Licence de Mathématiques
L3 - Semestre 5, Algèbre
Année universitaire 2023-2024,
F. Nacry

Théorie des anneaux

Exercice 1 Soit $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{Q}$. Montrer que l'ensemble $\mathbb{Q}[\sqrt{d}] := \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$ est un sous-anneau de $\mathbb{R}$. Est-ce un corps ?

Solution. Il est clair que $\mathbb{Q}[\sqrt{d}] \subset \mathbb{R}$. D'autre part, on a $1 \in \mathbb{Q}[\sqrt{d}]$ ainsi que pour chaque $x, y \in \mathbb{Q}[\sqrt{d}]$

$$x - y \in \mathbb{Q}[\sqrt{d}] \quad \text{et} \quad xy \in \mathbb{Q}[\sqrt{d}].$$

Ceci montre que $\mathbb{Q}[\sqrt{d}]$ est un sous-anneau de $\mathbb{R}$. Le fait que c'est un corps résulte d'une part de l'équivalence valide pour chaque $(a, b) \in \mathbb{Q}^2$

$$a + b\sqrt{d} = 0 \Leftrightarrow (a, b) = (0, 0)$$

et d'autre part de l'égalité

$$\frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - b^2 d} \quad \text{pour tout } (a, b) \in \mathbb{Q}^2 \setminus \{(0, 0)\}.$$

■

Exercice 2 (Anneau des entiers de Gauss) Montrer que $\mathbb{Z}[i] := \{a + ib : (a, b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$ stable par conjugaison complexe. On l'appelle l'*anneau des entiers de Gauss*.

Solution. On vérifie tout de suite que $\mathbb{Z}[i] \subset \mathbb{C}$, $1 \in \mathbb{Z}[i]$ et que pour tout $z_1, z_2 \in \mathbb{Z}[i]$,

$$z_1 - z_2 \in \mathbb{Z}[i] \quad \text{et} \quad z_1 z_2 \in \mathbb{Z}[i].$$

Ceci montre que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$. La stabilité de cet anneau par conjugaison complexe est immédiate. ■

Exercice 3 (Anneau des entiers d'Eisenstein) Montrer que $\mathbb{Z}[j] := \{a + jb : (a, b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$ stable par conjugaison complexe. On l'appelle l'*anneau des entiers d'Eisenstein*.

Solution. On vérifie tout de suite que $\mathbb{Z}[i] \subset \mathbb{C}$, $1 \in \mathbb{Z}[i]$ et que pour tout $z_1, z_2 \in \mathbb{Z}[i]$,

$$z_1 - z_2 \in \mathbb{Z}[i] \quad \text{et} \quad z_1 z_2 \in \mathbb{Z}[i].$$

Ceci montre que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$. La stabilité de cet anneau par conjugaison complexe est immédiate. ■

Exercice 4 (Décimaux) On considère l'ensemble des *décimaux*

$$\mathbb{D} = \{\frac{n}{10^k} : n \in \mathbb{Z}, k \in \mathbb{N}\}.$$

Montrer que $\mathbb{D}$ est un sous-anneau de $\mathbb{Q}$.

Solution. On a évidemment $\mathbb{D} \subset \mathbb{Q}$ et $1 \in \mathbb{D}$. Il reste alors à observer que pour tout $n, m \in \mathbb{Z}$ et pour tout $k, l \in \mathbb{N}$,

$$\frac{n}{10^k} - \frac{m}{10^l} = \frac{n10^l - m10^k}{10^{k+l}} \quad \text{et} \quad \frac{n}{10^k}\frac{m}{10^l} = \frac{nm}{10^{k+l}}$$

pour conclure que $\mathbb{D}$ est un sous-anneau de $\mathbb{Q}$. ■

Exercice 5 (Quaternions) Montrer que l'ensemble

$$\mathbb{H} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} : a, b \in \mathbb{C} \right\}$$

est un corps (non commutatif) lorsqu'il est muni des lois + et × de $M_2(\mathbb{C})$. Il est appelé *corps des quaternions*.

Solution. On vérifie que $\mathbb{H} \subset M_2(\mathbb{C})$ ainsi que $\mathbb{I}_2 \in \mathbb{H}$, où I_2 désigne la matrice identité de taille 2. Les propriétés de la conjugaison complexe garantissent sans difficultés les inclusions

$$M - M' \in \mathbb{H} \quad \text{et} \quad MM' \in \mathbb{H}$$

pour tout $M, M' \in \mathbb{H}$. On conclut que $\mathbb{H}$ est un sous-anneau de $M_2(\mathbb{C})$. Pour vérifier que $\mathbb{H}$ est un corps, il suffit de voir que tout élément de $\mathbb{H}$ est inversible dans $M_2(\mathbb{C})$ d'inverse appartenant à $\mathbb{H}$. ■

Exercice 6 Soient $(A; +, \times)$ un anneau. On dit que A est un *anneau de Boole* lorsque

$$x^2 = x \quad \text{pour tout } x \in A.$$

1. Montrer que si A est un anneau de Boole, alors pour tout $x \in A$, $x = -x$. En déduire que tout anneau de Boole est commutatif.
2. Soit E un ensemble. On note $\mathcal{P}(E)$ l'ensemble des parties de E. On rappelle que la différence symétrique sur E est définie par

   $$A \Delta B = (A \cup B) \setminus (A \cap B) \quad \text{pour tout } A, B \in \mathcal{P}(E).$$

   On note $\overline{X}$ le complémentaire de $X \subset E$ dans E, i.e., $\overline{X} := X \setminus E$.
   (a) Montrer que pour tout $X, Y \subset E$, on a

   $$X \Delta Y = (X \cap \overline{Y}) \cup (\overline{X} \cap Y).$$

   (b) Montrer que pour tout $X, Y \subset E$, on a

   $$\overline{X \Delta Y} = (\overline{X} \cap \overline{Y}) \cup (X \cap Y).$$

   (c) En déduire que pour tout $A, B, C \subset E$, $(A \Delta B) \Delta C$ est l'ensemble des éléments de E appartenant à la fois aux trois parties A, B, C ou à exactement une seule des trois parties A, B, C.
   (d) Conclure que pour tout $A, B, C \subset E$, $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.
   (e) Montrer que $(\mathcal{P}(E); \Delta, \cap)$ est un anneau de Boole.

Solution.

1. On suppose que A est un anneau de Boole. Soit $x, y \in A$. On a

   $$x + x = (x + x)^2 = 4x^2 = 4x,$$

   i.e., $x = -x$. D'autre part, on a

   $$(x + y) = (x + y)^2 = x^2 + y^2 + xy + yx = x + y + xy + yx,$$

   ce qui s'écrit encore $xy = -yx$. Il reste à appliquer ce qui précède pour obtenir $xy = yx$.
   (a) Une double inclusion immédiate montre l'égalité souhaitée.
   (b) Soit $X, Y \subset E$. D'après (a), on a

   $$\overline{X \Delta Y} = \overline{(X \cap \overline{Y}) \cup (\overline{X} \cap Y)} = \overline{X \cap \overline{Y}} \cap \overline{\overline{X} \cap Y} = (\overline{X} \cup Y) \cap (X \cup \overline{Y}) = (\overline{X} \cap \overline{Y}) \cup (X \cap Y).$$

(c) Soient trois parties A, B et C de E. D'après (a), on a

$$(A\Delta B)\Delta C = [(A\Delta B)\cap \overline{C}]\cup[\overline{(A\Delta B)}\cap C]$$

tandis que (b) donne

$$\overline{(A\Delta B)} = (\overline{A}\cap\overline{B})\cup(A\cap B).$$

On déduit de tout ceci

$$(A\Delta B)\Delta C = (A\cap B\cap C)\cup(\overline{A}\cap\overline{B}\cap C)\cup(\overline{A}\cap\overline{C}\cap B)\cup(\overline{B}\cap\overline{C}\cap A),$$

i.e., $(A\Delta B)\Delta C$ est l'ensemble des éléments de E qui appartiennent à la fois aux trois parties A, B et C ou à exactement une seule des trois parties A, B, C.

(d) De la même manière, on montre que $A\Delta(B\Delta C)$ n'est nul autre que l'ensemble des éléments de E qui appartiennent à la fois aux trois parties A, B et C ou à exactement une seule des trois parties A, B, C. On conclut

$$(A\Delta B)\Delta C = A\Delta(B\Delta C).$$

(e) Le fait que $(\mathcal{P}(E);\Delta,\cap)$ soit un anneau ne pose aucune difficulté à l'exception du caractère associatif de la différence symétrique qui a fait l'objet des questions ci-dessus. Il reste à voir que la propriété de Boole de l'anneau provient de l'égalité évidente $A\cap A = A$ pour tout $A\in\mathcal{P}(E)$.

■

Exercice 7 (Anneau des polynômes à une indéterminée) Soient $(A;+,\times)$ un anneau commutatif. Montrer que l'ensemble des suites de A nulles à partir d'un certain rang muni des opérations $\dot{+}$ et $\dot{\times}$ définies pour tout $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}\in A^{\mathbb{N}}$ par

$$(a_n)_{n\in\mathbb{N}}\dot{+}(b_n)_{n\in\mathbb{N}} = (a_n+b_n)_{n\in\mathbb{N}}$$

et

$$(a_n)_{n\in\mathbb{N}}\dot{\times}(b_n)_{n\in\mathbb{N}} = (\sum_{k=0}^{n} a_k b_{n-k})_{n\in\mathbb{N}}$$

est un anneau commutatif. Traditionnellement, on note X la suite de A définie par $a_1 = 1_A$ et $a_n = 0_A$ pour tout $n\in\mathbb{N}$ avec $n\neq 1$ et on note $A[X]$ l'ensemble défini ci-dessus. Il est alors appelé *anneau des polynômes à une indéterminée sur A*.

Solution. Seule l'associativité de la loi $\dot{\times}$ mérite une justification. Elle découle des égalités

$$\sum_{k=0}^{n}(\sum_{j=0}^{k} a_j b_{k-j})c_{n-k} = \sum_{i,j,k\in\mathbb{N},i+j+k=n} a_i b_j c_k$$

et

$$\sum_{k=0}^{n} a_k(\sum_{j=0}^{n-k} b_j c_{n-k-j}) = \sum_{i,j,k\in\mathbb{N},i+j+k=n} a_i b_j c_k$$

valables pour tout $n\in\mathbb{N}$ et toutes familles de réels $(a_k)_{k\in\mathbb{N}}, (b_k)_{k\in\mathbb{N}}$ et $(c_k)_{k\in\mathbb{N}}$. ■

Exercice 8 Pour chaque $d\in\mathbb{N}$, on pose

$$A_d = \{(x,y)\in\mathbb{Z}^2 : y-x\in d\mathbb{Z}\}.$$

1. Montrer que pour tout $d\in\mathbb{N}$, A_d est un sous-anneau de $\mathbb{Z}^2$ muni de sa structure naturelle produit.

2. On considère A un sous-anneau de $\mathbb{Z}^2$ (muni de sa structure naturelle d'anneau produit). Montrer que $G = \{x \in \mathbb{Z} : (x, 0) \in A\}$ est un sous-groupe de $(\mathbb{Z}; +)$. En déduire que $A = A_d$ pour un certain entier d.

Solution.

1. Ceci ne pose aucune difficulté compte-tenu de la définition de la structure naturelle d'anneau produit de $\mathbb{Z}^2$.
2. L'ensemble G est bien sûr un sous-groupe de $(\mathbb{Z}; +)$. Un résultat élémentaire de théorie des groupes nous dit que $G = d\mathbb{Z}$ pour un certain $d \in \mathbb{N}$. Nous allons montrer que $A = A_d$. Fixons $(x, y) \in A$. En remarquant que

$$(x - y, 0) = (x, y) - (y, y) \in A,$$

on a $x - y \in G = d\mathbb{Z}$. Il s'ensuit $(x, y) \in A_d$ et donc $A \subset A_d$. L'inclusion renversée s'obtient de manière analogue.

■

Exercice 9 (Inverse à gauche, à droite) Soient $(A; +, \times)$ un anneau, $a \in A$. Montrer que si a est inversible à gauche et à droite dans A, alors a est inversible.

Solution. Supposons que a est inversible à gauche et à droite dans A. On dispose donc de $b, c \in A$ tels que $ba = 1_A = ac$. Il suffit d'écrire

$$c = (ba)c = b(ac) = b$$

et de poser $d := b = c$ pour obtenir

$$ad = da = 1_A.$$

Supposons maintenant qu'il existe $d' \in A$ tel que $ad' = d'a = 1_A$. Il vient sans difficultés

$$d' = (da)d' = d(ad') = d.$$

■

Exercice 10 Soient A un anneau non nul et $a \in A$ un élément *nilpotent* (i.e., pour lequel il existe un entier $n \geq 1$ tel que $a^n = 0_A$).

1. Montrer que $1_A - a \in A^\times$ et donner son inverse.
2. Soit $x \in A^\times$ qui commute avec a (i.e., $ax = xa$). Justifier que $x^{-1}a$ est nilpotent. En déduire que $x - a \in A^\times$ et donner son inverse.

Solution. Pour éviter une convention concernant 0_A^0, on peut supposer dans tout l'exercice $a \neq 0_A$ (si $a = 0_A$, il n'y a rien à établir). On note n l'*indice de nilpotence* de A, i.e., le plus petit entier $n \geq 1$ tel que $a^n = 0_A$.

1. L'idée fondamentale ici est de penser au développement en série entière valide pour tout $u \in]-1, 1[$,

$$(1 - u)^{-1} = \frac{1}{1 - u} = \sum_{k=0}^{+\infty} u^k.$$

L'égalité ci-dessus nous amène alors à poser $b = 1_A + a + \ldots + a^{n-1}$ et à vérifier que

$$ab = ba = 1_A.$$

Ainsi, a est inversible dans A, d'inverse b.

2. Puisque x commute avec a, on voit tout de suite que x^{-1} commute avec a également et

$$(x^{-1}a)^n = a^n x^{-n} = 0_A,$$

en particulier $x^{-1}a$ est nilpotent. Notons que le caractère inversible de x dans A entraîne que l'indice de nilpotence de $x^{-1}a$ n'est nul autre que l'entier n. Il reste à écrire

$$x - a = x(1_A - x^{-1}a)$$

et à appliquer la question précédente pour obtenir que $x - a$ est inversible dans A d'inverse y avec

$$y = \big(1_A + (x^{-1}a) + \ldots + (x^{-1}a)^{n-1}\big)x^{-1}.$$

■

Exercice 11 Soit $(A; +, \times)$ un anneau. Montrer que $(A^\times; \times)$ est un groupe.

Solution. Ceci ne pose aucune difficultés. ■

Exercice 12 Soit $(A; +, \times)$ un anneau commutatif, $a, b \in A$. Montrer que $ab \in A^\times$ si et seulement $a \in A^\times$ et $b \in A^\times$.

Solution. Evident. ■

Exercice 13 Déterminer les éléments du groupe $(\mathbb{Z}[i])^\times$ des éléments inversibles de l'anneau des entiers de Gauss et donner sa structure.

Solution. Soit $z \in \mathbb{Z}[i]$ un élément inversible (par rapport à $\times$). Par définition des entiers de Gauss, il existe $a, b \in \mathbb{Z}$ tels que $z = a + ib$. L'inversibilité de z quant à elle nous dit qu'il existe $c, d \in \mathbb{Z}$ tels que

$$(a + ib)(c + id) = 1.$$

En remarquant que $(a, b) \neq (0, 0)$, on peut écrire

$$c + id = \frac{1}{a + ib} = \frac{a - ib}{a^2 + b^2}$$

ce qui entraîne

$$\frac{a}{a^2 + b^2} = c \in \mathbb{Z} \quad \text{et} \quad -\frac{b}{a^2 + b^2} = d \in \mathbb{Z}.$$

Il n'est alors pas difficile de déduire $a, b \in \{-1, 0, 1\}$ puis $z \in \{-i, i, -1, 1\}$. Ceci combiné à l'inclusion évidente $\{-i, i, -1, 1\} \subset (\mathbb{Z}[i])^\times$ permet d'aboutir à l'égalité

$$(\mathbb{Z}[i])^\times = \{-i, i, -1, 1\}.$$

Il reste à observer que le groupe $(\mathbb{Z}[i])^\times, \times)$ est cyclique d'ordre 4, donc isomorphe (en tant que groupe) à $\mathbb{Z}/4\mathbb{Z}$. ■

Exercice 14 Déterminer les inversibles de $\mathbb{Z}[j] = \{a + jb : a, b \in \mathbb{Z}\}$ avec $j := e^{\frac{2i\pi}{3}}$. A quel groupe "mieux connu" cet ensemble est-il isomorphe (en tant que groupe) ?

Solution. On introduit $N : \mathbb{Z}[j] \to \mathbb{N}$ définie par

$$N(z) = |z|^2 \quad \text{pour tout } z \in \mathbb{Z}[j].$$

On a bien sûr $N(zz') = N(z)N(z')$ pour tout $z, z' \in \mathbb{Z}[j]$. D'autre part, pour tout $a, b \in \mathbb{Z}$, on vérifie que

$$N(a + jb) = a^2 + b^2 - ab = (a - b)^2 + ab = (a + b)^2 - 3ab.$$

Soit $u \in \mathbb{Z}[j]$ inversible. On a

$$N(u)N(u^{-1}) = N(uu^{-1}) = N(1) = 1,$$

d'où $N(u) = 1$. Ecrivons $u = x + jy$ avec $x, y \in \mathbb{Z}$. Si $xy \geq 0$, on a

$$(x-y)^2 + xy = 1$$

et ceci entraîne $(x-y)^2 = 0$ et $xy = 1$ ou $(x-y)^2 = 1$ et $xy = 0$, d'où l'inclusion

$$(x, y) \in \{(1,1), (-1,-1), (0,1), (0,-1), (1,0), (-1,0)\}.$$

On en déduit que

$$u \in \{1+j, -1-j, j, -j, 1, -1\} =: \Lambda.$$

Si $xy \leq 0$, on a

$$(x+y)^2 - 3xy = 1$$

et ceci implique $(x+y)^2 = 1$ et $xy = 0$. Il s'ensuit

$$(x, y) \in \{(0,1), (0,-1), (1,0), (-1,0)\},$$

d'où l'on tire

$$u \in \{j, -j, 1, -1\}.$$

Réciproquement, on vérifie que les six éléments de l'ensemble Λ ci-dessus sont bien inversibles dans $\mathbb{Z}[j]$. Bien sûr, 1 et -1 sont inversibles dans $\mathbb{Z}[j]$, de même que j et $-j$ puisque

$$j \times j^2 = j^3 = 1$$

et de même que $1+j$ et $-1-j$ car

$$1 + j = -j^2.$$

Le groupe des éléments inversibles de $\mathbb{Z}[j]$ est d'ordre 6 et cyclique car $1 + j = -j^2$ est d'ordre 6. Il est donc isomorphe à $(\mathbb{Z}/6\mathbb{Z}; +)$. ■

Exercice 15 Déterminer les éléments inversibles de $\mathbb{Z}[i\sqrt{3}] = \left\{a + ib\sqrt{3} : a, b \in \mathbb{Z}\right\}$. Montrer que 4 admet deux décompositions distinctes en produits d'irréductibles de $\mathbb{Z}[i\sqrt{3}]$.

Solution. On introduit l'application $N : \mathbb{Z}[i\sqrt{3}] \to \mathbb{N}$ définie par

$$N(a + i\sqrt{3}b) = a^2 + 3b^2 \quad \text{pour tout } a, b \in \mathbb{Z}.$$

On vérifie que N satisfait

$$N(zz') = N(z)N(z') \quad \text{pour tout } z, z' \in \mathbb{Z}[i\sqrt{3}].$$

Soit $z \in \mathbb{Z}[i\sqrt{3}]$ un élément inversible. On a

$$N(zz^{-1}) = 1 = N(z)N(z^{-1}).$$

Il s'ensuit que $N(z) \in \{-1, 1\}$. De ceci, il n'est pas difficile de voir que $z \in \{-1, 1\}$. Réciproquement, -1 et 1 sont inversibles dans l'anneau $\mathbb{Z}[i\sqrt{3}]$.

Supposons que $z := 1 + i\sqrt{3}$ ne soit pas irréductible dans $\mathbb{Z}[i\sqrt{3}]$. Il existe alors $x, y \in \mathbb{Z}[i\sqrt{3}]$ avec $z = xy$ et $x, y \notin \mathbb{Z}[i\sqrt{3}]^\times$. Il vient

$$4 = N(z) = N(xy) = N(x)N(y).$$

Puisque $N(x) \neq 1$ et $N(y) \neq 1$ (car x et y ne sont pas inversibles), on a nécessairement $N(x) = N(y) = 2$. Ceci est absurde car il n'existe pas deux entiers relatifs a, b tels que $a^2 + 3b^2 = 2$. Ainsi, z est irréductible dans l'anneau $\mathbb{Z}[i\sqrt{3}]$. De même, $1 - i\sqrt{3}$ et 2 sont irréductibles dans $\mathbb{Z}[i\sqrt{3}]$. Il reste à voir que

$$4 = 2.2 = (1 - i\sqrt{3})(1 + i\sqrt{3}).$$

■

Exercice 16 (Eléments inversibles de $\mathbb{Z}/n\mathbb{Z}$) Soit $n \geq 2$ un entier. Déterminer les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Solution. Nous allons montrer que les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les classes $\overline{m}$ avec $m \in \{1, \ldots, n-1\}$ et m premier avec n.

Soit $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. On peut écrire $x = \overline{k}$ pour un certain entier $k \in \{1, \ldots, n-1\}$. Par inversibilité, nous savons qu'il existe $a \in \{1, \ldots, n-1\}$ tel que $\overline{a}\overline{k} = \overline{1}$. Ceci nous dit qu'il existe un $b \in \mathbb{Z}$ tel que

$$ak + bn = 1.$$

D'après le théorème de Bézout, les entiers k et n sont premiers entre eux. Réciproquement, pour $y \in \mathbb{Z}/n\mathbb{Z}$ s'écrivant $y = \overline{l}$ avec $l \in \{1, \ldots, n-1\}$ et l et n premiers entre eux, on peut écrire

$$ul + vn = 1$$

pour un certain $(u, v) \in \mathbb{Z}^2$ et ceci entraîne $\overline{u}\overline{l} = \overline{1}$, en particulier $y \in (\mathbb{Z}/n\mathbb{Z})^\times$. ■

Exercice 17 Déterminer les éléments inversibles de l'anneau $M_2(\mathbb{Z})$ des matrices carrées d'ordre 2 à coefficients dans $\mathbb{Z}$.

Solution. Il suffit d'observer que pour $M \in M_2(\mathbb{Z})$ inversible dans $M_2(\mathbb{Z})$, on doit avoir

$$\det(M) = \frac{1}{\det(M^{-1})} \in \mathbb{Z}$$

ce qui entraîne $\det(M) \in \{-1, 1\}$. Réciproquement, si $M \in M_2(\mathbb{Z})$ satisfait l'inclusion $\det(M) \in \{-1, 1\}$, la matrice M est inversible dans $M_2(\mathbb{R})$ d'inverse

$$M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

et ceci montre que $M^{-1} \in M_2(\mathbb{Z})$. ■

Exercice 18 (Diviseurs de zéro) Soient $(A; +, \times)$ un anneau, $a \in A$ avec $a \neq 0_A$. On dit que a est un *diviseur de zéro à gauche* (resp. un *diviseur de zéro à droite*) dans A lorsqu'il existe $b \in A$ avec $b \neq 0_A$ tel que $ab = 0_A$ (resp. $ba = 0_A$). Si a est un diviseur de zéro à gauche ou à droite dans A, on dit que a est un *diviseur de zéro* dans A.

1. Déterminer les diviseurs de zéro dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{R}[X]$.
2. Déterminer les diviseurs de zéro dans $\mathbb{Z}/4\mathbb{Z}$.
3. Montrer que si $a \in A$ est inversible à droite (resp. à gauche) dans A, alors a n'est pas un diviseur à droite (resp. à gauche) de zéro.
4. Montrer que si A est intègre, alors il n'admet aucun diviseur de zéro à gauche (resp. à droite).
5. Déterminer les diviseurs de zéro dans $\mathbb{Z}/n\mathbb{Z}$ avec $n \geq 2$.

Solution.

1. Il n'y a pas de diviseurs de zéro dans ces anneaux.

2. Seul $\overline{2}$ est un diviseur de zéro dans $\mathbb{Z}/2\mathbb{Z}$.
3. On montre le résultat à droite. Supposons $a \in A$ inversible à droite dans A. Il existe alors $b \in A$ avec $ab = 1_A$. Si a était un diviseur à droite dans A, on aurait $d \in A$ avec $d \neq 0_A$ tel que $da = 0_A$ et ceci donnerait $dab = d = 0_A$.
4. Evident.
5. Supposons $n > 2$ (sinon c'est trivial). Soit $x \in Z/n\mathbb{Z}$ avec $x \neq 0$ et tel que x n'est pas inversible dans $Z/n\mathbb{Z}$. Nous allons montrer que x est un diviseur de zéro dans $Z/n\mathbb{Z}$. Il existe donc $k \in \{2, \ldots, n-1\}$ avec $p := \text{p.g.c.d.}(n, k) > 1$ tel que $x = \overline{k}$. Il existe alors deux entiers $a, b > 0$ tels que $pa = k$ et $pb = n$. On remarque alors que $(pa)b = kb$ et $a(pb) = an$, d'où l'égalité $kb = an$ ou encore
$$\overline{k}\,\overline{b} = \overline{0}.$$
Il reste à voir que $\overline{b} \neq \overline{0}$ pour obtenir que $x = \overline{k}$ est un diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$.

■

Exercice 19 Montrer que $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n \in \mathbb{P}$.

Solution. Ceci résulte tout de suite de la description des éléments inversibles et des diviseurs de zéro de $\mathbb{Z}/n\mathbb{Z}$. ■

Exercice 20 (Réguliers à gauche, à droite) Soient $(A; +, \times)$ un anneau. On dit que $a \in A$ est *régulier à gauche* (resp. *régulier à droite*) lorsque pour tout $b, c \in A$,
$$ab = ac \Rightarrow b = c$$
(resp.
$$ba = ca \Rightarrow b = c).$$
On dit que $a \in A$ est *régulier* lorsqu'il est régulier à gauche et à droite.

1. Montrer que tout élément de A inversible à gauche (resp. à droite) est régulier à gauche (resp. à droite).
2. Soit $a \in A$ avec $a \neq 0_A$. Montrer que a est régulier à gauche (resp. à droite) si et seulement si a n'est pas un diviseur de zéro à gauche (resp. à droite).

Solution.

1. On montre le résultat à gauche. Soit $a \in A$ inversible à gauche. Il existe $b \in A$ tel que $ba = 1_A$. Fixons $c, d \in A$ tels que $ac = ad$. On a
$$(ba)c = (ba)d$$
d'où l'égalité attendue $c = d$. Ainsi, a est régulier à gauche.
2. On montre le résultat à gauche. Supposons que a ne soit pas un diviseur de zéro à gauche. Fixons $b, c \in A$ tels que $ab = ac$. Si $b \neq c$, alors l'égalité $a(b - c) = 0_A$ nous dit que a est un diviseur de zéro à gauche. En conséquence, on a $b = c$, d'où le fait que a est régulier à gauche. Supposons que a soit régulier à gauche. Par l'absurde, supposons que a est un diviseur de zéro à gauche. Il existe $b \in A$ avec $b \neq 0_A$ tel que $ab = 0_A$. L'égalité
$$ab = 0_A = a\,0_A$$
combinée au fait que a soit régulier à gauche nous dit que $b = 0_A$ ce qui est contradictoire.

■

Exercice 21 Soient B, C deux sous-anneaux d'un anneau $(A; +, \times)$. Montrer que si $C \subset B$, alors C est un sous-anneau de B muni des lois induites par celles de A.

Solution. C'est immédiat en utilisant la caractérisation des sous-anneaux donnée dans le cours. ■

Exercice 22 Montrer que $\mathbb{Q}$ n'admet pas de sous-corps autre que lui-même.

Solution. Soit K un sous-corps de $\mathbb{Q}$. On a $\{0, 1\} \subset K$. De ceci, on tire $\mathbb{N} \subset K$ puis $\mathbb{Z} \subset K$. De cette dernière inclusion, on déduit $1/k \in \mathbb{Q}$ pour tout entier $k \neq 0$. Il reste à invoquer la stabilité par produit pour aboutir à $\mathbb{Q} \subset K$. ■

Exercice 23 (Anneau produit) Soient I un ensemble non vide et $(A_i; +_i, \times_i)_{i \in I}$ une famille d'anneaux. Montrer que l'on peut munir (naturellement) le produit cartésien $\prod_{i \in I} A_i$ d'une structure d'anneaux.

Solution. On rappelle que $P = \prod_{i \in I} A_i$ désigne l'ensemble des applications f de I dans $\bigcup_{i \in I} A_i$ telles que pour chaque $i \in I$, $f(i) \in A_i$. Il est usuel et commode de noter un élément $f \in \prod_{i \in I} A_i$ sous la forme d'une famille $(x_i)_{i \in I}$, avec $x_i = f(i) \in A_i$ pour tout $i \in I$. On vérifie sans mal que les lois $\oplus$ et $\otimes$ définies pour chaque $(x_i)_{i \in I}, (y_i)_{i \in I} \in P$ par

$$(x_i)_{i \in I} \oplus (y_i)_{i \in I} = (x_i +_i y_i)_{i \in I}$$

et

$$(x_i)_{i \in I} \otimes (y_i)_{i \in I} = (x_i \times_i y_i)_{i \in I}$$

confèrent à P une structure d'anneau. ■

Exercice 24 (Anneau de fonctions) Soient $(A; +, \times)$ un anneau et T un ensemble non vide. Montrer que l'on peut munir (naturellement) l'ensemble $\mathcal{F}(T, A)$ des fonctions de T dans A d'une structure d'anneau (commutatif si A l'est).

Solution. On munit naturellement $\mathcal{F}(T, A)$ d'une structure d'anneaux via les deux lois internes $\oplus, \otimes : A^2 \to A$ définies pour tout $f, g \in \mathcal{F}(T, A)$ par

$$(f \oplus g)(t) := f(t) + g(t),$$

$$(f \otimes g)(t) := f(t) \times g(t).$$

Evidemment, $(\mathcal{F}(T, A); \oplus, \otimes)$ est un anneau commutatif lorsque A est lui-même commutatif. ■

Exercice 25 Montrer qu'un sous-anneau non nul d'un anneau intègre est intègre. Donner des exemples d'anneaux intègres et non intègres. Un produit d'anneaux intègres est-il intègre ? Soient A, B deux anneaux. Montrer que $A \times B$ est intègre si et seulement si l'un des deux anneaux est nul et l'autre est intègre.

Solution. Le fait qu'un sous-anneau non nul d'un anneau intègre est intègre résulte des définitions de sous-anneaux et d'intégrité. Les anneaux $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ munis de leurs lois usuelles sont intègres. Tout corps est un anneau intègre. L'anneau $M_n(\mathbb{K})$ (muni de l'addition et de la multiplication matricielle) n'est pas intègre dès lors que $n \geq 2$. Le produit d'anneaux intègres n'est pas nécessairement intègre, même pour la structure naturelle d'anneaux produits ! En effet, pour $\mathbb{R} \times \mathbb{R}$ muni de sa structure naturelle d'anneau, on a

$$(1, 0)(0, 1) = (0, 0).$$

Montrons l'équivalence voulue. Seule l'implication $\Rightarrow$ mérite une justification. Supposons que $A \times B$ soit intègre. Puisque $A \times B$ n'est pas réduit à zéro (car intègre) l'un des anneaux A ou B n'est pas réduit à zéro. Si A n'est pas réduit à zéro, on peut écrire pour $a_0 \in A \setminus \{0_A\}$ et pour tout $b \in B$

$$(a_0, 0_B)(0_A, b) = (0_A, 0_B) = (0_A, 0_B) = 0_{A \times B}$$

et ceci entraîne que B est nécessairement réduit à zéro, i.e., $A \times B = A \times \{0\}$. De même, si B n'est pas réduit à zéro, on a $A \times B = \{0\} \times B$. L'implication voulue est établie. ■

Exercice 26 Montrer que tout anneau A intègre fini est un corps. **Indication :** pour $a \in A$ avec $a \neq 0_A$, on pourra considérer l'application $\tau_a : A \to A$ définie par

$$\tau_a(x) := ax \quad \text{pour tout } x \in A.$$

Solution. Soit $a \in A$ avec $a \neq 0_A$. Il est clair que τ_a est un morphisme de groupe additifs. Il est injectif car l'anneau A est intègre et bijectif car A est fini. Cette bijectivité nous assure en particulier qu'il existe $b \in A$ tel que $ab = 1_A$. En considérant l'application $\tau'_a : A \to A$ définie par

$$\tau'_a(x) := xa \quad \text{pour tout } x \in A$$

on montre de même qu'il existe $c \in A$ tel quer $ca = 1_A$. Il reste à voir que

$$c = c(ab) = (ca)b = b$$

pour obtenir que a est inversible dans A. ■

Exercice 27 Soit $(A; +, \times)$ un anneau. Montrer que le *centre* $Z(A) := \{a \in A : \forall b \in A, ab = ba\}$ de A est un sous-anneau de A. Que dire d'un anneau égal à son centre ?

Solution. On a $1_A \in Z(A)$ et pour tout $a \in A$, $x, y \in Z(A)$,

$$(x - y)a = xa - ya = ax - ay = a(x - y)$$

et

$$(xy)a = x(ya) = x(ay) = (xa)y = axy.$$

Ceci montre que $Z(A)$ est un sous-anneau de $(A; +, \times)$. On vérifie sans mal que $A = Z(A)$ si et seulement si A est commutatif. ■

Exercice 28 Déterminer le centre de $\mathbb{H}$.

Solution. Soient $a, b \in \mathbb{C}$. Supposons que $\begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}$ soit un élément du centre de $\mathbb{H}$. On a alors

$$\begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix},$$

d'où l'on tire $b = 0$. De manière analogue, l'égalité

$$\begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix}$$

nous dit que $a \in \mathbb{R}$. Il n'est alors pas difficile de conclure que

$$Z(\mathbb{H}) = \{\lambda \mathrm{I}_2 : \lambda \in \mathbb{R}\}.$$

■

Exercice 29 Donner le plus petit sous-anneau de $\mathbb{Q}$ contenant $1/5$.

Solution. D'après la description donnée dans le cours, le plus petit sous-anneau de $\mathbb{Q}$ contenant $1/5$ est donné par

$$\mathbb{Q}[1/5] := \left\{ \frac{k}{5^n} : k \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

■

Exercice 30 Donner le sous-anneau de $\mathbb{C}$ engendré par $2i$.

Solution. On note A le sous-anneau recherché. On constate que $B := \{a + 2bi : a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$ qui contient $\{2i\}$. On a donc $A \subset B$. Montrons l'inclusion renversée. Soit $z \in B$. Il existe $p, q \in \mathbb{Z}$ tels que $x = p + 2qi$. On a evidemment $p \in A$ et $2qi \in A$, donc $x = p + 2qi \in A$. On conclut que $B \subset A$ puis $A = B$. ■

Exercice 31 Déterminer les idéaux de $\mathbb{Z}$.

Solution. On commence par observer que pour chaque $n \in \mathbb{N}$, l'ensemble $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$. Nous allons montrer que tout idéal de $\mathbb{Z}$ est de la forme $k\mathbb{Z}$ pour un certain entier k.

Soit K un idéal de $\mathbb{Z}$. On peut supposer que $K \neq \{0\}$. On pose

$$n := \min\{|k| : k \in K \setminus \{0\}\}.$$

On a évidemment $n\mathbb{Z} \subset K$. Montrons l'inclusion renversée. Soit $a \in K$. Il existe un couple $(q, r) \in \mathbb{Z}^2$ tel que $a = nq + r$ avec $0 \leq r < n$. Il s'ensuit $r = a - nq \in K$. Compte-tenu de la définition de n, on a nécessairement $r = 0$, i.e., $a = nq \in n\mathbb{Z}$.

En conclusion, les idéaux de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$ avec $n \in \mathbb{N}$. ■

Exercice 32 Soit $(I_j)_{j\in J}$ une famille non vide d'idéaux à gauche (resp. à droite (resp. bilatère)) d'un anneau $(A; +, \times)$. Montrer que $\bigcap_{j\in J} I_j$ est un idéal à gauche (resp. à droite (resp. bilatère)) de A.

Solution. C'est une conséquence directe de la définition de $\bigcap_{j\in J} I_j$ et d'idéaux à gauche (resp. à droite (resp. bilatère)) d'un anneau. ■

Exercice 33 Soit $(A; +, \times)$ un anneau. Que dire d'un idéal à gauche (resp. à droite) de A contenant un élément inversible à gauche (resp. à droite) ?

Solution. Soit I un idéal à gauche de A. Supposons qu'il existe $a \in I$ avec a inversible à gauche. Par définition d'inversibilité à gauche, il existe $b \in A$ tel que $ba \in I$. Puisque $ba = 1_A$, il vient $1_A \in I$. Il reste à exploiter le fait que I est un idéal à gauche pour obtenir pour tout $a' \in A$, $a' = a'.1_A \in I$, i.e., $A = I$. ■

Exercice 34 Soient $(A; +, \times)$ un anneau, B un sous-anneau de A et I un idéal à gauche (resp. à droite (resp. bilatère)) de A. Montrer que l'ensemble $B \cap I$ est un idéal à gauche (resp. à droite (resp. bilatère)) de B.

Solution. On traite le cas à gauche (celui de droite étant similaire). Puisque B et I sont des sous-groupes de $(A; +)$, l'ensemble $B \cap I$ est un sous-groupe de $(A; +)$. Soient $b \in B$ et $j \in B \cap I$. Le fait que B (resp. I) soit un sous-anneau de A (resp. idéal à gauche de B) garantit l'inclusion $bj \in B$ (resp. $bj \in I$). On conclut que I est un idéal à gauche de B. ■

Exercice 35 (Idéaux d'un produit) Soient A_1, A_2 deux anneaux. Montrer que tout idéal $\mathcal{I}$ à gauche (resp. à droite) de l'anneau produit $A_1 \times A_2$ est de la forme $\mathcal{I} = \mathcal{I}_1 \times \mathcal{I}_2$ où $\mathcal{I}_1$ un idéal à gauche (resp. à droite) de A_1 et où $\mathcal{I}_2$ est un idéal à gauche (resp. à droite) de A_2.

Solution. On montre le résultat dans le cas des idéaux à gauche (celui à droite étant totalement analogue). Soit $\mathcal{I}$ un idéal à gauche de $A_1 \times A_2$. On commence par introduire pour $i \in \{1, 2\}$ l'application $p_i : A_1 \times A_2 \to A_i$ définie par

$$p_i(a_1, a_2) := a_i \quad \text{pour tout } (a_1, a_2) \in A_1 \times A_2.$$

Nous allons montrer que $p_1(\mathcal{I}) =: \mathcal{I}_1$ est un idéal à gauche de A_1. On vérifie tout de suite que $\mathcal{I}_1$ est un sous-groupe additif de A_1. Soit $a_1 \in A$ et $i_1 \in \mathcal{I}_1$. Par définition de p_1, il existe $i_2 \in A_2$ tel que $(i_1, i_2) \in \mathcal{I}$. On peut alors écrire

$$a_1 i_1 = p_1(a_1, 1_{A_2}) p_1(i_1, i_2) = p_1[(a_1, 1_{A_2})(i_1, i_2)] \in p_1(\mathcal{I}) = \mathcal{I}_1,$$

où l'inclusion résulte du fait que $\mathcal{I}$ est un idéal à gauche de $A_1 \times A_2$. On montre de même que $\mathcal{I}_2 := p_2(\mathcal{I})$ est un idéal à gauche de A_2. Il nous reste à établir que $\mathcal{I} = \mathcal{I}_1 \times \mathcal{I}_2$. L'inclusion $\mathcal{I} \subset \mathcal{I}_1 \times \mathcal{I}_2$ est une conséquence immédiate des définitions de $\mathcal{I}_1$ et de $\mathcal{I}_2$. Fixons $(a_1, a_2) \in \mathcal{I}_1 \times \mathcal{I}_2$. En choisissant $a_2' \in A_2$ et $a_1' \in A_1$ tels que $(a_1, a_2'), (a_1', a_2) \in \mathcal{I}$ et en écrivant

$$(a_1, a_2) = (1_{A_1}, 0_{A_2})(a_1, a_2') + (0_{A_1}, 1_{A_2})(a_1', a_2)$$

on constate que (a_1, a_2) est la somme de deux éléments de $\mathcal{I}$ (puisque $\mathcal{I}$ est un idéal à gauche de A) et donc un élément de $\mathcal{I}$. L'égalité attendue est ainsi démontrée. ■

Exercice 36 Montrer qu'un anneau intègre $(A; +, \times)$ possédant un nombre fini d'idéaux est un corps.

Solution. Soit $a \in A$ avec $a \neq 0_A$. Pour chaque entier $n \geq 1$, on pose $I_n = Aa^n$ qui est évidemment un idéal à gauche dans A. Il existe $p, q \geq 1$ deux entiers avec $p < q$ tels que $I_p = I_q$. Cette dernière égalité nous dit alors qu'il existe $b \in A$ tel que $a^p = ba^q$. En écrivant

$$(1_A - ba^{q-p})a^p = 0_A$$

et en exploitant l'intégrité de $(A; +, \times)$, on aboutit à

$$ba^{q-p} = 1_A.$$

Ceci nous dit que $(ba^{q-p-1})a = 1_A$, en particulier a est inversible à gauche dans A. En procédant de même avec la suite d'idéaux à droite $(J_n)_{n\geq 1}$ de A définie par $J_n = a^n A$ pour chaque entier $n \geq 1$, on obtient que a est inversible à droite dans A. En conséquence, l'élément a est inversible dans A. ■

Exercice 37 Soient K un corps commutatif et $n \geq 2$ un entier. On considère I un idéal bilatère non nul de $M_n(K)$.

1. Montrer qu'il existe $M = (m_{p,q})_{1\leq p,q\leq n} \in I$ telle que $m_{1,1} \neq 0$.
2. Soit $(p, q) \in \{1, \ldots, n\}$. Effectuer le produit matriciel $E_{p,1}ME_{1,q}$. En déduire que $\mathrm{I}_n \in I$.
3. Conclure.

Solution.

1. Il existe $M_0 \in I$ avec M_0 non nulle. En permutant des lignes et des colonnes de M_0, nous pouvons donc obtenir $M = (m_{p,q})_{1\leq p,q\leq n} \in M_n(K)$ telle que $m_{1,1} \neq 0$. Matriciellement, ceci s'écrit $M = PM_0Q$ avec $P, Q \in GL_n(K)$. Puisque $M_0 \in I$ et que I est un idéal bilatère de $M_n(K)$, nous pouvons conclure que $M \in I$.
2. Un calcul élémentaire montre que $E_{p,1}ME_{1,q} = m_{1,1}E_{p,q}$. Ceci montre que $E_{p,q} \in I$. Puisque p, q sont quelconques dans $\{1, \ldots, n\}$, on obtient $\mathrm{I}_n \in I$.
3. L'idéal I contient un élément inversible, donc $I = M_n(K)$.

■

Exercice 38 Soient A un anneau et S une partie non vide de A. On appelle *annulateur* de S la partie

$$\mathrm{Ann}(S) := \{x \in A : \forall y \in S, xy = 0_A\}.$$

Montrer que $\mathrm{Ann}(S)$ est un idéal à gauche de A.

Exercice 39

(a) Le produit d'anneaux principaux est-il principal ?

(b) Un sous-anneau non nul d'un anneau principal est-il principal ?

(c) Décrire les idéaux de l'anneau produit $A_1 \times A_2$ où A_1 et A_2 sont deux anneaux principaux.

Solution.

(a) En général non, car le produit d'anneaux intègres (et même de corps) n'est pas nécessairement intègre.

(b) Non, $\mathbb{R}[X]$ est principal tandis que $\mathbb{Z}[X]$ ne l'est pas.

(c) Soit I un idéal de $A_1 \times A_2$. On a déjà vu que I peut s'écrire $I = I_1 \times I_2$ où I_1 est un idéal de A_1 et I_2 est un idéal de A_2. Par principalité, on a $I_1 = (a_1)$ et $I_2 = (a_2)$ pour un certain $(a_1, a_2) \in A_1 \times A_2$. On conclut que $I = (a_1 a_2)$.

■

Exercice 40 Montrer que $\mathbb{D}$ est un anneau principal.

Solution. L'anneau $(\mathbb{D}; +, \times)$ est évidemment intègre et commutatif. Soit I un idéal de $\mathbb{D}$. On a déjà vu que $I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$ ce qui permet d'écrire $I \cap \mathbb{Z} = k\mathbb{Z}$ pour un certain $k \in \mathbb{N}$. Il n'est alors pas difficile de voir que $I = k\mathbb{D}$. Ceci confirme que $\mathbb{D}$ est principal. ■

Exercice 41 Montrer que l'ensemble $\mathbb{R}^{(\mathbb{N})}$ des suites réelles nulles à partir d'un certain rang est un idéal non principal de $\mathbb{R}^{\mathbb{N}}$.

Solution. Le fait que $\mathbb{R}^{(\mathbb{N})}$ soit un idéal de $\mathbb{R}^{\mathbb{N}}$ est évident. Supposons que $\mathbb{R}^{(\mathbb{N})}$ soit principal, i.e., supposons qu'il existe $\zeta \in \mathbb{R}^{\mathbb{N}}$ tel que $(\zeta) = \mathbb{R}^{(\mathbb{N})}$. Il existe un entier $N \geq 1$ tel que $\zeta(N) = 0$ pour tout entier $k \geq N$. Soit $\xi \in \mathbb{R}^{(\mathbb{N})}$ avec $\xi(N) \neq 0$. Il existe $\theta \in \mathbb{R}^{\mathbb{N}}$ tel que $\xi = \theta\zeta$. Il s'ensuit $\xi(N) = \theta(N)\zeta(N) = 0$ et ceci est contradictoire. ■

Exercice 42 (Une caractérisation des anneaux noethériens) Soit A un anneau commutatif. Montrer que A est noethérien si et seulement si toute suite croissante d'idéaux de A est stationnaire.

Solution. $\Rightarrow$, Supposons que A soit noethérien. Fixons $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A. Il n'est pas difficile de vérifier que $I := \bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A. Il existe alors $m \in \mathbb{N}$, $a_0, \ldots, a_m \in A$ tels que $I = (a_0, \ldots, a_m)$. Pour tout $k \in \{0, \ldots, m\}$, il existe $s(k) \in \{0, \ldots, m\}$ tel que $a_k \in I_{s(k)}$. Notons $s := \max_{0\leq k\leq m} s(k)$. La propriété de croissance de la suite $(I_n)_{n\in\mathbb{N}}$ nous dit alors que

$$\bigcup_{n\in\mathbb{N}} I_n = (a_0, \ldots, a_m) \subset I_s.$$

Ceci entraîne alors que $I_{s+k} \subset I_s \subset I_{s+k}$ pour tout $k \in \mathbb{N}$. En particulier, la suite $(I_n)_{n\in\mathbb{N}}$ est stationnaire.

$\Leftarrow$, Supposons que toute suite croissante d'idéaux de A est stationnaire. Par l'absurde, supposons que A ne soit pas un anneau noethérien. On peut alors trouver un idéal J de A qui n'est pas de type fini. Fixons $a_0 \in J$. Puisque J n'est pas de type fini, on a $J \setminus (a_0) \neq \emptyset$ et ceci justifie l'existence de $a_1 \in J$ tel que $a_1 \notin (a_0)$. De même, il existe $a_2 \in J$ tel que $a_2 \notin (a_0, a_1)$. On construit ainsi par récurrence une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de J telle que

$$a_{n+1} \notin (a_0, \ldots, a_n) \quad \text{pour tout } n \in \mathbb{N}.$$

Notons $I_n := (a_0, \ldots, a_n)$ pour chaque $n \in \mathbb{N}$. Il est clair que la suite $(I_n)_{n\in\mathbb{N}}$ est croissante : elle est donc stationnaire par hypothèse. Il existe alors $r \in \mathbb{N}$ tel que $I_r = I_{r+1}$ et ceci entraîne $a_{r+1} \in (a_0, \ldots, a_r)$. Cette dernière inclusion est contradictoire. ■

Exercice 43 (Radical d'un idéal) Soient $(A; +, \times)$ un anneau commutatif et I un idéal de A. On appelle *radical* de I l'ensemble

$$\sqrt{I} := \{a \in A : \exists n \geq 1, a^n \in I\}.$$

Montrer que $\sqrt{I}$ est un idéal de A. En déduire que l'ensemble des éléments nilpotents de A est un idéal de A.

Solution. Montrons tout d'abord que $\sqrt{I}$ est un sous-groupe de $(A;+)$. On a evidemment l'inclusion $0_A \in \sqrt{I}$. Soient $x, y \in \sqrt{I}$. Fixons $m, n \geq 1$ deux entiers tels que $x^m \in I$ et $y^n \in I$. L'anneau $(A;+,\times)$ étant commutatif, il vient

$$(x-y)^{m+n} = \sum_{k=0}^{m+n} C_{m+n}^k (-1)^{m+n-k} x^k y^{m+n-k}. \tag{1}$$

Fixons $k_0 \in \{0, \ldots, m+n\}$ et observons que deux cas se présentent.
Cas 1 : $k_0 \geq m$. Dans ce cas, on a $x^{k_0} y^{m+n-k_0} = x^m x^{k_0-m} y^{m+n-k_0} \in I$.
Cas 2 : $k_0 < m$. On a alors $m+n-k_0 > n$ puis $x^{k_0} y^{m+n-k_0} = x^{k_0} y^{m-k_0} y^n \in I$.
En combinant les deux cas ci-dessus à l'égalité (1) et au fait que I est un sous-groupe de $(A;+)$, nous obtenons

$$(x-y)^{m+n} \in I,$$

en particulier $x - y \in \sqrt{I}$. Enfin, il reste à voir que pour $a \in A$ et $b \in \sqrt{I}$, on a toujours $ab \in \sqrt{I}$. En effet, par définition de radical, on dispose d'un entier $l \geq 1$ tel que $b^l \in I$, en particulier (car I est un idéal de A)

$$(ab)^l = a^l b^l \in I$$

ce qui montre que $ab \in \sqrt{I}$. Enfin, l'ensemble des éléments nilpotents de A n'est nul autre que $\sqrt{\{0_A\}}$ qui est un idéal de A puisque $\{0_A\}$ est un idéal de A. ■

Exercice 44 Déterminer $\sqrt{m\mathbb{Z}}$ avec $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ où $r \in \mathbb{N}^\star$, $p_1, \ldots, p_r \in \mathbb{P}$ et $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^\star$. En déduire les idéaux $\mathcal{I}$ de $\mathbb{Z}$ tels que $\sqrt{\mathcal{I}} = \mathcal{I}$.

Solution. Nous allons montrer que $\sqrt{m\mathbb{Z}} = p_1 \ldots p_r \mathbb{Z}$. Soit $a \in \sqrt{m\mathbb{Z}}$. Choisissons $n \geq 1$ entier tel que $a^n \in m\mathbb{Z}$. Sans perte de généralités, on peut supposer que $a \geq 1$. Il existe (c'est la décomposition en facteurs premiers de a) un entier $l \geq 1$, des nombres premiers $q_1, \ldots, q_l$ et des entiers $\beta_1, \ldots, \beta_l \geq 1$ tels que

$$a = q_1^{\beta_1} \ldots q_l^{\beta_l}.$$

Il découle de ceci et de l'inclusion $a^n \in m\mathbb{Z}$ que $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r} \mid q_1^{n\beta_1} \ldots q_l^{n\beta_l}$. Cette dernière relation de divisibilité nous dit en particulier que les nombres premiers $p_1, \ldots, p_r$ sont dans la décomposition en facteurs premiers de a. Ceci montre que

$$\sqrt{m\mathbb{Z}} \subset p_1 \ldots p_r \mathbb{Z}$$

et cette inclusion est en fait une égalité puisqu'il est évident que $p_1 \ldots p_r \mathbb{Z} \subset \sqrt{m\mathbb{Z}}$.

Les idéaux $\mathcal{I}$ de $\mathbb{Z}$ satisfaisant $\sqrt{\mathcal{I}} = \mathcal{I}$ sont les idéaux engendrés par les éléments de la forme $p_1 \ldots p_r$ où $r > 1$ est un entier et où $p_1, \ldots, p_r \in \mathbb{P}$ sont distincts deux à deux. ■

Exercice 45 (Somme d'idéaux) Soit A un anneau. On considère I et J deux idéaux de A **de même nature**.

1. Montrer que $I + J := \{i + j : (i,j) \in I \times J\}$ est un idéal de même nature que I et J.
2. L'ensemble $I \cup J$ est-il un idéal de A ?
3. Montrer que si I et J sont des idéaux à gauche, alors

$$I + J = (I \cup J)_g.$$

Procéder de même pour le cas à droite. Que dire dans le cas où I et J sont des idéaux bilatères ?

Solution.

1. L'ensemble $I+J$ est évidemment un sous-groupe de $(A;+)$. Supposons que I et J soient des idéaux à gauche de A. On observe sans difficultés que pour tout $a \in A$ et pour tout $(i,j) \in I \times J$, on a
$$a(i+j) = ai + aj \in I + J.$$
Ceci montre que $I+J$ est un idéal à gauche de A. On procède de même pour le cas à droite. Lorsque I et J sont bilatères, l'ensemble $I+J$ est un idéal à gauche et à droite de A, i.e., est un idéal bilatère de A.
2. L'union d'idéaux n'est pas un idéal en général : $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un idéal de $\mathbb{Z}$.
3. On a toujours
$$I \cup J \subset I + J.$$
Supposons que I et J soient des idéaux de A à gauche. Ce qui précède montre que $I+J$ est un idéal de A à gauche qui contient $I \cup J$ et ceci donne
$$(I \cup J)_g \subset I + J.$$
Pour obtenir l'inclusion renversée, il suffit de remarquer que
$$I \subset (I \cup J)_g \quad \text{et} \quad J \subset (I \cup J)_g$$
d'où l'on tire
$$I + J \subset (I \cup J)_g.$$
On procède de même pour le cas à droite. Lorsque I et J sont bilatères, on a
$$I + J = (I \cup J)_g = (I \cup J)_d \subset (I \cup J)_b \subset I + J,$$
d'où les égalités
$$I + J = (I \cup J)_g = (I \cup J)_d = (I \cup J)_b.$$

■

Exercice 46 (Produit d'idéaux) Soit A un anneau. On considère I et J deux idéaux de A **bilatères**.

1. L'ensemble $\mathcal{P} = \{ij : i \in I, j \in J\}$ est-il un idéal de A ?
2. Montrer que l'ensemble
$$IJ := \left\{ \sum_{k=1}^{m} i_k j_k : m \geq 1, \forall 1 \leq k \leq m, (i_k, j_k) \in I \times J \right\}$$
est l'idéal bilatère engendré par $\mathcal{P}$, i.e., $(\mathcal{P})_b = IJ$.
3. Montrer que
$$IJ \subset I \cap J.$$
Cette inclusion est-elle une égalité en général ?
4. Montrer que si $I + J = A$, alors $IJ = I \cap J$.
5. Montrer que
$$(I+J)K = IK + JK.$$

Exercice 47 Soient A un anneau commutatif et I un idéal de A.

1. Que dire de $\sqrt{\sqrt{I}}$?

2. Soit J un autre idéal de l'anneau A. Montrer que

$$\sqrt{I+J} = \sqrt{\sqrt{I}+\sqrt{J}} \quad \text{et} \quad \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} = \sqrt{IJ}.$$

Exercice 48 Un anneau commutatif peut-il être isomorphe à un anneau non commutatif ? Même question en remplaçant "commutatif" par "intègre".

Solution. Soient A un anneau commutatif et B un anneau. Supposons que A et B soient isomorphes. Soit $f : A \to B$ un isomorphisme. Fixons $b_1, b_2 \in B$. Il existe $a_1, a_2 \in A$ tels que $f(a_1) = b_1$ et $f(a_2) = b_2$. On a

$$b_1 b_2 = f(a_1)f(a_2) = f(a_1 a_2) = f(a_2)f(a_1) = b_2 b_1.$$

Ceci montre que B est commutatif. En conclusion, un anneau commutatif ne peut-être isomorphe qu'à un anneau commutatif. Soient A un anneau intègre et B un anneau. Supposons que A et B soient isomorphes. Soit $f : A \to B$ un isomorphisme d'anneaux. Puisque $A \neq \{0\}$ et f bijective, on a nécessairement $B \neq \{0\}$. Fixons $b_1, b_2 \in B$. Il existe $a_1, a_2 \in A$ tels que $f(a_1) = b_1$ et $f(a_2) = b_2$. Il vient alors

$$b_1 b_2 = f(a_1)f(a_2) = f(a_1 a_2).$$

Supposons $b_1 b_2 = 0$. On a tout de suite $a_1 a_2 \in \ker(f)$, i.e., $a_1 a_2 = 0$. L'intégrité de A donne alors $a_1 = 0$ ou $a_2 = 0$. On conclut que B est intègre puisque $b_1 = f(a_1) = 0$ ou $b_2 = f(a_2) = 0$. ■

Exercice 49 Soient A, B, C trois anneaux avec A et B isomorphes et B et C isomorphes. A t-on que A et C sont isomorphes ?

Solution. On dispose par hypothèse de deux isomorphismes d'anneaux $f : A \to B$ et $g : B \to C$. Il suffit alors de considérer l'application $g \circ f : A \to C$ qui est un isomorphisme d'anneaux. ■

Exercice 50 Soient A, B deux anneaux non nuls et $\varphi : A \to B$ un isomorphisme d'anneaux. Montrer que si $a \in A$ est irréductible dans A, alors $\varphi(a)$ est irréductible dans B.

Solution. Soit $a \in A$ irréductible dans A. Commençons par observer que puisque $a \notin A^\times$ on doit avoir $\varphi(a) \notin B^\times$. Fixons $b_1, b_2 \in B$. Supposons que $\varphi(a) = b_1 b_2$. Il existe $a_1, a_2 \in A$ tels que $\varphi(a_1) = b_1$ et $\varphi(a_2) = b_2$. Il s'ensuit $\varphi(a) = \varphi(a_1 a_2)$ puis $a = a_1 a_2$. Par irréductibilité de a, nous avons $a_1 \in A^\times$ ou $a_2 \in A^\times$ et ceci entraîne que $b_1 = \varphi(a_1) \in B^\times$ ou $b_2 = \varphi(a_2) \in B^\times$. On conclut que $\varphi(a)$ est irréductible dans A. ■

Exercice 51 Soient A un anneau et T un ensemble non vide. On suppose $\mathcal{F}(T, A)$ muni de sa structure naturelle d'anneau induite par celle de A. Montrer que l'application $\mathrm{ev}_t : \mathcal{F}(T, A) \to A$ définie par

$$\mathrm{ev}_t(f) := f(t) \quad \text{pour tout } f \in \mathcal{F}(T, A)$$

est un morphisme d'anneaux.

Solution. Ceci découle de la structure d'anneau (naturelle) sur $\mathcal{F}(T, A)$. ■

Exercice 52 Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme d'anneaux.

1. Montrer que $f(q) = q$ pour tout $q \in \mathbb{Q}$.
2. Montrer que pour tout $x \in \mathbb{R}_+$, $f(x) \geq 0$. En déduire que f est croissante.
3. Conclure que $f = \mathrm{Id}_{\mathbb{R}}$.

Solution.

1. Par définition de morphisme d'anneaux, on a tout de suite pour tout entier $n \geq 1$

$$f(n) = f(1 + \ldots + 1) = nf(1) = n.$$

L'extension de cette égalité aux entiers relatifs est immédiate en utilisant $f(-1) = -1$, i.e.,

$$f(n) = n \quad \text{pour tout } n \in \mathbb{Z}.$$

Fixons à présent $p \in \mathbb{Z}$ et $q \geq 1$ entier. On a tout de suite

$$f(p/q) = f(1/q + \ldots + 1/q) = f(p)f(1/q) = pf(1/q) = p/q,$$

où la dernière égalité résulte de

$$1 = f(1) = f(q \times 1/q) = f(q)f(1/q) = qf(1/q).$$

2. Il suffit d'écrire pour tout réel $x \geq 0$,

$$f(x) = f(\sqrt{x}\sqrt{x}) = (f(\sqrt{x})^2 \geq 0$$

pour obtenir le résultat désiré. De ceci, nous déduisons que f est croissante sur $\mathbb{R}$ puisque pour tout $t_1 \leq t_2$, on a

$$f(t_2) - f(t_1) = f(t_2 - t_1) \geq 0,$$

où l'inégalité résulte du fait que $t_2 - t_1 \geq 0$.

3. Fixons $x \in \mathbb{R}$. Nous savons qu'il existe deux suites de rationnels $(q_n)_{n\geq 1}$ et $(r_n)_{n\geq 1}$ qui convergent vers x et qui vérifient

$$q_n \leq x \leq r_n \quad \text{pour tout } n \geq 1.$$

Par croissance de f sur $\mathbb{R}$, nous obtenons alors

$$q_n = f(q_n) \leq f(x) \leq f(r_n) = r_n \quad \text{pour tout } n \geq 1.$$

Il reste à effectuer un passage à la limite pour arriver à $f(x) = x$.

■

Exercice 53 Soit $f : \mathbb{C} \to \mathbb{C}$ un morphisme d'anneaux.

1. Montrer que $f(q) = q$ pour tout $q \in \mathbb{Q}$.
2. Montrer les équivalences :
   (i) $f = \mathrm{id}_{\mathbb{C}}$ ou f est la conjugaison.
   (ii) f est continu.
   (iii) $f(\mathbb{R}) \subset \mathbb{R}$.
   (iv) $f(x) = x$ pour $x \in \mathbb{R}$.

Solution.

1. On procède comme l'exercice précédent.
2. L'implication $(i) \Rightarrow (ii)$ est immédiate. L'implication $(ii) \Rightarrow (iii)$ provient de la densité de $\mathbb{Q}$ dans $\mathbb{R}$ et de l'égalité $f(q) = q$ pour tout $q \in \mathbb{Q}$. Pour l'implication $(iii) \Rightarrow (iv)$, il commence par voir que l'inclusion $f(\mathbb{R}) \subset \mathbb{R}$ induit un morphisme d'anneaux $g : \mathbb{R} \to \mathbb{R}$ qui coïncide avec f sur $\mathbb{R}$. On applique alors l'exercice précédent qui nous dit que g est l'identité de $\mathbb{R}$. Enfin, l'implication $(iv) \Rightarrow (i)$ s'obtient en observant que $-1 = f(i^2) = f(i)^2$, i.e., $f(i) \in \{-i, i\}$.

■

Exercice 54 Montrer qu'il n'y a aucun morphisme d'anneaux de X dans Y pour les anneaux suivants (munis de leurs lois usuelles) :

1. $X = \mathbb{C}$ et $Y = \mathbb{R}$;
2. $X = \mathbb{R}$ et $Y = \mathbb{Q}$;
3. $X = \mathbb{Z}/n\mathbb{Z}$ (avec $n \geq 2$ entier) et $Y = \mathbb{Z}$.

Solution.

1. Par l'absurde, supposons qu'il existe un morphisme d'anneaux $\varphi : \mathbb{C} \to \mathbb{R}$. On a tout de suite une contradiction en observant que
$$(\varphi(i))^2 = \varphi(i^2) = \varphi(-1) = -\varphi(1) = -1,$$
où l'avant-dernière égalité résulte de $\varphi(0) = 0$ (puisque $\varphi(0) = 2\varphi(0)$) qui entraîne $\varphi(1+(-1)) = \varphi(1) + \varphi(-1) = 0$.
2. Par l'absurde, supposons qu'il existe un morphisme d'anneaux $\varphi : \mathbb{R} \to \mathbb{Q}$. Il vient alors
$$\varphi(\sqrt{2}\sqrt{2}) = \varphi(2) = 2 = \varphi(\sqrt{2})^2,$$
ce qui donne en particulier l'inclusion $\sqrt{2} \in \mathbb{Q}$. Ceci est la contradiction recherchée.
3. Par l'absurde, supposons qu'il existe un morphisme d'anneaux $\varphi : \mathbb{Q} \to \mathbb{Z}$. Il suffit d'écrire
$$2\varphi(1/2) = \varphi(1) = 1$$
pour aboutir à une contradiction, à savoir l'inclusion $1/2 \in \mathbb{Z}$.
4. Soit $n \geq 2$ un entier. Supposons qu'il existe un morphisme d'anneaux $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$. En observant que $\varphi(\overline{k}) = k\varphi(\overline{1}) = k$ pour tout $k \in \mathbb{Z}$, on peut écrire
$$n = \varphi(\overline{n}) = \varphi(\overline{0}) = 0$$
ce qui est absurde.

■

Exercice 55 Soit A un anneau tel que $x^3 = x$ pour tout $x \in A$.

(a) Donner un exemple d'un tel anneau.
(b) Quels sont les éléments nilpotents d'un tel anneau ?
(c) Montrer que $6A = \{0_A\}$.
(d) Montrer que $2A$ et $3A$ sont des idéaux bilatères de A.
(e) Montrer que $2A$ et $3A$ sont étrangers et que $2A \cap 3A = \{0_A\}$.
(f) Soient X un anneau (pas nécessairement commutatif) et I, J deux idéaux bilatères de X avec $I + J = X$. Montrer que $X/(I_1 \cap I_2)$ est isomorphe à l'anneau $X/I_1 \times A/I_2$.
(g) Montrer que A est isomorphe à $A/2A \times A/3A$.
(h) Soit B un anneau avec $2B = \{0\}$ tel que $x^3 = x$ pour tout $x \in B$. Montrer que B est commutatif.
(i) Soit C un anneau avec $3B = \{0\}$ tel que $x^3 = x$ pour tout $x \in C$. Montrer que C est commutatif.
(j) Conclure que A est commutatif.

Solution.

(a) On vérifie que $\mathbb{Z}/6\mathbb{Z}$ satisfait la propriété de l'énoncé.
(b) Soit $a \in A$. Par récurrence, montrons pour chaque entier $k \geq 1$, $a^k \in \{a, a^2\}$. La propriété est acquise au rang 1. Fixons un entier $k \geq 1$ et supposons que $a^k \in \{a, a^2\}$. On a $a^{k+1} = a^k.a \in \{a^2, a^3\} = \{a, a^2\}$. La récurrence est terminée. Supposons maintenant que $a^r = 0_A$ pour un certain entier $r \geq 1$. Si $a^r = a$, alors $a = 0_A$ et si $a^r = a^2$, alors $0_A = a^2.a = a^3 = a$. On conclut que le seul élément nilpotent de A est 0_A.

(c) Il suffit d'écrire pour tout $a \in A$,

$$8a = 8a^3 = (a+a)^3 = a + a$$

pour aboutir à $6a = 0_A$.

(d) Le fait que $2A$ soit un idéal bilatère résulte des égalités valides pour tout $a, b \in A$,

$$b(2a) = 2(ba) \quad \text{et} \quad (2a)b = 2(ab).$$

De même, on montre que $3A$ est un idéal bilatère de A.

(e) Pour établir que $2A$ et $3A$ sont étrangers, il suffit d'écrire pour $a \in A$ que $a = -5a$ puis

$$a = (-2a) + (-3a) = 2(-a) + 3(-a) \in 2A + 3A.$$

Pour établir la seconde égalité, on procède comme suit : pour $a \in 2A \cap 3A$, il existe $b, c \in A$ tels que $a = 2b$ et $a = 3c$. Il vient $3a = 6b$ et $2a = 6c$ ce qui donne $a = 6b - 6c = 0_A$ où la dernière égalité résulte de $6A = \{0_A\}$.

(f) On introduit l'application $f : X/(I_1 \cap I_2) \to X/I_1 \times X/I_2$ définie par

$$f(x + I_1 \cap I_2) = (x + I_1, x + I_2) \quad \text{pour tout } x \in X.$$

On voit facilement que l'application f est un morphisme d'anneaux. Montrons qu'elle est bijective. Pour tout $x, y \in X$ avec $f(x + I_1 \cap I_2) = f(y + I_1 \cap I_2)$, on a

$$x - y \in I_1 \cap I_2$$

et ceci donne l'égalité $x + I_1 \cap I_2 = y + I_1 \cap I_2$. Ceci montre que l'application f est injective. Soient $x \in X/I_1$ et $y \in X/I_2$. Il existe $a, b \in X$ tels que $x = \pi_1(a)$ et $y = \pi_2(b)$ avec π_k la surjection canonique de X dans X/I_k pour $k \in \{1, 2\}$. Puisque $I_1 + I_2 = X$, il existe $i_1 \in I_1$ et $i_2 \in I_2$ tels que $1_X = i_1 + i_2$. On pose maintenant $c = ai_2 + bi_1$. On vérifie que

$$\pi_1(c) = \pi_1(ai_2) = \pi_1(a(1_A - i_1)) = \pi_1(a) = x$$

et

$$\pi_2(c) = \pi_2(bi_1) = \pi_2(b(1_A - i_2)) = \pi_2(b) = y.$$

L'application f est donc surjective.

(g) En combinant (e) et (f), on aboutit au fait que $A/\{0_A\}$ est isomorphe à $A/2A \times A/3A$. Puisque $A/\{0_A\}$ est isomorphe à A, on obtient l'isomorphisme souhaité.

(h) On a pour $b \in B$,

$$(b + 1_B) = (b + 1_B)^3 = b^3 + 3b^2 + 3b + 1_B = b^3 + b^2 + b + 1_B = b^2 + 2b + 1_B = b^2 + 1_B,$$

d'où $b^2 = b$. Soient $x, y \in B$. En remarquant que

$$x + y = (x + y)(x + y) = x^2 + xy + yx + y^2 = x + xy + yx + y$$

il vient $xy = -yx$. Il reste à exploiter le fait que $-yx = yx$ pour conclure que $xy = yx$.

(i) Fixons $a, b \in C$. Commençons par écrire

$$a + b = (a + b)^3 = a^3 + a^2b + aba + ab^2 + ba^2 + bab + b^2a + b^3$$

et

$$a - b = (a - b)^3 = a^3 - a^2b - aba + ab^2 - ba^2 + bab + b^2a - b^3.$$

Puisque $a + b = a^3 + b^3$ par hypothèse, la première égalité donne

$$a^2b + aba + ab^2 + ba^2 + bab + b^2a = 0_C.$$

De même, la deuxième égalité donne

$$-a^2b - aba + ab^2 - ba^2 + bab + b^2a = 0_C.$$

En additionnant les deux dernières égalités, on obtient

$$2ab^2 + 2bab + 2b^2a = 0_C.$$

En combinant ceci et l'égalité $3ab^2 + 3bab + 3b^2a = 0_C$, il s'ensuit

$$ab^2 + bab + b^2a = 0_C.$$

En multipliant à gauche (resp. à droite) par b on a

$$0_C = bab^2 + b^2ab + b^3a = bab^2 + b^2ab + ba$$

(resp.

$$0_C = ab^3 + bab^2 + b^2ab = ab + bab^2 + b^2ab.)$$

On conclut que $ab = ba$.

(j) L'anneau A est commutatif car il est isomorphe au produit de deux anneaux commutatifs à savoir $A/2A \times A/3A$.

■

Exercice 56

1. Existe t-il un anneau de caractéristique 20 ? un corps de caractéristique 20 ?
2. Existe t-il un anneau fini de caractéristique nulle ?
3. Peut-on trouver un corps K de caractéristique 11 et un sous-corps K' de caractéristique 0 ?

Solution.

1. L'anneau $\mathbb{Z}/20\mathbb{Z}$ est un anneau de caractéristique 20. Un corps étant un anneau intègre, sa caractéristique est soit nulle soit un nombre premier. Il n'existe donc pas de corps de caractéristique 20.
2. Supposons qu'il existe A un anneau fini de caractéristique nulle. L'injectivité du morphisme d'anneaux $\varphi_A : \mathbb{Z} \to A$ défini par

$$\varphi_A(k) = k1_A \quad \text{pour tout } k \in \mathbb{Z}$$

nous voyons que A contient une infinité d'éléments.

3. Non, K et K' ont même caractéristique.

■

Exercice 57 Soit A un anneau. A quel anneau A/A est-il isomorphe ? Même question pour $A/\{0_A\}$.

Solution. Une application directe du 1er théorème d'isomorphisme (au morphisme d'anneaux $\mathrm{Id}_A : A \to A$) nous dit que $A/\{0_A\}$ est isomorphe à A. Par ailleurs, l'ensemble quotient A/A est réduit à un élément, il est donc isomorphe à l'anneau nul. ■

Exercice 58 A quel anneau $\mathbb{Z}[X]/(X^2+1)$ est il isomorphe ?

Solution. C'est une application directe du 1er théorème d'isomorphisme avec le morphisme $\varphi : \mathbb{Z}[X] \to \mathbb{C}$ défini par

$$\varphi(P) = P(i) \quad \text{pour tout } P \in \mathbb{Z}[X].$$

On a évidemment $\operatorname{im}\varphi = \mathbb{Z}[i]$ et $\ker\varphi = (X^2+1)$. On conclut que l'anneau $\mathbb{Z}[i]$ est isomorphe à l'anneau $\mathbb{Z}[X]/(X^2+1)$. ■

Exercice 59 Soit I_1 (resp. I_2) un idéal bilatère d'un anneau A_1 (resp. A_2). On a vu dans un exercice précédent que $I_1 \times I_2$ est un idéal bilatère de $A_1 \times A_2$ muni de sa structure naturelle d'anneau produit. Montrer que l'anneau $(A_1 \times A_2)/(I_1 \times I_2)$ est isomorphe à $(A_1/I_1) \times (A_2/I_2)$.

Solution. Pour $i \in \{1, 2\}$, on note $\pi_i : A \to A_i/I_i$ la surjection canonique. On vérifie sans difficultés que l'application $f : A_1 \times A_2 \to (A_1/I_1) \times (A_2/I_2)$ définie par

$$f(a_1, a_2) = (\pi_1(a_1), \pi_2(a_2)) \quad \text{pour tout } (a_1, a_2) \in A_1 \times A_2$$

est un morphisme d'anneaux surjectif de noyau $I_1 \times I_2$. Il reste alors à appliquer le premier théorème d'isomorphisme d'anneaux pour conclure. ■

Exercice 60 Soient I un idéal d'un anneau $(A; +, \times)$. On **rappelle** que le *radical* d'un idéal I de A est l'idéal de A défini par

$$\sqrt{I} := \{x \in A : \exists n \geq 1, x^n \in I\}.$$

Montrer que $\sqrt{I} = I$ si et seulement si l'anneau quotient A/I n'a pas d'élément nilpotent non trivial (i.e., n'a pas d'élément nilpotent différent de $0_{A/I}$). En déduire les entiers $k \geq 2$ tels que $\mathbb{Z}/k\mathbb{Z}$ n'a pas d'élément nilpotent non trivial.

Exercice 61 Soit I un idéal d'un anneau A commutatif noethérien. Montrer que l'anneau quotient A/I est noethérien.

Solution. Soit J un idéal de A/I. Notons $\pi : A \to A/I$ la surjection canonique. Nous savons que $J = \pi(K)$ pour un idéal K de A contenant I. Puisque A est noethérien, il existe un entier $m \geq 1$ et $a_0, \ldots, a_m \in A$ tels que $K = (a_0, \ldots, a_m)$. Nous allons établir que $J = (\pi(a_0), \ldots, \pi(a_m))$. L'inclusion $\supset$ est évidente puisque $\pi(a_k) \in J$ pour tout $k \in \{0, \ldots, m\}$. Montrons l'inclusion $\subset$. Soit $y \in J$. Il existe $x \in K$ tel que $y = \pi(x)$. L'égalité $K = (a_0, \ldots, a_m)$ donne alors $b_0, \ldots, b_m \in A$ tels que $x = \sum_{k=0}^{m} b_k a_k$. Il s'ensuit $y = \sum_{k=0}^{m} \pi(b_k)\pi(a_k) \in (\pi(a_0), \ldots, \pi(a_m))$. On conclut que J est de type fini. ■

Exercice 62 Soient A un anneau commutatif noetherien, $f : A \to A$ un morphisme d'anneaux surjectif.

1. Montrer qu'il existe un entier $n_0 \geq 1$ tel que
$$\ker f^n = \ker f^{n_0} \quad \text{pour tout } n \geq n_0.$$
2. Montrer que $\ker f^{n_0} \cap \operatorname{im} f^{n_0} = \{0\}$.
3. En déduire que $\ker f^{n_0} = \{0\}$.
4. Conclure que f est un isomorphisme d'anneaux.

Solution.

1. La suite $(\ker f^n)_{n \geq 1}$ est une suite croissante d'idéaux de A. Le caractère noetherien de A permet alors de conclure que celle-ci stationne.
2. Soit $y \in \ker f^{n_0} \cap \operatorname{im} f^{n_0}$. Il existe $x \in A$ tel que $y = f^{n_0}(x)$. On a alors $f^{2n_0}(x) = f^{n_0}(y) = 0$. On en déduit $x \in \ker f^{2n_0} = \ker f^{n_0}$, i.e., $y = f^{n_0}(x) = 0$.
3. Puisque f est surjective, on a $\operatorname{im} f^{n_0} = A$. La question précédente nous dit alors que $\ker f^{n_0} = \{0\}$.
4. La question précédente permet de conclure que f est injective.

■

Exercice 63 Soient A un anneau commutatif noetherien et I un idéal de A. On suppose que A/I est isomorphe à A. Montrer que la projection canonique $\pi : A \to A/I$ est injective et conclure que $I = \{0\}$.

Solution. Commençons par rappeler que π est un morphisme d'anneaux surjectif. Soit $\varphi : A/I \to A$ un morphisme d'anneaux surjectif. L'application $f := \varphi \circ \pi : A \to A$ est un morphisme d'anneaux surjectif. Puisque A est noetherien, nous savons d'après l'exercice précédent que f est injective. Soient $x, y \in A/I$ tels que $\pi(x) = \pi(y)$. On a $f(x) = f(y)$ puis $x = y$. On en déduit que π est injective, i.e., $I = \ker \pi = \{0\}$. ■

Exercice 64 Un anneau noethérien peut-il être isomorphe à un anneau non noethérien ?

Exercice 65 Montrer que $\mathbb{Z}[i\sqrt{5}]$ est noethérien.

Exercice 66 Quels sont les idéaux de $\mathbb{Z}/n\mathbb{Z}$ avec $n \geq 2$ entier ?

Solution. Soit $n \geq 2$ entier. Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $\Pi(m\mathbb{Z})$ avec $m \geq 1$ et $m\mathbb{Z} \supset n\mathbb{Z}$ (i.e., $m \mid n$), où Π désigne la projection canonique de Z sur $\mathbb{Z}/n\mathbb{Z}$. ■

Exercice 67 Soient $n \geq 2$ un entier, $A = M_n(\mathbb{Z})$ l'anneau des matrices carrées de taille n à coefficients dans $\mathbb{Z}$. On note I l'ensemble des éléments de $M_n(\mathbb{Z})$ à coefficients pairs. Montrer que I est un idéal bilatère de A et que l'anneau quotient A/I est isomorphe à un anneau de matrices à déterminer.

Solution. La vérification du fait que I est un idéal bilatère est immédiate. Pour obtenir l'isomorphisme d'anneaux souhaité, il suffit d'introduire l'application $\varphi : M_n(\mathbb{Z}) \to M_n(\mathbb{Z}/2\mathbb{Z})$ qui à une matrice $M \in M_n(\mathbb{Z})$ fait correspondre la matrice $\varphi(M)$ dont les coefficients sont les classes modulo 2 des coefficients de M. Il est clair que φ est un morphisme d'anneaux surjectif et de noyau $\ker(\varphi) = I$. Ainsi, l'anneau quotient A/I est isomorphe (en tant qu'anneau) à $M_n(\mathbb{Z}/2\mathbb{Z})$. ■

Exercice 68 Soient M_1, M_2 deux idéaux maximaux distincts d'un anneau A. Montrer l'égalité $M_1 + M_2 = A$.

Solution. Supposons $M_1 + M_2 \neq A$. On a $M_1 \subset M_1 + M_2$ ce qui entraîne $M_1 = M_1 + M_2$. Il vient $M_2 \subset M_1$ puis (car $M_1 \neq M_2$) $M_1 = A$. Ceci est contradictoire et nous permet de conclure que $M_1 + M_2 = A$. ■

Exercice 69 Soient (E, d) un espace métrique compact et $A = C(E, \mathbb{R})$ l'ensemble des fonctions continues de E dans $\mathbb{R}$. On munit l'anneau A de la norme $\|\cdot\|_\infty : A \to \mathbb{R}$ définie par

$$\|f\|_\infty := \sup_{x \in E} |f(x)| \quad \text{pour tout } f \in A.$$

Déterminer $A^\times$ et montrer que tout idéal maximal de A est fermé dans A relativement à $\|\cdot\|_\infty$.

Solution. L'ensemble $A^\times$ n'est nul autre que l'ensemble des éléments de A qui ne s'annulent pas sur E, i.e.,

$$A^\times = \{f \in A : \forall x \in E, f(x) \neq 0\}.$$

Soit M un idéal maximal de A. On vérifie sans peine que l'adhérence $\overline{M}$ de M dans $(A, \|\cdot\|_\infty)$ est un idéal de A. Puisque $M \subset \overline{M}$, on a $\overline{M} = M$ ou $\overline{M} = A$. Supposons que $\overline{M} = A$. Notons $\mathbf{1}$ la fonction de E dans $\mathbb{R}$ constante de valeur 1. Puisque $\mathbf{1} \in \overline{M}$, on peut trouver $f \in M$ telle que $\|f - \mathbf{1}\|_\infty < 1$. Cette dernière inégalité entraîne tout de suite que f ne s'annule pas sur E, i.e., $f \in A^\times$. On en déduit $M = A$ et ceci est contradictoire. On conclut que $\overline{M} = M$, i.e., M est fermé dans $(A, \|\cdot\|_\infty)$. ■

Exercice 70 Soit A un anneau commutatif non réduit à zéro qui n'est pas un corps. Montrer que les assertions suivantes sont équivalentes :
(a) La somme de deux non-inversibles de A est non-inversible.
(b) Les non-inversibles de A forment un idéal de A distinct de A.
(c) L'anneau A possède un idéal maximal unique.

Solution. On pose $B := A \setminus A^\times$.
$(a) \Rightarrow (b)$, Supposons que la somme de deux non-inversibles de A soit non-inversible. De cette hypothèse, il n'est pas difficile de voir que $(B;+)$ est un sous-groupe de $(A;+)$. Par ailleurs, pour $b \in B$ et $a \in A$ on a évidemment $ab \in B$ (si $ab \notin B$, alors il existe $c \in A$ tel que $abc = 1_A$ et ceci entraîne que $b \in A^\times$). On conclut que B est un idéal de A.

$(b) \Rightarrow (c)$, Supposons que B soit un idéal de A distinct de A. Nous allons montrer que B est maximal. Soit I un idéal de A avec $B \subset I$ et $B \neq I$. Choisissons $i \in I \setminus B$. On a $i \in A^\times$ et ceci nous dit que $I = A$. Nous allons voir que A n'admet que B pour idéal maximal. Soit K un idéal maximal de A. On a $K \neq A$ de sorte que K ne contient que des éléments non-inversibles de A. Il s'ensuit $K \subset B$ puis (par maximalité de B) $K = B$.

$(c) \Rightarrow (a)$, Supposons que A possède un unique idéal maximal noté I. Soit $b \in B$. D'après le théorème de Krull, il existe un idéal maximal K_b tel que $(b) \subset K_b$. Notre hypothèse nous dit alors que $K_b = I$. On en déduit que I contient tous les éléments non-inversibles de A, i.e., $B \subset I$. Puisque I est maximal, on a $A \neq I$ et ceci nous dit que I ne contient aucun élément inversible. On en déduit $I = B$. ■

Exercice 71
1. Soit $f : A \to B$ un morphisme d'anneaux surjectif entre deux anneaux A et B. Montrer que si J est un idéal maximal de B, alors $f^{-1}(B)$ est un idéal maximal de A.
2. On considère l'injection canonique f de $A := \mathbb{Z}[X]$ dans $B := \mathbb{R}[X]$. Montrer que l'idéal $J := X\mathbb{R}[X]$ est maximal. Que pensez-vous de l'idéal $f^{-1}(J)$?

Solution.

1. On note $\pi_B : B \to B/J$ la surjection canonique. On applique alors le premier théorème d'isomorphisme au morphisme $\varphi : \pi_B \circ f : A \to B/J$ pour obtenir que $\operatorname{im}\varphi$ est isomorphe à $A/\ker(\varphi)$. Il reste à voir que $\operatorname{im}\varphi = B/J$ et $\ker(\varphi) = f^{-1}(J)$ pour conclure que $A/f^{-1}(J)$ est un corps, i.e., $f^{-1}(J)$ est maximal.
2. Soit I un idéal de $\mathbb{R}[X]$ contenant J avec $I \neq J$. Soit $P \in I \setminus J$. La division euclidienne de P par X nous permet d'écrire $P = QX + R$ pour $Q, R \in \mathbb{R}[X]$ avec R de degré strictement inférieur à 1. Il s'ensuit $R = P - QX \in I$. Si $R = 0$, alors $P \in I$ et c'est contradictoire, de sorte que $R \neq 0$. Ainsi, R est un polynôme constant non nul de $\mathbb{R}[X]$, en particulier inversible dans $R[X]$. On conclut que $I = \mathbb{R}[X]$.
   Par définition de f et J, on a $f^{-1}(J) = \{P \in \mathbb{Z}[X] : \exists Q \in \mathbb{R}[X], P = XQ\}$. On vérifie alors aisément que
   $$f^{-1}(J) = \{P \in \mathbb{Z}[X] : \exists Q \in \mathbb{Z}[X], P = XQ\} = X\mathbb{Z}[X]$$
   et cet idéal n'est éviemment pas maximal car l'idéal $(2, X)$ de $\mathbb{Z}$ contient $f^{-1}(J)$ mais n'est pas $\mathbb{Z}$ tout entier (il ne contient pas le polynôme constant égal à 3).

■

Exercice 72 Soit $A = \mathcal{C}([0,1];\mathbb{R})$ l'anneau des fonctions continues de $[0,1]$ dans $\mathbb{R}$ muni de sa structure naturelle d'anneau.

1. Soit $x \in [0,1]$. Montrer que $I_x = \{f \in A : f(x) = 0\}$ est un idéal maximal de A.
2. Tous les idéaux de A sont-ils maximaux ? premiers ?
3. Montrer que I_x n'est pas un idéal principal.

Solution.

1. Il suffit d'introduire le morphisme d'évaluation $\varphi_x : A \to \mathbb{R}$

$$\varphi_x(f) = f(x) \quad \text{pour tout } f \in A$$

et d'appliquer le 1er théorème d'isomorphisme pour obtenir $A/I_x \simeq \mathbb{R}$.

2. Soit $J = \{f \in A : f(1/2) = f(1/3) = 0\}$ qui est évidemment un idéal de A. Introduisons les fonctions $h_{1/2}, h_{1/3} : [0,1] \to \mathbb{R}$ définies par

$$h_{1/2}(x) = x - 1/2 \quad \text{et} \quad h_{1/3}(x) = x - 1/3 \quad \text{pour tout } x \in \mathbb{R}.$$

Il reste à observer que $h_{1/2}h_{1/3} \in J$ mais que $h_{1/2}, h_{1/3} \notin J$. Ceci montre que J n'est pas un idéal premier.

3. Sans perte de généralités, montrons que I_0 n'est pas un idéal principal. Par l'absurde, considérons $g \in A$ tel que $I_0 = (g)$. Puisque $\sqrt{|g|} \in I_0$, on peut écrire $\sqrt{|g|} = fg$ pour un certain $f \in A$. Il s'ensuit $g = f^2g^2$ puisque $g(1 - f^2g) = 0_A$. D'autre part, la continuité de $1 - f^2g$ nous dit que $\lim\limits_{u \downarrow 0}(1 - f^2g)(u) = 1$. Ceci entraîne qu'il existe un réel $\varepsilon > 0$ tel que g soit nulle sur $[0, \varepsilon[$. Il reste à voir que $\mathrm{Id}_{\mathbb{R}} \in I_0$ et doit donc s'annuler en chaque point de $[0, \varepsilon[$ ce qui est contradictoire.

■

Exercice 73 Soit I un idéal d'un anneau commutatif A. Déterminer les idéaux maximaux de A/I.

Solution. On note $\mathcal{M}$ l'ensemble des idéaux maximaux de A et $\pi : A \to A/I$ la surjection canonique. Nous allons établir que l'ensemble des idéaux maximaux de A/I n'est nul autre que l'ensemble

$$\{\pi(J) : J \in \mathcal{M}, J \supset I\}.$$

Méthode 1. Soit $\mathcal{I}$ un idéal maximal de A/I. La description des idéaux d'un anneau quotient nous permet d'écrire $\mathcal{I} = \pi(J)$ pour un certain idéal J de A contenant I. Remarquons tout de suite que $J \neq A$ (sinon $\mathcal{I} = A/I$ et ceci contredit la maximalité de $\mathcal{I}$). Soit K un idéal de A contenant J avec $J \neq K$. On a évidemment $\pi(J) \subset \pi(K)$ ce qui entraîne (par maximalité de $\mathcal{I} = \pi(J)$) $\pi(K) = \pi(J)$ ou $\pi(K) = A/I$. Nous allons voir que la première égalité n'a pas lieu, i.e., $\pi(K) \neq \pi(J)$. Soit $k \in K$ avec $k \notin J$. Si $\pi(K) = \pi(J)$, alors $\pi(k) = \pi(j)$ pour un certain $j \in J$ puis $k \in j + I \subset J + J \subset J$ et ceci est contradictoire. On a donc l'égalité $\pi(K) = A/I$. Montrons que $A = K$. Il n'y a bien sûr qu'une seule inclusion à établir. Soit $a \in A$. On a $\pi(a) = \pi(l)$ pour un certain $l \in K$ puis $a \in l + I \subset K + K \subset K$. On conclut que J est un idéal maximal de A, i.e., $J \in \mathcal{M}$.

Soit $J \in \mathcal{M}$ avec $J \supset I$. L'ensemble $\pi(J)$ est un idéal de $\operatorname{im}\pi = A/I$. On a $\pi(J) \neq A/I$ (sinon, $1_{A/I} \in \pi(J)$ puis $1_A \in J + I \subset J$). Soit $\mathcal{K}$ un idéal de A/I contenant $\pi(J)$ avec $\mathcal{K} \neq \pi(J)$. La description des idéaux d'un anneau quotient nous dit que $\mathcal{K} = \pi(K)$ pour un certain idéal K de A contenant I. On a évidemment l'inclusion $\pi^{-1}(\pi(J)) \subset \pi^{-1}(\pi(K))$. En combinant cette inclusion et l'inclusion $I \subset J$ on obtient facilement $J \subset K$. La maximalité de J nous dit alors que $K = J$ ou $K = A$. Si $K = J$, alors $\pi(K) = \pi(J)$ et ceci est contradictoire. On a donc $K = A$ puis $\mathcal{K} = \pi(K) = A/I$. On conclut que $\pi(J)$ est un idéal maximal de A.

Méthode 2. Soit $\mathcal{I}$ un idéal maximal de A/I. Il existe J un idéal de A contenant I tel que $\pi(J) = \mathcal{I}$. Par le troisième théorème d'isomorphisme, les anneaux $(A/I)/\pi(J)$ et A/J sont isomorphes. Ceci et la maximalité de $\pi(J)$ entraînent alors que A/J est un corps. Il reste à voir que $J \neq A$ (car $\pi(J) \neq A/I$) pour conclure que J est maximal.

Soit $J \in \mathcal{M}$ avec $A \neq J \supset I$. L'ensemble $\pi(J)$ est un idéal de $\operatorname{im}\pi = A/I$. Par le troisième théorème d'isomorphisme, les anneaux $(A/I)/\pi(J)$ et A/J sont isomorphes. Ceci et la maximalité de J nous disent alors que $(A/I)/\pi(J)$ est un corps. Il reste à écrire que $\pi(J) \neq A/I$ (si $\pi(J) = A/I = \pi(A)$, alors en choisissant $a \in A \setminus J$ on aurait $\pi(a) = \pi(j)$ pour un certain $j \in J$ puis $a \in j + I \subset J$ ce qui est absurde) pour conclure que $\pi(J)$ est un idéal maximal de A/I. ■

Exercice 74 Soit I un idéal d'un anneau commutatif A. Déterminer les idéaux premiers de A/I.

Solution. On note $\mathcal{P}$ l'ensemble des idéaux premiers de A et $\pi : A \to A/I$ la surjection canonique. La description des idéaux d'un anneau quotient permet d'établir de manière analogue à la Méthode 1 ou à la Méthode 2 de l'exercice précédent que l'ensemble des idéaux premiers de A/I n'est nul autre que l'ensemble

$$\{\pi(J) : J \in \mathcal{P}, J \supset I\}.$$

■

Exercice 75 (Idéal de Jacobson) Soit $(A; +, \times)$ un anneau commutatif non nul. On définit l'ensemble (qui est évidemment un idéal de A)

$$\operatorname{Jac}(A) = \bigcap_{I \in \mathcal{M}(A)} I,$$

où $\mathcal{M}(A)$ désigne l'ensemble des idéaux maximaux de A (qui est un ensemble non vide d'après le théorème de Krull). Montrer que

$$\operatorname{Jac}(A) = \left\{x \in A : \forall y \in A, 1 + xy \in A^\times\right\}.$$

Solution. Soit $m \in \operatorname{Jac}(A)$ et $y \in A$ fixés. Considérons l'idéal $(1 + my)$ de A. Si $(1 + my) \neq A$, il existe (d'après le théorème de Krull) un idéal maximal M de A le contenant, i.e.,

$$(1 + my) \subset M.$$

Puisque $m \in \operatorname{Jac}(A)$, on a $m \in M$. Ceci et l'inclusion ci-dessus nous donnent alors $1 \in M$. En conséquence, on a $M = A$ ce qui est contradictoire. Finalement, on a $(1+my) = A$, d'où l'inversibilité de $1 + my$ dans A.

Soit $x \in A$ tel que pour tout $y \in A$, $1 + xy \in A^\times$. Supposons que $x \notin \operatorname{Jac}(A)$. Il existe donc un idéal maximal M de A tel que $x \notin M$. En particulier, l'idéal $I := xA + M$ n'est nul autre que A tout entier. Ceci nous permet d'écrire $1_A = xa + m$ pour un certain $a \in A$ et $m \in M$. Il vient alors $m = 1 + x(-a) \in A^\times$ puis $M = A$ ce qui est absurde. ■

Exercice 76 Soit $(A; +, \times)$ un anneau tel que

$$a^2 = a \quad \text{pour tout } a \in A.$$

Justifier que $a = -a$ pour tout $a \in A$. En déduire que $(A; +, \times)$ est commutatif. Montrer que l'anneau est un corps lorsqu'il est de plus supposé intègre. Montrer que tout idéal premier de A est maximal.

Solution. Fixons $a \in A$. Il suffit d'écrire

$$(a + a)^2 = (a + a)(a + a) = a + a = a + a + a + a$$

pour obtenir la relation voulue, i.e., $a = -a$. Soient $x, y \in A$. En remarquant que

$$x + y = (x + y)(x + y) = x^2 + xy + yx + y^2 = x + xy + yx + y$$

il vient $xy = -yx$. Il reste à exploiter le fait que $-yx = yx$ pour conclure que $xy = yx$. Si $(A; +, \times)$ est intègre, alors A n'est pas l'anneau nul et la relation

$$a(a - 1_A) = 0_A$$

valide pour chaque $a \in A$, entraîne que A est réduit à deux éléments : 0_A et 1_A. Il est immédiat que $(A; +, \times)$ est alors un corps (isomorphe à $\mathbb{Z}/2\mathbb{Z}$). Soit I un idéal premier de A et $J \supset I$ un idéal avec $J \neq I$. Fixons $x \in J \setminus I$. On a tout de suite $\pi(x) \neq 0_{A/I}$ où π est la projection canonique de A sur A/I. D'autre part, on a

$$\pi(x)(\pi(x) - 1_{A/I}) = 0_{A/I}.$$

Par intégrité de A/I (puisque I est premier), on a

$$\pi(x) = 1_{A/I}.$$

On peut donc écrire $x - i = 1_A$ pour un certain $i \in I$. Ceci nous dit que $1_A \in J$ et donc $J = A$. En conséquence, l'idéal I est maximal. ■

Exercice 77 Soit $(A; +, \times)$ un anneau commutatif fini non nul. Montrer que tout idéal premier de A est maximal.

Solution. Soit I un idéal premier de A. Nous savons que l'anneau quotient A/I est intègre et fini, donc c'est un corps (voir l'un des exercices ci-dessus). Ceci nous dit que I est un idéal maximal de A. ■

Exercice 78 Montrer que 2 n'est pas premier dans $\mathbb{Z}[i]$.

Solution. On a tout de suite $2 = (1 - i)(1 + i)$ et (à l'aide de $N := |\cdot|^2$) on a $2 \not| 1 - i$ et $2 \not| 1 + i$. Ceci montre que 2 n'est pas premier dans $\mathbb{Z}[i]$. ■

Exercice 79 Vérifier que 89 est un nombre premier de $\mathbb{Z}$. L'idéal (89) est-il premier dans $\mathbb{Z}[i]$? On pourra écrire 89 comme somme de deux carrés d'entiers.

Solution. On vérifie que 89 est un nombre premier. Par ailleurs, $89 = 5^2 + 8^2$ et ceci donne

$$89 = (5 + 8i)(5 - 8i).$$

Puisque $5+8i$ et son conjugué ne sont pas inversibles dans $\mathbb{Z}[i]$, on obtient que 89 n'est pas irréductible dans $\mathbb{Z}[i]$. Ainsi, 89 n'est pas premier dans $\mathbb{Z}[i]$ et donc l'idéal (89) de $\mathbb{Z}[i]$ n'est pas premier. ■

Exercice 80 (Irréductible n'entraîne pas premier) Montrer que $1 + i\sqrt{5}$ est irréductible dans $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} : a, b \in \mathbb{Z}\}$. Est-il premier dans ce même anneau ?

Solution. On observe facilement que

$$z := (1 - i\sqrt{5})(1 + i\sqrt{5}) = 2 \times 3,$$

en particulier $2 \mid z$. Puisque $2 \not| (1 + i\sqrt{5})$ et $2 \not| (1 - i\sqrt{5})$, on conclut que 2 n'est pas premier dans A.

Pour obtenir l'irréductibilité, on introduit l'application $N : A \to \mathbb{N}$ définie par

$$N(a + i\sqrt{5}b) := a^2 + 5b^2 \quad \text{pour tout } a, b \in \mathbb{Z}.$$

On vérifie que N est multiplicative, i.e., $N(zz') = N(z)N(z')$ pour tout $z, z' \in A$. Il découle de ceci que $A^\times = \{-1, 1\}$ et donc 2 n'est pas inversible dans A. Il reste à voir que si $2 = xy$ pour un certain couple $(x, y) \in A^2$, on a $4 = N(2) = N(xy) = N(x)N(y)$ et nécessairement $N(x) = 1$ ou $N(y) = 1$. On conclut que 2 est irréductible dans A. ■

Exercice 81 Montrer que $\mathbb{Z}[i]$ est euclidien.

Solution. Notons $A := \mathbb{Z}[i]$. On introduit $\nu : A \setminus \{0\} \to \mathbb{N}$ définie par

$$\nu(z) = |z|^2 \quad \text{pour tout } z \in A \setminus \{0\}.$$

Soient $z_1 \in A$ et $z_2 \in A \setminus \{0\}$. Il existe $a, b \in \mathbb{Q}$ tels que

$$\frac{z_1}{z_2} = a + ib.$$

Soient $x, y \in \mathbb{Z}$ tels que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$. En posant $q := x + iy$ et $r := z_1 - qz_2$, il vient

$$\left|\frac{z_1}{z_2} - q\right| = \sqrt{(a-x)^2 + (b-y)^2} \leq \frac{1}{\sqrt{2}} < 1$$

et

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

Ceci montre que $\mathbb{Z}[i]$ est euclidien. ■

Exercice 82 Montrer que $\mathbb{Z}[i]/(1+3i)$ est isomorphe (en tant qu'anneaux) à $\mathbb{Z}/10\mathbb{Z}$. Retrouver ainsi que $1 + 3i$ n'est pas irréductible dans $\mathbb{Z}[i]$.

Solution. On considère l'application $\varphi : \mathbb{Z}[i] \to \mathbb{Z}/10\mathbb{Z}$ définie par

$$\varphi(a + ib) := \overline{a} + 3\overline{b} \quad \text{pour tout } a, b \in \mathbb{Z}.$$

On vérifie que φ est un morphisme d'anneaux. Puisque $\mathbb{Z}[i]$ est euclidien, l'idéal $\ker \varphi$ est principal. Ceci et l'inclusion $1 + 3i \in \ker \varphi$ nous disent que $(1 + 3i) = \ker \varphi$. Par ailleurs, on a bien sûr $\operatorname{im} \varphi = \mathbb{Z}/10\mathbb{Z}$. Il reste à appliquer le 1er théorème d'isomorphisme pour conclure quant à l'isomorphisme souhaité. Bien sûr, $\mathbb{Z}/10\mathbb{Z}$ n'étant pas un corps, l'idéal $(1 + 3i)$ n'est pas maximal et donc $1 + 3i$ n'est pas irréductible dans $\mathbb{Z}[i]$ (ce que l'on savait déjà via l'égalité $1 + 3i = (2 + i)(1 + i)$). ■

Exercice 83 Montrer que $\mathbb{Z}[j]$ est euclidien.

Solution. Soient $z_1 \in \mathbb{Z}[j]$ et $z_2 \in \mathbb{Z}[j] \setminus \{0\}$. Soient $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ tels que $z_k = a_k + jb_k$ pour $k \in \{1, 2\}$. On a

$$\frac{z_1}{z_2} = \frac{(a_1 + jb_1)(a_2 + \overline{j}b_2)}{|z_2|^2} = \frac{a_1a_2 + b_1b_2 + a_1b_2\overline{j} + b_1a_2j}{|z_2|^2}.$$

Ceci, l'inclusion $|z_2|^2 \in \mathbb{N}$ et l'égalité $\overline{j} = j^2 = -1 - j$ entraînent facilement l'existence de $u, v \in \mathbb{Q}$ tels que

$$\frac{z_1}{z_2} = u + jv.$$

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ tels que $|u - a| \leq \frac{1}{2}$ et $|v - b| \leq \frac{1}{2}$. On a tout de suite

$$|(u-a) + j(v-b)|^2 = (u-a)^2 + (v-b)^2 - (u-a)(v-b) \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4}.$$

Posons alors $q := a + jb \in \mathbb{Z}[j]$ puis $r := z_1 - z_2q$. On considère la fonction $\nu : \mathbb{Z}[j] \setminus \{0\} \to \mathbb{N}$ définie par

$$\nu(z) = |z|^2 \quad \text{pour tout } z \in \mathbb{Z}[j] \setminus \{0\}.$$

On a bien sûr

$$z_1 - z_2q = z_2(u + jv) - z_2q = z_2\big((u-a) + j(v-b)\big),$$

d'où l'on tire

$$|r|^2 = \nu(z_1 - z_2q) = |z_2|^2|(u-a) + j(v-b)|^2 = \frac{3}{4}\nu(z_2) < \nu(z_2).$$

On conclut que $\mathbb{Z}[j]$ est euclidien. ■

Exercice 84 Montrer que tout corps commutatif est euclidien.

Solution. Soit K un corps commutatif (qui évidemment un anneau commutatif intègre). Soient $a \in K$ et $b \in K^\star$. On a bien sûr $a = b(b^{-1}a) + 0_K$ et ceci montre que n'importe quelle application de $K^\star$ dans $\mathbb{N}$ est un stathme sur K. ■

Exercice 85 (Idéaux premiers d'un anneau euclidien) Soient A un anneau euclidien et I un idéal premier non nul de A.

1. Justifie que $I = (p)$ pour $p \in A$ non nul et non inversible.
2. Montrer que p est premier.
3. Montrer que I est maximal.
4. Conclure que A/I est euclidien.

Solution.

1. L'anneau A est principal, donc il existe $p \in A$ tel que $I = (p)$. Puisque $I \neq A$ et $I \neq \{0\}$, l'élément p n'est ni inversible dans A, ni nul.
2. L'élément p est premier car l'idéal $(p) = I$ est premier.
3. Puisque p est premier et non nul, il est irréductible dans A. Le fait que A soit principal nous dit alors que $(p) = I$ est maximal.
4. L'anneau quotient A/I est un corps puisque I est maximal : en particulier, A/I est euclidien.

■

Exercice 86 Soit A un anneau euclidien de sthame associé ν. Pour tout idéal I de A, on note π_I la surjection canonique de A dans A/I. **L'objectif de l'exercice** est d'établir l'existence de $x \in A \setminus A^\times$ tel que l'application $J : A^\times \cup \{0_A\} \to A/(x)$ définie par

$$J(a) = \pi_{(x)}(a) \quad \text{pour tout } a \in A^\times \cup \{0_A\}$$

soit surjective.

1. On suppose ici que $A = A^\times \cup \{0_A\}$. Montrer que $x = 0_A$ convient.
2. On suppose maintenant que $A \setminus (A^\times \cup \{0_A\}) \neq \emptyset$. Justifier que l'ensemble

   $$\left\{\nu(a) : a \in A \setminus (A^\times \cup \{0_A\})\right\}$$

   admet un plus petit élément que l'on notera m.
3. Soit $x \in A \setminus (A^\times \cup \{0_A\})$ tel que $\nu(x) = m$. Soit $y \in A/(x)$.
   (i) Justifier qu'il existe $a \in A$ tel que $\overline{a} = y$.
   (ii) En utilisant le fait que A est euclidien, montrer qu'il existe $r \in A^\times \cup \{0_A\}$ tel que $\overline{a} = \overline{r}$.
   (iii) Conclure.

Solution.

1. Si A est un corps, on a $A^\times \cup \{0_A\} = A$ et il suffit alors de considérer la surjection canonique $\pi : A \to A/(0_A)$ de A dans $A/(0_A)$.
2. Supposons $A \setminus (A^\times \cup \{0_A\}) \neq \emptyset$. L'ensemble

   $$\left\{\nu(a) : a \in A \setminus (A^\times \cup \{0_A\})\right\}$$

   est une partie non vide de $\mathbb{N}$. Elle admet donc un plus petit élément noté m, i.e.,

   $$m := \min\left\{\nu(a) : a \in A \setminus (A^\times \cup \{0_A\})\right\}.$$

(i) C'est une conséquence directe de la surjectivité de la projection canonique de A dans le quotient $A/(x)$.

(ii) Le caractère euclidien de A et le fait que $x \neq 0_A$ nous donnent $q, r \in A$ avec $r = 0_A$ ou $\nu(r) < \nu(x)$. On a $a = xq + r$ puis $\overline{a} = \overline{xq} + \overline{r} = \overline{r}$. Si $r = 0_A$, l'égalité voulue a lieu. Si $r \neq 0_A$, alors on a $\nu(r) < \nu(x)$ et ceci entraîne (compte-tenu de la définition de m) que $r \in A^\times$.

(iii) On a ainsi justifié que l'application $J : A^\times \cup \{0_A\} \to A/(x)$ définie par

$$J(a) = \pi_{(x)}(a) \quad \text{pour tout } a \in A^\times \cup \{0_A\}$$

est surjective.

■

Exercice 87 L'objectif de l'exercice est d'établir que pour $\alpha = \frac{1+i\sqrt{19}}{2}$ l'anneau $\mathbb{Z}[\alpha] := \{a + b\alpha : a, b \in \mathbb{Z}\}$ n'est pas euclidien. Nous allons procéder par l'absurde en supposant que $A := \mathbb{Z}[\alpha]$ soit euclidien. Pour tout idéal I de A, on note π_I la surjection canonique de A dans A/I. D'après l'exercice précédent, nous savons qu'il existe $x \in A \setminus A^\times$ tel que l'application $J : A^\times \cup \{0_A\} \to A/(x)$ définie par

$$J(a) = \pi_{(x)}(a) \quad \text{pour tout } a \in A^\times \cup \{0_A\}$$

est surjective.

1. Montrer qu'un anneau B qui contient 2 éléments est de caractéristique 2. En déduire par le 1er théorème d'isomorphisme que B est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Même question en remplaçant 2 par 3.
2. Montrer que dans $A/(x)$, on a $\overline{0_A} \neq \overline{1_A}$ et que tout élément non nul de $A/(x)$ est inversible, i.e., $A/(x)$ est un corps.
3. Montrer que $A/(x)$ à 2 ou 3 éléments.
4. En déduire qu'il existe un morphisme d'anneaux φ de A dans $\mathbb{Z}/p\mathbb{Z}$ pour un entier $p \in \{2, 3\}$.
5. Soit $p \in \{2, 3\}$. On note $\overline{k}$ la classe d'un entier $k \in \{0, 1, \ldots, p\}$. Montrer que $X^2 - \overline{1}X + 5.\overline{1}$ n'a pas de racines de dans $\mathbb{Z}/p\mathbb{Z}$.
6. Observer que α est racine de $X^2 - X + 5$. Conclure à une contradiction à l'aide de $\varphi(\alpha)$.

Solution.

1. Soit B un anneau qui contient deux éléments. L'anneau B est nécessairement de caractéristique 2 et donc (par le 1er théorème d'isomorphisme) isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Soit C un anneau à trois éléments. L'anneau C contient le neutre additif 0_C, le neutre multiplicatif 1_C et son symétrique pour la loi $+$, à savoir -1_C. Ce dernier élément est distinct de 0_C et 1_C. L'anneau C est de caractéristique 3 et donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$.
2. Si $\overline{0_A} = \overline{1_A}$, on a $1_A \in (x)$ et ceci entraîne que $x \in A^\times$. L'anneau $A/(x)$ contient donc au moins deux éléments. Soit $u \in A/(x)$ avec $u \neq \overline{0_A}$. Il existe $a \in A^\times \cup \{0_A\}$ tel que $\overline{a} = u$. Si $a = 0_A$, alors $u = \overline{0_A}$ et c'est contradictoire. On a donc $a \neq 0_A$ et ceci nous dit que a est inversible. Il s'ensuit $u\overline{a^{-1}} = \overline{1_A}$ ce qui traduit l'inversibilité de u. On conclut que $A/(x)$ est un corps.
3. La surjectivité de J et le fait que $A^\times = \{-1, 1\}$ entraînent que $A/(x)$ a 2 ou 3 éléments.
4. Ceci découle du fait que $A/(x)$ est un corps à 2 ou à 3 éléments et donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$ ou à $\mathbb{Z}/3\mathbb{Z}$.
5. Il s'agit de vérifications immédiates.
6. On pose $\beta = \varphi(\alpha)$. On a $\alpha^2 - \alpha + 5 = 0$, d'où $\varphi(\alpha^2 - \alpha + 5) = \beta^2 - \overline{1}\beta + 5.\overline{1}$. Ainsi, $X^2 - \overline{1}X + 5.\overline{1}$ a une racine dans $\mathbb{Z}/p\mathbb{Z}$ pour un entier $p \in \{2, 3\}$.

■

Exercice 88 (L'existence d'un p.g.c.d. n'entraîne pas celle d'un p.p.c.m.) Soit $A = \mathbb{Z}[i\sqrt{5}] := \{a + ib\sqrt{5} : a, b \in \mathbb{Z}\}$.

(a) Montrer que $A^\times = \{-1, 1\}$.
(b) Montrer que les seuls diviseurs commun à $a := 2$ et à $b := 1 + i\sqrt{5}$ sont les inversibles de A. En déduire que 1 est un diviseur commun à a et à b.
(c) Par l'absurde, supposons qu'il existe un p.p.c.m. m de a et b. Justifier que m et $2(1 + i\sqrt{5})$ sont associés. Montrer que $m \mid 6$, $b \mid 3$. Conclure à une contradiction.

Solution.
(a) On définit l'application $N : A \to \mathbb{N}$ par

$$N(x + iy\sqrt{5}) = x^2 + 5y^2 \quad \text{pour tout } a, b \in \mathbb{Z}.$$

On vérifie sans difficultés que N est multiplicative. A l'aide de cette application, on montre que $A^\times = \{-1, 1\}$.
(b) L'application N permet d'établir sans difficultés que les seuls diviseurs communs à $a := 2$ et à $b := 1 + i\sqrt{5}$ sont les inversibles. Ainsi, $d := 1$ est un p.g.c.d. de a et de b.
(c) Supposons que a et b admettent un p.p.c.m. noté m. Le cours nous dit alors que $m1 = m \sim ab = 2(1 + i\sqrt{5})$. Par ailleurs, 6 est un multiple commun de a et b puisque

$$(1 - i\sqrt{5})(1 + i\sqrt{5}) = 6 = 3 \times 2.$$

On en déduit que $m \mid 6$ puis $b = 1 + i\sqrt{5} \mid 3$. Il existe alors $z \in A$ tel que $bz = 3$. Ceci entraîne $N(b)N(z) = N(3) = 9$, i.e., $6N(z) = 9$. Ceci étant absurde, on conclut que a et b n'ont pas de p.p.c.m.

■

Exercice 89 Soient A un anneau commutatif intègre, $a, b \in A \setminus \{0_A\}$. On suppose que a et b ont un p.g.c.d. noté $d \in A$, i.e. $d \in \text{P.G.C.D.}(a, b) \neq \emptyset$.

1. On suppose que $b \mid a$. Montrer que $\text{P.G.C.D.}(a, b) = bA^\times$.
2. On suppose qu'il existe $q \in A$ et $r \in A \setminus \{0_A\}$ tels que $a = bq + r$. Montrer que $\text{P.G.C.D.}(a, b) = \text{P.G.C.D}(b, r)$.
3. Etendre l'algorithme d'Euclide au cadre des anneaux euclidiens.

Exercice 90 Déterminer l'ensemble des P.G.C.D. de $5 + 14i$ et $5 + i$ dans l'anneau $\mathbb{Z}[i]$.

Solution. On écrit

$$\frac{5 + 14i}{5 + i} = \frac{39}{26} + i\frac{65}{26}.$$

On effectue alors

$$5 + 14i - (5 + i)(1 + 2i) = 2 + 3i.$$

Ceci montre que

$$\text{P.G.C.D.}(5 + 14i, 5 + i) = \text{P.G.C.D.}(5 + i, 2 + 3i).$$

De même, on a

$$\frac{5 + i}{2 + 3i} = 1 - i$$

et cette égalité nous dit que $2 + 3i \mid 5 + i$. On aboutit alors à

$$\text{P.G.C.D.}(5 + i, 2 + 3i) = (2 + 3i)\mathbb{Z}[i]^\times.$$

On conclut que

$$\text{P.G.C.D.}(5 + 14i, 5 + i) = \{2 + 3i, -2 - 3i, -3 + 2i, 3 - 2i\}.$$

■

Exercice 91 Soient A, B deux anneaux isomorphes. On suppose que A est euclidien. Que dire de B ?

Solution. L'anneau A étant euclidien, il est en particulier commutatif et intègre. Puisque B est isomorphe à A, nous savons que B est également commutatif et intègre. Soit $\nu_A : A \setminus \{0_A\} \to \mathbb{N}$ un stathme euclidien. Notons $\phi : B \to A$ un isomorphisme d'anneaux. Pour $b_0 \in B \setminus \{0_B\}$, on a évidemment $\phi(b_0) \in A \setminus \{0_A\}$ et ceci permet de définir l'application $\nu_B : B \setminus \{0_B\} \to \mathbb{N}$ par

$$\nu_B(b) := \nu_A(\phi(b)) \quad \text{pour tout } b \in B.$$

Soient $b_1, b_2 \in B$ avec $b_2 \neq 0_B$. Puisque $\phi(b_2) \in A \setminus \{0_A\}$, nous pouvons exploiter le caractère euclidien de A pour trouver $q, r \in A$ tels que $\phi(b_1) = \phi(b_2)q + r$ et $r = 0_A$ ou $\nu_A(r) < \nu_A(\phi(b_1))$. Le fait que ϕ^{-1} soit un morphisme d'anneaux permet d'écrire

$$b_1 = \phi^{-1}(\phi(b_1)) = \phi^{-1}(\phi(b_2)q + r) = b_2\phi^{-1}(q) + \phi^{-1}(r).$$

Par ailleurs, si $\phi^{-1}(r) \neq 0_B$, alors $r \neq 0_A$ et ceci entraîne $\nu_A(r) < \nu_A(\phi(b_1))$, i.e., $\nu_B(\phi^{-1}(r)) < \nu_B(b_1)$. On conclut que B est euclidien. ■