Université Aix–Marseille 2019–2020

Licence – Mathématiques
Algèbre 2

Cours à distance – Semaine 2 – Anneaux – Corrigé TD2

Exercice 1. *Soit $n \in \mathbb{N}^* \setminus \{1\}$.*

1. *Soit $M \in \mathcal{M}_n(\mathbb{R}) \setminus \mathrm{GL}_n(\mathbb{R})$.*
   (a) *Montrer qu'il existe $A \in \mathcal{M}_n(\mathbb{R})$ telle que $\mathrm{Im}(A) = \mathrm{Ker}(M)$.*
   Soit $p : \mathbb{R}^n \to \mathbb{R}^n$ l'application linéaire définie comme la projection sur le sous-espace $\mathrm{Ker}(M)$ parallèlement à un supplémentaire (n'importe lequel). On note A la matrice représentative de p. Par définition d'une projection, on a $\mathrm{Im}(A) = \mathrm{Ker}(M)$.
   (b) *En déduire que M est un diviseur de zéro.*
   Comme M n'est pas inversible, $\mathrm{Ker}(M)$ n'est pas réduit à $\{0\}$, donc $\mathrm{Im}(A)$ non plus, ce qui implique $A \neq 0$. Or, pour tout $x \in \mathbb{R}^n$, on a $MAx = 0$ car $Ax \in \mathrm{Ker}(M)$; donc $MA = 0$. La matrice M est donc un diviseur de zéro.
2. *Déterminer l'ensemble des diviseurs de zéro dans $\mathcal{M}_n(\mathbb{R})$.*
   On vient de voir que toutes les matrices non inversibles de $\mathcal{M}_n(\mathbb{R})$ sont des diviseurs de zéro. Or, d'une manière générale dans un anneau, les éléments inversibles ne peuvent pas être des diviseurs de zéro. Donc l'ensemble des diviseurs de zéro de $\mathcal{M}_n(\mathbb{R})$ est $\mathcal{M}_n(\mathbb{R}) \setminus \mathrm{GL}_n(\mathbb{R})$.

Exercice 2. *Soit $n \in \mathbb{N}^* \setminus \{1\}$.*

1. *Montrer que $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times = \left\{\overline{k} \mid k \in \mathbb{Z} \text{ premier avec } n\right\}$.*
   Soit k un entier. Supposons k premier avec n. Alors il existe des entiers u et v tels que $uk + vn = 1$, ce qui donne $\overline{u}\overline{k} = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$. Donc $\overline{k}$ est inversible.
   Réciproquement, si $\overline{k}$ est inversible, il existe $\overline{\ell} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{k\ell} = \overline{1}$, c'est-à-dire $k\ell = 1 + sn$ pour un certain entier s. On a donc une relation de Bachet–Bézout $\ell k - sn = 1$ pour k et n, donc ils sont premiers entre eux.
2. *Déterminer les diviseurs de zéro de l'anneau $\mathbb{Z}/n\mathbb{Z}$.*
   On a vu que les classes $\overline{k}$ où k est premier avec n sont inversibles, elles ne peuvent donc pas être des diviseurs de zéro. Prenons un entier k non premier avec n. Dans ce cas, $d = \mathrm{pgcd}(k, n) > 1$. Il existe des entiers ℓ et m tels que $k = d\ell$ et $n = dm$. Notons que $0 < m < n$, donc $\overline{m} \neq \overline{0}$. On a alors $km = d\ell m = n\ell$, donc $\overline{k}\overline{m} = \overline{0}$ et $\overline{k}$ est un diviseur de zéro. Ainsi les diviseurs de zéro sont les classes $\overline{k}$ où k n'est pas premier avec n.
3. *Pour quels n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il intègre ? Dans ce cas, montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps.*
   Si n n'est pas premier, on a $n = ab$ avec $a, b > 1$. Alors $1 < a, b < n$, donc $\overline{a} \neq \overline{0}$ et $\overline{b} \neq \overline{0}$. Or $\overline{a}\overline{b} = \overline{n} = \overline{0}$, donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.
   Supposons maintenant n premier. Si $\overline{k}$ est un diviseur de zéro, d'après la question précédente, k n'est pas premier avec n. Comme n est premier, cela signifie que k est un multiple de n, donc $\overline{k} = \overline{0}$. Donc $\mathbb{Z}/n\mathbb{Z}$ est intègre.
   Finalement, $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier. Dans ce cas, pour $k \in [\![1, n-1]\!]$, k est premier à n, donc, d'après la première question, $\overline{k}$ est inversible. Ainsi tous les éléments non triviaux de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles, donc $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Exercice 3. *Soit A un anneau unitaire. On dit que $a \in A$ est nilpotent s'il existe $k \in \mathbb{N}^*$ tel que $a^k = 0$.*

1. *Montrer qu'un élément inversible ne peut pas être nilpotent.*
   Soit $a \in A$ un élément inversible. Supposons que a est aussi nilpotent. Alors $a^k = 0$ pour un certain entier $k > 0$. En multipliant par $(a^{-1})^{k-1}$, on obtient $a = 0$, or 0 n'est pas inversible.

2. *Soit $a \in A$ un élément niloptent. À l'aide d'une identité remarquable, montrer que $1+a$ est inversible.*
   Soit $k > 0$ tel que $a^k = 0$. Alors $1 = 1^n - (-a)^k = (1+a)\sum_{j=0}^{k-1}(-a)^j$, donc $(1+a)$ est inversible d'inverse $\sum_{j=0}^{k-1}(-a)^j$.

3. *Soient $a, b \in A$ des éléments nilpotents qui commutent. Montrer que ab et $a+b$ sont nilpotents.*
   Soient $k, \ell > 0$ tels que $a^k = 0$ et $b^\ell = 0$. Alors $(ab)^{k+\ell} = a^{k+\ell}b^{k+\ell}$ car a et b commutent, donc $(ab)^{k+\ell} = a^k a^\ell b^k b^\ell = 0$. Ainsi ab est nilpotent. Maintenant, comme a et b commutent, on peut appliquer le binôme de Newton, donc $(a+b)^{k+\ell} = \sum_{j=0}^{k+\ell} a^j b^{k+\ell-j}$. Si $j \leq k$, on a $k + \ell - j \geq \ell$, donc $b^{k+\ell-j} = 0$. Si $j \geq k$, alors $a^j = 0$. Finalement, $(a+b)^{k+\ell} = 0$ et $a+b$ est nilpotent.

4. *Soit $n \in \mathbb{N}^*$.*
   (a) *Montrer que si $M \in \mathcal{M}_n(\mathbb{R})$ admet une valeur propre non nulle, alors M n'est pas nilpotente.*
   Soit $\lambda \neq$ une valeur propre de M et soit $x \in \mathbb{R}^n$ un vecteur propre associé. On vérifie par récurrence sur $k \in \mathbb{N}^*$ que $M^k x = \lambda^k x$. Ainsi, pour tout $k > 0$, la matrice M^k est non nulle, donc M n'est pas nilpotente.

   (b) *Déterminer l'ensemble des éléments nilpotents de $\mathcal{M}_n(\mathbb{R})$.*
   Soit $M \in \mathcal{M}_n(\mathbb{R})$ une matrice nilpotente. On peut voir M comme une matrice à coefficients complexes et utiliser le même argument qu'à la question pour montrer que M n'a pas d'autre valeur propre que 0. Ainsi le polynôme caractéristique de M n'a pas d'autre racine (réelle ou complexe) que 0, donc ce polynôme caractéristique est X^n. Comme il est scindé, on en déduit que la matrice M est trigonalisable. Donc il existe une matrice $P \in \mathrm{GL}_n(\mathbb{R})$ telle que $T = PMP^{-1}$ est triangulaire supérieure avec des termes diagonaux nuls (ce sont les valeurs propres de M), c'est-à-dire que T est triangulaire supérieure stricte.
   Réciproquement, soit M une matrice semblable à une matrice triangulaire supérieure stricte, c'est-à-dire $M = PTP^{-1}$ avec $P \in \mathrm{GL}_n(\mathbb{R})$ et T triangulaire supérieure stricte. On montre d'abord que $T^n = 0$, en vérifiant par récurrence sur $k > 0$ que $(T^k)_{ij} = 0$ si $i > j - k$. Ensuite, on remarque que $(PTP^{-1})^n = P^n T^n P^{-n}$ (en simplifiant les $p^{-1}P$ qui apparaissent dans le produit). Donc $M^n = P^n T^n P^{-n} = 0$ et M est niloptente.
   Les éléments niloptents de $\mathcal{M}_n(\mathbb{R})$ sont donc les matrices semblables à une matrice triangulaire supérieure stricte (ça marche aussi avec inférieure).

Exercice 4. *Soit A un anneau unitaire. On considère, pour $a \in A$, l'équation $x^2 = a$.*

1. *Montrer que, si A est intègre, alors l'équation admet au plus deux solutions.*
   Soit A intègre. Supposons que l'équation $x^2 = a$ admet une solution x_0. Alors pour toute solution x, on a $x^2 = a = x_0^2$, donc $x^2 - x_0^2 = 0$, donc $(x - x_0)(x + x_0) = 0$. Comme A est intègre, cela implique $x - x_0 = 0$ ou $x + x_0 = 0$, donc $x = \pm x_0$. Ainsi l'équation admet au plus deux solutions.

2. *On fixe maintenant $n \in \mathbb{N}^*$ et on se place dans le cas $A = \mathcal{M}_n(\mathbb{R})$ avec $a = \mathrm{Id}$. Montrer que l'équation possède alors au moins 2^n solutions.*
   Les matrices diagonales dont tous les termes diagonaux valent ± 1 sont des solutions et il y en a 2^n.

Exercice 5. *Soit A un anneau unitaire. Pour tout ensemble $X \subset A$, on note $\langle X \rangle$ l'intersection de tous les sous-anneaux unitaires de A contenant X.*

1. *Montrer qu'une intersection quelconque de sous-anneaux unitaires de A est un sous-anneau unitaire de A.*
   Soient $B_1, \dots, B_k$ des sous-anneaux unitaires de A et $B = \cap_{1 \leq i \leq k} B_i$. On a $1_A \in B_i$ pour tout i, donc $1_A \in B$. Si $a, b \in B$, alors $a, b \in B_i$ pour tout i. Comme chaque B_i est un sous-anneau, on en déduit $a + b \in B_i$, $a^{-1} \in B_i$ et $ab \in B_i$, pour tout i. Donc $a + b \in B$, $a^{-1} \in B$ et $ab \in B$. Ainsi B est un sous-ensemble non vide de A, stable par addition, passage à l'opposé et multiplication, qui contient 1_A, donc c'est un sous-anneau unitaire de A.

2. *Montrer que, pour tout $X \subset A$, $\langle X \rangle$ est le plus petit sous-anneau unitaire de A contenant X dans le sens où il est contenu dans tout sous-anneau unitaire de A contenant X.*
   Par définition, $\langle X \rangle$ est l'intersection de tous les sous-anneaux unitaires de A contenant X, donc il est contenu dans chaque sous-anneau unitaire de A contenant X, et on vient de voir que c'est un sous-anneau unitaire de A.

3. *On se place maintenant dans le cas $A = \mathbb{C}$.*
   Notons, car on va l'utiliser souvent ci-dessous, que si un anneau contient un élément a, alors, par stabilité par addition et passage à l'opposé, il contient tous les multiples entiers de a, c'est-à-dire tous les ka avec $k \in \mathbb{Z}$.
   (a) *Montrer que $\langle \emptyset \rangle = \mathbb{Z}$.*
   On a $\emptyset \subset \mathbb{Z}$ et on vérifie facilement que $\mathbb{Z}$ est un sous-anneau unitaire de $\mathbb{C}$, donc $\langle \emptyset \rangle \subset \mathbb{Z}$. Réciproquement, $\langle \emptyset \rangle$ est un sous-anneau unitaire de $\mathbb{C}$ qui contient 1 et donc tous ses mutiples entiers, donc il contient $\mathbb{Z}$. Finalement $\langle \emptyset \rangle = \mathbb{Z}$.

   (b) *Montrer que $\langle \{\frac{1}{10}\} \rangle$ est l'ensemble des nombres décimaux.*
   On vérifie que l'ensemble $\mathcal{D}$ des nombres décimaux est un sous-anneau unitaire de $\mathbb{C}$, et il contient $\frac{1}{10}$, donc $\langle \{\frac{1}{10}\} \rangle \subset \mathcal{D}$. Réciproquement, comme $\langle \{\frac{1}{10}\} \rangle$ est un sous-anneau unitaire de $\mathbb{C}$ qui contient $\frac{1}{10}$, par stabilité par multiplication, il contient $\frac{1}{10^n}$ pour tout $n \in \mathbb{N}$. Du coup, $\langle \{\frac{1}{10}\} \rangle$ contient $\frac{k}{10^n}$ pour tout $k \in \mathbb{Z}$ et tout $n \in \mathbb{N}$. Autrement dit, $\mathcal{D} \subset \langle \{\frac{1}{10}\} \rangle$. Ainsi $\langle \{\frac{1}{10}\} \rangle = \mathcal{D}$.

   (c) *Montrer que $\langle \{i\} \rangle = \{a + ib \mid a, b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss.*
   L'anneau des entiers de Gauss est bien un sous-anneau unitaire de $\mathbb{C}$, et il contient i, donc $\langle \{i\} \rangle \subset \{a + ib \mid a, b \in \mathbb{Z}\}$. Réciproquement, comme $\langle \{i\} \rangle$ est unitaire, il contient 1, et donc tous ses multiples entiers, donc il contient $\mathbb{Z}$. De plus, $\langle \{i\} \rangle$ contient i et tous ses multiples entiers. Donc $\langle \{i\} \rangle$ contient les $a \in \mathbb{Z}$ et les ib avec $b \in \mathbb{Z}$, donc par stabilité par addition, il contient les $a + ib$ avec $a, b \in \mathbb{Z}$. Finalement $\langle \{i\} \rangle = \{a + ib \mid a, b \in \mathbb{Z}\}$.

   (d) *Montrer que $\langle \{e^{\frac{2i\pi}{3}}\} \rangle = \left\{ \frac{a+ib\sqrt{3}}{2} \;\middle|\; a, b \in \mathbb{Z} \text{ tels que } a \equiv b \,[2] \right\}$.*
   Notons $A = \left\{ \frac{a+ib\sqrt{3}}{2} \;\middle|\; a, b \in \mathbb{Z} \text{ tels que } a \equiv b \,[2] \right\}$. Vérifions que A est un sous-anneau unitaire de $\mathbb{C}$. Déjà, $1 \in A$ (avec $a = 2$ et $b = 0$). Ensuite, A est stable par addition et passage à l'opposé car les deux sont compatibles avec la congruence. Voyons la stabilité par multiplication. Soient $a, b, c, d \in \mathbb{Z}$ avec $a \equiv b \,[2]$ et $c \equiv d \,[2]$. Alors

$$\frac{a + ib\sqrt{3}}{2} . \frac{c + id\sqrt{3}}{2} = \frac{x + iy\sqrt{3}}{2} \quad \text{avec} \quad \begin{cases} x = \dfrac{ac - 3bd}{2} \\ \\ y = \dfrac{ad + bc}{2} \end{cases} .$$

   Modulo 2, on a $a \equiv b$ et $c \equiv d$, donc $ac \equiv bd \equiv 3bd$ et $ad \equiv bc \equiv -bc$. Ainsi x et y sont des entiers. De plus, on a $y - x = \frac{1}{2}\big[(a - b)(d - c) + 4bd\big]$. On sait que $2|(a - b)$ et $2|(d - c)$, donc $4|(a-b)(d-c)$ et donc $2|(y - x)$. Finalement $\frac{x+iy\sqrt{3}}{2} \in A$, ainsi A est stable par multiplication

et donc A est un sous-anneau unitaire de $\mathbb{C}$. Comme $e^{\frac{2i\pi}{3}} = \frac{1+i\sqrt{3}}{2}$, on a $\langle\{e^{\frac{2i\pi}{3}}\}\rangle \subset A$.
Réciproquement, $\langle\{e^{\frac{2i\pi}{3}}\}\rangle$ contient $\frac{1+i\sqrt{3}}{2}$, donc il contient tous les $\frac{b+ib\sqrt{3}}{2}$ avec $b \in \mathbb{Z}$. De plus, il contient 1, donc il contient $\mathbb{Z}$. Par stabilité par addition, $\langle\{e^{\frac{2i\pi}{3}}\}\rangle$ contient donc tous les $c + \frac{b+ib\sqrt{3}}{2} = \frac{2c+b+ib\sqrt{3}}{2}$ avec $b, c \in \mathbb{Z}$, c'est-à-dire tous les $\frac{a+ib\sqrt{3}}{2}$ avec $a, b \in \mathbb{Z}$ et $a \equiv b\,[2]$. Finalement, $\langle\{e^{\frac{2i\pi}{3}}\}\rangle = A$.

Exercice 6. *Pour tout entier $n \geq 2$, on note $\varphi(n) := \left|\left\{k \in [\![1, n]\!] \mid \text{pgcd}(k, n) = 1\right\}\right|$. C'est ce qu'on appelle la fonction indicatrice d'Euler.*

1. *Montrer que, pour tout entier $n \geq 2$, $\varphi(n) = \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right|$.*
   Cela découle directement de l'exercice 2, question 1.

2. *Montrer que, pour tout nombre premier p, $\varphi(p) = p - 1$.*
   Si p est premier, alors $\left\{k \in [\![1, n]\!] \mid \text{pgcd}(k, n) = 1\right\} = [\![1, p-1]\!]$.

3. *Montrer que, pour tout nombre premier p et tout $k \in \mathbb{N}^*$, $\varphi(p^k) = p^k - p^{k-1}$.*
   Soit p premier et $k \in \mathbb{N}^*$. Un entier ℓ est premier à p^k si et seulement si il est premier à p, si et seulement si il n'est pas multiple de p. Ainsi

   $$\left\{\ell \in [\![1, p^k]\!] \mid \text{pgcd}(\ell, p^k) = 1\right\} = [\![1, p^k]\!] \setminus \left\{ap \,|\, a \in [\![1, p^{k-1}]\!]\right\},$$

   et donc $\varphi(p^k) = p^k - p^{k-1}$.

4. *Montrer que, pour tous entiers $n_1, n_2 \geq 2$ premiers entre eux, $\varphi(n_1.n_2) = \varphi(n_1).\varphi(n_2)$.*
   D'après le théorème des restes chinois, l'application

   $$\pi : \left\{\begin{array}{ccc} \mathbb{Z}/n_1n_2\mathbb{Z} & \to & \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \\ k\,[n_1n_2] & \mapsto & (k\,[n_1]\,,\, k\,[n_2]) \end{array}\right.$$

   est bijective. Comme k est premier à n_1n_2 si et seulement si k est premier à n_1 et à n_2, on a $\pi\left(\left(\mathbb{Z}/n_1n_2\mathbb{Z}\right)^\times\right) = \left(\mathbb{Z}/n_1\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/n_2\mathbb{Z}\right)^\times$, donc $\varphi(n_1n_2) = \varphi(n_1)\varphi(n_2)$.

5. *Montrer que, pour tout entier $n \geq 2$, $\varphi(n) = n.\prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$, où $p_1, \ldots, p_r$ sont les nombres premiers intervenant dans la décomposition de n en facteurs premiers.*
   On note $a_1, \ldots, a_r$ les entiers tels que $n = p_1^{a_1} \ldots p_r^{a_r}$. Alors

   $$\varphi(n) = \varphi\left(\prod_{i=1}^r p_i^{a_i}\right) = \prod_{i=1}^r \varphi\left(p_i^{a_i}\right) = \prod_{i=1}^r \left(p_i^{a_i} - p_i^{a_i - 1}\right) = \prod_{i=1}^r p_i^{a_i}\left(1 - \frac{1}{p_i}\right) = n.\prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

6. *On fixe maintenant l'entier $n \geq 2$ et, pour tout diviseur d de n, on note*

   $$A_d := \left\{k \in [\![1, n]\!] \mid \text{pgcd}(k, n) = d\right\}.$$

   La fonction φ a été définie pour les entiers $n \geq 2$, mais la définition marche aussi pour $n = 1$ (on en a besoin dans la dernière question).

   (a) *Montrer que, pour tout diviseur d de n, $|A_d| = \varphi\left(\frac{n}{d}\right)$.*
   Fixons un diviseur (positif) d de n. Notons $m = \frac{n}{d} \in \mathbb{N}^*$ et $B := \left\{k \in [\![1, m]\!] \mid \text{pgcd}(k, m) = 1\right\}$. Les applications

   $$\psi : \left\{\begin{array}{ccc} A_d & \to & B \\ k & \mapsto & \frac{k}{d} \end{array}\right. \quad \text{et} \quad \phi : \left\{\begin{array}{ccc} B & \to & A_d \\ k & \mapsto & dk \end{array}\right.$$

sont bien définies. En effet, si $k \in A_d$, alors il s'écrit $k = d\ell$ avec $\ell \in \mathbb{N}^*$. Comme $n = dm$, on a $\mathrm{pgcd}(k,n) = d\mathrm{pgcd}(\ell,m)$, donc $\mathrm{pgcd}(\ell,m) = 1$. Comme $1 \leq \ell \leq m$, on a $\ell = \frac{k}{d} \in B$. De même, pour ϕ, on voit que si $k \in B$, alors $1 \leq dk \leq dm = n$ et $\mathrm{pgcd}(dk,n) = \mathrm{pgcd}(dk,dm) = \mathrm{pgcd}(k,m) = 1$, donc $dk \in A_d$. Maintenant, il est clair que ψ et ϕ sont inverses l'une de l'autre, donc elles sont bijectives et les ensembles A_d et B ont le même nombre d'éléments. Ainsi $|A_d| = |B| = \varphi(\frac{n}{d})$.

(b) *En déduire que* $n = \sum_{d|n} \varphi(d)$.
On a $[\![1,n]\!] = \sqcup_{d|n} A_d$ l'union sur tous les diviseurs positifs de n des A_d. Comme c'est une union disjointe, on en déduit l'égalité de cardinaux $\left|[\![1,n]\!]\right| = \sum_{d|n} |A_d|$, donc

$$n = \sum_{\substack{d|n \\ d>0}} \varphi\left(\frac{n}{d}\right) = \sum_{\substack{d\delta=n \\ d,\delta>0}} \varphi\left(\frac{n}{d}\right) = \sum_{\substack{d\delta=n \\ d,\delta>0}} \varphi(\delta) = \sum_{\substack{\delta|n \\ \delta>0}} \varphi(\delta).$$

Exercice 7.

1. *On note* $\mathcal{G} := \{a+ib \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$ *l'ensemble dit des entiers de Gauss.*
   (a) *Montrer que* $\mathcal{G}$ *est un sous-anneau unitaire de* $\mathbb{C}$.
   L'ensemble $\mathcal{G}$ contient 0 et est stable par addition et passage à l'opposé, donc c'est un sous-groupe additif de $\mathbb{C}$. Il est aussi stable par multiplication et il contient 1, donc c'est un sous-anneau unitaire de $\mathbb{C}$.

   (b) *Montrer* $\mathcal{G}^\times$ *possède exactement* 4 *éléments.*
   Soit x un inversible de $\mathcal{G}$. On écrit $x = a+ib$ avec $a,b \in \mathbb{Z}$. Il existe $c,d \in \mathbb{Z}$ tels que $(a+ib)(c+id) = 1$. Alors $ac-bd+i(ad+bc) = 1$, donc $ac-bd = 1$ et $ad+bc = 0$. Si $b = 0$, alors $ac = 1$, donc $a = \pm 1$ et $x = \pm 1$. Si $b \neq 0$, alors $c = -\frac{ad}{b}$, donc l'égalité $ac-bd = 1$ donne $(a^2+b^2)d = 1$. Alors $a^2+b^2 = 1$, donc soit $a = \pm 1$ et $b = 0$, c'est-à-dire $x = \pm 1$, soit $a = 0$ et $b = \pm 1$, c'est-à-dire $x = \pm i$. Les quatre valeurs obtenues sont bien inversibles dans $\mathcal{G}$: $1.1 = 1$, $(-1).(-1) = 1$ et $i.(-i) = 1$. Donc $\mathcal{G}^\times = \{\pm 1, \pm i\}$.

2. *On note* $\mathbb{Z}[\sqrt{2}] := \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$.
   (a) *Montrer que* $\mathbb{Z}[\sqrt{2}]$ *est un sous-anneau unitaire de* $\mathbb{C}$.
   L'ensemble $\mathbb{Z}[\sqrt{2}]$ contient 0 et est stable par addition et passage à l'opposé, donc c'est un sous-groupe additif de $\mathbb{C}$. Il est aussi stable par multiplication et il contient 1, donc c'est un sous-anneau unitaire de $\mathbb{C}$.

   (b) i. *Soit* $n \in \mathbb{N}$. *On pose* $a_n := \frac{(1+\sqrt{2})^n+(1-\sqrt{2})^n}{2}$ *et* $b_n := \frac{(1+\sqrt{2})^n-(1-\sqrt{2})^n}{2\sqrt{2}}$. *Montrer que* $a_n, b_n \in \mathbb{N}$ *et que* $a_n^2 - 2b_n^2 = (-1)^n$.

$$\begin{aligned} a_n &= \frac{1}{2}\left[(1+\sqrt{2})^n + (1-\sqrt{2})^n\right] \\ &= \frac{1}{2}\left[\sum_{k=0}^{n} \binom{n}{i} (\sqrt{2})^k + \sum_{k=0}^{n} \binom{n}{i} (-1)^k (\sqrt{2})^k\right] \\ &= \sum_{\substack{k=0 \\ k\ pair}}^{n} \binom{n}{i} (\sqrt{2})^k = \sum_{\substack{k=0 \\ k\ pair}}^{n} \binom{n}{i} 2^{\frac{k}{2}} \ \in \mathbb{N} \end{aligned}$$

$$\begin{aligned} b_n &= \frac{1}{2\sqrt{2}}\left[(1+\sqrt{2})^n - (1-\sqrt{2})^n\right] \\ &= \frac{1}{2\sqrt{2}}\left[\sum_{k=0}^{n}\binom{n}{i}(\sqrt{2})^k - \sum_{k=0}^{n}\binom{n}{i}(-1)^k(\sqrt{2})^k\right] \\ &= \frac{1}{\sqrt{2}}\sum_{\substack{k=0\\ k\ impair}}^{n}\binom{n}{i}(\sqrt{2})^k = \sum_{\substack{k=0\\ k\ impair}}^{n}\binom{n}{i}2^{\frac{k-1}{2}} \in \mathbb{N} \end{aligned}$$

Pour tous réels x et y, $(x+y)^2-(x-y)^2 = x^2+2xy+y^2-(x^2-2xy+y^2) = 4xy$. Donc :

$$\begin{aligned} a_n^2 - 2b_n^2 &= \frac{1}{4}\left[(1+\sqrt{2})^n + (1-\sqrt{2})^n\right]^2 - \frac{1}{4}\left[(1+\sqrt{2})^n - (1-\sqrt{2})^n\right]^2 \\ &= (1+\sqrt{2})^n(1-\sqrt{2})^n = (1-2)^n = (-1)^n \end{aligned}$$

ii. *Montrer $\mathbb{Z}[\sqrt{2}]^\times$ possède une infinité d'éléments.*
Pour $n \in \mathbb{N}$, $(a_n+ib_n)(a_n-ib_n) = a_n^2-2b_n^2 = (-1)^n$, donc a_n+ib_n est inversible d'inverse a_n-ib_n si n est pair et $-a_n+ib_n$ si n est impair. Pour conclure, on va montrer que les a_n prennent une infinité de valeurs distinctes. S'ils ne prenaient qu'un nombre fini de valeurs disctintes, alors la suite $(a_n)_{n\in\mathbb{N}}$ serait stationnaire, donc en particulier convergente. Or

$$a_n = \frac{1}{2}\left[(1+\sqrt{2})^n + (1-\sqrt{2})^n\right] = \frac{1}{2}(1+\sqrt{2})^n\left[1+\left(\frac{1-\sqrt{2}}{1+\sqrt{2}}\right)^n\right].$$

Comme $\left|\frac{1-\sqrt{2}}{1+\sqrt{2}}\right| < 1$ et $\left|1+\sqrt{2}\right| > 1$, $\left(\frac{1-\sqrt{2}}{1+\sqrt{2}}\right)^n$ tend vers 0 et a_n tend vers $+\infty$. Finalement $\{a_n+ib_n \,|\, n\in\mathbb{N}\}$ est une famille infinie d'inversibles de $\mathbb{Z}[\sqrt{2}]$.