Université de Rennes 1 Année universitaire 2019-2020
Licence de mathématiques
Module Anneaux et Arithmétique

Contrôle continu n°3
Mercredi 6 mai 2020, 13h – 18h
Corrigé

Exercice

1 On rappelle qu'on note $\mathbf{F}_3$ le corps $\mathbf{Z}/3\mathbf{Z}$. Déterminer, en expliquant soigneusement votre démarche, un élément P de $\mathbf{F}_3[X]$ de degré 3 et irréductible. On pose désormais $\mathbf{K} := \mathbf{F}_3[X]/\langle P\rangle$ et on note α l'image de X dans $\mathbf{K}$.

Correction *: De manière générale, un polynôme de degré 3 à coefficients dans un corps* $\mathbf{L}$ *est irréductible dans* $\mathbf{L}[X]$ *si et seulement s'il n'a pas de racine dans* $\mathbf{L}$*. Il suffit donc de trouver un quadruplet* $(c_0, c_1, c_2, c_3) \in \mathbf{F}_3[X]$ *tel que* $c_3 \neq 0$ *et tel qu'on ait les relations (correspondant aux évaluations en les trois éléments de* $\mathbf{F}_3 = \{[0]_3, [1]_3, [-1]_3\}$*)*

$$c_0 \neq 0, \quad c_0 + c_1 + c_2 + c_3 \neq 0, \quad c_0 - c_1 + c_2 - c_3 \neq 0$$

Ainsi par exemple $P = X^3 - X^2 - X - [1]_3$ *est un élément irréductible de* $\mathbf{F}_3[X]$*.*

2 Donner *sans justification* la caractéristique et le cardinal de $\mathbf{K}$.

Correction *: La caractéristique de* $\mathbf{K}$ *est* 3 *et son cardinal est* $3^3 = 27$*.*

3 Choisir un triplet (a_0, a_1, a_2) d'éléments de $\mathbf{F}_3 \setminus \{0\}$; soit $x = a_0 + a_1.\alpha + a_2.\alpha^2$. Calculer les décompositions dans la $\mathbf{F}_3$-base $(1, \alpha, \alpha^2)$ de x^3 et de l'inverse de x. Le détail des calculs doit apparaître sur la copie.

Correction *: Prenons par exemple* $x = \alpha^2 - \alpha - [1]_3$ *(on verra ci-dessous que ce choix n'est pas innocent). Comme la caractéristique de* $\mathbf{K}$ *est* 3*, on a* $x^3 = (\alpha^2)^3 - \alpha^3 - [1]_3^3 = (\alpha^3)^2 - \alpha^3 - [1]_3$*. Comme* $P(\alpha) = 0$*, on a* $\alpha^3 = \alpha^2 + \alpha + [1]_3$*. Ainsi*

$$(\alpha^3)^2 = \alpha^4 + \alpha^2 + [1]_3^2 + 2\alpha^3 + 2\alpha^2 + 2\alpha$$

soit

$$(\alpha^3)^2 = \alpha(\alpha^2 + \alpha + [1]_3) + \alpha^2 + [1]_3^2 + 2(\alpha^2 + \alpha + [1]_3) + 2\alpha^2 + 2\alpha = \alpha^3 + 2\alpha$$

soit

$$(\alpha^3)^2 = \alpha^2 + \alpha + [1]_3 + 2\alpha = \alpha^2 + [1]_3$$

et au final

$$x^3 = (\alpha^3)^2 + \alpha^3 - [1]_3 = (\alpha^2 + [1]_3) - (\alpha^2 + \alpha + [1]_3) - [1]_3 = -\alpha - [1]_3.$$

Passons au calcul de x^{-1}*. De manière générale si* Q *est le polynôme de degré* 2 *de* $\mathbf{F}_3[X]$ *tel que* $x = Q(\alpha)$*, il s'agit de déterminer, via l'algorithme d'Euclide, une relation de Bezout pour* P *et* Q*, c'est à dire un couple* $(U, V) \in \mathbf{F}_3[X]$ *tel que* $U.P + V.Q = [1]_3$ *(noter que comme* P *est irréductible de degré* 3 *et* Q *est de degré* 2*,* P *et* Q *sont nécessairement premiers entre eux). En évaluant en* α*, on trouve* $U(\alpha).P(\alpha) + V(\alpha).Q(\alpha) = [1]_3$ *soit comme* $P(\alpha) = 0$*,* $V(\alpha).x = [1]_3$*, donc* $x^{-1} = V(\alpha)$*.*

Ici par une astuce malhonnête on a pris soin de choisir $x = Q(\alpha)$ *de sorte que* $P = XQ - [1]_3$ *d'où on déduit sans autre calcul que* $x^{-1} = \alpha$*.*

4 **(*)** Soit $\varphi\colon \mathbf{F}_3[X] \to \mathbf{K}$ l'unique morphisme de $\mathbf{F}_3$-algèbres qui envoie X sur x. Déterminer l'image de φ.

Correction : *$\varphi(\mathbf{F}_3[X])$ est un sous-anneau du corps fini $\mathbf{K}$, c'est donc en particulier un anneau intègre fini et donc un sous-corps de $\mathbf{K}$. Par ailleurs $\varphi(\mathbf{F}_3[X])$ contient $\varphi(\mathbf{F}_3) = \mathbf{F}_3$ et $\varphi(X) = x$ et comme $a_1 \neq 0$ (ou comme $a_2 \neq 0$), x n'est pas un élément de $\mathbf{F}_3$. Anisi $\varphi(\mathbf{F}_3[X])$ est un sous-corps de $\mathbf{K}$ contenant strictement $\mathbf{F}_3$. Comme le cardinal de $\mathbf{K}$ est 3^3, et que l'exposant 3 est premier, le théorème 15 du chapitre sur les corps finis entraîne que $\varphi(\mathbf{F}_3[X]) = \mathbf{K}$.*

Problème

Soit A le sous-ensemble de $\mathbf{C}$ défini par $A := \{a + i\,b\,\sqrt{2}, \quad (a,b) \in \mathbf{Z}^2\}$.

1 Montrer que A est un sous-anneau de $\mathbf{C}$ contenant $\mathbf{Z}$. En déduire que A est un anneau intègre.

Correction : *Soit z_1, z_2 des éléments de A, et $a_1, b_2, a_2, b_2 \in \mathbf{Z}$ tels que $z_1 = a_1 + i\,b_1\,\sqrt{2}$ et $z_2 = a_2 + i\,b_2\,\sqrt{2}$.*

On a

$$z_1 + z_2 = (a_1 + i\,b_1\,\sqrt{2}) + (a_2 + i\,b_2\,\sqrt{2}) = (a_1 + a_2) + i\,(b_1 + b_2)\,\sqrt{2}.$$

Comme $a_1, b_1, a_2, b_2 \in \mathbf{Z}$, on a $a_1 + a_2 \in \mathbf{Z}$ et $b_1 + b_2 \in \mathbf{Z}$. Donc $z_1 + z_2 \in A$.

On a

$$-z_1 = -(a_1 + i\,b_1\,\sqrt{2}) = (-a_1) + i\,(-b_1)\,\sqrt{2}.$$

Comme $a_1, b_1 \in \mathbf{Z}$, on a $-a_1 \in \mathbf{Z}$ et $-b_1 \in \mathbf{Z}$. Donc $-z_1 \in A$.

On a

$$z_1 z_2 = (a_1 + i\,b_1\,\sqrt{2})(a_2 + i\,b_2\,\sqrt{2}) = (a_1 a_2 - 2b_1 b2) + i\,(b_1 a_2 + b_2 a_1)\,\sqrt{2}.$$

Comme $a_1, b_1, a_2, b_2 \in \mathbf{Z}$, on a $a_1 a_2 - 2b_1 b2 \in \mathbf{Z}$ et $b_1 a_2 + b_2 a_1 \in \mathbf{Z}$. Donc $z_1 z_2 \in A$.

Par ailleurs $1 = 1 + i.0.\sqrt{2}$ et $0 = 0 + i.0.\sqrt{2}$ sont des éléments de A.

Tout ceci montre que A est un sous-anneau de $\mathbf{C}$.

Soit $a \in \mathbf{Z}$. On a $a = a + i.0.\sqrt{2} \in A$. Ainsi on a bien $\mathbf{Z} \subset A$.

Comme $\mathbf{C}$ est un corps, c'est un anneau intègre. Comme A est un sous-anneau de $\mathbf{C}$, A est également un anneau intègre.

2 *(la réponse à cette question n'est pas utilisée dans la suite)* **(*)** Décrire le corps des fractions de A ; déterminer en particulier s'il est ou non égal à $\mathbf{C}$.

Correction : *Comme A est un sous-anneau du corps $\mathbf{C}$, on sait d'après le cours que son corps des fractions* $\mathrm{Frac}(A)$ *est le sous-corps de $\mathbf{C}$ décrit par*

$$\mathrm{Frac}(A) = \left\{ \frac{z_1}{z_2}, \quad (z_1, z_2) \in A \times (A \setminus \{0\}) \right\}.$$

On peut montrer sur cette description que l'inclusion $\mathrm{Frac}(A) \subset \mathbf{C}$ *est stricte. Par exemple, montrons que $i \notin \mathrm{Frac}(A)$. Si c'était le cas, on aurait l'existence de $a_1, b_2, a_2, b_2 \in \mathbf{Z}$, avec $(a_2, b_2) \neq (0,0)$ tels que*

$$(a_2 + i\,b_2\,\sqrt{2})i = (a_1 + i\,b_1\,\sqrt{2}).$$

En identifiant les parties réelles, on obtient $a_2 = b_1\sqrt{2}$ et $a_1 = -b_2\sqrt{2}$. Comme $\sqrt{2}$ est irrationnel, on doit avoir $b_2 = b_1 = 0$ et de $b_2 = 0$ on tire $a_2 = 0$, donc $(a_2, b_2) = (0,0)$, contradiction.

On peut aussi montrer à partir de la description ci-dessus que

$$\mathrm{Frac}(A) = \{a + i\,b\,\sqrt{2}, \quad (a,b) \in \mathbf{Q}^2\}.$$

Il est à noter que le fait que $\mathrm{Frac}(A)$ *est un sous-corps strict de* $\mathbf{C}$ *ne démontre pas a priori que les corps* $\mathrm{Frac}(A)$ *et* $\mathbf{C}$ *ne sont pas isomorphes (*$\mathbf{Q}(T^2)$ *est un sous-corps strict du corps* $\mathbf{Q}(T)$*, et pourtant* $\mathbf{Q}(T^2)$ *et* $\mathbf{Q}(T)$ *sont isomorphes). Pour montrer que* $\mathrm{Frac}(A)$ *et* $\mathbf{C}$ *ne sont pas isomorphes, on peut par exemple montrer que l'équation*

$$(a + i\,b\,\sqrt{2})^2 = -1, \quad (a, b) \in \mathbf{Q}^2$$

n'a pas de solution (développer et identifier parties réelles et imaginaires, et utiliser l'irrationnalité de $\sqrt{2}$*).*

3 Pour tout élément z de $\mathbf{C}$, on note $\overline{z}$ le conjugué de z et on pose $\mathcal{N}(z) := z\,\overline{z}$.

1. Montrer que pour tous $z_1, z_2 \in \mathbf{C}$, on a $\mathcal{N}(z_1 z_2) = \mathcal{N}(z_1)\mathcal{N}(z_2)$.
   Correction *: Soit* $z_1, z_2 \in \mathbf{C}$*. On a*
   $$\mathcal{N}(z_1 z_2) = z_1 z_2\,\overline{z_1 z_2} = z_1 z_2\,\overline{z_1}\,\overline{z_2} = z_1\overline{z_1}.\,z_2\overline{z_2} = \mathcal{N}(z_1)\mathcal{N}(z_2).$$

2. Montrer qu'on a $\mathcal{N}(A) \subset \mathbf{N}$.
   Correction *: Soit* $z \in A$ *et* $a, b \in \mathbf{Z}$ *tel que* $z = a + i\,b\,\sqrt{2}$*. On a* $\mathcal{N}(z) = a^2 + 2b^2$*. Comme* a *et* b *sont dans* $\mathbf{Z}$*,* $a^2 + 2b^2$ *est un entier positif. Donc* $\mathcal{N}(z) \in \mathbf{N}$*. On a bien montré l'inclusion* $\mathcal{N}(A) \subset \mathbf{N}$*.*

3. Déterminer, si c'est possible, un élément de z de A tel que $\mathcal{N}(z) = 3$, puis un élément z de A tel que $\mathcal{N}(z) = 5$.
   Correction *: Déterminer un élément de* z *de* A *tel que* $\mathcal{N}(z) = 3$ *revient à chercher une solution de l'équation*
   $$a^2 + 2b^2 = 3, \quad (a, b) \in \mathbf{Z}^2.$$
   Soit $(a, b) \in \mathbf{Z}^2$*. Si* $|b| \geqslant 2$*, on a* $a^2 + 2b^2 \geqslant 8 > 3$ *donc* (a, b) *n'est pas solution de l'équation. Si* $b = 0$*, comme* 3 *n'est pas un carré dans* $\mathbf{Z}$*,* (a, b) *n'est pas non plus solution. Donc si* (a, b) *est solution de l'équation, nécessairement* $|b| = 1$*. Et* $(\pm 1, \pm 1)$ *sont bien des solutions. Ainsi* $z = 1 + i\sqrt{2}$ *est un élément de* A *qui vérifie* $\mathcal{N}(z) = 3$*.*
   Déterminer un élément de z *de* A *tel que* $\mathcal{N}(z) = 5$ *revient à chercher une solution de l'équation*
   $$a^2 + 2b^2 = 5, \quad (a, b) \in \mathbf{Z}^2.$$
   Soit $(a, b) \in \mathbf{Z}^2$*. Si* $|b| \geqslant 2$*, on a* $a^2 + 2b^2 \geqslant 8 > 5$ *donc* (a, b) *n'est pas solution de l'équation. Si* $b = 0$*, comme* 5 *n'est pas un carré dans* $\mathbf{Z}$*,* (a, b) *n'est pas non plus solution. Donc si* (a, b) *est solution de l'équation, nécessairement* $|b| = 1$*, et donc* $a^2 + 2 = 5$*; mais c'est impossible car* 3 *n'est pas un carré dans* $\mathbf{Z}$*. Ainsi il n'existe pas d'élément* z *de* A *qui vérifie* $\mathcal{N}(z) = 5$*.*

4 Soit B un sous-anneau de $\mathbf{C}$ stable par conjugaison (c'est à dire que pour tout $z \in B$, on a $\overline{z} \in B$) et tel que $\mathcal{N}(B) \subset \mathbf{N}$.

1. Donner deux exemples d'un tel sous-anneau B.
   Correction *: Pour* $a, b \in \mathbf{Z}$*, on a* $\overline{a + i\,b\,\sqrt{2}} = a - i\,b\,\sqrt{2}$*. Ceci montre que* A *est stable par conjugaison. Ainsi, d'après la question précédente,* A *est un exemple d'un tel sous-anneau* B*. On peut aussi vérifier que l'anneau* $\mathbf{Z}[i]$ *étudié en cours est un exemple.*

2. Montrer que l'ensemble $B^\times$ des éléments inversibles de B est égal à $\{z \in B, \quad \mathcal{N}(z) = 1\}$.
Correction *: Montrons l'inclusion*

$$B^\times \subset \{z \in B, \quad \mathcal{N}(z) = 1\}.$$

Soit $b \in B^\times$ et $c \in B$ tel que $bc = 1$. En utilisant la multiplicativité de $\mathcal{N}$ vue précédemment, on a

$$1^2 = \mathcal{N}(1) = \mathcal{N}(bc) = \mathcal{N}(b)\mathcal{N}(c).$$

Par hypothèse $\mathcal{N}(b)$ et $\mathcal{N}(c)$ sont des entiers naturels. Comme leur produit est 1, on a nécessairement $\mathcal{N}(b) = 1$.
Montrons à présent l'inclusion

$$\{z \in B, \quad \mathcal{N}(z) = 1\} \subset B^\times.$$

Soit $z \in B$ tel que $\mathcal{N}(z) = 1$. On a donc $z\overline{z} = 1$. Mais par hypothèse sur B on a $\overline{z} \in B$. Donc l'écriture $z\overline{z} = 1$ montre que z est un élément inversible de B, ce qui conclut.

3. Rappelons une caractérisation des éléments irréductibles d'un anneau intègre : un élément a d'un anneau intègre R est irréductible s'il est non nul, non inversible et pour tout couple (b, c) d'éléments de R tel que $a = bc$, b ou c est inversible.
Soit $z \in B$ tel que $\mathcal{N}(z) > 1$. On suppose que pour tout diviseur positif d de $\mathcal{N}(z)$ distinct de 1 et de $\mathcal{N}(z)$ on a : $d \notin \mathcal{N}(B)$. Montrer qu'alors z est un élément irréductible de B.
Correction *: Comme $\mathcal{N}(z) > 1$, on a $\mathcal{N}(z) \neq 0$, donc z est non nul, et $\mathcal{N}(z) \neq 1$, donc z est non inversible d'après la question 4.2. Soit $z_1, z_2 \in B$ tels que $z = z_1 z_2$. On a donc $\mathcal{N}(z) = \mathcal{N}(z_1 z_2) = \mathcal{N}(z_2)\mathcal{N}(z_2)$ Par hypothèse sur B, on a $\mathcal{N}(z_1)$ et $\mathcal{N}(z_2)$ sont des diviseurs positifs de $\mathcal{N}(z)$. L'hypothèse sur les diviseurs de $\mathcal{N}(z)$ montre alors que nécessairement $\{\mathcal{N}(z_1), \mathcal{N}(z_2)\} = \{1, \mathcal{N}(z)\}$. Donc nécessairement $\mathcal{N}(z_1) = 1$ ou $\mathcal{N}(z_2) = 1$; d'après la question 4.2, z_1 ou z_2 est inversible, et on conclut que z est irréductible.*

5 Déduire de la question 4.2 une description de l'ensemble $A^\times$ des éléments inversibles de A. Déterminer un élément $d \in \mathbf{N}$ tel que le groupe $A^\times$ est isomorphe au groupe $\mathbf{Z}/d\mathbf{Z}$.
Correction *: D'après la question 4.2, déterminer $A^\times$ revient à résoudre l'équation*

$$a^2 + 2b^2 = 1, \quad (a, b) \in \mathbf{Z}.$$

En raisonnant comme à la question 3, on voit que l'ensemble des solutions de cette équation est $\{(1, 0), (-1, 0)\}$. Ainsi $A^\times = \{1, -1\}$.

En particulier, $A^\times$ est un groupe d'ordre 2. Comme 2 est premier, $A^\times$ est cyclique, et donc isomorphe à $\mathbf{Z}/2\mathbf{Z}$. On peut bien sûr vérifier directement que l'application $A^\times \to \mathbf{Z}/2\mathbf{Z}$ qui à 1 associe $[0]_2$ et à -1 associe $[1]_2$ est un isomorphisme de groupes.

6 Soit n un entier naturel. On considère la propriété $(\mathcal{P})$ suivante : il existe $a, b \in \mathbf{Z}$ tel que $n = a^2 + 2\,b^2$.

1. Traduire la propriété $(\mathcal{P})$ en termes de l'application $\mathcal{N}$ et de l'anneau A.
Correction *: Si n est un entier naturel, dire que n vérifie $(\mathcal{P})$ sigifie exactement qu'il existe $z \in A$ tel que $n = \mathcal{N}(z)$. Autrement dit, n vérifie $(\mathcal{P})$ si et seulement si $n \in \mathcal{N}(A)$.*

2. Donner trois exemples de nombres premiers vérifiant $(\mathcal{P})$, et trois exemples de nombres premiers ne vérifiant pas $(\mathcal{P})$.

Correction *: Pour trouver des exemples, on peut considèrer les nombres premiers* $p = 2, 3, 5 \ldots$ *et chercher à résoudre, en raisonnant comme à la question 3, l'équation*

$$a^2 + 2b^2 = p, \quad (a, b) \in \mathbf{Z}^2.$$

Ainsi les nombres premiers $2 = 0^2 + 2.1^2$, $3 = 1^2 + 2.1^2$, *et* $11 = 3^2 + 2.1^2$ *vérifient la propriété* $(\mathcal{P})$. *Les nombres premiers* 5 *(déjà vu à la question 3),* 7 *et* 13 *ne la vérifient pas.*

3. En utilisant la question 4.3, en déduire un exemple explicite d'un élément de $\mathbf{Z}$ qui est un élément irréductible de A.
Correction *: Tout nombre premier* p *qui ne vérifie pas* $(\mathcal{P})$ *est irréductible dans* A. *En effet on a* $\mathcal{N}(p) = p^2 > 1$ *et comme* p *est premier le seul diviseur de* $\mathcal{N}(p)$ *distinct de* 1 *et* $\mathcal{N}(p)$ *est* p, *qui n'est pas dans* $\mathcal{N}(A)$ *puisque* p *ne vérifie pas* $(\mathcal{P})$. *D'après la question 4.3,* p *est irréductible dans* A. *Ainsi,* 5 *est un exemple explicite d'un élément de* $\mathbf{Z}$ *qui est un élément irréductible de* A.

4. Montrer que si le nombre premier p vérifie $(\mathcal{P})$ alors -2 est un carré dans $\mathbf{F}_p$, c'est à dire il existe $x \in \mathbf{F}_p$ tel que $x^2 = [-2]_p$.
Correction *: Soit* p *un nombre premier vérifiant la propriété* $(\mathcal{P})$. *Montrons que* -2 *est un carré dans* $\mathbf{F}_p$. *Soit* $a, b \in \mathbf{Z}$ *tel que* $p = a^2 + 2\,b^2$.
Montrons tout d'abord que p *ne divise pas* b. *Si tel était le cas, la relation* $p = a^2 + 2b^2$ *montre que* p *divise aussi* a^2, *donc, comme* p *est premier, également* a. *Si* $a', b' \in \mathbf{Z}$ *sont tels que* $a = pa'$ *et* $b = pb'$, *la relation* $p = a^2 + 2b^2$ *entraîne* $1 = p(a')^2 + p(b')^2$. *Donc* p *divise* 1, *contradiction.*
Ainsi on a $[b]_p \neq 0$, *et comme* $\mathbf{Z}/p\mathbf{Z}$ *est un corps,* $[b]_p$ *est inversible dans* $\mathbf{Z}/p\mathbf{Z}$. *En réduisant la relation* $p = a^2 + 2b^2$ *modulo* p, *on obtient* $0 = [a^2 + 2b^2]_p = [a]_p^2 + [2]_p[b]_p^2$ *d'où* $[-2]_p = \left(\frac{[a]_p}{[b]_p}\right)^2$. *Ainsi* -2 *est bien un carré dans* $\mathbf{F}_p$.

7 Soit p un nombre premier impair tel que -2 est un carré dans $\mathbf{F}_p$. Soit $c \in \mathbf{Z}$ tel que p divise $c^2 + 2$. Soit $\varphi\colon A \to \mathbf{Z}/p\mathbf{Z}$ l'application qui à $a + ib\sqrt{2} \in A$ associe $[a - c\,b]_p$.

1. Montrer que φ est un morphisme d'anneaux.
Correction *: Soit* z_1, z_2 *des éléments de* A, *et* $a_1, b_2, a_2, b_2 \in \mathbf{Z}$ *tels que* $z_1 = a_1 + i\,b_1\,\sqrt{2}$ *et* $z_2 = a_2 + i\,b_2\,\sqrt{2}$.
On a

$$\varphi(z_1 + z_2) = \varphi((a_1 + a_2) + i\,(b_1 + b_2)\,\sqrt{2}) = [(a_1 + a_2) - c(b_1 + b_2)]_p$$

Par ailleurs, en utilisant le fait que $a \mapsto [a]_p$ *est un morphisme de groupes, on a*

$$\varphi(z_1)+\varphi(z_2) = [a_1 - cb_1]_p + [a_2 - cb_2]_p = [(a_1 - cb_1) + (a_2 - cb_2)]_p = [(a_1 + a_2) - c(b_1 + b_2)]_p = \varphi(z_1 + z_2).$$

On a

$$\varphi(z_1 z_2) = \varphi((a_1 a_2 - 2b_1 b2) + i\,(b_1 a_2 + b_2 a_1)\,\sqrt{2}) = [(a_1 a_2 - 2b_1 b2) - c(b_1 a_2 + b_2 a_1)]_p$$

Par ailleurs, en utilisant le fait que $a \mapsto [a]_p$ *est un morphisme d'anneaux, on a*

$$\varphi(z_1)\varphi(z_2) = [a_1 - cb_1]_p [a_2 - cb_2]_p = [(a_1 - cb_1)(a_2 - cb_2)]_p = [a_1 a_2 + c^2 b_1 b_2 - c(b_1 a_2 + b_2 a_1)]_p$$

Par hypothèse, on a $[c^2]_p = [-2]_p$. *Ainsi, en utilisant à nouveau le fait que* $a \mapsto [a]_p$ *est un morphisme d'anneaux, on a*

$$\varphi(z_1)\varphi(z_2) = [a_1 a_2 - 2b_1 b_2 - c(b_1 a_2 + b_2 a_1)]_p = \varphi(z_1 z_2).$$

Par ailleurs

$$\varphi(1) = \varphi(1 + i.0.\sqrt{2}) = [1 - c.0]_p = [1]_p = 1_{\mathbf{Z}/p\mathbf{Z}}.$$

Ainsi φ est bien un morphisme d'anneaux.

2. *On admet que l'idéal* $\mathrm{Ker}(\varphi)$ *est engendré par un élément* $\alpha \in A$. **(*)** En utilisant le fait que $\mathrm{Ker}(\varphi)$ contient p et $c + i\sqrt{2}$, en déduire que p vérifie la propriété $(\mathcal{P})$.
Correction *: Noter qu'on a bien*

$$\varphi(p) = \varphi(p + i.0.\sqrt{2}) = [p - c.0]_p = [p]_p = [0]_p$$

et

$$\varphi(c + i\sqrt{2}) = [c - c.1]_p = [0]_p.$$

D'après la propriété admise, il existe $\beta, \gamma \in A$ tel que $p = \alpha\beta$ et $c + i\sqrt{2} = \alpha\gamma$. En particulier $p^2 = \mathcal{N}(p) = \mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta)$. Donc $N(\alpha) \in \{1, p, p^2\}$.
Si $N(\alpha) = 1$, on a $\alpha \in A^\times$ d'après la question 4.2, et donc $\mathrm{Ker}(\varphi) = A$. *C'est impossible car $\mathbf{Z}/p\mathbf{Z}$ n'est pas l'anneau nul.*
Si $N(\alpha) = p^2$, on a $\mathcal{N}(\beta) = 1$. D'après la question 4.2, p et α sont associés, et quitte à multiplier γ par un inversible de A, on a $c + i\sqrt{2} = p\gamma$. Soit $(a, b) \in \mathbf{Z}^2$ tel que $\gamma = a + ib\sqrt{2}$ En identifiant les parties imaginaires dans l'égalité $c + i\sqrt{2} = p(a + ib\sqrt{2})$ on trouve que p divise 1, contradiction.
Finalement, on a nécessairement $N(\alpha) = p$, ce qui montre que p vérifie la propriété $(\mathcal{P})$.

8 Soit $\mathbf{K}$ un corps et $x \in \mathbf{K}$. On dit que x est un carré dans $\mathbf{K}$ s'il existe $y \in \mathbf{K}$ tel que $x = y^2$. Soit Q l'anneau quotient $Q := \mathbf{K}[X]/\langle X^2 - x\rangle$.

1. Montrer que Q est un corps si et seulement si Q est intègre si et seulement si x n'est pas un carré dans $\mathbf{K}$.
Correction *: Comme $X^2 - x$ est un polynôme de degré 2, c'est un élément irréductible de $\mathbf{K}[X]$ si et seulement s'il n'a pas de racine dans $\mathbf{K}$; cette dernière condition équivaut clairement au fait que x n'est pas un carré dans $\mathbf{K}$; le résultat découle alors du cours.*

2. *(la réponse à cette question n'est pas utilisée dans la suite)* **(*)** Si x est un carré dans $\mathbf{K}$, montrer qu'on est dans l'un des deux cas suivants, suivant une condition sur x et $\mathbf{K}$ que l'on précisera :
   - l'anneau Q est isomorphe à l'anneau produit $\mathbf{K} \times \mathbf{K}$; c'est un anneau réduit (on rappelle qu'un anneau est réduit si pour tout élément a de cet anneau et tout entier naturel n, si $a^n = 0$ alors $a = 0$) ;
   - l'anneau Q est un anneau non réduit.

Correction *: Supposons tout d'abord que x est non nul et que la caractéristique de $\mathbf{K}$ n'est pas 2. Soit $y \in \mathbf{K}$ tel que $x = y^2$, de sorte que $X^2 - x = (X - y)(X + y)$. Comme x est non nul, y est non nul et comme la caractéristique de $\mathbf{K}$ n'est pas 2, y et $-y$ sont distincts. Ainsi les polynômes $X + y$ et $X - y$ sont premiers entre eux, et le théorème chinois montre que Q est isomorphe à l'anneau produit $\mathbf{K}[X]/\langle X - y\rangle \times \mathbf{K}[X]/\langle X + y\rangle$ et chacun des facteurs est isomorphe à $\mathbf{K}$ (déjà vu au CC2).*
Plus prosaïquement, on peut montrer directement que l'application $\mathbf{K}[X] \to \mathbf{K} \times \mathbf{K}$ qui à $P \in \mathbf{K}[X]$ associe (r_1, r_2) où r_1 (respectivement r_2) est le reste de la division euclidienne de P par $X - y$ (respectivement $X + y$) est un morphisme d'anneaux surjectif de noyau $\langle X^2 - x\rangle$

L'anneau $\mathbf{K}\times\mathbf{K}$ *est réduit. Soit* $(\alpha,\beta)\in\mathbf{K}\times\mathbf{K}$ *et* $n\in\mathbf{N}$ *tel que* $(\alpha,\beta)^n=0_{\mathbf{K}\times\mathbf{K}}$*. Par définition de la structure d'anneau produit, on a* $\alpha^n=0_{\mathbf{K}}$ *et* $\beta^n=0_{\mathbf{K}}$*. Comme* $\mathbf{K}$ *est un corps,* $\mathbf{K}$ *est intègre, donc* $(\alpha,\beta)=(0,0)$
Supposons à présent que x *est nul ou la caractéristique de* $\mathbf{K}$ *est* 2*. Soit* $y\in\mathbf{K}$ *tel que* $x=y^2$*. Les hypothèses permettent d'écrire* $X^2-x=(X-y)^2$*. Soit* α *l'image de* X *dans* Q*. On a donc* $(\alpha-y)^2=0$ *et* $\alpha-y\neq 0$ *(car* $(1,\alpha)$ *est une* $\mathbf{K}$*-base du* $\mathbf{K}$*-espace vectoriel* Q*). Ainsi* Q *n'est pas réduit*

9 Soit $\theta\colon \mathbf{Z}[X]\to\mathbf{C}$ l'unique morphisme d'anneaux qui envoie X sur $i\sqrt{2}$. Montrer que $\theta(\mathbf{Z}[X])=A$ et que le noyau de θ est l'idéal engendré par X^2+2.
Correction *: Soit* $P\in\mathbf{Z}[X]$ *que l'on écrit* $P=\sum_{i=0}^N a_iX^i$ *où* N *est un entier positf et* $(a_i)\in\mathbf{Z}^{N+1}$*. Alors* $\theta(P)=\sum_{i=0}^N a_i(i\sqrt{2})^i$*.*
Ainsi, si $(a,b)\in\mathbf{Z}^2$*, on a* $\theta(a+bX)=a+ib\sqrt{2}$*. Ceci montre l'inclusion* $A\subset\theta(\mathbf{Z}[X])$*.*
Par ailleurs, pour tout $Q\in\mathbf{Z}[X]$ *on a*

$$\theta(Q(X^2+2))=\theta(Q)\theta(X^2+2)=\theta(Q).[(i\sqrt{2})^2+2]=\theta(Q).0=0.$$

Ceci montre l'inclusion $\langle X^2+2\rangle\subset\mathrm{Ker}(\theta)$*.*
Montrons les inclusions réciproques $\theta(\mathbf{Z}[X])\subset A$ *et* $\mathrm{Ker}(\theta)\subset\langle X^2+2\rangle$*. Soit* $P\in\mathbf{Z}[X]$*. Comme le polynôme* X^2+2 *est un élément* unitaire *de* $\mathbf{Z}[X]$*, il existe* (Q,R) *un couple d'éléments de* $\mathbf{Z}[X]$ *tel que* $\deg(R)<\deg(P)=2$ *et* $P=(X^2+2)Q+R$*. En appliquant le morphisme d'anneaux* θ*, on trouve*

$$\theta(P)=\theta(X^2+2)\theta(Q)+\theta(R)=0.\theta(Q)+\theta(R)=\theta(R).$$

Comme $\deg(R)\leqslant 1$*, il existe* $(a,b)\in\mathbf{Z}^2$ *tel que* $R=a+bX$*, et donc* $\theta(R)=a+ib\sqrt{2}\in A$*. Ceci montre que* $\theta(P)\in A$*. Par ailleurs, par unicité des parties réelles et imaginaires d'un nombre complexe, on a* $\theta(R)=0$ *si et seulement si* $a=b=0$ *si et seulement si* $R=0$*. Donc* $\theta(P)=0$ *si et seulement si* $P=(X^2+2)Q$*. Ceci montre bien les inclusions annoncées et conclut la démonstration demandée.*

10 **(*)** Soit p un nombre premier. Déduire de la question précédente que l'idéal pA est un idéal premier de A si et seulement si -2 n'est pas un carré dans $\mathbf{F}_p$.
Correction *: La question précédente montre que* A *est isomorphe à l'anneau quotient* $\mathbf{Z}[X]/\langle X^2+2\rangle$*. Par l'un des théorèmes d'isomorphisme,* A/pA *est donc isomorphe à* $\mathbf{Z}/p\mathbf{Z}[X]/\langle X^2+[2]_p\rangle$*. Comme* p *est premier,* $\mathbf{Z}/p\mathbf{Z}$ *est un corps. D'après la question 8.1, l'anneau quotient* A/pA *est donc intègre si et seulement si* $[-2]_p$ *n'est pas un carré dans* $\mathbf{F}_p$*, d'où le résultat.*

11 On considère un rectangle du plan euclidien dont les côtés ont pour longueur 1 et $\sqrt{2}$.

1. Montrer que pour tout point du rectangle (au sens large : intérieur et côtés compris) il existe un sommet du rectangle tel que ce point est à distance <1 de ce sommet.
   Correction *: Choisissons un repère orthonormé. Quitte à effectuer une rotation et une translation, on peut supposer que les sommets du rectangle sont* $(0,0)$*,* $(1,0)$*,* $(1,\sqrt{2})$ *et* $(0,\sqrt{2})$*. Quitte à appliquer des symétries par rapport aux axes du rectangle, on peut supposer que le point considéré est dans le « petit » rectangle de sommets* $(0,0)$*,* $(\frac{1}{2},0)$*,* $(\frac{1}{2},\frac{\sqrt{2}}{2})$ *et* $(0,\frac{\sqrt{2}}{2})$*. Le carré de la distance de ce point à l'origine est alors majorée par*

$$\left(\frac{1}{2}\right)^2+\left(\frac{\sqrt{2}}{2}\right)^2=\frac{1}{4}+\frac{2}{4}=\frac{3}{4}<1$$

2. En déduire que pour tous $\alpha, \beta \in A$, avec $\beta \neq 0$, il existe $(q, r) \in A^2$ tel que $\alpha = \beta.q + r$ et $\mathcal{N}(r) < \mathcal{N}(\beta)$.
Correction *: Identifions* $\mathbf{C}$ *au plan euclidien, de sorte que pour* $z_1, z_2 \in \mathbf{C}$, $\mathcal{N}(z_1 - z_2)$ *représente le carré de la distance de* z_1 *à* z_2*. Pour un choix adéquat de* $(a, b) \in \mathbf{Z}^2$*, le quotient* $\frac{\alpha}{\beta}$ *définit un point d'un rectangle dont les sommets sont* $(a, b\sqrt{2})$*,* $(a+1, b\sqrt{2})$*,* $(a, (b+1)\sqrt{2})$ $((a+1), (b+1)\sqrt{2})$*. D'après la question précédente, il existe donc* $q \in A$ *tel que* $\mathcal{N}\left(\frac{\alpha}{\beta} - q\right) < 1$ *En multipliant cette inégalité par* $\mathcal{N}(\beta)$ *qui est strictement positif (car* β *est non nul) et en utilisant la question 3.1, on obtient* $\mathcal{N}(\alpha - \beta.q) < \mathcal{N}(\beta)$*. On conclut en posant* $r := \alpha - \beta.q$*.*

3. **(*)** En utilisant le résultat de la question précédente ainsi que ceux d'autres questions antérieures, en déduire que les conditions suivantes sont équivalentes :
   - (i) p est un élément irréductible de A ;
   - (ii) -2 n'est pas un carré modulo p ;
   - (iii) p ne vérifie pas la propriété $(\mathcal{P})$.

Correction *: La question précédente montre que A est un anneau euclidien, donc principal. Ceci montre le résultat admis de la question 7.2, et la question 7 montre que (iii) implique (ii). Par ailleurs, p étant non nul, on sait qu'alors p est est un élément irréductible de A si et seulement si pA est un idéal premier de A D'après la question 10, (i) et (ii) sont équivalents. D'après la question 6.4, (ii) implique (iii).*

12 **(*)** Expliciter un algorithme permettant, connaissant c, de déterminer l'élément α de la question 7.2.
Correction *: Commençons par constater que* $\mathrm{Ker}(\varphi)$ *est engendré par* p *et* $c + i\sqrt{2}$*. Soit en effet* $(a, b) \in \mathbf{Z}^2$ *tel que* $z := a + ib\sqrt{2} \in \mathrm{Ker}(\varphi)$*. Il existe donc* $k \in \mathbf{Z}$ *tel que* $a - cb = kp$*. On a alors*

$$z = a + ib\sqrt{2} = (a - cb) + b(c + i\sqrt{2}) = kp + b(c + i\sqrt{2})$$

ce qui montre bien que z *est dans l'idéal engendré par* p *et* $c + i\sqrt{2}$ *La réciproque est immédiate puisque* $c + i\sqrt{2}$ *et* p *sont dans* $\mathrm{Ker}(\varphi)$

Comme A est eucliden, l'élément α *est donc un pgcd de* p *et* $c + i\sqrt{2}$*, qui peut se déterminer en utilisant l'algorithme d'Euclide basé sur la division euclidienne de stathme* $\mathcal{N}$*.*

13 **(*)** Soit I_1 l'ensemble des nombres premiers qui ne vérifient pas la propriété $\mathcal{P}$ ainsi que les opposés de ces nombres premiers et I_2 l'ensemble des $z \in A$ tel que $\mathcal{N}(z)$ est un nombre premier qui vérifie la propriété $(\mathcal{P})$. Montrer que l'ensemble des éléments irréductibles de A est la réunion des ensembles I_1 et I_2.
Correction *: La question 4.3 montre que tous les éléments de* I_1 *sont irréductibles. La question 4.3 montre que tous les élément de* I_2 *sont irréductible.*

Soit z *un élément irréductible de A. On a* $\mathcal{N}(z) = z\overline{z}$*. Comme* z *est irréductible et le lemme d'Euclide vaut dans A (car A est euclidien),* z *divise l'un des facteurs premiers* p *de* $\mathcal{N}(z)$*. On en déduit que* $\mathcal{N}(z)$ *divise* $\mathcal{N}(p) = p^2$*, donc* $\mathcal{N}(z) \in \{1, p, p^2\}$

Comme z *est irréductible,* z *n'est pas inversible et donc* $\mathcal{N}(z) \neq 1$*. Si* $\mathcal{N}(z) = p$*,* z *est un élément de* I_2*. Si* $\mathcal{N}(z) = p^2$*, écrivons* $p = uz$ *avec* $u \in A$*. En appliquant* $\mathcal{N}$*, on trouve* $\mathcal{N}(u) = 1$ *donc u est inversible. D'après la question 5, on a* $z = \pm p$*. D'après la question 11, p ne vérifie la*

propriété $\mathcal{P}$ et donc $z \in I_1$.

14 (*) Le polynôme $P_1 := X^3 + 5i\sqrt{2}X + 5$ est-il un élément irréductible de $A[X]$? Même question pour les polynômes $P_2 := X^4 + (3 + 3i\sqrt{2})X^3 + 5 + 5i\sqrt{2}$ et $P_3 := (1 + i\sqrt{2})X + 3$.
Correction *: Notons que comme A est euclidien, A est factoriel.*

Le polynôme P_1 est unitaire, et 5 est un élément irréductible de A qui divise tous les coefficients de P_1 sauf le coefficient dominant, et 5^2 ne divise pas le terme constant qui est 5. Par le critère d'Eisenstein, P_1 est irréductible dans $A[X]$.

On peut également appliquer le critère d'Eisenstein à P_2 avec l'élément irréductible $1 + i\sqrt{2}$; noter que $(1 + i\sqrt{2})^2$ ne peut pas diviser le terme constant $5 + 5i\sqrt{2}$, sinon $\mathcal{N}((1 + i\sqrt{2})^2) = 3^2$ diviserait $\mathcal{N}(5 + 5i\sqrt{2}) = 3.5^2$ (on peut aussi raisonner sur les valuations)

Par contre, $3 = (1 + i\sqrt{2})(1 - i\sqrt{2})$, donc l'élément irréductible $1 + i\sqrt{2}$ divise tous les coefficients de P_3. P_3 n'est donc pas primitif et n'est donc pas un élément irréductible de $A[X]$; bien sûr, P_3 étant de degré 1, il est irréductible dans $\mathrm{Frac}(A)[X]$.