sujet

— La première partie du sujet établit quelques points techniques utiles pour la suite du problème : la division euclidienne dans $\mathbf{Z}[X]$ par un polynôme unitaire ; le fait que l'anneau $\mathbf{Z}[j]$ est euclidien donc factoriel ; l'irréductibilité du p-ième polynôme cyclotomique et le résultat suivant sur le polynômes : si $Q \in A[X]$ où A un sous-anneau de $\mathbf{C}$ et si $P \in A[X]$ dont on note $\alpha_1, \dots, \alpha_n$ les racines complexes, le polynôme $\prod_{k=1}^{n}(X - Q(\alpha_k))$ est dans $A[X]$.
— Dans la deuxième partie, on démontre des résultats classiques sur les nombres algébriques et on établit que l'ensemble des entiers algébriques de $\mathbf{C}$ est un sous-anneau.
— Dans la troisième partie, on démontre que l'anneau des entiers du corps cyclotomique $\mathbf{Q}(\zeta_p)$ est $\mathbf{Z}[\zeta_p]$ et on détermine la structure des unités de $\mathbf{Z}[\zeta_p]$.
— Dans la quatrième partie, on démontre le théorème de Fermat pour $p = 3$ par un argument de descente et en utilisant la factorialité de $\mathbf{Z}[j]$.
— Dans la cinquième et dernière partie, on démontre le résultat de Fermat pour les premiers p réguliers (dans le cas $p \nmid xyz$) en admettant le fait que l'anneau des entiers d'un corps de nombres est un anneau de Dedekind.

Pour plus de détails, on consultera avec profit [F2] dont le sujet est largement inspiré.

Bibliographie

[F1] P. Ribenboim, *13 Lectures on* Fermat*'s Last Theorem*, Springer, 1979.

[F2] I.N. Stewart, D.O. Tall, *Algebraic Number Theory*, Chapman and Hall, 1979.

Commentaires généraux sur les copies

Dans l'immense majorité des copies, seules les deux premières parties ont été abordées. Les meilleures copies ont avancé dans la partie 3, sans toutefois traiter significativement les parties 4 ou 5.

La présentation et l'orthographe laissent trop souvent à désirer. On rappelle également qu'il est inutile et contre-productif de recopier les énoncés des questions avant de les traiter. Les candidats devraient tout particulièrement soigner la rédaction de la première partie. Certains rares candidats ont sauté les premières parties pour tenter de traiter des questions isolées de la quatrième partie, une stratégie qui n'est pas recommandée. Au contraire, il était important dans ce sujet de traiter aussi intégralement que possible la première partie. Sur les premières questions du sujet, le jury attend une rédaction exemplaire. On rappelle notamment qu'expliquer et justifier, en particulier par des références claires et explicites à des théorèmes ou/et des questions correctement identifiées, est une qualité utile aux futurs enseignants.

Il était nécessaire, tout au long du sujet, de préciser les ensembles dans lesquels on prenait les objets : « soit P un polynôme » ne dit pas si $P \in \mathbf{C}[X]$, $\mathbf{Q}[X]$ ou $\mathbf{Z}[X]$ par exemple. Les variables introduites doivent être quantifiées ; les correcteurs ont noté certaines confusions inquiétantes dans les objets manipulés : polynôme et évaluation d'un polynôme, polynôme et polynôme de matrice, polynôme de matrice et vecteur, etc.

Commentaires détaillés sur certaines questions

I.1 : cette question a posé beaucoup de difficulté, donnant lieu à des rédactions souvent longues et maladroites. Pour l'hérédité, il était peu pertinent d'écrire $A = a_0 + XC$, la logique de l'algorithme de division euclidienne veut qu'on compense directement le terme de plus haut degré.

I.2(a) : le caractère minimal du polynôme $X^2 + X + 1$ est fréquemment oublié.

I.2(b) : quelques copies invoquent un passage au quotient, qui ne peut prouver l'égalité demandée.

I.2(c) : de nombreux candidats se lancent dans une étude laborieuse du signe de a^2+b^2-ab, alors même que le module suffisait pour la positivité. Trop de candidats ignorent la mise sous forme canonique d'un trinôme, et de ce fait échouent dans la résolution de $a^2+b^2-ab=1$. Il ne fallait pas omettre en fin de question la vérification que les 6 éléments trouvés étaient effectivement des inversibles de $\mathbf{Z}[j]$.

I.2(d) : très peu de copies ont produit un dessin permettant de visualiser l'élément q du réseau $\mathbf{Z}[j]$ recherché, et on peut penser que c'est ce qui a empêché beaucoup de trouver le bon candidat pour l'élément q.

I.3 : des candidats confondent $\mathbf{U}_n$ et μ_n^* et pensent donc pouvoir identifier Φ_n et X^n-1.

I.3(a) : très peu de copies donnent des arguments précis pour cette question : la structure du groupe des racines n-ièmes de l'unité semble très mal maîtrisée. La multiplicité des racines n'est presque jamais évoquée par les candidats qui prouvent l'égalité des polynômes en montrant qu'ils ont les mêmes racines.

I.3(b) : certains candidats prennent pour acquis que $\Phi_n \in \mathbf{Q}[X]$ alors que la définition ne donne que $\Phi_n \in \mathbf{C}[X]$.

I.3(c)ii) dans de nombreuses copies, on se contente de montrer que $P(1)$ *ou* $Q(1)$ sont des entiers multiples de p.

I.4(a) et (b) : les arguments de liberté/base sont essentiels et ne sauraient être masqués par une écriture matricielle abusive (c'est-à-dire sans avoir mentionné la base) des vecteurs.

I.4(e) : bien qu'immédiate avec la question précédente, cette question a été peu réussie. Des candidats ont produit des raisonnements utilisant les polynômes symétriques élémentaires, ce qui pouvait aboutir à condition de bien rédiger.

II.1(a) le complémentaire d'une partie infinie de $\mathbf{N}$ peut être infini. Il ne suffit donc pas de montrer qu'il y a une infinité d'entiers n tels que $\varphi(n)>d$. Par ailleurs, la distinction entre racine n-ième de l'unité et racine *primitive* n-ième de l'unité n'est pas toujours faite par les candidats.

II.1.(b) : des passages en force en citant la question précédente mais sans donner d'arguments.

II.2(a) : cette question était une question de cours, et aurait dû être mieux réussie. Des candidats utilisent directement que $\mathbf{Q}[\alpha]$ (souvent confondu avec $\mathbf{Q}(\alpha)$) est un corps, ce qu'il fallait montrer ici.

II.2(b) : peu de candidats ont justifié que π_α n'admettait que des racines simples dans $\mathbf{C}$. À l'exception des toutes meilleures copies, la *construction* des morphismes σ_k n'est jamais faite.

II.3(a) : bien qu'élémentaire, cette question a rarement été réussie.

II.3(b) : des confusions entre θ et α. Certains candidats veulent appliquer ce qu'ils savent pour α à θ ; ils pensent notamment que les $\sigma_k(\theta)$ sont encore les d racines distinctes de π_θ (ce qui simplifie le 3.c).

II.5(a) : beaucoup de candidats parlent de « combinaison linéaire » en oubliant de préciser que les coefficients sont dans $\mathbf{Z}$.

II.6 : la stabilité par somme et différence est souvent oubliée.

III.1 et III.2 : ces questions étaient faciles mais n'ont pas été souvent traitées.

3.2 Corrigé de l'épreuve écrite de mathématiques générales

Exercices préliminaires

1. On écrit $B=X^m+\sum_{k=0}^{m-1} b_k X^k$ où les b_k sont entiers. Soit H_n l'énoncé : pour tout polynôme $A\in\mathbf{Z}[X]$ de degré inférieur strictement à n, il existe $Q,R\in\mathbf{Z}[X]$ tels que $A=BQ+R$ et $\deg R<m$.

   On montre le résultat par récurrence sur n. L'énoncé H_m est vrai, il suffit de poser $Q=0$ et $R=A$. Soit $n\geqslant m$ et on suppose H_n. On montre H_{n+1}. Soit $A\in\mathbf{Z}[X]$ de degré strictement

inférieur à $n+1$. On note $A = \sum_{k=0}^{n} a_k X^k$ et on pose $A_1 = A - a_n X^{n-m} B$. Alors on a $A_1 \in \mathbf{Z}[X]$ et $\deg A_1 \leqslant n-1$ donc on peut appliquer l'hypothèse de récurrence à A_1. Il existe $Q_1, R_1 \in \mathbf{Z}[X]$ tels que $A_1 = BQ_1 + R_1$ avec $\deg R_1 < m$. En posant $Q = Q_1 + a_n X^{n-m}$, on a alors $A = BQ + R_1$, avec $Q \in \mathbf{Z}[X]$ et $\deg R_1 < m$ ce qui prouve H_{n+1}. D'après le principe de récurrence, pour tout $n \geqslant m$, H_n est vraie, ce qui conclut.

2. (a) On a $j^2 + j + 1 = 0$, donc j est algébrique et son polynôme minimal divise $X^2 + X + 1$ dans $\mathbf{Q}[X]$. Le polynôme $X^2 + X + 1$ étant unitaire et irréductible dans $\mathbf{Q}$ (il est de degré 2 et n'a pas de racines rationnelles), c'est le polynôme minimal de j.

   (b) L'inclusion $\{a + bj,\ (a,b) \in \mathbf{Z}^2\} \subseteq \mathbf{Z}[j]$ est immédiate. Réciproquement, soit $P(j)$ avec $P \in \mathbf{Z}[X]$ un élément de $\mathbf{Z}[j]$. Le polynôme $X^2 + X + 1$ étant unitaire, d'après la question 1, on peut effectuer la division euclidienne de P par $X^2 + X + 1$ dans $\mathbf{Z}[X]$: il existe $Q, R \in \mathbf{Z}[X]$ avec $\deg R \leqslant 1$ tels que $P = (X^2 + X + 1)Q + R$. En évaluant en j, il vient $P(j) = R(j)$ donc $P(j)$ est de la forme $a + bj$ avec $a, b \in \mathbf{Z}$.

   (c) Tout d'abord, on remarque que la fonction $z \mapsto \mathrm{N}(z) = |z|^2$ est à valeurs positives et multiplicative : pour tout $z_1, z_2 \in \mathbf{C}$, $\mathrm{N}(z_1 z_2) = |z_1 z_2|^2 = |z_1|^2 |z_2|^2 = \mathrm{N}(z_1)\,\mathrm{N}(z_2)$.
   Soit $z = a + bj \in \mathbf{Z}[j]$; $\mathrm{N}(z) = (a + bj)(a + b\overline{j}) = a^2 + b^2|j|^2 + ab(j + \overline{j}) = a^2 + b^2 - ab \in \mathbf{Z}$. Par ailleurs, $\mathrm{N}(z)$ est un réel positif, donc $\mathrm{N}(z) \in \mathbf{N}$.
   Soit $z = a + bj \in \mathbf{Z}[j]$ un élément inversible ; il existe $z' \in \mathbf{Z}[j]$ tel que $zz' = 1$. En appliquant N qui est multiplicatif, il vient $\mathrm{N}(z)\,\mathrm{N}(z') = 1$. Ainsi, $\mathrm{N}(z)$ est un entier positif inversible, c'est-à-dire $\mathrm{N}(z) = 1$. On a donc $\left(a - \frac{b}{2}\right)^2 + \frac{3}{4}b^2 = 1$. Ceci force $|b| \leqslant 1$. Si $b = 0$, alors $|a| = 1$, donc $z = \pm 1$. Si $b = 1$, alors $\left(a - \frac{1}{2}\right)^2 = \frac{1}{4}$, donc $a = 0$ ou $a = 1$, c'est-à-dire $z = j$ ou $z = 1 + j$. Si $b = -1$, alors $\left(a + \frac{1}{2}\right)^2 = \frac{1}{4}$, donc $a = 0$ ou $a = -1$, c'est-à-dire $z = -j$ ou $z = -1 - j$. Réciproquement, on vérifie que chacun des éléments $\pm 1, \pm j$ et $\pm(1 + j)$ est bien inversible (l'inverse étant donné par le conjugué qui est un élément de $\mathbf{Z}[j]$).

   (d) En multipliant par $\overline{y}$ le numérateur et le dénominateur de $\frac{x}{y}$, on montre que $\frac{x}{y} \in \mathbf{Q}(j)$. On note $\frac{x}{y} = s + tj$ avec $s, t \in \mathbf{Q}$. Soit a l'entier relatif le plus proche de s, de sorte que $|s - a| \leqslant \frac{1}{2}$ et b l'entier relatif le plus proche de t. On pose $q = a + bj \in \mathbf{Z}[j]$. On a

$$\mathrm{N}\left(\frac{x}{y} - q\right) = \left(s - a - \frac{t-b}{2}\right)^2 + \frac{3}{4}(t-b)^2 \leqslant \left(\frac{3}{4}\right)^2 + \frac{3}{4} \cdot \frac{1}{4} = \frac{3}{4} < 1.$$

   Comme N est multiplicatif et que $\mathrm{N}(y) > 0$, on a $\mathrm{N}(x - qy) < \mathrm{N}(y)$. Ainsi, en posant $r = x - qy \in \mathbf{Z}[j]$, on peut écrire $x = qy + r$ avec $\mathrm{N}(r) < \mathrm{N}(y)$; on dispose donc d'une division euclidienne dans $\mathbf{Z}[j]$, et cet anneau étant intègre car inclus dans $\mathbf{C}$, c'est un anneau euclidien.

3. (a) Le groupe $\mathbf{U}_n$ des racines n-ièmes de l'unité est l'union disjointe des groupes μ_d^* pour d divisant n (en effet, si $z \in \mathbf{U}_n$, en notant d l'ordre de z, on a $z \in \mu_d^*$; réciproquement, si $z \in \mu_d^*$ pour un d divisant n, alors z est une racine n-ième de l'unité. Enfin, l'union est disjointe par unicité de l'ordre d'un élément dans un groupe).
   On a donc $\prod_{\mu \in \mathbf{U}_n} (X - \mu) = \prod_{d|n} \prod_{\mu \in \mu_d^*} (X - \mu)$, soit $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

   (b) On prouve le résultat par récurrence forte sur n. Pour $n = 1$, on a $\Phi_1 = X - 1 \in \mathbf{Z}[X]$. On suppose le résultat vrai pour tout entier $d < n$ et on montre que $\Phi_n(X) \in \mathbf{Z}[X]$. Par hypothèse, le polynôme $P = \prod_{d|n, d \neq n} \Phi_d(X)$ est élément de $\mathbf{Z}[X]$. On a la relation $X^n - 1 = \Phi_n(X)P(X)$ et par ailleurs, la division euclidienne de $X^n - 1$ par P dans $\mathbf{Z}[X]$ (possible parce que P est unitaire, voir q1 de cette partie) s'écrit $X^n - 1 = PQ + R$ avec $Q, R \in \mathbf{Z}[X]$ et $\deg R < \deg P$. On en déduit la relation $R(X) = P(X)(\Phi_n(X) - Q(X))$, qui implique $\Phi_n = Q$, sinon $\deg R \geqslant \deg P$. Finalement, $\Phi_n \in \mathbf{Z}[X]$.

(c) i. Le binôme de Newton donne

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

Or, pour tout $k \in [\![1, p-1]\!]$, on a $p \mid \binom{p}{k}$; en effet, $k\binom{p}{k} = p\binom{p-1}{k-1}$ donc p divise $k\binom{p}{k}$ et comme p est premier avec k, p divise $\binom{p}{k}$. On en déduit que $\widehat{\pi}(X^p - 1) = (X-1)^p$ puisque $(-1)^p = -1 \pmod p$ (y compris pour $p = 2$).

ii. En appliquant le morphisme d'anneaux $\widehat{\pi}$, on obtient l'égalité $(X - 1_{\mathbf{F}_p})^p = \widehat{\pi}(P)\widehat{\pi}(Q)$ dans l'anneau factoriel $\mathbf{F}_p[X]$. Comme $p \geqslant 2$, et que $\widehat{\pi}(P)$ et $\widehat{\pi}(Q)$ sont non constants (P et Q sont unitaires, donc $\widehat{\pi}(P)$ et $\widehat{\pi}(Q)$ ont même degré que P et Q respectivement), $X - 1_{\mathbf{F}_p}$ divise $\widehat{\pi}(P)$ et $\widehat{\pi}(Q)$, ce qui entraîne que $P(1) = 0 \pmod p$ et $Q(1) = 0 \pmod p$.

iii. On suppose par l'absurde que Φ_p n'est pas irréductible dans $\mathbf{Z}[X]$. Il existe donc deux polynômes unitaires non constants P et Q de $\mathbf{Z}[X]$ tels que $\Phi_p = PQ$. En multipliant par $X - 1$, on obtient que $X^p - 1 = (X-1)PQ$ et d'après la question précédente appliquée à $(X-1)P$ et Q, on a que $Q(1) = 0 \pmod p$. De même, on a aussi $P(1) = 0 \pmod p$. Or $\Phi_p(1) = p$ et $P(1)Q(1)$ est un multiple de p^2, ce qui est absurde.

On a montré que Φ_p est irréductible sur $\mathbf{Z}$; il est donc aussi irréductible sur $\mathbf{Q}$ d'après le lemme de Gauss rappelé dans l'introduction du sujet. En effet, si $\Phi_p = PQ$ avec $P, Q \in \mathbf{Q}[X]$ non constants, il existe $r \in \mathbf{Q}^*$ tel que $rP \in \mathbf{Z}[X]$ et $\frac{1}{r}Q \in \mathbf{Z}[X]$, si bien que l'on peut écrire $\Phi_p = (rP)\left(\frac{1}{r}Q\right)$ comme produit de polynômes non constants de $\mathbf{Z}[X]$, ce qui est absurde.

iv. Le polynôme Φ_p est unitaire, irréductible sur $\mathbf{Q}$, et annulateur de ζ. C'est donc le polynôme minimal de ζ et le degré de l'extension $\mathbf{Q}(\zeta)/\mathbf{Q}$ est le degré de Φ_p, c'est-à-dire $p-1$.

4. (a) Pour tout $k \in [\![1, n-1]\!]$, $\mathrm{C}_P^k e_1 = \mathrm{C}_P e_k = e_{k+1}$. Soit $Q = \sum_{k=0}^{n-1} q_k X^k \in \mathbf{C}[X]$ non nul et de degré inférieur ou égal à $n-1$; on a $Q(\mathrm{C}_p)e_1 = \sum_{k=0}^{n-1} q_k e_{k+1}$. Ce vecteur est non nul, sinon, par liberté de la famille $\mathcal{E}$, on aurait pour tout $k \in [\![0, n-1]\!]$, $q_k = 0$ si bien que Q serait le polynôme nul.

Aucun polynôme non nul de $\mathbf{C}_{n-1}[X]$ n'est annulateur de C_p, donc le degré du polynôme minimal de C_P est supérieur ou égal à n. D'après le théorème de Cayley-Hamilton, ce degré est inférieur ou égal à n, il est donc exactement égal à n.

(b) On a $\mathrm{C}_P^n e_1 = \mathrm{C}_P e_n = -\sum_{k=0}^{n-1} a_k e_{k+1}$. On obtient donc que

$$P(\mathrm{C}_P)e_1 = \mathrm{C}_P^n e_1 + \sum_{k=0}^{n-1} a_k \mathrm{C}_P^k e_1 = \mathrm{C}_P e_n + \sum_{k=0}^{n-1} a_k e_{k+1} = 0.$$

Ensuite, pour tout $i \in [\![2, n]\!]$, on a, en faisant commuter C_P et $P(\mathrm{C}_P)$ (qui est un polynôme en C_P) :

$$P(\mathrm{C}_P)e_i = P(\mathrm{C}_P)\mathrm{C}_P^{i-1} e_1 = \mathrm{C}_P^{i-1} P(\mathrm{C}_P) e_1 = 0.$$

On conclut que $P(\mathrm{C}_P) = 0$. Le polynôme P est annulateur de C_P, unitaire et de degré n, c'est donc son polynôme minimal d'après la question précédente.

(c) Le polynôme caractéristique de C_P est unitaire, de degré n et annulateur de C_P. Il est donc ici égal au polynôme minimal de C_P, c'est-à-dire égal à P.

(d) On suppose dans un premier temps que M est triangulaire ; ses valeurs propres α_i comptées avec multiplicité sont donc ses éléments diagonaux. La matrice $Q(M)$ est encore triangulaire, avec les $Q(\alpha_i)$ comme éléments diagonaux. On en déduit que $\chi_{Q(M)} = \prod_{i=1}^{n}(X - Q(\alpha_i))$. Dans le cas général, on trigonalise M dans $\mathcal{M}_n(\mathbf{C})$: il existe T, matrice triangulaire avec

les α_i comme éléments diagonaux, semblable à M. Les matrices $Q(M)$ et $Q(T)$ sont encore semblables, donc ont le même polynôme caractéristique, ce qui donne $\chi_{Q(M)} = \chi_{Q(T)} = \prod_{i=1}^{n}(X - Q(\alpha_i))$.

(e) D'après la question précédente, $\prod_{i=1}^{n}(X - Q(\alpha_i))$ est le polynôme caractéristique de $Q(M)$, où M est la matrice compagnon du polynôme P. Or $Q(M) \in \mathcal{M}_n(A)$, donc $\chi_{Q(M)} \in A[X]$.

Nombres algébriques

1. (a) Soit $d \in \mathbf{N}^*$. Soit n un entier tel que $\varphi(n) \leqslant d$, dont on note $n = \prod_{i=1}^{r} p_i^{m_i}$ sa décomposition en facteurs premiers. On a $\varphi(n) = \prod_{i=1}^{r}(p_i - 1)p_i^{m_i-1}$. Nécessairement, les p_i vérifient $p_i \leqslant d+1$, sinon $p_i - 1 > d$ et $\varphi(n) > d$. Il n'existe donc qu'un nombre fini de diviseurs premiers possibles pour un tel entier n. On continue de les noter $p_1 < \ldots < p_r$. Par ailleurs, pour tout i, $p_i^{m_i-1} \leqslant \varphi(n) \leqslant d$, donc $m_i \leqslant 1 + \frac{\ln d}{\ln p_i} \leqslant 1 + \frac{\ln d}{\ln 2}$, donc les m_i sont aussi en nombre fini. On conclut qu'il n'y a qu'un nombre fini d'entiers n tels que $\varphi(n) \leqslant d$.

   (b) Par l'absurde, on suppose que $\mathbf{K}$ contient une infinité de racines de l'unité. Alors il y a une infinité d'entiers n tels que $\mathbf{K}$ contienne une racine de l'unité d'ordre n, ce qui fait que l'ensemble S des racines *primitives* de l'unité contenues dans $\mathbf{K}$ est également infini. On note d le degré de l'extension de corps $\mathbf{K}/\mathbf{Q}$. Une racine primitive n-ième de l'unité μ_n est de degré $\varphi(n)$ sur $\mathbf{Q}$ parce que son polynôme minimal est le n-ième polynôme cyclotomique. Pour tout $n \in S$, L' inclusion de corps $\mathbf{Q}(\mu_n) \subseteq \mathbf{K}$ entraîne que $\varphi(n) \leqslant d$, et comme S est infini, cela contredit le résultat de la question précédente.

2. (a) Si π_α n'est pas irréductible dans $\mathbf{Q}$, on peut écrire $\pi_\alpha = PQ$ où P et Q sont de degré au moins 1. Donc l'un de ces polynômes est annulateur de α et de degré strictement inférieur à $\deg \pi_\alpha$, ce qui est absurde.

   Le corps $\mathbf{Q}(\alpha)$ est l'ensemble des $P(\alpha)$ avec $P \in \mathbf{Q}[X]$. On note $n = \deg \pi_\alpha$; par division euclidienne de tout polynôme P par π_α, on obtient que la famille $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ est génératrice du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}(\alpha)$. De plus, cette famille est libre, sinon il existerait un polynôme non nul annulateur de α et de degré strictement inférieur à n, ce qui contredirait la minimalité de π_α. Finalement, $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ est une base de $\mathbf{Q}(\alpha)$, donc $n = d = [\mathbf{Q}(\alpha) : \mathbf{Q}]$.

   (b) Soit $\sigma : \mathbf{K} \to \mathbf{C}$ un morphisme de $\mathbf{Q}$-algèbres ; on a $\pi_\alpha(\sigma(\alpha)) = \sigma(\pi_\alpha(\alpha)) = \sigma(0) = 0$, donc $\sigma(\alpha)$ est une racine de π_α. Un tel morphisme de $\mathbf{Q}$-algèbres est entièrement déterminé par l'image de α, qui est l'une des racines complexes de π_α. Or le polynôme π_α admet d racines distinctes dans $\mathbf{C}$ (en effet, il est irréductible sur $\mathbf{Q}$, donc π_α et π'_α sont premiers entre eux dans $\mathbf{Q}[X]$, donc aussi dans $\mathbf{C}[X]$, ce qui entraîne que toutes les racines dans $\mathbf{C}$ de π_α sont simples). Il y a donc au plus d tels morphismes, qu'il reste à construire.

   La construction du morphisme d'algèbres σ_k tel que $\sigma_k(\alpha) = \alpha_k$ peut se faire *via* les isomorphismes de corps $\mathbf{Q}(\alpha) \cong \mathbf{Q}[X]/(\pi_\alpha) \cong \mathbf{Q}(\alpha_k)$, ou alors plus élémentairement : on définit, pour tout élément $\theta = \sum_{i=0}^{d-1} a_i\alpha^i \in \mathbf{Q}(\alpha)$ (l'écriture étant unique) $\sigma_k(\theta) = \sum_{i=0}^{d-1} a_i\alpha_k^i$. Le fait que σ_k laisse $\mathbf{Q}$ invariant et est un morphisme additif est immédiat. On vérifie le caractère multiplicatif : soit $\theta_1 = P_1(\alpha)$ et $\theta_2 = P_2(\alpha)$ deux éléments de $\mathbf{Q}(\alpha)$, où P_1 et P_2 sont deux polynômes de $\mathbf{Q}_{d-1}[X]$. Soit $P_1P_2 = Q\pi_\alpha + R$ la division euclidienne de P_1P_2 par π_α. On a $\sigma_k(\theta_1\theta_2) = \sigma_k(P_1P_2(\alpha)) = \sigma_k(R(\alpha)) = R(\alpha_k)$. Par ailleurs, $\sigma_k(\theta_1)\sigma_k(\theta_2) = P_1(\alpha_k)P_2(\alpha_k)$, aussi égal à $R(\alpha_k)$. L'application σ_k est bien un morphisme de $\mathbf{Q}$-algèbres.

3. (a) L'extension $\mathbf{Q}(\theta)/\mathbf{Q}$ est de degré fini puisque $\mathbf{Q}(\theta) \subseteq \mathbf{K}$. Donc l'élément θ est algébrique sur $\mathbf{Q}$.

   (b) On note, pour $1 \leqslant k \leqslant d$, $\alpha_k = \sigma_k(\alpha)$. Comme $\theta \in \mathbf{Q}(\alpha)$, il existe $P \in \mathbf{Q}[X]$ tel que $\theta = P(\alpha)$. On a alors pour tout $1 \leqslant k \leqslant d$, $\sigma_k(\theta) = \sigma_k(P(\alpha)) = P(\sigma_k(\alpha)) = P(\alpha_k)$, et en appliquant la question 4(e) de la partie 1, on conclut que $P_\theta \in \mathbf{Q}[X]$.

(c) On note d'abord que θ est une racine de P_θ puisque l'un des σ_k (celui qui envoie α sur α) est l'identité. Il s'ensuit que π_θ divise P_θ, et comme π_θ est irréductible, on peut écrire $P_\theta = \pi_\theta^m Q$ avec $m \in \mathbf{N}^*$ et $Q(\theta) \neq 0$ dans l'anneau factoriel $\mathbf{Q}[X]$.
Il s'agit à présent de montrer que le polynôme Q est constant, comme P_θ et π_θ sont unitaires, on aura $Q = 1$. Si Q n'est pas constant, il admet une racine qui ne peut être que l'un des $\sigma_k(\theta)$. Or $\sigma_k(\theta) = \sigma_k(P(\alpha)) = P(\sigma_k(\alpha)) = P(\alpha_k)$. Il s'en suit que α_k est racine du polynôme $Q \circ P \in \mathbf{Q}[X]$. Donc α est également racine de $Q \circ P$ puisque les α_k sont conjugués. Ainsi, $\theta = P(\alpha)$ est racine de Q, ce qui entraîne que π_θ divise Q, contradictoire avec l'hypothèse.

4. Soit α un nombre algébrique. Si le polynôme minimal de α est à coefficients entiers, α est bien un entier algébrique.
Réciproquement, on suppose que α soit un entier algébrique. Il existe un polynôme $P \in \mathbf{Z}[X]$ unitaire qui annule α. On a donc $\pi_\alpha \mid P$ dans $\mathbf{Q}[X]$. On écrit $P = \pi_\alpha Q$. D'après le lemme de Gauss, il existe $r \in \mathbf{Q}^*$ tel que $r\pi_\alpha \in \mathbf{Z}[X]$ et $\frac{1}{r}Q \in \mathbf{Z}[X]$. En considérant les coefficients dominants, du fait que P et π_α sont unitaires, on obtient que $r \in \mathbf{Z}$, puis que $r = \pm 1$. On conclut que $\pi_\alpha \in \mathbf{Z}[X]$.

5. (a) Si α est un entier algébrique, et si d est le degré de son polynôme minimal, alors en effectuant la division euclidienne de X^n par π_α dans $\mathbf{Z}[X]$ (cf. I.1), on obtient que pour tout $n \in \mathbf{N}$, α^n est une combinaison linéaire à coefficients entiers des $1, \alpha, \ldots, \alpha^{d-1}$, qui est donc une partie génératrice finie du groupe G engendré par les puissances de α.

(b) Réciproquement, on suppose que le groupe G engendré par les puissances de α est de type fini. On note $(g_1, \ldots, g_n)$ une partie génératrice de ce groupe. Pour tout $i \in [\![1, n]\!]$, $\alpha g_i \in G$, donc il existe des entiers $a_{ij} \in \mathbf{Z}$ tels que

$$\alpha g_i = \sum_{j=1}^{n} a_{ij} g_j,$$

ce qui se réécrit en un système

$$\begin{cases} (a_{1,1} - \alpha)g_1 + a_{1,2}g_2 + \cdots + a_{1,n}g_n = 0 \\ \vdots \\ a_{n,1}g_1 + \cdots + a_{n,n-1}g_{n-1} + (a_{n,n} - \alpha)g_n = 0 \end{cases}$$

Le déterminant de ce système est nul puisqu'il existe une solution non triviale $(g_1, \ldots, g_n)$. Ce déterminant est de la forme $\det(A - \alpha I_n)$ avec $A = (a_{ij}) \in \mathcal{M}_n(\mathbf{Z})$, et χ_A est un polynôme unitaire de $\mathbf{Z}[X]$ qui annule α.

6. On a évidemment $1 \in \mathfrak{O}_\mathbf{C}$; soit $\alpha, \beta \in \mathfrak{O}_\mathbf{C}$. Il s'agit de vérifier que $\alpha - \beta$ et $\alpha\beta$ sont encore dans $\mathfrak{O}_\mathbf{C}$. Pour cela, on utilise la caractérisation des entiers algébriques de la question précédente. Soit (g_i) une famille génératrice finie du groupe engendré par les puissances de α, et (g'_j) une famille génératrice finie du groupe engendré par les puissances de β. Les puissances de $\alpha - \beta$ et de $\alpha\beta$ sont des combinaisons linéaires à coefficients entiers des $\alpha^i\beta^j$, donc des combinaisons linéaires à coefficients entiers des $g_i g'_j$. Le groupe engendré par les puissances de $\alpha - \beta$ et celui engendré par les puissances de $\alpha\beta$ sont donc contenus dans celui engendré par les $g_i g'_j$, ce qui prouve qu'ils sont de type fini.

7. L'inclusion $\mathbf{Z} \subseteq \mathfrak{O}_\mathbf{C} \cap \mathbf{Q}$ est claire. Réciproquement, soit $\alpha \in \mathfrak{O}_\mathbf{C} \cap \mathbf{Q}$. Le polynôme minimal de α (sur $\mathbf{Q}$) est donc $X - \alpha$. On conclut avec II.4 que $\alpha \in \mathbf{Z}$.

$\mathbf{Q}(\zeta)$ et $\mathbf{Z}[\zeta]$

1. (a) Un tel $\mathbf{Q}$-morphisme σ_k est entièrement déterminé par l'image de ζ (cf. II 2(b)). Or ζ s'envoie sur l'un de ses conjugués, c'est-à-dire l'un des ζ^k, $1 \leqslant k \leqslant p-1$, puisque le polynôme minimal de ζ est $\Phi_p = \prod_{k=1}^{p-1}(X - \zeta^k)$.

(b) i. $\mathrm{N}(\zeta)$ est le coefficient constant de Φ_p, donc $\mathrm{N}(\zeta) = 1$ et $\mathrm{Tr}(\zeta)$ est l'opposé du coefficient en X^{p-2}, à savoir -1.

ii. $\mathrm{N}(1-\zeta) = \prod_{k=1}^{p-1}(1-\zeta^k) = \Phi_p(1) = p$. De même,

$$\mathrm{N}(1+\zeta) = \prod_{k=1}^{p-1}(1+\zeta^k) = \prod_{k=1}^{p-1}(-1-\zeta^k) = \Phi_p(-1) = 1.$$

2. Soit $\theta \in \mathbf{Z}[\zeta]$. Il existe donc $P \in \mathbf{Z}[X]$ tel que $\theta = P(\zeta)$ et on conclut avec II.6 que $\theta \in \mathfrak{O}_{\mathbf{C}} \cap \mathbf{K} = \mathfrak{O}_{\mathbf{K}}$.

3. On établit deux résultats préalables, qui seront utiles dans la suite de cette partie : pour tout $z \in \mathbf{Z}[\zeta]$, on a $\mathrm{N}(z) \in \mathbf{Z}$. En effet, si $z \in \mathbf{Z}[\zeta]$, d'après la question précédente, z est un entier algébrique ; d'après II.4, son polynôme minimal est à coefficients entiers et en utilisant II.3(c), on obtient que le polynôme $\prod_{k=1}^{p-1}(X - \sigma_k(z))$ est à coefficients entiers, donc $\mathrm{N}(z)$, qui est le coefficient constant de ce polynôme, est un entier. De même pour $\mathrm{Tr}(z)$.

   Le deuxième résultat est la multiplicativité de la norme N : elle découle immédiatement du fait que les σ_k sont des morphismes multiplicatifs.

   (a) On a $\mathrm{N}(z) \in \mathbf{Z}$. Si z est inversible, il existe $z' \in \mathbf{Z}[\zeta]$ tel que $zz' = 1$ et en passant à la norme, on trouve que $\mathrm{N}(z)$ est inversible dans $\mathbf{Z}$, donc $\mathrm{N}(z) = \pm 1$. Réciproquement, si $\mathrm{N}(z) = \pm 1$, on a $\prod_{k=1}^{p-1}\sigma_k(z) = \pm 1$, où chaque $\sigma_k(z)$ est dans $\mathbf{Z}[\zeta]$, et l'un des morphismes σ_k est l'identité, donc z est inversible dans $\mathbf{Z}[\zeta]$.

   (b) Soit $x, y \in \mathbf{Z}[\zeta]$ tels que $z = xy$. En passant à la norme, il vient $\mathrm{N}(z) = \mathrm{N}(x)\,\mathrm{N}(y)$; or $\mathrm{N}(z)$ est un nombre premier, donc $\mathrm{N}(x) = \pm 1$ ou $\mathrm{N}(y) = \pm 1$, c'est-à-dire x ou y est inversible.

4. (a) Comme l'extension $\mathbf{K}/\mathbf{Q}$ est de degré $p-1$ sur $\mathbf{Q}$, on déduit de II.1(b) que G est un ensemble fini.

   L'ensemble G est clairement un sous-groupe de $\mathbf{U}_n$, le groupe des racines n-ièmes de l'unité dans $\mathbf{C}$; il est donc cyclique.

   (b) L'ensemble $\{\pm\zeta^k,\ 0 \leqslant k \leqslant p-1\}$ est un sous-groupe de G de cardinal $2p$ (ses éléments sont bien 2 à 2 distincts, car si $\zeta^k = -\zeta^\ell$, alors -1 est dans le groupe engendré par ζ, ce qui est absurde puisque -1 est d'ordre 2 et le groupe engendré par ζ est d'ordre p impair), donc d'après le théorème de Lagrange, $2p \mid n$. On a $\mathbf{Q}(\omega) \subseteq K = \mathbf{Q}(\zeta)$ et comme ζ est une racine de l'unité de $\mathbf{K}$, il existe $k \in \mathbf{N}$ tel que $\zeta = \omega^k$ donc $\mathbf{Q}(\zeta) \subseteq \mathbf{Q}(\omega)$. Finalement $\mathbf{Q}(\omega) = \mathbf{Q}(\zeta)$.

   (c) L' élément ω étant une racine primitive n-ième de l'unité, l'extension de corps $\mathbf{Q}(\omega)/\mathbf{Q}$ est de degré $\varphi(n)$. On en déduit avec la question précédente que $\varphi(n) = p-1$. En écrivant $n = 2p \times m$, on montre que nécessairement $m = 1$ pour avoir $\varphi(n) = p-1$. En effet, si $m > 1$ est premier avec $2p$, alors $\varphi(n) = (p-1)\varphi(m) > p-1$, et si $2 \mid m$ ou $p \mid m$, on aboutit également à $\varphi(n) > p-1$.

   En définitive, $n = 2p$ donc il y a exactement $2p$ racines de l'unité dans $\mathbf{K}$ qui sont les $\pm\zeta^k$ avec $k \in \{0, \ldots, p-1\}$.

5. (a) Soit $x \in \langle\lambda\rangle \cap \mathbf{Z}$. Alors d'une part $\mathrm{N}(x) = x^{p-1}$ puisque $x \in \mathbf{Z}$, et d'autre part, d'après III.1(b), $p = \mathrm{N}(\lambda) \mid \mathrm{N}(x)$ puisque N est multiplicatif. On en déduit que $p \mid x$, c'est-à-dire $x \in p\mathbf{Z}$. Réciproquement, on a $p\mathbf{Z} \subseteq \mathbf{Z}$ et $p\mathbf{Z} \subseteq \langle\lambda\rangle$ (car $p = \lambda\prod_{k=2}^{p-1}(1-\zeta^k)$) donc $p\mathbf{Z} \subseteq \mathbf{Z} \cap \langle\lambda\rangle$.

   (b) Soit $k \in [\![1, p-1]\!]$; alors k est inversible dans $\mathbf{Z}/p\mathbf{Z}$, donc il existe $k' \in \mathbf{Z}$ tel que $kk' = 1 \pmod p$. On écrit alors

$$\frac{1-\zeta}{1-\zeta^k} = \frac{1-(\zeta^k)^{k'}}{1-\zeta^k} = 1 + \zeta^k + \cdots + (\zeta^k)^{k'-1} \in \mathbf{Z}[\zeta].$$

On a aussi $\frac{1-\zeta^k}{1-\zeta} = 1+\zeta+\cdots+\zeta^{k-1} \in \mathbf{Z}[\zeta]$. Ainsi, $\frac{1-\zeta}{1-\zeta^k} \in \mathbf{Z}[\zeta]^\times$.

On rappelle que $p = (1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{p-1})$. Pour tout $k \in [\![1, p-1]\!]$, on peut écrire $1-\zeta = \frac{1-\zeta}{1-\zeta^k}(1-\zeta^k)$, donc $1-\zeta \sim 1-\zeta^k$. Il s'ensuit que $\langle p\rangle = \langle (1-\zeta)^{p-1}\rangle = \langle \lambda^{p-1}\rangle$.

(c) Le morphisme ψ est surjectif comme composée de $\mathbf{Z}[X] \to \mathbf{Z}[\zeta]$ et $\mathbf{Z}[\zeta] \to \mathbf{Z}[\zeta]/\langle\lambda\rangle$ qui sont surjectifs. Son image est donc $\mathbf{Z}[\zeta]/\langle\lambda\rangle$.

Soit $P \in \mathbf{Z}[X]$. On a $P \in \ker\psi$ si et seulement si $P(\zeta) = 0 \pmod{\langle\lambda\rangle}$. On montre que ceci équivaut à $P(1) = 0 \pmod{p\mathbf{Z}}$.

Si $P(\zeta) = 0 \pmod{\langle\lambda\rangle}$, alors $P(1) = 0 \pmod{\langle\lambda\rangle}$ puisque $\zeta = 1 \pmod{\langle\lambda\rangle}$. En passant à la norme, on obtient $P(1)^{p-1} = 0 \pmod{p\mathbf{Z}}$ (en se rappelant que $\mathrm{N}(\lambda) = p$), donc $P(1) = 0 \pmod{p\mathbf{Z}}$.

Réciproquement, si $P(1) = 0 \pmod{p\mathbf{Z}}$, on a *a fortiori* $P(1) = 0 \pmod{\langle\lambda\rangle}$ car $p \in \langle\lambda\rangle$, et donc $P(\zeta) = 0 \pmod{\langle\lambda\rangle}$ puisque $\zeta = 1 \pmod{\langle\lambda\rangle}$.

(d) D'après le premier théorème d'isomorphisme, l'anneau $\mathbf{Z}[\zeta]/\langle\lambda\rangle$ est isomorphe à $\mathbf{Z}[X]/\ker\psi$. Ce dernier anneau est isomorphe à $\mathbf{F}_p$ en appliquant le même théorème d'isomorphisme à $\mathbf{Z}[X] \to \mathbf{F}_p,\ P \mapsto P(1) \pmod{p\mathbf{Z}}$.

(e) Comme l'anneau quotient $\mathbf{Z}[\zeta]/\langle\lambda\rangle$ est un corps, l'idéal $\langle\lambda\rangle$ est maximal, en particulier premier.

6. (a) i. On a pour tout $1 \leqslant k \leqslant d$, $|a_k| = \left|\sum_{I\in\mathcal{P}_{d-k}(\{1,\dots,d\})} \prod_{i\in I} \alpha_i\right|$, où $\mathcal{P}_{d-k}(\{1,\dots,d\})$ est l'ensemble des parties à $d-k$ éléments de $\{1,\dots,d\}$. Le cardinal de cet ensemble étant égal à $\binom{d}{d-k} = \binom{d}{k}$, on conclut par inégalité triangulaire que $|a_k| \leqslant \binom{d}{k}$.

Un entier algébrique α de degré d dont tous les conjugués sont de module 1 a un polynôme minimal $P \in \mathbf{Z}[X]$ unitaire dont les coefficients sont bornés par $M = \max_{0\leqslant k\leqslant d}\binom{d}{k}$. Il n'y a qu'un nombre fini d'entiers qui vérifient cette propriété, donc il n'y a qu'un nombre fini de tels polynômes et par suite, un nombre fini de tels entiers algébriques.

ii. On fixe $k \in [\![1, d]\!]$. Pour tout $n \in \mathbf{N}^*$, le polynôme $P_n = \prod_{i=1}^d (X - \alpha_i^n)$ est dans $\mathbf{Z}[X]$ d'après I.4(e). De plus, P_n est unitaire, de degré d et ses racines sont de module 1. On en déduit que α_k^n est algébrique de degré inférieur ou égal à d et que ses conjugués (qui sont parmi les α_i^n) sont de module 1. D'après la question précédente, il y a un nombre fini d'entiers algébriques de degré d, donc aussi un nombre fini d'entiers algébriques de degré inférieur ou égal à d. La famille $(\alpha_k^n)_{n\in\mathbf{N}}$ est donc finie, ce qui entraîne l'existence de deux entiers n et m avec $n \neq m$ tels que $\alpha_k^n = \alpha_k^m$. On conclut que α_k est une racine de l'unité.

(b) Soit $P \in \mathbf{Z}[X]$ tel que $u = P(\zeta)$. Les conjugués de u sont les $\sigma_k(u)$, où σ_k est le $\mathbf{Q}$-morphisme de $\mathbf{Q}(\zeta)$ dans $\mathbf{C}$ défini par $\sigma_k(\zeta) = \zeta^k$. On a donc $\sigma_k(u) = P(\zeta^k) = u_k$. De plus, u étant une unité, on a $\mathrm{N}(u) = \pm 1 = \prod_{k=1}^{p-1} u_k$, ce qui montre que les u_k sont des unités.

(c) Soit $k \in [\![1, p-1]\!]$; $u_{p-k} = P(\zeta^{p-k}) = P(\zeta^{-k})$. Sachant que $\overline{\zeta} = \zeta^{-1}$, on a $u_{p-k} = P(\overline{\zeta}^k) = \overline{P(\zeta^k)} = \overline{u_k}$. Donc $\frac{u_k}{u_{p-k}}$ est de module 1. L'élément $\frac{u_1}{u_{p-1}}$ fait partie du groupe $\mathbf{Z}[\zeta]^\times$, c'est en particulier un entier algébrique. Ses conjugués sont les

$$\sigma_k\left(\frac{u_1}{u_{p-1}}\right) = \frac{\sigma_k(u)}{\sigma_k(u_{p-1})} = \frac{u_k}{P(\sigma_k(\zeta^{-1}))} = \frac{u_k}{P(\zeta^{p-k})} = \frac{u_k}{u_{p-k}}.$$

(d) D'après la question 6(a)ii, $\frac{u}{u_{p-1}}$ est une racine de l'unité de $\mathbf{K}$. On en déduit avec III.4 qu'il existe $m \in \mathbf{Z}$ tel que $\frac{u}{u_{p-1}} = \pm\zeta^m$.

(e) i. Il existe des entiers $a_0, \dots, a_{p-2}$ tels que $\theta = \sum_{k=0}^{p-2} a_k\zeta^k$. Or pour tout k, $\zeta^k = 1 \pmod{\langle\lambda\rangle}$ puisque $\zeta = 1 \pmod{\langle\lambda\rangle}$. On en déduit que $\theta = \sum_{k=0}^{p-2} a_k \pmod{\langle\lambda\rangle}$ et en posant $a = \sum_{k=0}^{p-2} a_k \in \mathbf{Z}$, on a bien $\theta = a \pmod{\langle\lambda\rangle}$.

Soit $\theta \in \mathbf{Z}[\zeta]$ et $\sigma_k(\theta)$ l'un de ses conjugués ; en notant $\theta = \sum_{i=0}^{p-2} a_i\zeta^i$, on a $\sigma_k(\theta) = \sum_{i=0}^{p-2} a_i\zeta^{ik}$, donc θ et $\sigma_k(\theta)$ sont congrus tous les deux à $a = \sum_{i=0}^{p-2} a_i$ modulo $\langle\lambda\rangle$.

ii. On suppose que $u = -u_{p-1}\zeta^m$. On aurait alors $u = -u_{p-1} \pmod{\langle\lambda\rangle}$ et aussi $u = u_{p-1} \pmod{\langle\lambda\rangle}$ d'après la question précédente, d'où $2u = 0 \pmod{\langle\lambda\rangle}$. On a démontré que l'idéal $\langle\lambda\rangle$ est premier, donc on a soit $2 \in \langle\lambda\rangle$, soit $u \in \langle\lambda\rangle$. Si l'on avait $2 \in \langle\lambda\rangle$, en prenant la norme on obtiendrait $p \mid 2$, ce qui est absurde. On a donc nécessairement $u \in \langle\lambda\rangle$. Or u est une unité donc $\mathrm{N}(u) = \pm 1$ et en prenant une nouvelle fois la norme, on aurait $p \mid 1$, ce qui est absurde. En définitive, on a $u = +u_{p-1}\zeta^m$.

(f) Si m est pair, l'existence de r est immédiate, et si m est impair, $m+p$ est pair, d'où l'existence de r dans ce cas. Le fait que ϵ est une unité découle immédiatement de la structure de groupe multiplicatif de $\mathbf{Z}[\zeta]^\times$.

De plus,

$$\overline{\epsilon} = \zeta^r\overline{u} = \zeta^r u_{p-1} = \zeta^r\zeta^{-m}u = \zeta^r\zeta^{-2r}u = \zeta^{-r}u = \epsilon,$$

donc $\epsilon \in \mathbf{R}$.

Réciproquement, tout élément de la forme $\zeta^r\epsilon$ est bien inversible donc on a bien la structure voulue pour $\mathbf{Z}[\zeta]^\times$.

7. (a) Le raisonnement est le même qu'en III.3 : θ est un entier algébrique, donc son polynôme minimal est à coefficients entiers, et comme $P_\theta = \prod_{k=1}^{p-1}(X - \sigma_k(\theta))$ est une puissance de π_θ, la norme et la trace de θ sont des entiers.

(b) i. Soit $0 \leqslant k \leqslant p-2$; par linéarité de la trace, et en utilisant que pour tout $i \in \{1, \dots, p-2\}$, $\mathrm{Tr}(\zeta^i) = \mathrm{Tr}(\zeta) = -1$ (ces nombres étant conjugués) et $\mathrm{Tr}(1) = p-1$, il vient

$$b_k = \mathrm{Tr}(\theta\zeta^{-k} - \theta\zeta) = pa_k - (a_0 + \cdots + a_{p-2}) - (-a_0 - \cdots - a_{p-2}) = pa_k.$$

Par ailleurs, on a $\theta\zeta^{-k} - \theta\zeta \in \mathfrak{O}_\mathbf{K}$ (puisque $\mathfrak{O}_\mathbf{K}$ est un anneau) donc d'après III.7(a), on a $b_k \in \mathbf{Z}$.

ii. D'après la question précédente, $p\theta = \sum_{k=0}^{p-2} b_k\zeta^k = \sum_{k=0}^{p-2} b_k(1-\lambda)^k$. En développant par le binôme de Newton et par permutation d'indice, il vient

$$c_k = \sum_{j=k}^{p-2}(-1)^k\binom{j}{k}b_j \in \mathbf{Z}.$$

Comme $\lambda = 1 - \zeta$, on a aussi par symétrie des rôles

$$b_k = \sum_{j=k}^{p-2}(-1)^k\binom{j}{k}c_j \quad (1).$$

NB : l'énoncé comportait ici une erreur sur les noms d'indices, il fallait lire « $b_k = \sum_{\ell=k}^{p-2}(-1)^k\binom{\ell}{k}c_\ell$ ».

iii. On remarque d'abord que l'égalité $\mathrm{N}(1-\zeta) = p$ peut s'écrire

$$p = (1-\zeta)^{p-1}\prod_{i=1}^{p-1}\left(1 + \zeta + \cdots + \zeta^{i-1}\right),$$

qui est de la forme $p = \lambda^{p-1}\beta$ avec $\beta \in \mathbf{Z}[\zeta] \subseteq \mathfrak{O}_\mathbf{K}$. En regardant l'égalité

$$p\theta = \sum_{i=0}^{p-2} c_i\lambda^i \quad (2)$$

modulo l'idéal $\lambda\mathfrak{O}_\mathbf{K}$, on obtient donc $0 = c_0 \pmod{\lambda\mathfrak{O}_\mathbf{K}}$. En passant à la norme, on obtient que $p \mid c_0$.

On montre à présent par récurrence que pour tout $k \in [\![0, p-2]\!]$, $p \mid c_k$. Soit $k \in [\![0, p-2]\!]$ et on suppose que pour tout $i \leqslant k-1$, $p \mid c_i$. En considérant l'égalité (2) modulo $\lambda^{k+1}\mathfrak{O}_{\mathbf{K}}$, il vient $0 = c_k\lambda^k \pmod{\lambda^{k+1}\mathfrak{O}_{\mathbf{K}}}$. En effet, les entiers $c_i, i \leqslant k-1$ sont divisibles par p donc congrus à 0 modulo $\lambda^{k+1}\mathfrak{O}_{\mathbf{K}}$ et les $c_i\lambda^i$ pour $i \geqslant k+1$ sont aussi congrus à 0 modulo $\lambda^{k+1}\mathfrak{O}_{\mathbf{K}}$. On en déduit que $c_k = 0 \pmod{\lambda\mathfrak{O}_K}$, donc $p \mid c_k$. La récurrence est prouvée.

On déduit alors de l'égalité (1) que tous les b_k sont divisibles par p et en se rappelant que $b_k = pa_k$, on conclut finalement que $a_k \in \mathbf{Z}$.

Ainsi, $\theta \in \mathbf{Z}[\zeta]$, ce qui prouve l'inclusion $\mathfrak{O}_{\mathbf{K}} \subseteq \mathbf{Z}[\zeta]$. L'autre inclusion a été prouvée en III.2, donc on peut conclure que $\mathbf{Z}[\zeta] = \mathfrak{O}_{\mathbf{K}}$.

Le cas $p = 3$

1. Comme 3 ne divise pas x, on a $x = 1$ ou $x = -1 \pmod 3$. En élevant au cube une égalité de la forme $x = \pm 1 + 3k$, on trouve que $x^3 = \pm 1 \pmod 9$. De même pour y^3 et z^3. L'égalité $x^3 + y^3 + z^3 = 0 \pmod 9$ ne peut alors être vérifiée donc l'équation (1) n'a pas de solutions.
2. On a $3 = \mathrm{N}(\lambda) = (1-j)(1-j^2) = (1-j)^2(1+j)$. Comme $1+j$ est inversible, on conclut que $3 \sim \lambda^2$.
3. Soit $s = a + bj \in \mathbf{Z}[j]$. On a $s = (a+b) - b\lambda$, donc $s = a + b \pmod{\langle\lambda\rangle}$. Or $a+b$ est un entier relatif, donc congru à 0 ou $\pm 1 \pmod 3$, et comme $\lambda \mid 3$ (cf. question précédente), on a aussi $a + b = 0$ ou $\pm 1 \pmod{\langle\lambda\rangle}$. Ainsi, tout élément de $\mathbf{Z}[j]$ est congru à $0, 1$ ou $-1 \pmod{\langle\lambda\rangle}$.
   On suppose que $s = 1 \pmod{\langle\lambda\rangle}$. Il existe donc $\mu \in \mathbf{Z}[j]$ tel que $s - 1 = \mu\lambda$.

   $$s^3 - 1 = (s-1)(s-j)(s-j^2) = (s-1)(s-1+(1-j))(s-1+(1-j^2)) = \lambda^3\mu(\mu+1)(\mu+1+j).$$

   On remarque que $1 + j = -j^2 = (1-j^2) - 1 = (1+j)\lambda - 1$; comme μ est congru à l'un des entiers $0, 1$ ou $-1 \pmod{\langle\lambda\rangle}$, on a que $\mu(\mu+1)(\mu+1+j) = 0 \pmod{\langle\lambda\rangle}$, et on conclut.
   Le cas $s = -1 \pmod{\langle\lambda\rangle}$ se traite de manière analogue en partant de la factorisation $s^3 + 1 = (s+1)(s+j)(s+j^2)$.
4. On suppose (P_n) vérifiée pour un quadruplet $(\alpha, \beta, \delta, \omega)$. D'après la question précédente, comme α et β ne sont pas divisibles par λ, on a $\alpha^3 = \pm 1 \pmod{\langle\lambda^4\rangle}$ et $\beta^3 = \pm 1 \pmod{\langle\lambda^4\rangle}$. On en déduit que $\omega\lambda^{3n}\delta^3 = 0$ ou $\pm 2 \pmod{\langle\lambda^4\rangle}$. Comme λ ne divise pas ± 2 (la norme de λ vaut 3), on a nécessairement $\omega\lambda^{3n}\delta^3 = 0 \pmod{\langle\lambda^4\rangle}$. Comme $\lambda \nmid \delta$, on en déduit que $3n \geqslant 4$, donc $n \geqslant 2$.
5. On suppose (P_n) vérifiée pour un triplet (α, β, δ).
   (a) Immédiat par la factorisation $\alpha^3 + \beta^3 = (\alpha+\beta)(\alpha+j\beta)(\alpha+j^2\beta)$.
   (b) On rappelle que l'on a montré en partie 1 que l'anneau $\mathbf{Z}[j]$ est euclidien. Il est donc principal. De l'égalité $-\omega\lambda^{3n}\delta^3 = (\alpha+\beta)(\alpha+j\beta)(\alpha+j^2\beta)$, on déduit, puisque λ est irréductible, qu'il divise l'un des facteurs $\alpha+\beta$, $\alpha+j\beta$ ou $\alpha+j^2\beta$. Or, comme $1 = j = j^2 \pmod{\langle\lambda\rangle}$, on a $\alpha+\beta = \alpha+j\beta = \alpha+j^2\beta \pmod{\langle\lambda\rangle}$ donc λ divise chacun de ses facteurs.
   (c) On note γ un pgcd de $\alpha+\beta$ et $\alpha+j\beta$. D'après la question précédente, λ divise γ. La relation $(\alpha+\beta) - (\alpha+j\beta) = \lambda\beta$ montre que λ^2 ne divise pas γ puisque λ ne divise pas β. Enfin, λ est le seul facteur premier de γ : si $\mu \neq \lambda$ est premier et divise $\alpha+\beta$ et $\alpha+j\beta$, alors il divise $\alpha+\beta-(\alpha+j\beta) = \lambda\beta$ donc divise β et il divise aussi $j(\alpha+\beta)-(\alpha+j\beta) = -\lambda\alpha$ donc divise α, ce qui est absurde puisque l'on a supposé α et β premiers entre eux. On conclut qu'un pgcd de $\alpha+\beta$ et $\alpha+j\beta$ est λ.
   D'après la question précédente, on peut écrire l'égalité suivante dans $\mathbf{Z}[j]$:

   $$-\omega\lambda^{3(n-1)} = \frac{\alpha+\beta}{\lambda} \cdot \frac{\alpha+j\beta}{\lambda} \cdot \frac{\alpha+j^2\beta}{\lambda}. \quad (*)$$

D'après IV.4, on a nécessairement $n \geqslant 2$, donc λ divise le membre de droite de l'égalité (*). On a vu qu'un pgcd de $\alpha+\beta$ et $\alpha+j\beta$ est λ, et il en va de même pour $\alpha+\beta$ et $\alpha+j^2\beta$, ainsi que de $\alpha+j\beta$ et $\alpha+j^2\beta$. Donc seul l'un d'entre eux est divisible par λ^2.

(d) En multipliant les trois égalités qui définissent les κ_i, on obtient immédiatement $-\omega\delta^3 = \kappa_1\kappa_2\kappa_3$. Ainsi, $\kappa_1\kappa_2\kappa_3 \sim \delta^3$. Comme l'anneau $\mathbf{Z}[j]$ est factoriel (puisqu'euclidien), chacun des κ_i est associé à un cube.

(e) On écrit $\kappa_i = u_i\gamma_i^3$ avec u_i inversible. De $1+j+j^2=0$, on déduit que $(\alpha+\beta)+j(\alpha+j\beta)+j^2(\alpha+j^2\beta)=0$, soit $\lambda^{3n-2}u_1\gamma_1^3 + j\lambda u_2\gamma_2^3 + j^2\lambda u_3\gamma_3^3 = 0$. En simplifiant par λ et en multipliant par $(ju_2)^{-1}$, on obtient une égalité de la forme

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

avec $\tau, \tau' \in \mathbf{Z}[j]^\times$.

(f) Comme λ ne divise pas $\kappa_1\kappa_2\kappa_3$, λ ne divise pas $\gamma_1\gamma_2\gamma_3$. De plus, γ_2 et γ_3 sont premiers entre eux parce que κ_2 et κ_3 le sont. On suppose que $\tau = 1$: alors $\gamma_2^3+\gamma_3^3+\tau'\lambda^{3(n-1)}\gamma_1^3 = 0$, donc (P_{n-1}) est vérifiée.

On suppose que $\tau = -1$: alors $\gamma_2^3 + (-\gamma_3)^3 + \tau'\lambda^{3(n-1)}\gamma_1^3 = 0$, donc (P_{n-1}) est vérifiée.

(g) Sachant que les inversibles de $\mathbf{Z}[j]$ sont ± 1, $\pm j$ et $\pm j^2$, il reste à examiner les cas $\tau = \pm j$ et $\tau = \pm j^2$. D'après IV.3, on a $\gamma_2^3 = \pm 1 \pmod{\langle\lambda^4\rangle}$ et $\gamma_3^3 = \pm 1 \pmod{\langle\lambda^4\rangle}$ puisque λ ne divise pas $\gamma_2\gamma_3$. Par ailleurs, comme (P_n) est supposée vraie, on a $n \geqslant 2$ donc $\gamma_2^3 + \tau\gamma_3^3 = 0 \pmod{\langle\lambda^3\rangle}$. On en déduit que $\pm 1 \pm \tau = 0 \pmod{\langle\lambda^3\rangle}$. Or $\pm 1 \pm j$ et $\pm 1 \pm j^2$ ne sont pas multiples de λ^3 (passer à la norme), donc on ne peut avoir $\tau = \pm j$ ni $\tau = \pm j^2$.

6. La question IV.5 a montré que si (P_n) est vérifiée, alors (P_{n-1}) est vérifiée. Ceci conduit à une contradiction puisque si l'on suppose que (P_n) est vérifiée pour un $n \geqslant 2$, on obtient par récurrence descendante que (P_1) est vérifiée, ce qui est faux d'après IV.4. Finalement, l'équation (1) n'a pas de solutions non triviales dans le cas $3 \mid xyz$.

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

1. L'égalité $x^p + y^p = (-z)^p$ se factorise dans $\mathbf{Z}[\zeta]$ en

$$\prod_{k=0}^{p-1}(x+\zeta^k y) = (-z)^p.$$

Si $\alpha, \beta \in \mathbf{Z}[\zeta]$, on vérifie facilement que $\langle\alpha\beta\rangle = \langle\alpha\rangle\langle\beta\rangle$. En passant aux idéaux, on obtient

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

2. (a) Comme $\mathfrak{P}$ divise $\langle x+\zeta^k y\rangle$ et $\langle x+\zeta^l y\rangle$, il divise l'idéal engendré par $(x+\zeta^l y)-(x+\zeta^k y)$. Or on a $(x+\zeta^l y)-(x+\zeta^k y) = y\zeta^k(\zeta^{l-k}-1)$; de plus ζ^k est une unité, et $\zeta^{l-k}-1 \sim \zeta-1 = -\lambda$ (cf. III.5) donc $\mathfrak{P}$ divise l'idéal engendré par λy.

(b) Comme l'idéal $\mathfrak{P}$ est premier, on a $\lambda \in \mathfrak{P}$ ou $y \in \mathfrak{P}$. On suppose que $y \in \mathfrak{P}$; d'après la question 1, $\mathfrak{P}$ divise $\langle z^p\rangle$, donc on aurait $z \in \mathfrak{P}$. Or y et z sont premiers entre eux donc d'après l'identité de Bézout, il existe $u, v \in \mathbf{Z}$ tels que $uy + vz = 1$, ce qui implique que $1 \in \mathfrak{P}$, absurde.

On a donc $\lambda \in \mathfrak{P}$, donc $\langle\lambda\rangle = \mathfrak{P}$ puisque $\langle\lambda\rangle$ est premier (cf. III.5). Or $x+y = x+\zeta^k y \pmod{\langle\lambda\rangle}$ (on se rappelle que $\zeta^k = 1 \pmod{\langle\lambda\rangle}$) et par définition de $\mathfrak{P}$, $x+\zeta^k y = 0 \pmod{\langle\lambda\rangle}$. Donc $x+y = 0 \pmod{\langle\lambda\rangle}$. On a donc $x+y \in \mathbf{Z} \cap \langle\lambda\rangle = p\mathbf{Z}$ (cf. III.5(a)). Or $x^p+y^p+z^p = 0$, d'où l'on déduit avec le petit théorème de Fermat que $z^p = -(x+y) \pmod{p\mathbf{Z}} = 0 \pmod{p\mathbf{Z}}$. Ainsi, $p \mid z$, ce qui est contraire à nos hypothèses.

3. D'après l'égalité de la question 1, comme les idéaux $\langle x+\zeta^k y\rangle$ sont 2 à 2 premiers entre eux et qu'il y a unicité de la décomposition des idéaux en idéaux premiers dans $\mathbf{Z}[\zeta]$, chaque idéal $\langle x+\zeta^k y\rangle$ est une puissance p-ième d'un idéal, c'est en particulier vrai pour $\langle x+\zeta y\rangle$.
4. D'après l'hypothèse de régularité sur le nombre premier p, comme l'idéal I^p est principal, l'idéal I est aussi principal. Ainsi, il existe $\alpha\in\mathbf{Z}[\zeta]$ tel que $\langle x+\zeta y\rangle=\langle\alpha^p\rangle$, c'est-à-dire il existe $u\in\mathbf{Z}[\zeta]^\times$ tel que $x+\zeta y=u\alpha^p$. D'après la structure de $\mathbf{Z}[\zeta]^\times$ (cf. Partie III), on peut écrire u sous la forme $u=\zeta^r\epsilon$ avec $r\in\mathbf{Z}$ et ϵ une unité réelle.
5. On écrit $\alpha=a_0+a_1\zeta+\cdots+a_{p-2}\zeta^{p-2}\in\mathbf{Z}[\zeta]$. Pour tout k, $\zeta^k=1 \pmod{\langle\lambda\rangle}$, donc $\alpha=a_0+a_1+\cdots+a_{p-2} \pmod{\langle\lambda\rangle}$. On note $b=a_0+a_1+\cdots+a_{p-2}\in\mathbf{Z}$. On a $\alpha^p-b^p=\prod_{k=0}^{p-1}(\alpha-\zeta^k b)$. Chacun des facteurs $\alpha-\zeta^k b$ est congru à $\alpha-b \pmod{\langle\lambda\rangle}$, donc à $0 \pmod{\langle\lambda\rangle}$. En multipliant ces congruences, on obtient $\alpha^p-b^p=0 \pmod{\langle\lambda^p\rangle}$. D'après III.5(b), on a $\langle\lambda^{p-1}\rangle=\langle p\rangle$, donc $\alpha^p=b^p \pmod{\langle p\rangle}$ et $a=b^p$ convient.

   On peut donc écrire $x+\zeta y=\zeta^r\epsilon a \pmod{\langle p\rangle}$, puis, en multipliant par ζ^{-r}, $\zeta^{-r}(x+\zeta y)=\epsilon a \pmod{\langle p\rangle}$. En conjugant cette égalité, on obtient $\zeta^r(x+\zeta^{-1}y)=\epsilon a \pmod{\langle p\rangle}$, ce qui conduit en éliminant ϵa à l'égalité

$$x\zeta^{-r}+y\zeta^{1-r}-x\zeta^r-y\zeta^{r-1}=0 \pmod{\langle p\rangle}.$$

6. On suppose que $r=0 \pmod p$. Alors $\zeta^r=1$ et l'égalité de la question précédente devient $y(\zeta-\zeta^{-1})=0 \pmod{\langle p\rangle}$, soit $y(1+\zeta)(1-\zeta)=0 \pmod{\langle p\rangle}$. Or $1+\zeta$ est une unité (d'après III.1.b(ii) et III.3(a)), donc $\lambda y=0 \pmod{\langle p\rangle}$. On en déduit que λ divise y dans $\mathbf{Z}[\zeta]$, puis, en passant à la norme, que p divise y, ce qui est contraire aux hypothèses.
7. D'après les deux questions précédentes, p ne divise aucun des entiers $\pm r,\pm(1-r)$. On écrit

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

   Si aucun des exposants $\pm r,\pm(1-r)$ n'était égal modulo p, comme $(1,\zeta,\dots,\zeta^{p-2})$ est une $\mathbf{Q}$-base de $\mathbf{Q}(\zeta)$ et que $\beta\in\mathbf{Z}[\zeta]$, on aurait en particulier $\frac{x}{p}\in\mathbf{Z}$, ce qui est contraire aux hypothèses. Donc deux de ces quatre exposants sont égaux modulo p, et comme $r\neq 0,1 \pmod{p\mathbf{Z}}$, ce ne peut être que r et $1-r$, autrement dit on a $2r=1 \pmod{p\mathbf{Z}}$.
8. On peut maintenant réécrire l'égalité de la question 7 :

$$\beta p\zeta^r=x+y\zeta-x\zeta-y=(x-y)\lambda.$$

   En prenant la norme, comme $p-1>2$, on obtient que $p\mid(x-y)$, c'est-à-dire $x=y \pmod{p\mathbf{Z}}$.
9. Par symétrie des rôles de x,y et z, on a aussi $y=z \pmod{p\mathbf{Z}}$. En considérant l'égalité $x^p+y^p+z^p=0$ modulo p, on obtient $3x^p=0 \pmod{p\mathbf{Z}}$, et comme $p>3$, $x=0 \pmod{p\mathbf{Z}}$, ce qui est contraire aux hypothèses.