Université Paris Diderot
Master de Mathématiques

Algèbre
Année 2019-20
E. Letellier, L. Merel

CORRIGÉ DU CONTRÔLE du 18 octobre 2019

Soit j une racine 3-ème primitive de l'unité dans $\mathbf{C}$. Posons $\mathbf{Z}[j] = \{a + bj/a, b \in \mathbf{Z}\}$ et $\mathbf{Q}(j) = \{a + bj/a, b \in \mathbf{Q}\}$. Pour $a, b \in \mathbf{R}$, posons $\mathrm{N}(a + bj) = (a + bj)(a + bj^2)$.

1. Montrer que $\mathbf{Z}[j]$ est un anneau.

C'est un sous-anneau de $\mathbf{C}$, puisque pour $a+bj$, $a'+b'j \in \mathbf{Z}[j]$, on a $(a+bj)+(a'+b'j) = a + a' + (b + b')j$, $(a + bj)(a' + b'j) = aa' - bb' + (ab' + a'b - bb')j \in \mathbf{Z}[j]$ et $1 \in \mathbf{Z}[j]$.

2. Montrer que, pour $z, z' \in \mathbf{Z}[j]$, on a $\mathrm{N}(zz') = \mathrm{N}(z)N(z')$.

Notons qu'on a, pour $z = a + bj$, $\mathrm{N}(z) = z\bar{z} = a^2 + b^2 - ab \in \mathbf{A}$. La relation cherchée résulte de la multiplicativité de la conjugaison complexe.

3. Montrer que si z est inversible dans $\mathbf{Z}[j]$, on a $\mathrm{N}(z) = 1$.

Notons z' l'inverse de z. On a $1 = \mathrm{N}(1) = \mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$. Comme $\mathrm{N}(z)$ et $\mathrm{N}(z')$ sont des entiers ≥ 0 inverses l'un de l'autre, ils sont égaux à 1.

4. En déduire que les inversibles de $\mathbf{Z}[j]$ sont 1, -1, j, $-j$, $-1 - j = j^2$ et $1 + j = -j^2$.

Ils sont inversibles. Montrons que ce sont les seuls. Soit $z = a + jb \in \mathbf{Z}[j]$ tel que $a^2 + b^2 - ab = 1$. On note que $a^2 + b^2 - ab = (a^2 + b^2 + (a - b)^2)/2$, cette quantité est > 1 si $|a|$ ou $|b|$ ou $|a - b|$ est ≥ 2. Il ne reste que 0 et les six inversibles déjà identifiés.

5. Montrer que tout nombre complexe s'écrit comme la somme d'un élément de $\mathbf{Z}[j]$ et d'un nombre complexe z tel que $\mathrm{N}(z) < 1$.

Pour $z = a+bj \in \mathbf{C}$, avec a, $b \in \mathbf{R}$, considérons $z' = a'+b'j$, avec a', $b' \in \mathbf{Z}$, $|a-a'| \leq 1/2$ et $|b-b'| \leq 1/2$. On a donc $|z - z'|^2 = (a-a')^2 + (b-b')^2 - (a-a')(b-b') \leq 3/4 < 1$.

6. Soit $z \in \mathbf{Z}[j]$ et $d \in \mathbf{Z}[j]$, $d \neq 0$. Montrer qu'il existe $q \in \mathbf{Z}[j]$ et $r \in \mathbf{Z}[j]$ tels que $z = dq + r$ avec $\mathrm{N}(r) < \mathrm{N}(d)$.

D'après la question 6., il existe $q \in \mathbf{Z}[j]$ et $s \in \mathbf{C}$ avec $\mathrm{N}(s) < 1$ tel que $z/d = q + s$. On a donc $z = qd + sd$. Posons $r = sd$, qui convient puisque $\mathrm{N}(r) = \mathrm{N}(s)\mathrm{N}(d) < \mathrm{N}(d)$.

7. En déduire que $\mathbf{Z}[j]$ est un anneau euclidien.

La question 7. établit l'existence d'une division euclidienne dans $\mathbf{Z}[j]$.

8. L'anneau $\mathbf{Z}[j][X]$ est-il factoriel ?

L'anneau $\mathbf{Z}[j]$ est euclidien et donc factoriel. On sait que si A est un anneau factoriel, $A[X]$ est lui aussi factoriel.

Pour n entier ≥ 3, posons dans $\mathbf{Z}[j][X]$: $P_n = X^n+(1-j)X+3$ et $\bar{P}_n = X^n+(1-j^2)X+3$.

9. Soient α, β, γ les racines de P_3 dans $\mathbf{C}$. Calculer $1/\alpha + 1/\beta + 1/\gamma$.

On a $1/\alpha + 1/\beta + 1/\gamma = (\alpha\beta + \alpha\gamma + \beta\gamma)/(\alpha\beta\gamma)$. Puisque α, β, γ sont les racines de P_3, on a $\alpha\beta + \alpha\gamma + \beta\gamma = 1 - j$ et $\alpha\beta\gamma = -3$. Donc on a $1/\alpha + 1/\beta + 1/\gamma = (j - 1)/3$.

10. Montrer que $1 - j$ est irréductible dans $\mathbf{Z}[j]$.

On a $\mathrm{N}(1 - j) = 3$. Soient u, $v \in \mathbf{Z}[j]$ tels que $1 - j = uv$. On a donc $\mathrm{N}(u)\mathrm{N}(v) = 3$. Comme 3 est premier dans $\mathbf{Z}$, on a $\mathrm{N}(u) = 1$ ou $\mathrm{N}(v) = 1$, si bien que u ou v est une unité.

11. Montrer que P_3 a des racines multiples dans le corps $\mathbf{Z}[j]/(1 - j)$.

La réduction modulo $(1 - j)$ de P_3 est X^3, qui a des racines multiples.

12. L'élément 2 est-il irréductible dans $\mathbf{Z}[j]$?

Soient u, $v \in \mathbf{Z}[j]$ tels que $2 = uv$. On a $\mathrm{N}(u)\mathrm{N}(v) = 4$. Supposons $\mathrm{N}(u) = 2$ et posons $u = a+bj$. On a $2 = a^2+b^2-ab$ ce qui est impossible (par exemple : $a^2+b^2-ab \equiv (a+b)^2 \pmod 3$, et 2 n'est pas un carré modulo 3). Donc $\mathrm{N}(u) = 1$ ou $\mathrm{N}(v) = 1$, si bien que u ou v est une unité. Ainsi 2 est irréductible.

13. Montrer que $k = \mathbf{Z}[j]/(2)$ est un corps à 4 éléments formé des classes de 0, 1, j, j^2.

Puisque 2 est irréductible, $\mathbf{Z}[j]/(2)$ est un corps de caractéristique 2. Comme la classe de $a + jb$ est déterminée par les classes de a et b modulo 2, il possède au plus 4 éléments. Or les classes des 0, 1, j, $-1 - j = j^2$ sont distinctes dans $\mathbf{Z}[j]/(2)$.

14. Pour n entier non congru à 1 modulo 3, montrer que P_n est sans racine dans k.

Dans k, la classe $\tilde{P}_n$ de P_n est $X^n + j^2X + 1$. On a $\tilde{P}_n(0) = 1$, $\tilde{P}_n(1) = j^2$, $\tilde{P}_n(j) = j^n$ et $\tilde{P}_n(j^2) = j^{2n} + j + 1$. Ce dernier est nul si et seulement si $j^{2n} = j^2$, c'est-à-dire si et seulement si n est congru à 1 modulo 3. Ainsi $\tilde{P}_n$ n'a pas de racine dans k.

15. En déduire que P_3 est irréductible sur $\mathbf{Z}[j]$.

Si P_3 était réductible, il aurait un facteur de degré 1, puisque P_3 est de degré 3. L'image dans $k[X]$ de ce facteur de degré 1 serait lui aussi de degré 1, si bien que P_3 aurait des racines dans k.

16. Montrer que $Q_n = P_n\bar{P}_n$ appartient à $\mathbf{Z}[X]$.

On a $Q_n = X^{2n} + 3X^{n+1} + 6X^n + 3X^2 + 9X + 9$.

17. Montrer que, si P_n est irréductible dans $\mathbf{Z}[j][X]$, $\bar{P}_n$ est irréductible dans $\mathbf{Z}[j][X]$, puis que Q_n est irréductible dans $\mathbf{Z}[X]$.

Posons $\bar{P}_n = QR$, avec Q, R dans $\mathbf{Z}[j][X]$. En passant aux conjugés, on trouve $P_n = \bar{Q}\bar{R}$, si bien que $\bar{Q}$ ou $\bar{R}$ est constant, et donc Q ou R est constant. Ainsi, $\bar{P}_n$ est irréductible dans $\mathbf{Z}[j][X]$. Les diviseurs unitaires de Q_n sont donc 1, P_n, $\bar{P}_n$ et Q_n. Comme P_n et $\bar{P}_n$ ne sont pas à coefficients entiers, Q_n est irréductible.

18. Soit A un anneau factoriel. Soit $P = \sum_{k=0}^{n} a_k X^k \in A[X]$. Soit $p \in A$ un élément irréductible. Supposons que $a_n = 1$, que $p|a_k$ pour $0 \leq k \leq n-1$. Montrer que si p^2 ne divise pas a_1, P est irréductible dans $A[X]$ ou possède une racine dans A.

Supposons qu'il existe $Q = \sum_{k=0}^{n} b_k X^k \in A[X]$ et $R = \sum_{k=0}^{n} c_k X^k \in A[X]$ unitaires tels que $P = QR$. En réduisant cette factorisation modulo p, on trouve que Q et R sont congrus à $X^{\mathrm{d}^0(Q)}$ et $X^{\mathrm{d}^0(R)}$ respectivement, si bien que p divise tous les coefficients non dominants de Q et R. On a $a_1 = b_0c_1 + b_1c_0$. Si les degrés de Q et R sont > 1, c_1 et b_1 ne sont pas les coefficients dominants de R et Q. Donc p divise c_0, b_0, c_1 et b_1. Donc p^2 divise a_1 ce qui contredit l'hypothèse. Donc Q ou R est de degré 1. Comme ces polynômes sont unitaires, l'un d'eux a une racine dans A, si bien que P a une racine dans A.

19. Lorsque n est ≥ 4, montrer que le polynôme P_n est sans racine dans $\mathbf{Z}[j]$.

Soit x une racine de P_n dans $\mathbf{Z}[j]$. Comme le coefficient constant de P_n est 3, on a $x|3$. Comme $(1-j)$ divise 3, on a $(1-j)|x^n$ et, comme $(1-j)$ est irréductible, $(1-j)|x$. Or les diviseurs de 3 dans $\mathbf{Z}[j]$ sont de la forme $u(1-j)^\alpha$ avec u unité, et α entier naturel ≤ 2. On a donc $x = u(1-j)^\alpha$ avec $\alpha = 1$ ou 2. Si $\alpha = 2$, on a $(1-j)^3|3$, ce qui est absurde. Donc $\alpha = 1$. D'après 18. la classe de x dans k est j^2 et on a $n \equiv 1 \pmod 3$, si bien que $u = \pm j$ et $\alpha = 1$. On a donc $(1-j)^n|(1-j)^2u + 3$. Or $(1-j)^n$ ne divise ni $j(1-j)^2 + 3 = 3(1-j^2)$ ni $-j(1-j)^2 + 3 = -3j$ lorsque $n \geq 3$. C'est absurde.

20. En déduire que P_n est irréductible sur $\mathbf{Z}[j]$ pour tout $n \geq 3$.

Cela résulte de la question 18. appliquée à $p = 1 - j$, et de la question précédente.