

## CORRIGÉ DU CONTRÔLE du 10 novembre 2017

### I

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  $N(a + bj) = (a + bj)(a + bj^2)$ .

1. Ecrire le 3-ème polynôme cyclotomique  $\Phi_3$ .

On a  $\Phi_3(X) = X^2 + X + 1$  et donc  $j^2 + j + 1 = 0$ .

2. 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  $1 \in \mathbf{Z}[j]$ .

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

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

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

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

5. 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  $\geq 2$ . Il ne reste que 0 et les six inversibles déjà identifiés.

6. 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  $N(z) < 1$ .

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  $|z - z'|^2 = (a - a')^2 + (b - b')^2 - (a - a')(b - b') \leq 3/4 < 1$ .

7. 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  $N(r) < N(d)$ .

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

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

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

9. 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.

### II

Pour  $n$  entier  $\geq 3$ , posons  $P_n = X^n + (1 - j)X + 3 \in \mathbf{Z}[j][X]$ .

10. Calculer le discriminant  $\Delta_{P_3}$  de  $P_3$ .

Pour  $P = X^3 + aX + b$ , on a  $\Delta_P = -27b^2 - 4a^3$ . Ainsi  $\Delta_{P_3} = -255 - 24j$ .

11. Soient  $\alpha, \beta, \gamma$  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  $\alpha, \beta, \gamma$  sont les racines de  $P_3$ , on a  $\alpha\beta + \alpha\gamma + \beta\gamma = 1 - j$  et  $\alpha\beta\gamma = -3$ . Donc on a  $1/\alpha + 1/\beta + 1/\gamma = (j - 1)/3$ .

12. Calculer  $((\alpha - \beta)(\beta - \gamma)(\alpha - \gamma))^2$ .

C'est le discriminant de  $P_3$ .

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

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

14. 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.

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

Soient  $u, v \in \mathbf{Z}[j]$  tels que  $2 = uv$ . On a  $N(u)N(v) = 4$ . Supposons  $N(u) = 2$  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  $N(u) = 1$  ou  $N(v) = 1$ , si bien que  $u$  ou  $v$  est une unité. Ainsi 2 est irréductible.

16. 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  $\mathbf{Z}[j]/(2)$ .

### III

17. 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  $X^{d^0(Q)}$  et  $X^{d^0(R)}$  respectivement, si bien que  $p$  divise tous les coefficients non dominants de  $Q$  et  $R$ . On a  $a_1 = b_0 c_1 + b_1 c_0$ . 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  $A$ .

18. 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  $X^n + j^2 X + 1$ . 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  $k$ .

19. Lorsque  $n$  est  $\geq 4$ , 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  $\alpha$  entier naturel  $\leq 2$ . 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  $(1 - j)^n|(1 - j)^2 u + 3$ . 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 17. appliquée à  $p = 1 - j$ , et de la question précédente.