CORRIGÉ du DEVOIR MAISON

Corrigé du problème visant à montrer que l'anneau $\mathbb{Z}[\alpha]$, où $\alpha = \frac{1+i\sqrt{19}}{2}$, est principal mais non euclidien.

Première partie.

1. Par définition de conjugué dans $\mathbb{C}$, nous avons

$$\bar{\alpha} = \frac{1-i\sqrt{19}}{2} = \frac{1}{2} - \frac{i\sqrt{19}}{2} = 1 - (\frac{1}{2} + \frac{i\sqrt{19}}{2}) = 1 - \alpha.$$

   D'autre part,

$$\alpha\bar{\alpha} = (\frac{1+i\sqrt{19}}{2})(\frac{1-i\sqrt{19}}{2}) = \frac{1+19}{4} = 5.$$

2. Le morphisme

$$P(X) \in \mathbb{Z}[X] \mapsto P(\alpha) \in \mathbb{Z}[\alpha]$$

   est surjectif par définition. Son noyau est formé des polynômes qui s'annulent en α. Supposons que $P(\alpha) = 0$. Puisque P a des coefficients entiers (et donc réels), et α est complexe non réel, on a $P(\bar{\alpha}) = 0$. Donc les polynômes multiples de $(X-\alpha)(X-\bar{\alpha}) = X^2 - X + 5$ sont dans le noyau. D'autre part, comme $X^2 - X + 5$ est unitaire, si $P(X) = (X^2 - X + 5)Q(X)$ avec $P(X) \in \mathbb{Z}[X]$, alors $Q(X)$ a coefficients entiers, ce qui donne que $\langle X^2 - X + 5\rangle$ est le noyau. Par le théorème de factorisation on obtient un isomorphisme $\mathbb{Z}[X]/(X^2 - X + 5) \simeq \mathbb{Z}[\alpha]$.

3. Le polynôme $X^2 - X - \bar{5} = X^2 - X - \bar{1}$ dans $(\mathbb{Z}/2\mathbb{Z})[X]$ est réductible si et seulement si ils existent deux polynômes $P(X)$ et $Q(X)$ de degré 1 tels que $X^2 - X - \bar{1} = P(X)Q(X)$. En fait, comme $\mathbb{Z}/2\mathbb{Z}$ est un corps, tout polynôme de degré zéro est inversible. On obtient l'irréductibilité de $X^2 - X - \bar{1}$ en montrant que de tels $P(X)$ et $Q(X)$ ne peuvent pas exister : ou bien analysant tout les cas possbiles (il n'y a que deux polynômes de degré exactement 1 dans $(\mathbb{Z}/2\mathbb{Z})[X]$, ce sont X et $X + \bar{1}$), ou bien en montrant que ni $\bar{1}$ ni $\bar{0}$ sont racines.

4. Considérons la composée de morphismes, où les polynômes de degré 1, $aX + b$ et $\bar{a} + \bar{b}X$ forment des systèmes de représentants des classes des quotients correspondants :

$$a + b\alpha \in \mathbb{Z}[\alpha] \mapsto a + bX \in \mathbb{Z}[X]/(X^2 - X + 5) \mapsto \bar{a} + \bar{b}X \in \mathbb{Z}/2\mathbb{Z}[X]/(X^2 - X + \bar{5}).$$

   Ce morphisme est clairement surjectif, et $\bar{a} + \bar{b}X = 0$ si et seulement si $a + b\alpha \in (2)$. D'où l'isomorphisme $\mathbb{Z}[\alpha]/(2) \simeq \mathbb{Z}/2\mathbb{Z}[X]/(X^2 - X + \bar{5})$ par le théorème de factorisation.

5. $X^2 - X + \bar{5} = X^2 + X + \bar{1}$ est de degré 2 sans racine sur $\mathbb{Z}/2\mathbb{Z}$, donc irréductible. Comme $\mathbb{Z}/2\mathbb{Z}$ est un corps, il en suit que $(X^2 - X + 5)$ est maximal et donc que $\mathbb{Z}/2\mathbb{Z}[X]/(X^2 - X + 5)$ est un corps. D'autre part, on aurait pu observer que comme $X^2 + X + \bar{1}$ est irréductible, l'idéal est premier, et donc $\mathbb{Z}/2\mathbb{Z}[X]/(X^2 - X + 5)$ est intègre. Comme ce dernier ensemble est fini, on déduit qu'il est un corps. Comme $\mathbb{Z}[\alpha]/(2) \simeq \mathbb{Z}/2\mathbb{Z}[X]/(X^2 - X + 5)$, $\mathbb{Z}[\alpha]/(2)$ est aussi un corps. Donc (2) est un idéal maximal de $\mathbb{Z}[\alpha]$.

Deuxième partie.

1. Soient a et b dans $\mathbb{Z}[\alpha]$, c'est à dire $a = a_0 + a_1\alpha$ et $b = b_0 + b_1\alpha$ avec a_i, b_i entiers. Alors on calcule le quotient des deux nombres complexes a/b :

$$\frac{a}{b} = \frac{a_0 + a_1\alpha}{b_0 + b_1\alpha} = \frac{a_0 + a_1\alpha}{b_0 + b_1\alpha}.\frac{b_0 - b_1\alpha}{b_0 - b_1\alpha},$$

   dont le developpement explicite donne l'expression cherchée de a/b.

2. On travaille dans le sous-corps $\mathbb{Q}[\alpha] \subset \mathbb{C}$, en se souvenant que la norme $N(z) = z\bar{z}$ d'un élément $z = x + y\alpha$ de $\mathbb{Q}[\alpha]$ s'écrit $N(x + y\alpha) = x^2 + 5y^2 + xy$.
   On a donc $a, b \in \mathbb{Z}[\alpha]$, et on considère leur quotient dans $\mathbb{Q}(\alpha)$: $\frac{a}{b} = u + v\alpha$, avec $u, v \in \mathbb{Q}$.
   (a) Il existe $m \in \mathbb{Z}$ avec $|u - m| \leq 1/2$. Alors

$$N(u + v\alpha - m - n\alpha) = (u-m)^2 + 5(v-n)^2 + (u-m)(v-n) \leq \frac{1}{4} + \frac{5}{9} + \frac{1}{6} = \frac{35}{36} < 1.$$

   (b) En multipliant par b, et en utilisant $N(xy) = N(x)N(y)$:

$$N(a - b(m + n\alpha)) = N(b(u + v\alpha) - b(m + n\alpha)) < N(b)$$

   Donc en posant $q = m + n\alpha$, $r = a - b(m + n\alpha)$, c'est OK.
3. Maintenant si $|v - n| \geq 1/3$ pour tout n, alors on a $|2v - n| \leq 1/3$ pour un certain n, et on applique le raisonnement précédent à $\frac{2a}{b} = 2u + 2v\alpha$.

Troisième partie.

1. L'ensemble $\{N(x) | x \in I \setminus \{0\}\}$ est un sous-ensemble de $\mathbb{N}$, donc il admet un minimum n_0. Tout élément de $N^{-1}(n_0)$ réalise ce minimum. Soit $a \in I$ tel que $N(a) = n_0$.
2. Supposons donc qu'il existe $x \in I \setminus (a)$. Par la question précédente, on sait qu'on peut écrire $x = aq + r$ ou $2x = aq + r$ avec $r = 0$ ou $N(r) < N(a)$.
3. Comme $r \in I$, $r \neq 0$ et $N(r) < N(a)$ contredirait la minimalité de a. Donc $r = 0$. Si $x = qa$, alors $x \in (a)$, ce qui contredit l'hypothèse.
4. On a donc forcément $2x = aq$.
   (a) Comme (2) est premier (car maximal), on a $a \in (2)$ ou $q \in (2)$. Mais si $q = 2q'$, $x = aq' \in (a)$, absurde. Donc $a = 2a'$, ce qui entraine $x = a'q$.
   (b) Comme (2) est maximal, et $q \notin (2)$, l'idéal $(2, q)$ (qui contient (2)) est égal à $\mathbb{Z}[\alpha]$, et en particulier contient 1. Il existe u, v, $1 = 2u + qv$.
   (c) En multipliant la relation de Bézout par a' : $a' = 2a'u + a'qv = au + xv \in I$.
   (d) Nous avons $N(2)N(a') = N(a)$, donc $N(a') < N(a)$, ce qui contredit la minimalité de $N(a)$ dans I.

Quatrième partie.
Supposons $\mathbb{Z}[\alpha]$ euclidien de stathme ν, et cherchons une contradiction. Prenons $x \neq 0 \in \mathbb{Z}[\alpha]$ non inversible minimisant $\nu(x)$. Soit $\bar{y}$ un élément non nul du quotient $\mathbb{Z}[\alpha]/(x)$. On écrit $y = xq + r$ avec $r \neq 0$ (car $\bar{y} \neq \bar{0}$) vérifiant $\nu(r) < \nu(x)$.

1. Par minimalité de x, r est inversible dans $\mathbb{Z}[\alpha]$. Or, on vérifie que les inversibles de $\mathbb{Z}[\alpha]$ sont ± 1 : il suffit de montrer que pour z dans $\mathbb{Z}[\alpha]$, l'inverse de z dans $\mathbb{Q}[\alpha]$ a des coefficients entiers si et seulement si $z = \pm 1$.
2. Le quotient $K = \mathbb{Z}[\alpha]/(x)$ admet au plus 3 éléments (et au moins 2). Les seuls anneaux de telle cardinalité sont les corps $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$ (on se rappelle qu'il n'y a qu'un groupe d'ordre 2 et qu'un groupe d'ordre 3).
3. Maintenant rappelons nous que $\alpha^2 - \alpha + 5 = 0$, donc l'image $\bar{y}$ de α dans K vérifie une équation correspondante. Si $K \simeq \mathbb{Z}/2\mathbb{Z}$, $\bar{y} \in \{\bar{0}, \bar{1}\}$ devrait être racine de $X^2 + X + 1$: absurde.
4. Si $K \simeq \mathbb{Z}/3\mathbb{Z}$, $\bar{y} \in \{-\bar{1}, \bar{0}, \bar{1}\}$ devrait être racine de $X^2 - X - 1$: absurde.