Agrégation Externe 2019
Mathématiques Générales

Jérémy Le Borgne *
ENS Rennes

I Exercices préliminaires

1. On fixe $B \in \mathbb{Z}[X]$. On procède par récurrence sur $d = \deg A$ (éventuellement, $d = -\infty$ si $A = 0$). On suppose donc que pour pour tout polynôme P de degré $\leq d$, on peut écrire $P = QB + R$ avec $\deg R < \deg B$ (éventuellement $R = 0$).
Si $d \leq \deg B$, l'écriture $A = 0 \cdot B + A$ convient. Sinon, on note aX^d le terme dominant de A. On a $P = A - aX^{d-\deg B}B \in \mathbb{Z}[X]$, et $\deg P < d$. Par hypothèse de récurrence, il existe $Q, R \in \mathbb{Z}[X]$ avec $\deg R < \deg B$ tels que $P = QB + R$. Mais alors on a $A = (aX^{d-\deg B} + Q)B + R$, avec $X^{d-\deg B} + Q \in \mathbb{Z}[X]$ et $R \in \mathbb{Z}[X]$ de degré $< \deg B$, d'où le résultat.
2. **L'anneau** $\mathbb{Z}[j]$
   (a) On a $j^3 = 1$ donc j est algébrique de polynôme annulateur $X^3 - 1$. Comme $j \neq 1$, $X^2 + X + 1$ est annulateur de j. Ce polynôme est irréductible dans $\mathbb{Q}[X]$ (car il l'est dans $\mathbb{R}[X]$ puisque son discriminant -3 est strictement négatif). C'est donc le polynôme minimal de j.
   (b) Soit $P \in \mathbb{Z}[X]$. D'après la question 1., il existe $Q, R \in \mathbb{Z}[X]$ avec $\deg R < 2$ tels que $P = Q(X^2 + X + 1) + R$. En particulier, si on note $R = a + bX$, l'évaluation en j donne $P(j) = a + bj$. Ainsi, $\mathbb{Z}[j] = \{a + bj,\ a \in \mathbb{Z}, b \in \mathbb{Z}\}$.
   (c) Soit $z \in \mathbb{Z}[j]$. On a déjà $N(z) \geq 0$, il suffit donc de monter que $N(z) \in \mathbb{Z}$. Si $z = a + bj$, un calcul immédiat montre que $N(z) = a^2 + b^2 - ab \in \mathbb{Z}$, donc $N(z) \in \mathbb{N}$.
   Soit maintenant $z \in \mathbb{Z}[j]^\times$. Il existe $z' \in \mathbb{Z}[j]$ tel que $zz' = 1$. Comme N est multiplicative, on a $N(z)N(z') = 1$. Comme $N(z)$ et $N(z')$ sont dans $\mathbb{N}$, on a $N(z) = N(z') = 1$. On est donc ramené à résoudre l'équation $a^2 + b^2 - ab = 1$ avec $a, b \in \mathbb{Z}$. Soit $(a, b) \in \mathbb{Z}^2$ un couple solution. Quitte à échanger les rôles de a et b, on peut supposer que $a \geq b$. On a alors $(a - b)a + b^2 = 1$, donc $(a - b)a = 0$ et $b = \pm 1$, ou $(a - b)a = \pm 1$ et $b = 0$. Dans le premier cas, les seules solutions possibles sont : $(0, -1), (1, 1)$ et $(-1, -1)$. Le deuxième cas fournit $(1, 0)$. En échangeant les rôles de a et b, on obtient de plus $(-1, 0)$ et $(0, 1)$. Ce sont donc les six solutions possibles à cette équation, qui correspondent aux éléments de $\mathbb{Z}[j]$: $1, j + 1, j, -1, -1 - j, -j$, qui sont les racines sixièmes de l'unité donc inversibles dans $\mathbb{Z}[j]$.

*Pour toute question ou remarque, jeremy.leborgne@ens-rennes.fr

(d) Il suffit de montrer que si $z \in \mathbb{C}$, il existe $q \in \mathbb{Z}[j]$ tel que $N(z-q) < 1$. Soit $z \in \mathbb{C}$. Comme $\{1, j\}$ est une base de $\mathbb{C}$ on peut écrire $z = u+jv$. Si $a, b \in \mathbb{Z}$ et $q = a+jb$, on a $z-q = (u-a)+(v-b)j$. On a a lors $N(z-q) = (u-a)^2+(v-b)^2-(u-a)(v-b)$. Soit a (resp. b) l'entier le plus proche de u (resp. de v). Alors $|u-a| \leq 1/2$, $|v-b| \leq 1/2$, et $(u-a)(v-b) \geq -1/4$. Ainsi, pour ce choix de q, on a $N(z-q) \leq 1/4 < 1$. Soient maintenant $x, y \in \mathbb{Z}[j]$ avec $y \neq 0$. D'après ce qui précède, on peut écrire $x = qy+r$ avec $N(r) < N(y)$. Cela montre que $\mathbb{Z}[j]$ est euclidien pour le stathme N.

3. **Polynômes cyclotomiques**

(a) Soit μ une racine n-ème de l'unité. D'après le théorème de Lagrange, l'ordre de μ divise n. Par ailleurs, μ est d'ordre d si et seulement si μ est une racine primitive d-ème. Par unicité de l'ordre, on a donc $\mu_n = \sqcup_{d|n} \mu_d^*$. Ainsi,

$$\prod_{\mu \in \mu_n} (X - \mu) = \prod_{d|n} \Phi_d(X).$$

Enfin, les racines n-èmes sont précisément les n racines de $X^n - 1$, qui sont distinctes car $X^n - 1$ est premier avec son polynôme dérivé nX^{n-1}. Le membre de gauche est donc égal à $X^n - 1$, d'où le résultat.

(b) On procède par récurrence (forte) sur n. Si $n = 1$, $\Phi_n = X - 1 \in \mathbb{Z}[X]$. Supposons le résultat vrai pour tout $d < n$. Notons $B = \prod_{d|n, d<n} \Phi_d$. Le polynôme B est unitaire et, par hypothèse de récurrence, $B \in \mathbb{Z}[X]$. Par division euclidienne dans $\mathbb{Z}$, $X^n - 1 = QB + R$ avec $R = 0$ ou $\deg R < \deg P$. D'autre part, la division euclidienne dans $\mathbb{C}[X]$ s'obtient directement vu relation précédente : $X^n - 1 = \Phi_n B$. Par unicité de la division euclidienne dans $\mathbb{C}$, on a donc $Q = \Phi_n$ et $R = 0$. Cela montre en particulier que $\Phi_n \in \mathbb{Z}[X]$.

(c) i. Comme $\mathbb{F}_p[X]$ est de caractéristique p, l'élévation à la puissance p y est un morphisme d'anneaux. En particulier, $(\hat{\pi}(X) - \hat{\pi}(1))^p = \hat{\pi}(X)^p - \hat{\pi}(1)^p = \hat{\pi}(X)^p - \pi(1)$. Comme $\hat{\pi}$ est un morphisme, on a $\hat{\pi}(X^p - 1) = \hat{\pi}(X)^p - 1_{\mathbb{F}_p}$.

ii. On suppose que $X^p - 1 = PQ$ avec P, Q unitaires non constants. On a alors $\hat{\pi}(P)\hat{\pi}(Q) = (\hat{\pi}(X) - 1_{\mathbb{F}_p})^p$. Comme $\mathbb{F}_p[X]$ est factoriel, on a $\hat{\pi}(P) = (\hat{\pi}(X) - 1_{\mathbb{F}_p})^{\deg P}$ et $\hat{\pi}(Q) = (\hat{\pi}(X) - 1_{\mathbb{F}_p})^{\deg Q}$. En particulier, il existe $F, G \in \mathbb{Z}[X]$ tels que $P = (X-1)^{\deg P} + pF(X)$ et $Q = (X-1)^{\deg Q} + pG(X)$. L'évaluation en 1 montre que $P(1)$ et $Q(1)$ sont divisibles par p.

iii. Supposons que $\Phi_p = AB$ avec $A, B \in \mathbb{Q}[X]$ non constants. D'après le lemme de Gauss, il existe $r \in \mathbb{Q}^\times$ tel que $P = rA \in \mathbb{Z}[X]$ et $Q = r^{-1}B \in \mathbb{Z}[X]$. Enfin, comme Φ_P est unitaire, on peut supposer que P et Q le sont (quitte à multiplier P et Q par -1). On a alors $X^p - 1 = (X-1)P(X) \cdot Q(X)$, avec $(X-1)P$ et Q unitaires non constants. Ainsi, d'après la question précédente, $p|Q(1)$. De même, $p|P(1)$, d'où $p^2|P(1)Q(1) = \Phi_p(1) = p$. C'est absurde, donc Φ_p est irréductible dans $\mathbb{Q}[X]$.

iv. On a $\zeta^p - 1 = (\zeta - 1)\Phi_p(\zeta) = 0$. Comme $\zeta \neq 1$, on a $\Phi_p(\zeta) = 0$. Comme Φ_p est irréductible, c'est le polynôme minimal de ζ sur $\mathbb{Q}$. En particulier, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \Phi_p = p - 1$.

4. **Matrices compagnons**

(a) On a pour $1 \leq i \leq n-1$, $C_P e_i = e_{i+1}$. Une récurrence immédiate montre alors que pour $1 \leq k \neq n-1$, on a $C_P^k(e_1) = e_{k+1}$. En particulier, si $Q \in \mathbb{C}[X]$, avec

$Q = \sum_{i=0}^{n-1} \lambda_i X^i$, on a $Q(C_P)(e_1) = \sum_{i=1}^{n} \lambda_{i-1} e_i$. Comme la famille (e_i) est libre, si $Q \neq 0$, alors $Q(C_P)(e_1) \neq 0$, et en particulier $Q(C_P) \neq 0$.
D'après le théorème de Cayley-Hamilton, le polynôme caractéristique de C_P l'annule, son polynôme minimal est donc de degré au plus n, et la discussion précédente montre qu'il est de degré au moins n ; on a donc $\deg \pi_{C_P} = n$.

(b) On a $C_P^n e_1 = C_P e_n = a_0 e_1 + \cdots + a_{n-1} e_n$. Ainsi, $P(C_P)e_1 = 0$. En particulier, P doit diviser le polynôme minimal de C_P. Or il est unitaire de même degré que ce polynôme minimal. Ils sont donc égaux.

(c) Comme le polynôme minimal divise χ_{C_P} (encore Cayley-Hamilton), et qu'ils sont tous deux unitaires de degré n, on a $\chi_{C_P} = \pi_{C_P} = P$

(d) Comme $\mathbb{C}$ est algébriquement clos, χ_M est scindé. On sait alors que M est trigonalisable : il existe $U \in GL_n(\mathbb{C})$ telle que $M = U^{-1}TU$ avec T triangulaire supérieure. Les coefficients diagonaux de T sont alors les valeurs propres $\alpha_1, \ldots, \alpha_n$ de M comptées avec multiplicité (comme le montre directement le calcul du polynôme caractéristique). Si $Q \in \mathbb{C}[X]$, les coefficients diagonaux de $Q(T)$ sont alors $Q(\alpha_1), \ldots, Q(\alpha_n)$, et $Q(T)$ est semblable à $Q(M)$. En calculant le polynôme caractéristique, on obtient $\chi_{Q(M)} = \prod_{k=1}^{n}(X - Q(\alpha_k))$.

(e) Considérons la matrice compagnon C_P (c'est possible car P est supposé unitaire). D'après ce qui précède, $\chi_{C_P} = P = \prod_{k=1}^{n}(X - \alpha_k)$. La question précédente montre que le polynôme caractéristique de $Q(C_P)$ est $\prod_{k=1}^{n}(X - \alpha_k)$.
D'autre part, comme $Q \in A[X]$ et $C_P \in \mathcal{M}_n(A)$, on a $Q(C_P) \in \mathcal{M}_n(A)$. En particulier, le polynôme caractéristique de $Q(C_P)$ est bien à coefficients dans A. C'est le résultat voulu.

II Nombres algébriques

1. (a) Tout nombre premier $p < n$ est premier avec n. En particulier, $\varphi(n) \geq \pi(n) - 1$, où $\pi(n)$ désigne le nombre de nombres premiers $\leq n$. Comme il y a une infinité de nombres premiers, $\varphi(n)$ tend vers $+\infty$ avec n. Ainsi, il n'y a qu'un nombre fini de n tels que $\varphi(n) \leq d$.

   (b) Si K est un sous-corps de $\mathbb{C}$ contenant une racine primitive n-ème ζ, alors il contient $\mathbb{Q}(\zeta)$. Comme Φ_n est irréductible, c'est le polynôme minimal de ζ et donc $[\mathbb{Q}(\zeta) : Q] = \deg \Phi_n = \varphi(n)$. En effet, $\varphi(n)$ est aussi le nombre d'éléments d'ordre n dans un groupe cyclique d'ordre n, c'est donc le nombre de racines primitives n-èmes de l'unité dans $\mathbb{C}$. Par conséquent, si $\zeta \in K$, alors $[K : \mathbb{Q}] \geq \varphi(n)$ (on a même $\varphi(n) | [K : Q]$). D'après la question précédente, il n'y a qu'un nombre fini de tels n.

2. (a) On considère l'unique morphisme de $\mathbb{Q}$-algèbres $\eta : \mathbb{Q}[X] \to \mathbb{Q}(\alpha)$ tel que $\eta(X) = \alpha$. Par définition de $\mathbb{Q}(\alpha)$, il est surjectif. Par définition du polynôme minimal, on a $\ker \eta = (\pi_\alpha)$. Ainsi, η induit un isomorphisme $\mathbb{Q}[X]/(\pi_\alpha) \to \mathbb{Q}(\alpha)$. En particulier, l'idéal π_α est maximal, donc π_α est irréductible, et $\dim_{\mathbb{Q}} \mathbb{Q}[X]/(\pi_\alpha) = \deg \pi_\alpha$ est égal à $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

   (b) Soit $\sigma : K \to \mathbb{C}$ un morphisme de $\mathbb{Q}$-algèbres. Ainsi, si $P \in \mathbb{Q}[X]$, on a $\sigma(P(\alpha)) = P(\sigma(\alpha))$. En particulier, $\pi_\alpha(\sigma(\alpha)) = 0$, donc $\sigma(\alpha)$ est un conjugué de α. Comme π_α est irréductible de degré d, il possède exactement d racines dans $\mathbb{C}$ (il n'a pas de racines doubles car une telle racine devrait être annulée par son polynôme

dérivé, non nul et de degré $< d$, contredisant ainsi l'irréductiblité de π_α puisque $pgcd(\pi_\alpha, \pi'_\alpha)$ en serait un diviseur non trivial). Un morphisme de $\mathbb{Q}$-algèbres de K dans $\mathbb{C}$ est entièrement déterminé par l'image de α, il y a donc au plus d tels morphismes.

Soient maintenant $\alpha_1, \ldots, \alpha_d$ les d conjugués de α, dans $\mathbb{C}$. Pour tout $1 \leq i \leq d$, il existe un unique morphisme de $\mathbb{Q}$-algèbres $\mathbb{Q}[X] \to \mathbb{C}$ envoyant X sur α_i, et ce morphisme induit un morphisme $\mathbb{Q}[X]/(\pi_\alpha) \to \mathbb{C}$. En composant à la source avec l'isomorphisme induit par η entre $\mathbb{Q}[X]/(\pi_\alpha)$ et $\mathbb{Q}(\alpha)$, on construit un morphisme $K \to \mathbb{C}$ envoyant α sur α_i. On a donc bien construit ainsi les d morphismes attendus.

3. (a) On a $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ fini, donc la famille $\{\theta^n \mid n \in \mathbb{N}\}$ d'éléments de $\mathbb{Q}(\alpha)$ est finie ou liée sur $\mathbb{Q}$. Si elle est finie, alors il existe $m \neq n$ tels que $\theta^m = \theta^n$, donc θ est algébrique. Sinon, il existe une relation de dépendance linéaire non triviale entre ses éléments, c'est-à-dire un polynôme annulateur de θ à coefficients dans $\mathbb{Q}$ et non nul. Cela montre que θ est algébrique.

   (b) Comme $\theta \in K$, il existe $Q \in \mathbb{Q}[X]$ tel que $\theta = Q(\alpha)$. Comme $\pi_\alpha \in \mathbb{Q}[X]$, le résultat de I.4.(e) appliqué à $P = \pi_\alpha$ et ce choix de Q montre que $\tilde{P}_\theta = \prod_{k=1}^{d}(X - Q(\alpha_k)) \in \mathbb{Q}[X]$. Or pour tout $1 \leq k \leq d$, $Q(\alpha_k) = Q(\sigma_k(\alpha)) = \sigma_k(Q(\alpha)) = \sigma_k(\theta)$. On a donc bien $P_\theta = \tilde{P}_\theta \in \mathbb{Q}[X]$.

   (c) Le polynôme P_θ est annulateur de θ et à coefficients dans $\mathbb{Q}$, c'est donc un multiple de π_θ. Soit δ l'ordre de multiplicité de θ comme racine de P_θ. On a alors pour tout k, en faisant agir σ_k sur les coefficients, la relation $(X - \sigma_k(\theta))^\delta | P_\theta$. Donc toutes les racines de P_θ ont le même ordre de multiplicité. Comme π_θ est à racines simples dans $\mathbb{C}$, et qu'il a tous les $\sigma_k(\theta)$ comme racines, on a $\pi_\theta = \prod_{t \in T}(X - t)$ où $T = \{\sigma_k(\theta),\ 1 \leq k \leq d\}$. Enfin, pour tout $t \in T$, t est racine de P_θ de multiplicité δ. Ainsi, $P_\theta = \pi_\theta^\delta$.

4. Soit α un nombre algébrique. Si $\pi_\alpha \in \mathbb{Z}[X]$, alors α est entier algébrique. Réciproquement, supposons α entier algébrique. Soit $\pi_\alpha \in \mathbb{Q}[X]$ son polynôme minimal, et soit $A \in \mathbb{Z}[X]$ unitaire annulateur de A. On écrit la division euclidienne de A par π_α dans $\mathbb{Z}[X]$: $A = Q\pi_\alpha + R$ avec $Q, R \in \mathbb{Z}[X]$ et $R = 0$ ou $\deg R < \deg \pi_\alpha$. Cette division euclidienne est aussi valable dans $\mathbb{Q}[X]$, or dans cet anneau π_α divise A, donc $R = 0$. Par conséquent, A est divisible par π_α dans $\mathbb{Z}[X]$.

5. (a) Supposons que α est un entier algébrique, et notons d le degré de son polynôme minimal. Nous allons montrer que le groupe additif G engendré par les puissances de α est en fait engendré par $1, \alpha, \ldots, \alpha^{d-1}$. Soit $k \in \mathbb{N}$, on écrit la division euclidienne de X^k par π_α dans $\mathbb{Z}[X]$: $X^k = A_k\pi_\alpha + R_k$. On a alors $\alpha^k = R_k(\alpha)$, avec $R_k \in \mathbb{Z}[X]$ de degré $< d$. C'est bien le résultat voulu.

   (b) Supposons G de type fini et notons $g_1, \ldots, g_n$ une famille de générateurs de G. Par hypothèse, puisque G est stable par multiplication par α, pour tout i, αg_j s'écrit comme combinaison linéaire entière des g_i. On peut donc écrire

$$\begin{pmatrix} \alpha g_1 \\ \vdots \\ \alpha g_n \end{pmatrix} = M \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix},$$

   où $M \in \mathcal{M}_n(\mathbb{Z})$. On a donc $\det(\alpha I - M) = 0$ puisque le vecteur $\begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix}$ est non

nul. En particulier, $\chi_M(\alpha) = 0$, donc α est un entier algébrique.

6. Soient α, β des entiers algébriques. Il suffit de montrer que $\alpha - \beta$ et $\alpha\beta$ sont des entiers algébriques. Notons $\mathbb{Z}[\alpha, \beta]$ le sous-groupe additif engendré par les éléments de la forme $\alpha^i \beta^j$. Comme β est entier algébrique, $\mathbb{Z}[\alpha\beta]$ est de type fini sur $\mathbb{Z}[\alpha]$, et comme α est entier algébrique, il est de type fini sur $\mathbb{Z}$. En particulier, $Z[\alpha - \beta]$ et $\mathbb{Z}[\alpha\beta]$ sont de type fini, donc $\alpha - \beta$ et $\alpha\beta$ sont entiers algébriques.

7. Il est clair que tout entier est un rationnel qui est aussi un entier algébrique. Soit $\alpha = \frac{a}{b} \in \mathbb{Q}$ un entier algébrique, avec a et b premiers entre eux. Soit $P = \sum_{i=0}^{d} c_i X^i \in \mathbb{Z}[X]$ le polynôme minimal de α. On a alors, en multipliant par b^d :

$$a_0 b^d + a_1 b^{d-1} a + \cdots + a^d = 0$$

On en déduit immédiatement que b divise a^d. Comme a et b sont premiers entre eux, on a nécessairement $b = \pm 1$ donc $\alpha = \pm a \in \mathbb{Z}$.

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

1. (a) D'après II.2.(b), il suffit d'identifier les racines de $\pi_\zeta = \Phi_p$. Or il est clair que si ζ est racine primitive p-ème, et $1 \leq k \leq p-1$, alors ζ^k est aussi racine primitive p-ème. Ces nombres complexes sont deux à deux distincts, et il existe pour tout $1 \leq k \leq p-1$ un unique morphisme de $\mathbb{Q}$-algèbres $\sigma_k : \mathbb{Q}(\zeta) \to \mathbb{C}$ tel que $\sigma_k(\zeta) = \zeta^k$.

   (b) i. On a donc $N(\zeta) = \zeta \cdot \zeta^2 \cdots \zeta^{p-1} = \zeta^{p(p-1)/2}$. Comme p est impair, $\frac{p-1}{2}$ est entier et $N(\zeta) = (\zeta^p)^{(p-1)/2} = 1$.
   De même, $\mathrm{Tr}(\zeta) = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = \frac{1-\zeta^p}{1-\zeta} - 1 = -1$ car $\zeta \neq 1$.

   ii. On a $\sigma_k(1-\zeta) = 1-\zeta^k$ donc $N(1-\zeta) = (1-\zeta)\cdots(1-\zeta^{p-1}) = (-1)^{p-1}\Phi_p(1) = p$ car p est impair. De même, $N(1+\zeta) = (-1)^{p-1}\Phi_p(-1) = 1$.

2. Comme $\zeta \in \mathfrak{D}_K$, et que $\mathfrak{D}_K$ est un anneau, le sous-anneau de $\mathbb{C}$ engendré par ζ est contenu dans $\mathfrak{D}_K$, d'où $\mathbb{Z}[\zeta] \subset \mathfrak{D}_K$.

3. Remarquons préalablement que si $\theta \in \mathbb{Z}[\zeta]$, alors $N(\theta)$ et $\mathrm{Tr}(\theta)$ sont des nombres entiers. En effet, ce sont des entiers algébriques en tant qu'éléments de l'anneau $\mathbb{Z}[\zeta]$ (qui est stable par les σ_k), et ce sont des rationnels car ils sont (au signe près) coefficients de P_θ défini comme en II.2.

   (a) Si z est inversible, alors il existe $z' \in \mathbb{Z}[\zeta]$ tel que $zz' = 1$. Par multiplicativité de N (qui découle directement de la définition adoptée), on a $N(z)N(z') = 1$. Comme $N(z) \in \mathbb{Z}$, on a $N(z) \in \mathbb{Z}^\times = \{\pm 1\}$.
   Réciproquement, si $N(z) = \pm 1$, alors en posant $z' = N(z)\prod_{k=2}^{p-1}\sigma_k(z)$, on a $zz' = 1$, et $z' \in \mathbb{Z}[\zeta]$ par définition des σ_k. Donc $z \in \mathbb{Z}[\zeta]^\times$.

   (b) Supposons que $N(z) = \ell$ premier. Si z s'écrit $z_1 z_2$ avec $z_1, z_2 \in \mathbb{Z}[\zeta]$, on a $N(z_1)N(z_2) = \ell$ et comme $N(z_1)$ et $N(z_2)$ sont des entiers, alors $N(z_1) = \pm 1$ ou $N(z_2) = \pm 1$, ce qui équivaut d'après la question précédente à z_1 ou z_2 inversible, et donc z est bien irréductible.

4. (a) On sait par II.1 que G est fini. C'est évidemment un sous-groupe de $K^\times$. Or un sous-groupe du groupe multiplicatif d'un corps est cyclique, d'où le résultat. Si on veut éviter le recours à ce théorème, on peut considérer $m = ppcm\{ordre(g),\ g \in G\}$. Comme G est fini, m est bien défini, et tout élément de G est racine m-ème de

l'unité. En particulier, $G \subset \mu_m$, et en tant que sous-groupe d'un groupe cyclique, G est cyclique.

(b) Comme p est supposé impair, $-\zeta^k$ n'est jamais une racine p-ème de l'unité. On en déduit que les $\pm\zeta^k$ forment un sous-groupe de G d'ordre $2p$, car ils sont deux à deux distincts. D'après le théorème de Lagrange, $2p$ divise n.
Comme ω engendre le groupe G, et que ζ est une racine de l'unité contenue dans K, on a $\zeta \in \mathbb{Z}[\omega]$, donc $\mathbb{Z}[\zeta] \subset \mathbb{Z}[\omega]$. L'inclusion réciproque découle de l'hypothèse $\omega \in \mathbb{Z}[\zeta]$.

(c) On a $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$ et comme $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$, on a nécessairement $\varphi(n) = p - 1$. Notons $n = 2pa$ avec $a \in \mathbb{N}$. Si p divise a, alors $\varphi(2pa) > p - 1$, ce cas est donc exclu. Si a est pair, alors $\varphi(2pa) = 2(p-1)\varphi(a) > p - 1$, qui est donc aussi exclu. Il reste le cas a impair non divisible par p, pour lequel $\varphi(2pa) = (p-1)\varphi(a)$. On a donc nécessairement $\varphi(a) = 1$, d'où $a = 1$ puisque a est supposé impair. Ainsi, $n = 2p$ et G est exactement constitué des éléments de la forme annoncée.

5. (a) Soit $I = \mathbb{Z} \cap \lambda\mathbb{Z}[\zeta]$, alors I est un idéal de $\mathbb{Z}$, il est donc de la forme $n\mathbb{Z}$ pour un certain entier $n \in \mathbb{N}$. Par ailleurs, $p = N(\lambda) \in I$ car $N(\lambda)$ est entier et élément de $\mathbb{Z}[\zeta]$. Donc $p\mathbb{Z} \subset n\mathbb{Z}$. Comme $p\mathbb{Z}$ est maximal, on a $I = p\mathbb{Z}$ ou $I = \mathbb{Z}$. Comme λ n'est pas inversible, $1 \notin \lambda\mathbb{Z}[\zeta]$, donc $I = p\mathbb{Z}$.

(b) On sait que si $1 \leq k \leq p-1$, $N(1-\zeta^k) = N(1-\zeta)$ (puisque ces deux éléments sont conjugués). Il en résulte que $N\left(\frac{1-\zeta}{1-\zeta^k}\right) = 1$ pour tout $1 \leq k \leq p-1$. Or $\frac{1-\zeta}{1-\zeta^k} = 1 + \zeta^k + \cdots + \zeta^{(p-1)k} \in \mathbb{Z}[\zeta]$. On a donc bien $\frac{1-\zeta}{1-\zeta^k} \in \mathbb{Z}[\zeta]^\times$.
Notons $u_k = \frac{1-\zeta}{1-\zeta^k}$, on a alors $u = \prod_{1\leq k\leq p-1} u_k = \frac{\lambda^{p-1}}{N(\lambda)}$. Ainsi, $\lambda^{p-1} = uN(\lambda)$. Comme u est inversible, on a bien $\lambda^{p-1}\mathbb{Z}[\zeta] = p\mathbb{Z}[\zeta]$.

(c) Par définition, $P \mapsto P(\zeta)$ et $z \mapsto z \pmod{\langle\lambda\rangle}$ sont surjectifs, donc ψ est surjectif. Soit $P \in \ker\psi$. On a immédiatement $P(X) - P(1)$ divisible par $X - 1$ dans $\mathbb{Z}[X]$ par division euclidienne. En évaluant en ζ, il vient $P(\zeta) - P(1) \in \lambda\mathbb{Z}[\zeta]$. Ainsi, $\psi(P) \equiv P(1) \pmod{\lambda\mathbb{Z}[\zeta]}$. En particulier, $P \in \ker\psi$ si et seulement si $P(0) \in \lambda\mathbb{Z}[\zeta]$. Comme $P(0) \in \mathbb{Z}$, cette condition équivaut à $P(0) \in p\mathbb{Z}$ d'après le (a).

(d) La discussion précédente montre que ψ est surjectif de noyau $(1 - X, p)$, il induit donc un isomorphisme $\mathbb{Z}[X]/(1-X,p) \simeq \mathbb{Z}[\zeta]/\langle\lambda\rangle$. L'anneau de gauche est aussi isomorphe à $\mathbb{F}_p[X]/(1-X) \simeq \mathbb{F}_p$.

(e) Le quotient par $\langle\lambda\rangle$ est un corps donc cet idéal est maximal.

6. (a) i. On peut écrire $P = \prod_{i=1}^d (X - \alpha_i)$, le coefficient de X^k est donc $a_k = \sum_{|K|=d-k, K\subset\{1,\ldots,d\}} \prod_{i\in K} \alpha_i$. Ainsi, $|a_k| \leq \binom{d}{d-k} 1^k = \binom{d}{k}$.
En particulier, il n'y a qu'un nombre fini d'entiers possibles pour le coefficient a_k, et donc qu'un nombre fini de possibilités pour $P \in \mathbb{Z}[X]$ unitaire de degré d ayant toutes ses racines de module ≤ 1. Comme le polynôme minimal d'un entier algébrique de degré d ayant tous ses conjugués de module ≤ 1, le résultat suit.

ii. Suivant l'énoncé, on considère $P_n = \prod_{k=1}^d (X - \alpha_k^n)$. D'après I.4.(e) appliqué avec P et $Q = X^n$, on a $P_n \in \mathbb{Z}[X]$. Comme P_n est unitaire de degré d, c'est un élément de l'ensemble fini de polynômes considéré en (a). Ainsi, ses racines sont dans l'ensemble (lui aussi fini) des racines de tels polynômes. En

particulier, pour tout $1 \leq i \leq d$, la famille $\{\alpha_i^n,\ n \in \mathbb{N}\}$ est finie. Ainsi, il existe $m \neq n$ tels que $\alpha_i^m = \alpha_i^n$. Il en résulte que α_i est une racine de l'unité puisque $\alpha_i \neq 0$.

(b) D'après II.3, les racines de π_u sont les $\sigma_k(u)$. Lorsque $u = P(\zeta)$ avec $P \in \mathbb{Z}[X]$, on obtient que les conjugués de u sont les $u_k = P(\zeta^k)$, $1 \leq k \leq p-1$. En outre, comme u est inversible, il existe $v \in \mathbb{Z}[\zeta]$ tel que $uv = 1$. On a alors $u_k\sigma_k(v) = 1$ avec $\sigma_k(v) \in \mathbb{Z}[\zeta]$. Donc u_k est inversible.

(c) On a $\frac{u_1}{u_{p-1}} \in \mathbb{Z}[\zeta]^\times$, c'est donc un entier algébrique. Ses conjugués sont les $\frac{\sigma_k(u_1)}{\sigma_k(u_{p-1})} = \frac{u_k}{u_{p-k}}$ car $z^{(p-1)k} = \zeta^{p-k}$. Enfin, on a $\zeta^{p-k} = \bar{\zeta}^k$, donc comme $P \in \mathbb{Z}[X]$, $u_{p-k} = \bar{u}_k$ pour tout $1 \leq k \leq p-1$. Ces nombres complexes ont donc le même module. Ainsi, $\frac{u_1}{u_{p-1}}$ et tous ses conjugués sont de module 1.

(d) La question 6.(a) montre que $\frac{u_1}{u_{p-1}}$ est une racine de l'unité. La question III.4 montre qu'il est de la forme $\pm\zeta^k$ pour $1 \leq k \leq p-1$.

(e) i. Par définition, il existe $P \in \mathbb{Z}[X]$ tel que $\theta = P(\zeta)$. D'après III.5.(c), on a $P(\zeta) \equiv P(1) \pmod{\langle\lambda\rangle}$. On a bien $\theta \equiv a \pmod{\langle\lambda\rangle}$ avec $a \in \mathbb{Z}$. En particulier, si $\theta' = \sigma_k(\theta)$ est un conjugué de θ, on a $\theta' - \sigma_k(a) \in \sigma_k(\lambda)\mathbb{Z}[\zeta]$. Comme $\langle\sigma_k(\lambda)\rangle = \langle\lambda\rangle$ d'après 5.(b), et comme $\sigma_k(a) = a$, on a $\theta' \equiv \theta \pmod{\langle\lambda\rangle}$.

ii. On a donc $u_1 \equiv u_{p-1} \pmod{\langle\lambda\rangle}$, et comme u_{p-1} est inversible, $\frac{u_1}{u_{p-1}} \equiv 1 \pmod{\langle\lambda\rangle}$. En particulier, $\left(\frac{u_1}{u_{p-1}}\right)^p \equiv 1 \pmod{\langle\lambda\rangle}$. Or $(-\zeta^m)^p = -1$ car p est impair, et $-1 \neq 1$ dans $\mathbb{Z}[\zeta]/\langle\lambda\rangle$ qui est de caractéristique impaire. Ainsi, u ne peut être de la forme $-\zeta^m$, on a donc $\frac{u_1}{u_{p-1}} = \zeta^m$.

(f) La multiplication par 2 est bijective modulo p car p est impair. En particulier, il existe $r \in \mathbb{Z}$ tel que $2r \equiv m \pmod{p\mathbb{Z}}$. Soit $\varepsilon = \zeta^{-r}u$.
On a $\zeta^{-r}u = \zeta^r u_{p-1}$, ce qui signifie exactement $\varepsilon = \bar{\varepsilon}$ car $u_{p-1} = \bar{u}_1$. Ainsi ε est réel et u s'écrit bien $\zeta^r\varepsilon$ avec ε réel et $\varepsilon = \zeta^{-r}u \in \mathbb{Z}[\zeta]^\times$.

7. (a) Nous l'avons déjà montré en III.3 pour les éléments de $\mathbb{Z}[\zeta]$. Le raisonnement est identique : si $\theta \in \mathfrak{D}_K$, ses conjugués sont aussi des entiers algébriques donc $N(\theta)$ et $\mathrm{Tr}(\theta)$ aussi. De plus, ce sont des coefficients de P_θ défini en II.2 donc des nombres rationnels. Ainsi, ce sont des entiers.

(b) i. On a $\theta\zeta^{-k} = \sum_{j=0}^{p-2} a_j\zeta^{j-k}$. Tous les ζ^{j-k} sont de trace -1, sauf ζ^0 qui est de trace $p-1$. Ainsi, par linéarité, $b_k = (p-1)a_k - \sum_{j\neq k} a_j + \sum_{j=1}^{p-1} a_j = pa_k$.
On sait que θ est un entier algébrique, donc $\theta(\zeta^{-k} - \zeta)$ aussi, et donc b_k est un entier.

ii. On a $p\theta = \sum_{k=0}^{p-2} b_k\zeta^k \in \mathbb{Z}[\zeta] = \mathbb{Z}[\lambda]$ car $\lambda = 1 - \zeta$. Il existe donc bien des coefficients c_k comme annoncé.
Par définition, $\zeta = 1 - \lambda$. On a donc $p\theta = \sum_{k=0}^{p-2} b_k(1-\lambda)^k$. En utilisant la formule du binôme, il vient :

$$p\theta = \sum_{k=0}^{p-2}(-1)^k b_k \sum_{j=0}^{k}\binom{k}{j}\lambda^j.$$

En réindéxant la somme, on a :

$$p\theta = \sum_{j=0}^{p-2} \left(\sum_{k=j}^{p-2} (-1)^k b_k \binom{k}{j} \right) \lambda^j.$$

Un changement d'indice et l'identification des coefficients sur la base $1, \lambda, \ldots, \lambda^{p-2}$ de $\mathbb{Q}(\zeta)$ donnent alors :

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

La relation formelle $\sum_k c_k(1-X)^k = \sum_k b_k X^k$ montre aussi que c_k s'obtient à partir des b_l de la même manière :

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

iii. Comme on l'a vu en III.5.(b), λ^{p-1} et p engendrent le même idéal de $\mathbb{Z}[\zeta]$, donc il existe $\beta \in \mathbb{Z}[\zeta]^\times$ tel que $\beta\lambda^{p-1} = p$ (on a même donné une valeur explicite pour β en III.5.(b)).
En prenant la trace de la relation $p\theta = \sum_k c_k \lambda^k$, on obtient $p|c_0$ (car la trace de λ^k est p pour $1 \leq k \leq p-2$, ce qu'on voit en appliquant la formule du binôme à $(1-\zeta)^k$ et en utilisant $\mathrm{Tr}(\zeta^k) = -1$).
On obtient donc la relation $p\theta = \sum_{k=1}^{p-2} c_k \lambda^k$. En réduisant cette relation modulo $\lambda^2\mathfrak{D}_K$, il vient $0 \equiv \lambda^{p-1}\beta\theta \equiv c_1\lambda \pmod{\lambda^2\mathfrak{D}_K}$. On peut donc écrire $c_1 = \lambda v$ avec $v \in \mathfrak{D}_K$. En prenant la norme, on obtient $c_1^{p-1} = N(\lambda)N(v) = pN(v)$. On a donc $p|c_1^{p-1}$ et donc $p|c_1$ car p est premier.
Une récurrence immédiate sur k (par réductions successives modulo λ^{k+1}) montre que pour tout $0 \leq k \leq p-2$, $p|c_k$.
La relation $\mathbb{Z}$-linéaire exprimant les b_k en fonction des c_k montre alors que tous les b_k sont divisibles par p, et donc que $\theta \in \mathbb{Z}[\zeta]$.
On a donc bien montré que $\mathfrak{D}_K = \mathbb{Z}[\zeta]$.

IV Le théorème de Fermat pour $p = 3$

1. En vertu du théorème de Gauss, la condition $3 \nmid xyz$ signifie qu'aucun de ces trois entiers n'est divisible par 3, c'est-à-dire qu'ils sont tous inversibles modulo 9. Comme $(\mathbb{Z}/9\mathbb{Z})^\times$ est d'ordre 6 et donc cyclique, les entiers x^3, y^3, z^3 sont d'ordre divisant 2, donc égaux à ± 1 modulo 9. En particulier, les valeurs possibles pour $x^3 + y^3 + z^3$ modulo 9 sont $-3, -2, -1, 1, 2$ et 3. Cela montre qu'il n'y a pas de telle solution.
2. D'après lII.5.(b), λ^2 et 3 sont associés dans $\mathbb{Z}[j]$. Plus précisément, on a $3 = \beta\lambda^2$ avec $\beta = 1 + j$.
3. On sait que $\mathbb{Z}[j]/\langle\lambda\rangle \simeq \mathbb{F}_3$. En particulier, si $s \in \mathbb{Z}[j]$, s vaut $-1, 0$ ou 1 modulo λ. Si s n'est pas divisible par λ, il existe $\varepsilon \in \{\pm 1\}$ et $a \in \mathbb{Z}[j]$ tel que $s = \varepsilon + \lambda a$. On a alors $s^3 = \varepsilon^3 + 3a\varepsilon^2\lambda + 3a^2\varepsilon\lambda^2 + a^3\lambda^3$. Par suite, $s^3 = \varepsilon^3 + a\beta\lambda^3 + a^3\lambda^3 \pmod{\lambda^4}$. Il suffit donc de montrer que $a\beta + a^3 \in \lambda\mathbb{Z}[j]$. On a $a^3 = a \pmod{\lambda}$, donc $a\beta + a^3 = a(\beta+1) \pmod{\lambda}$. Or $\beta + 1 \in \lambda\mathbb{Z}[j]$ car $j \equiv 1 \pmod{\lambda}$, donc on a bien $s^3 \equiv \varepsilon^3 \equiv \varepsilon \pmod{\lambda^4}$.

4. D'après la question précédente, α^3 et β^3 valent ± 1 modulo λ^4. Les inversibles $1, 1+j, j, -1, -1-j$ et $-j$ sont respectivement égaux à $1, -1, 1, -1, 1$ et -1 modulo λ (il suffit de remarquer que $j \equiv 1 \pmod{1-\lambda}$, ce qui est clair). Comme $n \geq 1$, on voit que $\omega\lambda^{3n}\delta^3$ est égal ± 1 modulo λ^4 si $n = 1$, et 0 sinon. Comme $\alpha^3 + \beta^3 + \omega\lambda^{3n}\delta^3 = 0$, on a nécessairement $n \geq 2$ et $\alpha^3 + \beta^3 \equiv 0 \pmod{\lambda^4}$.

5. (a) Cela résulte immédiatement de l'identité $\alpha^3 + \beta^3 = (\alpha+\beta)(\alpha+j\beta)(\alpha+j^2\beta)$, qu'on obtient en évaluant $X^3 - 1 = (X-1)(X-j)(X-j^2)$ en $-\alpha/\beta$).

   (b) On sait que $\mathbb{Z}[j]$ est euclidien, donc factoriel. Comme λ est irréductible, il divise l'un des facteurs. Mais $\alpha+\beta-(\alpha+j\beta) = \lambda\beta$, $\alpha+\beta-(\alpha+j^2\beta) = \lambda(1+j)\beta$ et $\alpha+j\beta-(\alpha+j^2\beta) = \lambda j\beta$, de sorte que si λ divise l'un des trois facteurs, il doit diviser les trois.

   (c) Le calcul précédent montre que $pgcd(\alpha+\beta, \alpha+j\beta) = pgcd(\alpha+\beta, \lambda\beta)$. Comme λ est irréductible, si γ irréductible non associé à λ divise ce pgcd, alors γ divise β. Or comme α et β sont premier entre eux, γ ne peut diviser $\alpha+\beta$. Cela montre bien que λ est un $pgcd(\alpha+\beta, \alpha+j\beta)$.
   En particulier, λ^2 ne peut diviser simultanément $\alpha+\beta$ et $\alpha+j\beta$. Le même raisonnement vaut pour les autres paires de facteurs. Par ailleurs, comme $n \geq 2$, λ^2 doit diviser au moins l'un de ces trois facteurs, c'est donc qu'il en divise exactement un des trois.

   (d) En divisant par $\lambda^3 n$, on a immédiatement $-\omega\delta^3 = \kappa_1\kappa_2\kappa_3$. Comme κ_1, κ_2 et κ_3 sont deux à deux premiers entre eux (puisque λ est un pgcd de chaque paire de facteurs de $(\alpha+\beta)(\alpha+j\beta)(\alpha+j^2\beta)$), et que leur produit est associé à un cube, chacun d'entre eux est associé à un cube : pour $1 \leq i \leq 3$, il existe $\gamma_i \in \mathbb{Z}[j]$ tel que $\kappa_i \sim \gamma_i^3$.

   (e) Les relations précédentes s'écrivent

$$\left\{\begin{array}{rcl} \alpha+\beta & = & \tau_1\lambda^{3n-2}\gamma_1^3 \\ \alpha+j\beta & = & \tau_2\lambda\gamma_2^3 \\ \alpha+j^2\beta & = & \tau_3\lambda\gamma_3^3 \end{array}\right. ,$$

   avec $\tau_1, \tau_2, \tau_3 \in \mathbb{Z}[j]^\times$. En multipliant la i-ème ligne par j^{i-1}, il vient

$$\alpha + j\alpha + j^2\alpha + \beta + j^2\beta + j\beta = \tau_1\lambda^{3n-2}\gamma_1^3 + j\tau_2\lambda\gamma_2^3 + \tau_3\lambda\gamma_3^3,$$

   d'où on tire immédiatement

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

   en divisant par $\tau_2\lambda$ et en posant $\tau = \tau_2^{-1}\tau_3$ et $\tau' = \tau_2^{-1}\tau_1$.

   (f) Le cas $\tau = 1$ correspond exactement à (P_{n-1}) avec le quadruplet $(\gamma_2, \gamma_3, \gamma_1, \tau')$. Le cas $\tau = -1$ fournit également P_{n-1} avec le quadruplet $(\gamma_2, -\gamma_3, \gamma_1, \tau')$.

   (g) En réduisant la relation de IV.5.(e) modulo λ^3 (étant donné que $n \geq 2$), on trouve $\gamma_1^3 + \tau\gamma_3^3 \equiv 0 \pmod{\lambda^3}$. Or par définition des γ_i, on a $\lambda \nmid \gamma_1\gamma_2\gamma_3$. D'après IV.3., on sait que γ_1 et γ_3 valent $\pm 1 \pmod{\lambda^4}$, donc $\tau = \gamma_1^{-1}\gamma_3 \equiv \pm 1 \pmod{\lambda^3}$.
   Or $j - 1 = -\lambda$ et $j + 1 \in \mathbb{Z}[j]^\times$, donc aucun des deux n'est divisible par λ^3. De même, on vérifie que $-j \pm 1, j^2 \pm 1$ et $-j^2 \pm 1$ sont de valuation en λ au plus 1. Ainsi, on a nécessairement $\tau \in \{\pm 1\}$. Cela montre que (P_{n-1}) est vérifiée.

6. Il suffit de montrer que (1) n'admet pas de solution (x, y, z) dans $\mathbb{Z}[j]^3$ avec $\lambda | z$ et $\lambda \nmid xy$. Supposons qu'il existe une telle solution, et choisissons-en une pour laquelle $v_\lambda(z) = n$ est minimale. La question 5 montre alors que P_{n-1} est vérifiée, ce qui contredit la minimalité de la solution précédente.

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

1. On a $\prod_{k=0}^{p-1}(X - \zeta^k) = X^p - 1$. Comme $y \neq 0$, on peut évaluer cette relation en $-x/y$, ce qui donne (en multipliant chacun des facteurs par $-y$:

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

   Comme p est impair, on en déduit $-\prod_{k=0}^{p-1}(x + \zeta^k y) = x^p + y^p = -z^p$. En particulier, on a l'égalité d'idéaux annoncée.

2. (a) On a :

$$x + \zeta^\ell y - (x + \zeta^k y) = -\zeta^k(1 - \zeta^{\ell-k})y \in \mathfrak{P}.$$

   D'après III.5.(b), comme $0 < \ell - k \leq p - 1$, on sait que $\left\langle 1 - \zeta^{\ell-k} \right\rangle = \langle \lambda \rangle$, et comme $-\zeta$ est inversible, on a bien $\lambda y \in \mathfrak{P}$.

   (b) Si $y \in \mathfrak{P}$, alors $x = (x + \zeta^k y) - \zeta^k y \in \mathfrak{P}$ et donc $x\mathbb{Z} + y\mathbb{Z} \subset \mathfrak{P}$. En particulier, $x\mathbb{Z} + y\mathbb{Z} \neq \mathbb{Z}$, sinon, $\mathbb{Z} \subset \mathfrak{P}$ donc $\mathbb{Z}[\zeta] \subset \mathfrak{P}$, ce qui contredit la primalité de $\mathfrak{P}$.
   Par conséquent, $y \notin \mathfrak{P}$ et comme $\mathfrak{P}$ est premier, $\lambda \in \mathfrak{P}$, donc par maximalité de $\langle \lambda \rangle$, on a $\langle \lambda \rangle = \mathfrak{P}$. On a alors $x + y = x + \zeta^k y + (1 - \zeta^k)y \in \langle \lambda \rangle$. Comme $x + y \in \mathbb{Z}$, on a bien $x + y \in \mathbb{Z} \cap \langle \lambda \rangle = p\mathbb{Z}$. Mais alors p divise z^p et comme p est premier, il divise z, ce qui est contraire à l'hypothèse initiale.

3. Soit $\langle z \rangle = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ la factorisation de l'idéal $\langle z \rangle$ en produit d'idéaux premiers (les $\mathfrak{P}_i$ sont deux à deux distincts. On a alors $\langle z^p \rangle = \mathfrak{P}_1^{pe_1} \cdots \mathfrak{P}_r^{pe_r}$. Comme les $\left\langle x + \zeta^k y \right\rangle$ $(0 \leq k \leq p-1)$ sont deux à deux premiers entre eux et d'après la relation V.1, si $\mathfrak{P}$ est un idéal premier divisant $\langle x + \zeta y \rangle$, alors $\mathfrak{P} \in \{\mathfrak{P}_i,\ 1 \leq i \leq r\}$ et si $\mathfrak{P} = \mathfrak{P}_i$, alors $\mathfrak{P}_i^{pe_i}$ divise $\langle x + \zeta y \rangle$ (sinon, $\mathfrak{P}_i$ devrait contenir un $\left\langle x + \zeta^k y \right\rangle$ avec $k \neq 1$, ce qui contredirait le fait qu'ils sont premiers entre eux). En particulier, $\langle x + \zeta y \rangle = \prod_{\mathfrak{P}_i | \langle x+\zeta y \rangle} \mathfrak{P}_i^{pe_i} = I^p$ avec $I = \prod_{\mathfrak{P}_i | \langle x+\zeta y \rangle} \mathfrak{P}_i^{e_i}$.

4. Par hypothèse, p est régulier. Or l'idéal I de la question précédente vérifie que I^p est principal, donc I est principal. Notons $\alpha \in \mathbb{Z}[\zeta]$ un générateur de I, alors α^p est un générateur de I^p et il existe $u \in \mathbb{Z}[\zeta]^\times$ tel que $x + \zeta y = u\alpha^p$.
   D'après III.6., l'élément inversible u s'écrit $u = \zeta^r \varepsilon$, où $r \in \mathbb{Z}$ et $\varepsilon \in \mathbb{Z}[\zeta]^\times \cap \mathbb{R}$. On a alors bien $x + \zeta y = \zeta^r \varepsilon \alpha^p$, avec r, ε, α de la forme annoncée.

5. L'anneau $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta]$ est de caractéristique p. Si on écrit $\alpha = a_0 + \lambda b$ avec $a_0 \in \mathbb{Z}$ et $b \in \mathbb{Z}[\zeta]$, alors on a $\alpha^p \equiv a_0^p + \lambda^p b^p \pmod{\langle p \rangle}$. Comme p et λ^{p-1} sont associés, on a $\alpha^p \equiv a_0^p \pmod{\langle p \rangle}$. En posant $a = a_0^p$, on obtient le résultat.
   En prenant le conjugué (au sens de la conjugaison complexe) de $x + \zeta y$, on obtient $x + \zeta^{-1} y \equiv \zeta^{-r} \varepsilon \alpha^p \pmod{\langle p \rangle}$ car x, y, ε sont réels et $\bar{\alpha}^p \equiv \bar{a} \equiv a \pmod{\langle p \rangle}$.
   On en déduit, comme ζ est inversible, que

$$\zeta^{-r}(x + \zeta^r y) - \zeta^r(x + \zeta^{-1} y) \equiv 0 \pmod{\langle p \rangle},$$

   ce qui est la relation attendue.

6. Si p divise r, alors la relation $\zeta^r = 1$ et la précédente imposent que $y(\zeta - \zeta^{-1}) = x+y\zeta-x-y\zeta^{-1} \in p\mathbb{Z}[\zeta]$. On a donc $\langle y(\zeta - \zeta^{-1})\rangle \subset p\mathbb{Z}[\zeta]$ donc $\lambda y \in p\mathbb{Z}[\zeta] = \lambda^{p-1}\mathbb{Z}[\zeta]$. Ainsi, $y \in \lambda^{p-2}\mathbb{Z}[\zeta] \subset \langle\lambda\rangle$, d'où $y \in \langle\lambda\rangle \cap \mathbb{Z} = p\mathbb{Z}$. Ceci est contraire à l'hypothèse $p \nmid xyz$.
7. Si $r \notin \{\pm(1-r)\}$, comme $r \neq -r \pmod p$ et $r - 1 \neq 1 - r \pmod p$, l'ensemble $\{\zeta^r, \zeta^{-r}, \zeta^{r-1}, \zeta^{-r-1}\}$ est constitué quatre éléments de la base $\{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ de $\mathbb{Q}(\zeta)/\mathbb{Q}$. En écrivant βp sur cette base, on en déduit que les coordonnées $x, y, -x, -y$ sont des entiers divisibles par p, ce qui n'est pas. On doit donc avoir $r \in \{\pm(1-r)\}$, c'est-à-dire $2r = 1 \pmod p$ (car le cas $r = r - 1 \pmod p$ est exclu).
8. En multipliant l'égalité précédente par ζ^r, il vient $\beta p\zeta^r = x + \zeta y - x\zeta - y = \lambda(x - y)$. On a donc $x-y \in \lambda^{p-2}\mathbb{Z}[\zeta]$ et le même raisonnement qu'en V.6 montre que $x-y \in p\mathbb{Z}$.
9. La symétrie de l'équation montre que $x \equiv z \pmod p$, et donc que $0 \equiv 3x^p \pmod p$. Comme on a supposé que $p \nmid x$, on doit avoir $p|3$, donc $p = 3$. Mais ce cas a été traité dans la partie précédente. On en conclut que l'équation $x^p + y^p + z^p = 0$ n'a pas de solutions entières telles que $p \nmid xyz$.