
Exemple d'un anneau principal non euclidien

Décembre 2008
TANCRÈDE LEPOINT

Le but de ce problème est de montrer que l'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal, mais n'est pas euclidien, quelque soit le stathme δ

Notations

- La caractéristique d'un anneau A sera notée $\text{car}(A)$.
- Lorsque p sera un nombre premier, on notera \mathbb{F}_p l'anneau (ou le corps selon le contexte) $\mathbb{Z}/p\mathbb{Z}$.
- On notera $\text{card}(X)$ le cardinal d'un ensemble fini X .
- Si $\varphi: A \rightarrow B$ est un morphisme d'anneaux, on notera $\text{Ker}(\varphi)$ son noyau et $\text{Im}(\varphi)$ son image.
- Lorsqu'il n'y aura pas ambiguïté, on notera \bar{z} le conjugué d'un nombre complexe z .

Première partie

Sujet

A. PRÉLIMINAIRES.

- A.1) Soit p un nombre premier, et A un anneau à p éléments. Montrer que A est de caractéristique p , et en déduire que le morphisme

$$\Theta_A: \mathbb{Z} \rightarrow A, m \mapsto m \cdot 1_A$$

induit un isomorphisme d'anneaux $\mathbb{F}_p \cong A$.

- A.2) Soit (A, δ) un anneau euclidien. Montrer qu'il existe $x \in A, x \notin A^\times$ tel que le morphisme

$$A^\times \cup \{0\} \rightarrow A/(x), a \mapsto \bar{a}$$

obtenu par restriction de la projection canonique est surjectif.

Indication : Traiter le cas où A est un corps à part. Si ce n'est pas un corps, choisir $x \in A \setminus (A^\times \cup \{0\})$ tel que $\delta(x)$ soit minimal.

Dans la suite du problème, on note $\alpha = \frac{1+i\sqrt{19}}{2}$ et $A = \mathbb{Z}[\alpha]$.

B. A N'EST PAS EUCLIDIEN.

On pose $\nu(z) = |z|^2$ pour tout $z \in A$.

B.1) Vérifier que $\alpha^2 - \alpha + 5 = 0$, et que

$$\nu(a + b\alpha) = \left(a + \frac{b}{2}\right)^2 + \frac{19b^2}{4} = a^2 + ab/5b^2 \in \mathbb{N}$$

B.2) Montrer que $A^\times = \{\pm 1\}$.

On suppose maintenant que A est euclidien pour $\delta: A \setminus \{0\} \rightarrow \mathbb{N}$ jusqu'à la fin de la partie B.

B.3) Soit $x \in A$ comme dans A.2). Justifier soigneusement que $A/(x)$ a 2 ou 3 éléments.

B.4) En déduire l'existence d'un morphisme surjectif $\varphi: A \rightarrow \mathbb{F}_p$ avec $p = 2$ ou 3 .

B.5) Justifier que $\varphi(m) = \bar{m}$ pour tout $m \in \mathbb{Z}$, où \bar{m} est la classe de m modulo p (pour $p = 2$ ou 3).

B.6) En déduire l'existence d'une racine du polynôme $X^2 - x + \bar{5} \in \mathbb{F}_p[X]$ dans \mathbb{F}_p , $p = 2$ ou 3 .

B.7) Conclure.

C. QUELQUES ISOMORPHISMES D'ANNEAUX

C.1) Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré ≥ 1 , et soit p un nombre premier. Si $f \in \mathbb{Z}[X]$, on note par $\bar{f} \in \mathbb{F}_p[X]$ sa réduction modulo p .

Montrer que l'on a un isomorphisme d'anneau

$$\mathbb{Z}[X]/(p, P) \simeq \mathbb{F}_p[X]/(\bar{P})$$

C.2) Soit $S = \mathbb{Z}[X]/(P)$. Montrer que l'on a un isomorphisme d'anneaux

$$S/(p) \simeq \mathbb{Z}[X]/(p, P)$$

Indication : On pourra commencer par montrer que la projection canonique $\pi: \mathbb{Z}[X] \rightarrow \mathbb{Z}[X]/(p, P)$ induit un morphisme d'anneaux

$$\rho: S \rightarrow \mathbb{Z}[X]/(p, P), f + (P) \mapsto f + (p, P)$$

C.3) Montrer que l'on a un isomorphisme d'anneaux

$$A \simeq \mathbb{Z}[X]/(X^2 - x + 5)$$

D. A EST PRINCIPAL

Soient $z, z' \in A, z' \neq 0$. Le but des premières questions est de montrer l'existence de $q, r \in A$ tels que

i) $r = 0$ ou $\nu(r) < \nu(z')$

ii) $z = qz' + r$ ou $2z = qz' + r$.

D.1) Montrer que $\frac{z}{z'} = u + v\alpha$ pour certains $u, v \in \mathbb{Q}$. On notera alors $n \in \mathbb{Z}$ la partie entière de v .

D.2) On suppose que $v \notin \left]n + \frac{1}{3}, n + \frac{2}{3}\right]$. Montrer qu'il existe $s, t \in \mathbb{Z}$ tels que

$$|u - s| \leq \frac{1}{2} \quad \text{et} \quad |v - t| \leq \frac{1}{3}$$

En déduire que $q = s + t\alpha$ et $r = z - qz'$ conviennent.

D.3) On suppose que $v \notin \left]n + \frac{1}{3}, n + \frac{2}{3}\right]$, et on note m la partie entière de $2v$. En déduire l'existence de q et r satisfaisant les conditions requises.

On veut montrer maintenant que A est principal.

D.4) Etablir l'isomorphisme

$$A/(2) \simeq \mathbb{F}_2[X]/(X^2 + X + \bar{1})$$

et en déduire que (2) est maximal.

On suppose dans les dernières questions que I est un idéal de A non nul qui n'est pas principal. Soit $z' \in I \setminus \{0\}$ tel que $\nu(z')$ soit minimal. Par hypothèse, il existe $z \in I$ tel que $z \notin (z')$.

D.5) On suppose que $z = z'q + r$ avec $q, r \in A$, $r = 0$ ou $\nu(r) < \nu(z')$. Montrer que $r \in I$. En déduire une contradiction.

D.6) On suppose $2z = z'q + r$ avec $q, r \in A$, $r = 0$ ou $\nu(r) < \nu(z')$.

a) Montrer que $z'q = 2z$

b) Montrer que $z' \in (2)$ ou $q \in (2)$.

c) Exclure le second cas.

Ecrivons donc $z' = 2w$, $w \in A$, de sorte que $z = wq$.

d) Montrer que $(2, q) = A$

e) En déduire que $w \in I$. Comparer $\nu(w)$ et $\nu(z')$.

D.7) Conclure.

Deuxième partie

Corrigé

Remarque

Notons $\alpha = \frac{1 + i\sqrt{19}}{2}$. Si $z = a + b\alpha \in \mathbb{Z}[\alpha]$, on a $\bar{z} \in \mathbb{Z}[\alpha]$.

En effet, $\bar{z} = a + \frac{b}{2} - ib\frac{\sqrt{19}}{2} = \underbrace{a + \frac{b}{2}}_{\in \mathbb{Z}} + \underbrace{(-b)}_{\in \mathbb{Z}}\alpha \in \mathbb{Z}[\alpha]$

A. PRÉLIMINAIRES.

A.1) A est un anneau, donc un groupe à p éléments. Comme p est premier, alors A est un groupe cyclique, et en particulier l'ordre de 1_A est p . La caractéristique de l'anneau est l'entier $\text{car}(A) \leq 0$ défini par

$$\text{Ker}(\Theta_A) = \text{car}(A)\mathbb{Z}$$

Or $p \cdot 1_A = 0_A$ donc $\text{car}(A)$ divise p , c'est-à-dire $\text{car}(A) = 1$ ou p . Mais l'anneau A n'est pas trivial donc $\text{car}(A) = p$.

De plus, $\text{Im}(\Theta_A) = A$ car A est cyclique engendré par 1_A . Donc, par le premier théorème d'isomorphisme, il existe un isomorphisme $\overline{\Theta}_A: \mathbb{Z}/p\mathbb{Z} \rightarrow A$, et on a donc un isomorphisme d'anneaux $\mathbb{F}_p \simeq A$

A.2) Si A est un corps, on prend $x = 0$, d'où $(x) = (0)$ et $A/(x) = A/(0) = A$. Comme $A^\times \cup \{0\} = A$, le morphisme considéré est clairement surjectif (c'est l'identité). Si A n'est pas un corps, on choisit $x \in A$, $x \notin A^\times$, $x \neq 0$ tel que $\delta(x)$ soit minimal. En particulier, pour tout $y \in A$, $y \neq 0$ tel que $\delta(y) < \delta(x)$, on a $y \in A^\times$. On veut montrer que le morphisme $\psi: A^\times \cup \{0\} \rightarrow A/(x)$, $a \mapsto \bar{a}$ est surjectif, c'est-à-dire que tout élément \bar{a} de $A/(x)$ a un antécédent nul ou inversible. Soit $a \in A$. Comme l'anneau est euclidien, il existe $(q, r) \in A$ tels que $a = xq + r$ avec $r = 0$ ou $\delta(r) < \delta(x)$, c'est-à-dire $r \in A^\times \cup \{0\}$ d'après ce qui précède; et $\psi(r) = \bar{r} = \overline{a - qx} = \bar{a}$. On a montré que $\forall \bar{a} \in A/(x)$, $\exists r \in A^\times \cup \{0\}$ tel que $\psi(r) = \bar{a}$, donc ψ est bien surjectif.

Dans la suite du problème, on note $\alpha = \frac{1 + i\sqrt{19}}{2}$ et $A = \mathbb{Z}[\alpha]$.

B. A N'EST PAS EUCLIDIEN.

B.1) Comme $\alpha\bar{\alpha} = 5$, $\alpha + \bar{\alpha} = 1$ et que α est racine du polynôme $X - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha} = X^2 - X + 5$, on a $\alpha^2 - \alpha + 5 = 0$.

$$\begin{aligned}
\nu(a + b\alpha) &= |a + b\alpha|^2 = (a + b\alpha)\overline{(a + b\alpha)} \\
&= \left(\left(a + \frac{b}{2} \right) + i \frac{\sqrt{19}}{2} \right) \overline{\left(\left(a + \frac{b}{2} \right) + i \frac{\sqrt{19}}{2} \right)} \\
&= \left(\left(a + \frac{b}{2} \right) + i \frac{\sqrt{19}}{2} \right) \left(\left(a + \frac{b}{2} \right) - i \frac{\sqrt{19}}{2} \right) \\
&= \left(a + \frac{b}{2} \right)^2 + \frac{19b^2}{4} = a^2 + ab + 5b^2 \in \mathbb{N}
\end{aligned}$$

B.2) Soit $z \in A^\times$. On a $1 = \nu(1) = \nu(zz^{-1}) = \underbrace{\nu(z)}_{\in \mathbb{N}} \underbrace{\nu(z^{-1})}_{\in \mathbb{N}}$, donc $\nu(z) = 1$. On a donc, si $z = a + b\alpha$, la relation $a^2 + ab + 5b^2 = 1$ avec $a, b \in \mathbb{Z}$. Or, $a^2 + b^2 + ab \geq a^2 + b^2 - |ab| \geq (|a| - |b|)^2 \geq 0$ donc $1 = a^2 + ab + 5b^2 \geq 4b^2$ d'où $b = 0$ et du coup, $a = \pm 1$. On a donc $A^\times \subset \{\pm 1\}$, et l'inclusion réciproque étant évidente, $A^\times = \{\pm 1\}$.

B.3) A est maintenant supposé euclidien jusqu'à la fin de la partie B. D'après la question A.2), le morphisme $\psi: A^\times \cup \{0\} \rightarrow A/(x), a \mapsto \bar{a}$ est surjectif. On en déduit que $\text{card}(A/(x)) \leq \text{card}(A^\times \cup \{0\}) = \text{card}(A^\times) + \text{card}(\{0\})$ car l'anneau A n'est pas trivial (i.e $0 \neq 1, -1$). Si $-1 \neq 1$ (l'autre cas étant encore plus restrictif) alors $\text{card } A^\times = 2$ et $\text{card}(A/(x)) \leq 3$. Comme $\bar{0} \neq \bar{1}$ (car x non inversible), ils sont tous les deux dans $A/(x)$ et $\text{card}(A/(x)) \geq 2$. Donc $A/(x)$ a deux ou trois éléments.

B.4) $A/(x)$ est un anneau à 2 ou 3 éléments, or il n'y a qu'une seule structure de groupe à p éléments lorsque que $p = 2$ ou 3 , et c'est $\mathbb{Z}/p\mathbb{Z}$. Il existe donc un isomorphisme noté $\pi: A/(x) \rightarrow \mathbb{F}_p$ où $p = 2$ ou 3 , donc un morphisme surjectif. Si on pose

$$\begin{aligned}
\phi: \quad A &\longrightarrow A^\times \cup \{0\} \\
x \in A^\times &\longmapsto x \\
x \notin A^\times &\longmapsto 0
\end{aligned}$$

ϕ est clairement un morphisme surjectif.

Finalement, posons $\varphi = \pi \circ \psi \circ \phi$. On a $\varphi: A \xrightarrow{\phi} A^\times \cup \{0\} \xrightarrow{\psi} A/(x) \xrightarrow{\pi} \mathbb{F}_p$ qui est donc un morphisme surjectif (composée de morphismes surjectifs).

B.5) Comme φ est un morphisme d'anneaux, on a $\varphi(1_A) = \bar{0}$ ou $\bar{1}$ car $\varphi(1_A) = \varphi(1_A) \cdot \varphi(1_A)$. Or, $\varphi(1_A) = \bar{0}$ impliquerait que φ serait le morphisme nul, ce qui est impossible car φ est surjectif. Donc $\varphi(1_A) = \bar{1}$ et $\varphi|_{\mathbb{Z}}$ est la projection canonique de \mathbb{Z} sur \mathbb{F}_p , car

$$\forall m \in \mathbb{Z}, \varphi(m) = \varphi|_{\mathbb{Z}}(m) = \varphi(m \cdot 1_A) = m\varphi(1_A) = m\bar{1} = \bar{m}$$

B.6) Posons $\beta = \varphi(\alpha) \in \mathbb{F}_p$. On a

$$\bar{0} \stackrel{\text{B.5}}{=} \varphi(0) = \varphi(\alpha^2 - \alpha + 5) \stackrel{\varphi \text{ morphisme}}{=} \varphi(\alpha)^2 - \varphi(\alpha) + \varphi(5) \stackrel{\beta = \varphi(\alpha) \text{ et B.5}}{=} \beta^2 - \beta + \bar{5}$$

Donc $\beta \in \mathbb{F}_p$ est une racine de $X^2 - X + \bar{5} \in \mathbb{F}_p[X]$.

B.7) Posons $P = X^2 - X + \bar{5} \in \mathbb{F}_p[X]$. Dans \mathbb{F}_2 , $P = X^2 + X + \bar{1}$, donc $P(\bar{0}) = \bar{1}$ et $P(\bar{1}) = \bar{3} = \bar{1}$, donc le polynôme n'a pas de racine. De même, dans \mathbb{F}_3 , $P = X^2 - X - \bar{1}$ et $P(\bar{0}) = P(\bar{1}) = \bar{-1}$ et $P(\bar{-1}) = \bar{1}$, donc P n'a pas de racine. On aboutit à une contradiction alors qu'on avait supposé A euclidien.

Enfinement, $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ n'est pas euclidien.

C. QUELQUES ISOMORPHISMES D'ANNEAUX

C.1) Notons déjà que comme P est unitaire, alors $\bar{P} \in \mathbb{F}_p[X]$ n'est pas le polynôme nul (la division euclidienne est donc licite), et on a aussi que P a comme coefficient dominant un élément inversible de $\mathbb{Z}[X]$ (c'est-à-dire les mêmes que \mathbb{Z} , à savoir $\{\pm 1\}$), et on peut effectuer la division euclidienne des polynômes de $\mathbb{Z}[X]$ par P .

Posons $\varphi: \mathbb{Z}[X] \xrightarrow{\psi} \mathbb{F}_p[X] \xrightarrow{\pi} \mathbb{F}_p[X]/(\bar{P})$, où ψ est la réduction modulo p

$$Q \longmapsto \bar{Q} \longmapsto \bar{\bar{Q}}$$

d'un polynôme et π la réduction modulo l'idéal (\bar{P}) . On note à l'aide d'un $\bar{}$ les classes dans l'anneau $\mathbb{F}_p[X]/(\bar{P})$ la notation $\bar{}$ étant déjà utilisée pour la réduction modulo p . φ est clairement un morphisme d'anneaux surjectif (comme composée de deux morphismes surjectifs). En particulier, $\text{Im}(\varphi) = \mathbb{F}_p/(\bar{P})$. Soit maintenant $Q \in \text{Ker}(\varphi)$, c'est-à-dire $Q \in \mathbb{Z}[X]$ tel que $\varphi(Q) = \bar{\bar{Q}} = \bar{0}$. Donc $\bar{Q} \in (\bar{P})$, c'est-à-dire qu'il existe $\bar{R} \in \mathbb{F}_p[X]$ tel que $\bar{Q} = \bar{P} \cdot \bar{R} = \overline{PR}$. Donc $\bar{Q} - \overline{PR} = \bar{0}$, c'est-à-dire qu'il existe $S \in \mathbb{Z}[X]$ tel que $Q - PR = pS$, i.e. $Q = RP + pS \in (p, P)$. Réciproquement, on a clairement $(p, P) \subset \text{Ker}(\varphi)$, d'où l'égalité $\text{Ker}(\varphi) = (p, P)$ et par le premier théorème d'isomorphisme, on a un isomorphisme d'anneaux

$$\mathbb{Z}[X]/(p, P) = \mathbb{Z}[X]/\text{Ker}(\varphi) \simeq \text{Im}(\varphi) = \mathbb{F}_p[X]/(\bar{P})$$

C.2) Soit $\pi: \mathbb{Z}[X] \rightarrow \mathbb{Z}[X]/(p, P)$ la projection canonique modulo (p, P) . Soient $Q, Q' \in \mathbb{Z}[X]$ tels que $Q - Q' \in (P)$ (autrement dit, Q et Q' sont dans la même classe dans $\mathbb{Z}[X]/(P) = S$). On a $\pi(Q - Q') = \bar{0}$ d'où $\pi(Q) = \pi(Q')$. On peut restreindre π à S (puisque ça ne dépend pas du représentant choisi) et on pose $\rho = \pi|_S$ le morphisme

$\rho: S \rightarrow \mathbb{Z}[X]/(p, P)$. Le morphisme est clairement surjectif. Soit maintenant $f \in \text{Ker}(\rho)$, on a donc $f \in (p, P)$, c'est-à-dire $\exists f', f'' \in \mathbb{Z}[X]$ tels que $f = pf' + \underbrace{Pf''}_{=0}$

dans l'anneau $S = \mathbb{Z}[X]/(P)$ donc $f \in (p)$ et on déduit que $\text{Ker}(\rho) \subset (p)$ et comme l'inclusion réciproque est évidente, $\text{Ker}(\rho) = (p)$. Par le théorème d'isomorphisme, on déduit :

$$S/(p) = S/\text{Ker}(\rho) \simeq \text{Im}(\rho) = \mathbb{Z}[X]/(p, P)$$

C.3) Soit le morphisme $f: \mathbb{Z}[X] \rightarrow \mathbb{C}$.

$$P \longmapsto P(\alpha)$$

On a clairement $A = \mathbb{Z}[\alpha] \subset \text{Im}(f)$ car $\forall z \in A, \exists a, b \in \mathbb{Z}, z = a + b\alpha = \underbrace{f(a + bX)}_{\in \mathbb{Z}[X]}$.

Réciproquement, si $P = \sum_{k=0}^d a_k X^k \in \mathbb{Z}[X]$. Montrons par récurrence sur $n \in \mathbb{N}^*$ la

propriété

$$\mathcal{H}_n : " \exists u_n, v_n \in \mathbb{Z}, \alpha^n = u_n + v_n \alpha "$$

C'est clairement vrai au rang $n = 1$ (avec $u_1 = 0, v_1 = 1$). Supposons maintenant la propriété vraie au rang n . On a donc l'existence de $u_n, v_n \in \mathbb{Z}$ tels que $\alpha^n = u_n + v_n \alpha$. Notons que l'on a $\alpha^2 = -5 + \alpha$ (cf. B.1), d'où :

$$\begin{aligned} \alpha^{n+1} = \alpha^n \alpha &= (u_n + v_n \alpha) \alpha \\ &= \underbrace{-5v_n}_{=u_{n+1} \in \mathbb{Z}} + \underbrace{(u_n + v_n)}_{=v_{n+1} \in \mathbb{Z}} \alpha \end{aligned}$$

et on a \mathcal{H}_{n+1} . D'où

$$P(\alpha) = \sum_{k=0}^d a_k \alpha^k = a_0 + \sum_{k=1}^d a_k (u_k + v_k \alpha) = \underbrace{(a_0 + \sum_{k=1}^d a_k u_k)}_{\in \mathbb{Z}} + \alpha \underbrace{(\sum_{k=1}^d a_k v_k)}_{\in \mathbb{Z}} \in \mathbb{Z}[\alpha] = A$$

Donc $\text{Im}(f) = A$. Soit maintenant $P \in \text{Ker}(f)$. On a $P(\alpha) = 0$. Or, $\alpha \in \mathbb{C} \setminus \mathbb{R}$ donc $\bar{\alpha} \neq \alpha$ est aussi racine de P (car P est à coefficient entiers donc réels et $P(\bar{\alpha}) = \overline{P(\alpha)} = 0$). Donc $(X - \alpha) | P$ et $(X - \bar{\alpha}) | P$ et comme $X - \alpha$ et $X - \bar{\alpha}$ sont premiers entre eux, on a $(X - \alpha)(X - \bar{\alpha}) = (X^2 - X + 5) | P$ dans $\mathbb{C}[X]$ et donc dans $\mathbb{Z}[X]$. Donc $\text{Ker}(f) \subset (X^2 - X + 5)$ et l'inclusion réciproque est évidente donc $\text{Ker}(f) = (X^2 - X + 5)$. Par le théorème d'isomorphisme on a

$$\mathbb{Z}[X]/(X^2 - X + 5) = \mathbb{Z}[X]/\text{Ker}(f) \simeq \text{Im}(f) = A$$

D. A EST PRINCIPAL

D.1) Comme $z, z' \in A, z' \neq 0$, il existe $(n, m, n', m') \in \mathbb{Z}^4$ tels que $|z'|^2 \neq 0, z = n + m\alpha, z' = n' + m'\alpha$. On a

$$\frac{z}{z'} = \frac{n + m\alpha}{n' + m'\alpha} = \frac{(n + m\alpha)\overline{(n' + m'\alpha)}}{|z'|^2}$$

Comme on a $\overline{(n' + m'\alpha)} \in A$ (par la remarque au début du devoir), il existe $U, V \in \mathbb{Z}$ tels que $(n + m\alpha)\overline{(n' + m'\alpha)} = U + V\alpha$, d'où en posant $u = \frac{U}{|z'|^2} \in \mathbb{Q}$ et $v = \frac{V}{|z'|^2} \in \mathbb{Q}$, on a $\frac{z}{z'} = u + v\alpha$

D.2) Soit n la partie entière de v . On suppose dans cette question que $v \notin]n + \frac{1}{3}, n + \frac{2}{3}]$ et soient alors s et t les entiers les plus proches de u et v respectivement. On a donc $|u - s| \leq \frac{1}{2}$ et $|v - t| \leq \frac{1}{3}$. En posant $q = s + t\alpha$ et $r = z - qz'$, on a la condition ii). Or, si $r \neq 0, \nu(r) = \nu(z')\nu(\frac{z}{z'} - q)$ et

$$\nu(\frac{z}{z'} - q) = (s - u)^2 + (s - u)(t - v) + 5(t - v)^2 \leq \frac{1}{4} + \frac{1}{2} \frac{1}{3} + 5 \frac{1}{9} = \frac{9 + 6 + 20}{36} = \frac{35}{36} < 1$$

d'où le *i*).

N.B : Le calcul effectué en B.1 a été généralisé, et cela fonctionne car il n'a pas été utilisé que l'on ne travaillait qu'avec des entiers.

D.3) On suppose maintenant que $v \in]n + \frac{1}{3}, n + \frac{2}{3}]$. Soit m la partie entière de $2v$, on a $2v \in](2n) + \frac{2}{3}, (2n + 1) + \frac{1}{3}]$ donc que $m = 2n$ ou $m = 2n + 1$, on a $2v \notin]m + \frac{1}{3}, m + \frac{2}{3}]$. On est ramené au cas précédent avec $2z = 2u + 2v\alpha$, et la condition *ii*) est bien vérifiée puisque cette fois $2z = qz' + r$.

D.4) On veut montrer que

$$A/(2) \simeq \mathbb{F}_2[X]/(X^2 + X + \bar{1})$$

Par la question C.3), on a déjà un isomorphisme $A \simeq \mathbb{Z}[X]/(X^2 - X + 5)$. Par la question C.2), on déduit que $A/(2) \simeq (\mathbb{Z}[X]/(X^2 - X + 5))/(2) \simeq \mathbb{Z}[X]/(2, X^2 - X + 5)$. Finalement, par la question C.1), on déduit que $A/(2) \simeq \mathbb{Z}[X]/(2, X^2 - X + 5) \simeq \mathbb{F}_2/(\overline{X^2 - X + 5}) = \mathbb{F}_2/(X^2 + X + \bar{1})$. Et on a bien ce que l'on désirait.

De plus, \mathbb{F}_2 est un corps et $\bar{P} = X^2 + X + \bar{1}$ est irréductible dans $\mathbb{F}_2[X]$, donc $\mathbb{F}_2[X]/(X^2 + X + \bar{1})$ est un corps, donc $A/(2)$ aussi et (2) est maximal.

On suppose dans les dernières questions que I est un idéal de A non nul et non principal. Soit $z' \in I \setminus \{0\}$ tel que $\nu(z')$ soit minimal. Par hypothèse, il existe $z \in I$ tel que $z \notin (z')$.

D.5) On a $r = \underbrace{z}_{\in I} - \underbrace{z'}_{\in I} q \in I$ car I est un idéal. Si $r \neq 0$, on a $\nu(r) < \nu(z')$, ce qui est impossible par choix de z' puisque $\nu(z')$ est minimal. Donc $r = 0$ et $z \in (z')$, d'où la contradiction. Donc il n'existe pas $q, r \in A$ tels que $z = z'q + r$.

D.6) On suppose $2z = z'q + r$ avec $q, r \in A, r = 0$ ou $\nu(r) < \nu(z')$.

- De la même façon que précédemment, $r \in I$ donc $r = 0$ par choix de z' . On en déduit immédiatement que $2z = z'q$.
- Comme (2) est maximal, donc premier, $q \in (2)$ ou $z' \in (2)$.
- Si $q \in (2)$, il existe $q' \in A$ tel que $q = 2q'$ et $z = z'q' \in (z')$ par intégrité de A ce qui est impossible. Donc $z' \in (2)$ et il existe $w \in A$ tel que $z' = 2w$ et par intégrité $z = wq$.
- Comme l'idéal (2) est maximal et ne contient pas q , alors l'idéal $(2, q) = A$. On a donc une relation de Bezout, et il existe $a, b \in A$ tels que $2a + bq = 1$.
- On en déduit que $w = 2aw + bqw = az' + bz$ donc $w \in I$ car $z', z \in I$. Or, de $z' = 2w$, on tire $\nu(z') = \nu(2)\nu(w) > \nu(w)$.

D.7) Et cette inégalité stricte est absurde puisqu'elle contredit la minimalité de $\nu(z')$. Donc I est principal. Tout idéal de A est principal et comme A intègre (car sous-anneau de \mathbb{C}

qui est intègre), on déduit finalement que $\mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right]$ est principal.