Université Aix–Marseille 2019–2020

Licence – Mathématiques
Algèbre 2

Cours à distance – Semaine 7 – Propriétés d'anneaux – Corrigé TD

Exercice 1. *On considère l'anneau* $\mathbb{Z}[\sqrt{10}] := \{a + \sqrt{10}\, b \mid a, b \in \mathbb{Z}\}$. *L'objectif de cet exercice est de montrer que* $\mathbb{Z}[\sqrt{10}]$ *n'est pas factoriel.*

1. (a) *Montrer que* $\sqrt{10}$ *n'est pas rationnel.*
   Supposons par l'absurde que $\sqrt{10}$ soit rationnel, c'est-à-dire qu'il existe $p, q \in \mathbb{Z}^*$ premiers entre eux tels que $\sqrt{10} = \frac{p}{q}$. On a alors $p = \sqrt{10}q$ et donc $p^2 = 10q^2$. En particulier, 2 divise p^2 et donc, d'après le lemme d'Euclide, 2 divise p. Il existe de fait $p' \in \mathbb{Z}$ tel que $p = 2p'$ et on a $4{p'}^2 = 10q^2$, ainsi que $2{p'}^2 = 5q^2$. Mais alors 2 divise $5q^2$, donc q^2 d'après le lemme de Gauss, 2 et 5 étant premiers entre eux, et donc q d'après le lemme d'Euclide. Cela contredit l'hypothèse que p et q sont premiers entre eux. On en déduit que $\sqrt{10}$ est bien irrationnel.
   (b) *En déduire que, si* $a + \sqrt{10}b = a' + \sqrt{10}b'$ *avec* $a, a', b, b' \in \mathbb{Z}$, *alors* $a = a'$ *et* $b = b'$.
   Par hypothèse, on a $a - a' = \sqrt{10}(b' - b)$. On a alors $b = b'$, car sinon on aurait $b' - b \neq 0$ et donc $\sqrt{10} = \frac{a-a'}{b'-b}$, ce qui contredirait l'irrationalité de $\sqrt{10}$. Mais alors $a - a' = 0$ et donc $a = a'$.
2. (a) *Soit* $a + \sqrt{10}b \in \mathbb{Z}[\sqrt{10}]^\times$.
   i. *Montrer que* a *est non nul, et que* a *est premier avec* b *et avec* 10.
   Puisque $a + \sqrt{10}b$ est inversible dans $\mathbb{Z}[\sqrt{10}]$, il existe $a', b' \in \mathbb{Z}$ tels que
   $$1 = (a + \sqrt{10}b)(a' + \sqrt{10}b') = aa' + 10bb' + (ab' + a'b)\sqrt{10}.$$
   D'après la question 1.(b), on a alors $aa' + 10bb' = 1$ et $ab' + a'b = 0$. De la première égalité, on déduit déjà que $aa' = 1 - 10bb'$ est impair, et donc que a est lui-même impair donc non nul. De plus, elle donne simultanément une identité de Bézout entre a et b, ainsi qu'entre a et 10, montrant que a est premier avec b, mais aussi avec 10.
   ii. *Montrer que* $a^2 - 10b^2 = \pm 1$.
   En reprenant les notations de la question précédente, et en utilisant la seconde égalité, on a $b' = -\frac{a'b}{a}$ puisque $a \neq 0$. Réinjecté dans la première égalité, cela donne $aa' - 10\frac{a'b^2}{a} = 1$, et donc $a = a^2a' - 10a'b^2 = a'(a^2 - 10b^2)$. Considérons maintenant par l'absurde un diviseur $p \in \mathbb{N}^*$ premier de $a^2 - 10b^2$. D'après ce qui précède, c'est également un diviseur de a, et donc un diviseur de $10b^2 = a^2 - (a^2 - 10b^2)$. C'est de fait un diviseur commun à a et $10b^2$, et donc, d'après le lemme d'Euclide, soit un diviseur commun à a et 10, soit un diviseur commun à a et b. Dans les deux cas, cela contredit la question précédente. On en déduit que $a^2 - 10b^2$ n'a pas de diviseur premier, et donc que $a^2 - 10b^2 = \pm 1$.
   (b) *Montrer que* $\mathbb{Z}[\sqrt{10}]^\times = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}$ *tels que* $a^2 - 10b^2 = \pm 1\}$.
   A la question précédente, nous avons montré que
   $$\mathbb{Z}[\sqrt{10}]^\times \subset \{a + b\sqrt{10} \mid a, b \in \mathbb{Z} \text{ tels que } a^2 - 10b^2 = \pm 1\}.$$
   Mais réciproquement, pour tout $a, b \in \mathbb{Z}$ tels que $a^2 - 10b^2 = \varepsilon = \pm 1$, il est clair que $a + b\sqrt{10} \in \mathbb{Z}[\sqrt{10}]^\times$ car $(a + b\sqrt{10})(\varepsilon a - \varepsilon b\sqrt{10}) = \varepsilon(a^2 - 10b^2) = 1$.
3. (a) *Supposons dans cette question que* 2 *n'est pas irréductible dans* $\mathbb{Z}[\sqrt{10}]$.
   i. *Montrer qu'il existe* $a, b \in \mathbb{Z}$ *tels que* $a^2 - 10b^2 = \pm 2$.
   Puisque 2 n'est pas irréductible, il existe $a, a', b, b' \in \mathbb{Z}$ tels que $(a + b\sqrt{10})(a' + b'\sqrt{10}) = 2$, avec $a + b\sqrt{10}$ et $a' + b'\sqrt{10}$ non inversibles, c'est-à-dire tels que $a^2 - 10b^2, {a'}^2 - 10{b'}^2 \neq \pm 1$.

En développant, on obtient

$$aa' + 10bb' + (ab' + a'b)\sqrt{10} = 2,$$

et donc $aa' + 10bb' = 2$ et $ab' + a'b = 0$ d'après la question 1.(b). On en déduit

$$2 = 2 - 0\sqrt{10} = aa' + 10bb' - (ab' + a'b)\sqrt{10} = (a - b\sqrt{10})(a' - b'\sqrt{10})$$

et donc

$$\begin{aligned} 4 &= (a + b\sqrt{10})(a' + b'\sqrt{10})(a - b\sqrt{10})(a' - b'\sqrt{10}) \\ &= (a + b\sqrt{10})(a - b\sqrt{10})(a' + b'\sqrt{10})(a' - b'\sqrt{10}) \\ &= (a^2 - 10b^2)(a'^2 - 10b'^2). \end{aligned}$$

Les seuls facteurs de 4 étant ± 1, ± 2 et ± 4, et puisque $a^2 - 10b^2, a'^2 - 10b'^2 \neq \pm 1$, on en déduit que $a^2 - 10b^2 = a'^2 - 10b'^2 = \pm 2$.

ii. *Montrer que a est pair et b impair.*
On a $a^2 = 10b^2 \pm 2$ pair, donc a est pair, c'est-à-dire de la forme $a = 2\alpha$, avec $\alpha \in \mathbb{Z}$. En réinjectant cela dans l'équation, cela donne $4\widetilde{a}^2 - 10b^2 = \pm 2$, et donc $5b^2 = 1\alpha^2 \mp 1$ est impair, ce qui implique que b soit également impair.

iii. *On pose $\alpha, \beta \in \mathbb{Z}$ tels que $a = 2\alpha$ et $b = 2\beta + 1$. Montrer que $\alpha^2 - 10\beta(\beta + 1) \in \{2, 3\}$.*
En injectant dans l'équation, cela donne

$$\pm 2 = 4\alpha^2 - 10(2\beta^2 + 1)^2 = 4\alpha^2 - 40\beta^2 - 40\beta - 10$$

dont on déduit que $4\alpha^2 - 40\beta(\beta + 1) = 10 \pm 2$, c'est-à-dire $\alpha^2 - 10\beta(\beta + 1) = 2$ ou 3.

iv. *En déduire que, modulo 4, α^2 est congru à 2 ou -1.*
Comme, parmi deux entiers consécutifs, l'un est nécessairement pair, la quantité $\beta(\beta+1)$ est paire, et donc $10\beta(\beta+1)$ est divisible par 4. On en déduit que $\alpha^2 = 10\beta(\beta+1)+2$ ou 3 est congru à 2 ou 3 modulo 4, c'est-à-dire congru à 2 ou 3.

(b) *Montrer que 2 est irréductible dans $\mathbb{Z}[\sqrt{10}]$.*
A la question précédente, nous avons montré que, si 2 est irréductible dans $\mathbb{Z}[\sqrt{10}]$, alors il existe $\overline{\alpha} \in \mathbb{Z}/4\mathbb{Z}$ dont le carré vaut $\overline{2}$ ou $\overline{3}$. Or $\overline{0}^2 = \overline{2}^2 = \overline{0}$ et $\overline{1}^2 = \overline{3}^2\overline{1}$. Par l'absurde, on en déduit donc que 2 est irréductible dans $\mathbb{Z}[\sqrt{10}]$.

4. *Montrer que 2 n'est pas premier dans $\mathbb{Z}[\sqrt{10}]$.*
Commençons par remarquer que $(2) = \{2(a' + b'\sqrt{10}) \mid a', b' \in \mathbb{Z}\} = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z} \text{ pairs}\}$. Notamment, $\sqrt{10} \notin (2)$, or $\sqrt{10}.\sqrt{10} = 10 + 0\sqrt{10} \in (2)$. On en déduit que 2 n'est pas premier dans $\mathbb{Z}[\sqrt{10}]$.

5. *Conclure.*
Si $\mathbb{Z}[\sqrt{10}]$ était factoriel, alors les éléments irréductibles correspondraient exactement aux éléments premiers, or nous venons de voir que 2 est irréductible sans être premier.

Exercice 2. *On considère l'anneau $\mathbb{Z}[i\sqrt{5}] := \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$.*

1. *Montrer que l'application*

$$\varphi : \begin{array}{ccc} \mathbb{Z}[i\sqrt{5}] & \longrightarrow & \mathbb{N} \\ a + ib\sqrt{5} & \longmapsto & a^2 + 5b^2 \end{array}$$

vérifie, pour tous $x_1, x_2 \in \mathbb{Z}[i\sqrt{5}]$, $\varphi(x_1.x_2) = \varphi(x_1).\varphi(x_2)$.

Par calcul direct, pour tout $a, a', b, b' \in \mathbb{Z}$, on a

$$\begin{aligned}
\varphi\big((a+ib\sqrt{5})(a'+ib'\sqrt{5})\big) &= \varphi\big(aa'-5bb'+(ab'+a'b)i\sqrt{5}\big)\\
&= (aa'-5bb')^2+5(ab'+a'b)^2\\
&= a^2a'^2-10aa'bb'+25b^2b'^2+5a^2b'^2+10aa'bb'+5a'^2b^2\\
&= a^2a'^2+5a^2b'^2+5a'^2b^2+25b^2b'^2\\
&= (a^2+5b^2)(a'^2+5b'^2)\\
&= \varphi\big(a+ib\sqrt{5}\big)\varphi\big(a'+ib'\sqrt{5}\big).
\end{aligned}$$

2. *A l'aide de φ, déterminer tous les inversibles de $\mathbb{Z}[i\sqrt{5}]$.*

   Si $x \in \mathbb{Z}[i\sqrt{5}]^\times$, alors il existe $x^{-1} \in \mathbb{Z}[i\sqrt{5}]$ tel que $xx^{-1}=1$, et donc tel que $\varphi(x).\varphi(x^{-1})=1$. Puisque $\varphi(x), \varphi(x^{-1}) \in \mathbb{N}$, on en déduit en particulier que $\varphi(x)=1$. En notant $x=a+ib\sqrt{5}$, avec $a,b\in\mathbb{Z}$, on a donc $a^2+5b^2=1$, ce qui n'est possible que si $b=0$ et $a=\pm1$. Réciproquement, 1 et -1 sont clairement inversibles, étant chacun son propre inverse. On a donc $\mathbb{Z}[i\sqrt{5}]^\times=\{\pm1\}$.
3. *Soit $x_1, x_2 \in \mathbb{Z}[i\sqrt{5}]^*$. Montrer que si x_1 divise x_2 avec $x_1 \neq \pm x_2$, alors $\varphi(x_2) > \varphi(x_1)$.*

   Si x_1 divise x_2, alors il existe $d \in \mathbb{Z}[i\sqrt{5}]$ tel que $x_2=dx_1$. De plus, $d\neq\pm1$ puisque $x_1\neq\pm x_2$ et donc, d'après la solution à la question précédente, on a $\varphi(d)>1$. D'après la question 1, on a donc $\varphi(x_2)=\varphi(d)\varphi(x_1)>\varphi(x_1)$ puisque $\varphi(x_1)>0$, φ ne s'annulant qu'en 0.
4. *A l'aide de φ, déterminer tous les diviseurs non inversibles de 9, puis tous les diviseurs non inversibles de $3(2+i\sqrt{5})$.*

   Considérons $9=d_1d_2$, avec $d_1,d_2\in\mathbb{Z}[i\sqrt{5}]$, une décomposition de 9 dans $\mathbb{Z}[i\sqrt{5}]$. Alors $\varphi(d_1)\varphi(d_2)=\varphi(9)=81$ et $\varphi(d_1)\in\mathbb{N}$ est donc un diviseur de 81, c'est-à-dire, 1, 3, 9, 27 ou 81 :

   Si $\varphi(d_1)=1$ **:** alors $d_1=\pm1$ qui sont bien des diviseurs de 9 ;

   Si $\varphi(d_1)=3$ **:** alors, en notant $d_1=a+ib\sqrt{5}$, avec $a,b\in\mathbb{Z}$, on a $a^2+5b^2=3$, imposant $b=0$ et $a^2=3$, ce qui n'est pas possible ;

   Si $\varphi(d_1)=9$ **:** alors, en notant $d_1=a+ib\sqrt{5}$, avec $a,b\in\mathbb{Z}$, on a $a^2+5b^2=9$. Les seuls solutions sont $b=0$ et $a=\pm3$, et $b=\pm1$ et $a=\pm2$, c'est-à-dire $d_1=\pm3$ ou $d_1=\pm2\pm i\sqrt{5}$. Réciproquement, on a $(\pm3).(\pm3)=9$ et $(\pm2\pm i\sqrt{5})(\pm2\mp i\sqrt{5})=9$, tous correspondent donc bien à des diviseurs de 9 ;

   Si $\varphi(d_1)=27$ **:** alors $\varphi(d_2)=3$ et on a déjà vu que cela n'était pas possible ;

   Si $\varphi(d_1)=81$ **:** alors $\varphi(d_2)=1$, c'est-à-dire $d_2=\pm1$, et on a alors $d_1=\pm9$, lesquels sont bien tous des diviseurs de 9.

   Au final, l'ensemble des diviseurs de 9 est

   $$\big\{\pm1, \pm3, \pm(2+i\sqrt{5}), \pm(2-i\sqrt{5}), \pm9\big\}.$$

   Par une analyse tout à fait similaire, on trouve que l'ensemble des diviseurs de $3(2+i\sqrt{5})$ est

   $$\big\{\pm1, \pm3, \pm(2+i\sqrt{5}), \pm3(2+i\sqrt{5})\big\}.$$

5. *Montrer 9 et $3(2+i\sqrt{5})$ n'ont pas de plus grand diviseur commun dans $\mathbb{Z}[i\sqrt{5}]$.*

   D'après la question 3., les diviseurs communs à 9 et $3(2+i\sqrt{5})$ sont ±1, ±3 et $\pm(2+i\sqrt{5})$. D'après la question 3, cette liste ne contient pas de plus grand élément au sens de la divisibilité, 3 et $2+i\sqrt{5}$ étant tous les deux maximaux sans être comparable l'un à l'autre. En effet, ils maximisent tous les deux φ sans être opposé l'un de l'autre.
6. *Montrer que 3 et $2+i\sqrt{5}$ n'ont pas de plus petit multiple commun dans $\mathbb{Z}[i\sqrt{5}]$.*

   Puisque $9=3.3=(2+i\sqrt{5})(2-i\sqrt{5})$, 9 et $3(2+i\sqrt{5})$ sont deux multiples communs à 3 et $2+i\sqrt{5}$. Or, parmi les diviseurs communs à 9 et $3(2+i\sqrt{5})$, aucun n'est un multiple commun à 3 et $2+i\sqrt{5}$. Cela se vérifie facilement à l'aide de la question 3.

7. *L'application φ est-elle un stathme ?*

   Si φ était un stathme, alors $\mathbb{Z}[i\sqrt{5}]$ serait euclidien donc principal, et tout couple d'éléménts non nuls posséderaient un plus grand diviseur commun (et un plus petit multiple commun). D'après la question 5 (ou 6), l'application ne peut donc pas être un stathme.

Exercice 3. *Soit $\mathbb{Z}[i] \subset \mathbb{C}$ l'anneau des entiers de Gauss. On considère l'application*

$$\nu : \begin{array}{ccc} \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ a+ib & \longmapsto & a^2+b^2 \end{array}.$$

1. *Montrer que, pour tout $z \in \mathbb{C}$, il existe $\widetilde{z} \in \mathbb{Z}[i]$ tel que $|\widetilde{z}-z|^2 \leq \frac{1}{2}$.*

   On note $z =: a+ib$ avec $a, b \in \mathbb{R}$ et $\widetilde{z} =: \widetilde{a}+i\widetilde{b}$ avec $\widetilde{a}, \widetilde{b} \in \mathbb{Z}$, les entiers respectivement les plus proches [1] de a et b. On a donc $|\widetilde{a}-a|, |\widetilde{b}-b| \leq \frac{1}{2}$, et donc

$$|\widetilde{z}-z|^2 = (\widetilde{a}-a)^2 + (\widetilde{b}-b)^2 \leq \frac{1}{4}+\frac{1}{4} = \frac{1}{2}.$$

2. *En considérant, pour tout $z_1 \in \mathbb{Z}[i]$ et $z_2 \in \mathbb{Z}[i]^*$ une approximation dans $\mathbb{Z}[i]$ de $\frac{z_1}{z_2} \in \mathbb{C}$, montrer que $\mathbb{Z}[i]$ est un anneau euclidien.*

   Il suffit de montrer que ν est un stathme. Or :
   - pour tout $a+ib \in \mathbb{Z}[i]$, $\nu(a+ib) = a^2+b^2 = 0$ si et seulement si $a=b=0$ et donc si et seulement si $a+ib=0$;
   - pour tout $a+ib, a'+ib' \in \mathbb{Z}[i]$,

     $$\nu\big((a+ib)(a'+ib')\big) = \big|(a+ib)(a'+ib')\big| = |a+ib|.|a'+ib'| = \nu(a+ib)\nu(a'+ib') \geq \nu(a+ib)$$

     puisque $\nu(a'+ib') \geq 1$;
   - pour tout $z_1 \in \mathbb{Z}[i]$ et tout $z_2 \in \mathbb{Z}[i]^*$, il existe, d'après la question 1., $q \in \mathbb{Z}[i]$ tel que $\left|q - \frac{z_1}{z_2}\right| \leq \frac{1}{2}$. On pose $r = z_1 - qz_2 \in \mathbb{Z}[i]$. On a alors $z_1 = qz_2 + r$ et

$$\nu(r) = \nu(z_1-qz_2) = |z_1-qz_2| = |z_2|.\left|\frac{z_1}{z_2}-q\right| \leq \frac{1}{2}|z_2| < |z_2|.$$

3. *Déterminer un plus grand diviseur commun, ainsi qu'une relation de Bézout associée pour $1+3i$ et $3+i$.*

   Il suffit d'appliquer l'algorithme d'Euclide.

   Etape 1 : On a $\frac{1+3i}{3+i} = \frac{(1+3i)(3-i)}{|3+i|^2} = \frac{6+8i}{10}$ que l'on arrondit à $1+i$. Cela donne $1+3i = (1+i)(3+i)-1-i$.

   Etape 2 : On a $\frac{3+i}{-1-i} = -\frac{(3+i)(1-i)}{|1+i|^2} = -\frac{4-2i}{2} = -2+i$. Cela donne $3+i = (-1-i)(-2+i)+0$.

   En tant qu'opposé (pour limiter le nombre de signe $-$) du dernier reste non nul, on en déduit que $1+i$ est un plus grand diviseur commun de $1+3i$ et $3+i$. Par les calculs qui précèdent, on peut prend

$$1+i = (1+i)(3+i) - (1+3i)$$

   comme relation de Bézout.

1. si a et (resp. b) est un demi entier, alors $\widetilde{a}$ (resp. $\widetilde{b}$) n'est pas défini de manière unique, il peut être indifféremment égal à $a-\frac{1}{2}$ (resp. $b-\frac{1}{2}$) ou $a+\frac{1}{2}$ (resp. $b+\frac{1}{2}$). Dans ce cas, on choisit l'un ou l'autre