Algèbre générale

Anneaux

⋆ **Exercice 1.** *Une astuce pour simplifier.*

Soit A un anneau tel que $\forall x, y \in \mathrm{A}, (xy)^2 = x^2y^2$.

1. Montrer $\forall x, y \in \mathrm{A}, x^2y = xyx = yx^2$.
2. Montrer que A est commutatif.

Exercice 2. *Commutation au signe près.*

Soit A un anneau tel que $\forall x, y \in \mathrm{A}, xy = \pm yx$. Montrer que A est commutatif.

◦ **Exercice 3.** *Extension du cours.* *Mines*

Soit A un anneau commutatif intègre et $a_0, \dots, a_n \in \mathrm{A}$, avec a_n non nul.

Montrer que l'équation $a_n x^n + \cdots + a_0 = 0$ (d'inconnue $x \in \mathrm{A}$) possède au plus n solutions.

⋆ **Exercice 4.** *Si PGCD, alors PPCM.* *ÉNS*

Soit A un anneau commutatif et $x, y \in \mathrm{A}$.

1. Montrer que si l'idéal $(x, y) = \{ax + by \,|\, a, b \in \mathrm{A}\}$ est principal, alors $(x) \cap (y)$ aussi.
2. La réciproque est-elle vraie ?

Exercice 5. *Éléments nilpotents.*

On rappelle qu'un élément $x \in \mathrm{A}$ est dit *nilpotent* si $\exists n \in \mathbb{N} : x^n = 0$.

Dans toute la suite, A est un anneau et $x, y \in \mathrm{A}$.

1. Donner un exemple d'élément (non nul) nilpotent dans un anneau commutatif, et un autre dans un anneau non commutatif.
2. Un anneau est dit *réduit* si 0 est son seul élément nilpotent.
   Montrer que tout anneau intègre est réduit et donner un exemple d'anneau réduit non intègre.
3. (a) On suppose xy nilpotent. Montrer que yx l'est.
   (b) Trouver un exemple de situation où l'on a, pour un certain $n \in \mathbb{N}$, $(xy)^n = 0 \neq (yx)^n$.
4. (a) On suppose A commutatif et x, y nilpotents. Montrer que xy et $x + y$ sont nilpotents.
   (b) Donner un exemple de situation où x et y sont nilpotents mais ni xy ni $x + y$ ne le sont.

Exercice 6. *L'arnaque d'Eilenberg-Mazur.*

Soit A un anneau.

1. Soit $x \in A$ nilpotent. Donner un sens à l'élément $\sum_{k\in\mathbb{N}} x^k$ et montrer que $1-x$ est inversible.
2. Soit $x, y \in A$ tels que xy est nilpotent.
   Montrer que yx est nilpotent et exprimer $(1-yx)^{-1}$ en fonction de $(1-xy)^{-1}$.
3. On ne fait plus d'hypothèse de nilpotence. Soit $x, y \in A$. Montrer $1-xy \in A^\times \Rightarrow 1-yx \in A^\times$.

Morphismes

◦ **Exercice 7.** *$\mathbb{Z}$ est l'anneau initial.*

1. Soit A un anneau. Déterminer tous les morphismes d'anneaux $\mathbb{Z} \to A$.
2. Donner un exemple d'anneau tel qu'il n'existe pas de morphisme $A \to \mathbb{Z}$.

◦ **Exercice 8.** *Endomorphismes triviaux.*

1. Montrer que tout endomorphisme de l'anneau $\mathbb{Z}$ est l'identité. Même question pour $\mathbb{Q}$.
2. Soit φ un endomorphisme d'anneaux $\mathbb{R} \to \mathbb{R}$.
   (a) Montrer que $\forall x \in \mathbb{Q}, \varphi(x) = x$.
   (b) Montrer que $\varphi[\mathbb{R}_+^*] \subseteq \mathbb{R}_+^*$ et en déduire que φ est une application croissante.
   (c) En déduire que $\varphi = \mathrm{id}_\mathbb{R}$.
3. Montrer qu'il y a exactement deux endomorphismes φ de $\mathbb{C}$ tels que $\forall x \in \mathbb{R}, \varphi(x) = x$.

Exercice 9. *$\mathbb{Z}[X]$ représente le foncteur d'oubli.*

Soit A un anneau. Montrer que l'ensemble des morphismes $\mathbb{Z}[X] \to A$ est en bijection avec A.

Exercice 10. *$\mathbb{Q} \otimes \mathbb{F}_2$.*

Déterminer les anneaux A tels qu'il existe à la fois un morphisme d'anneaux $\mathbb{Q} \to A$ et un morphisme d'anneaux $\mathbb{Z}/2\mathbb{Z} \to A$.

Exercice 11. *Épimorphismes.*

1. Soit E et F deux K-espaces vectoriels et $f : E \to F$ une application linéaire. Montrer que les deux assertions suivantes sont équivalentes.
   (i) f est surjective ;
   (ii) quelles que soient les applications linéaires $g_1, g_2 : F \to G$ vers un troisième espace vectoriel, $g_1 \circ f = g_2 \circ f \Rightarrow g_1 = g_2$.
2. Montrer que la question précédente devient fausse si on remplace les espaces vectoriels par les anneaux, et les applications linéaires par les morphismes d'anneaux.

Exemples

Exercice 12. *Sous-anneaux de $\mathbb{Z}^2$.*

Pour tout $d \in \mathbb{N}$, on note $A_d = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \,\middle|\, x \equiv y \,(\mathrm{mod}\ d) \right\}$.

Montrer que tout sous-anneau de $\mathbb{Z}^2$ est égal à A_d, pour un certain $d \in \mathbb{N}$.

⋆ **Exercice 13.** *Un anneau d'entiers quadratiques imaginaire.* *ÉNS*

Soit $A = \left\{a + bi\sqrt{2} \,\middle|\, a, b \in \mathbb{Z}\right\}$.

1. Montrer que A est un sous-anneau de $\mathbb{C}$. Est-il intègre ?
2. Montrer que tout idéal de A est de la forme xA, pour un certain $x \in A$.
3. Déterminer les inversibles de A.
4. Trouver les couples $(x, y) \in \mathbb{Z}^2$ tels que $x^2 + 2 = y^3$.

Δ **Exercice 14.** *Un anneau d'entiers quadratiques totalement réel.*

Soit $A = \left\{a + b\sqrt{2} \,\middle|\, a, b \in \mathbb{Z}\right\}$.

1. Montrer que A est un sous-anneau de $\mathbb{R}$.
2. En montrant au passage qu'un tel endomorphisme doit nécessairement envoyer $\sqrt{2}$ sur $\pm\sqrt{2}$, montrer que l'anneau A n'a que deux endomorphismes : id_A et un endomorphisme non trivial que l'on notera c.
3. Montrer que pour tout $x \in A$, on a $x + c(x) \in \mathbb{Z}$ et $xc(x) \in \mathbb{Z}$.
4. En déduire que $A^\times = \left\{x \in A \,\middle|\, xc(x) = \pm 1\right\}$.
5. Montrer que $A^\times$ est infini.
6. Montrer que l'*équation de Pell-Fermat* $x^2 - 2y^2 = 1$ possède une infinité de solutions dans $\mathbb{Z}^2$.

Exercice 15. *Un anneau local, et son corps résiduel.*

Soit p un nombre premier et

$$A = \mathbb{Z}_{(p)} = \left\{\frac{a}{b} \,\middle|\, a \in \mathbb{Z}, b \in \mathbb{N}^*, b \wedge p = 1\right\}.$$

1. Montrer que A (muni des opérations usuelles) est un anneau intègre.
2. Déterminer les éléments inversibles de A.
3. Montrer qu'il existe un unique morphisme d'anneaux $\varphi : A \to \mathbb{Z}/p\mathbb{Z}$, et que $A^\times = A \setminus \ker\varphi$.
(On dit que $\mathbb{Z}/p\mathbb{Z}$ est le *corps résiduel* de l'anneau *local* A.)

Exercice 16. *Sous-anneaux de* $\mathbb{Q}$.

On note $\mathscr{S}$ l'ensemble des sous-anneaux de $\mathbb{Q}$ et Π l'ensemble des nombres premiers.

Montrer que $\begin{cases} \mathscr{S} \to \mathscr{P}(\Pi) \\ A \mapsto \Pi \cap A^\times \end{cases}$ est une bijection.

Exercice 17. *Suites stationnaires.*

On note A l'ensemble des suites de $\mathbb{Z}^\mathbb{N}$ qui sont stationnaires. Il s'agit d'un sous-anneau de $\mathbb{Z}^\mathbb{N}$ (on ne demande pas de le vérifier).

Déterminer tous les morphismes d'anneaux $A \to \mathbb{Z}$.

Anneau $\mathbb{Z}/n\mathbb{Z}$

◦ **Exercice 18.** *Éléments d'ordre* 2.

Résoudre l'équation $x^2 = 1$ dans l'anneau $\mathbb{Z}/666\mathbb{Z}$.

Exercice 19. *Réciproque du lemme chinois.*

Soit $n_1, n_2 \geq 2$. Montrer que les anneaux $\mathbb{Z}/n_1n_2\mathbb{Z}$ et $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ sont isomorphes si et seulement si n_1 et n_2 sont premiers entre eux.

Exercice 20. *Idéaux de $\mathbb{Z}/n\mathbb{Z}$.*

Soit $n \geq 2$. Déterminer les idéaux de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 21. *Groupes multiplicatifs d'exposant 2.*

Soit $n \in \mathbb{N}^*$. Montrer que $\forall x \in (\mathbb{Z}/n\mathbb{Z})^\times, x^2 = 1$ si et seulement si $n \mid 24$.

Diverses propriétés des anneaux commutatifs

Δ **Exercice 22.** *Anneaux booléiens.* *Ulm*

Soit A un anneau dans lequel tout élément $x \in A$ est *nilpotent* ($\exists n \in \mathbb{N}^* : x^n = 0$) ou *idempotent* ($x^2 = x$).

1. Montrer que tout élément de A est idempotent.
2. Montrer que A est commutatif.
3. On suppose A fini. Montrer qu'il existe $n \in \mathbb{N}$ tel que A soit isomorphe à l'anneau produit $(\mathbb{Z}/2\mathbb{Z})^n$.

Exercice 23. *Anneaux connexes.*

Dans tout l'exercice, A désigne un anneau commutatif non nul.

- Un élément $p \in A$ est dit *idempotent* si $p^2 = p$.
- L'anneau A est dit *connexe* si, étant donné deux anneaux R et S et un isomorphisme $A \to R \times S$, on a R ou S nul.

1. Montrer que A est connexe si et seulement s'il possède exactement deux idempotents : 0_A et 1_A.
2. En déduire que tout anneau intègre est connexe.
3. Montrer que $C^0(\mathbb{R})$ est connexe mais que $C^0(\mathbb{R}^*)$ ne l'est pas.
4. Soit $r, s \in \mathbb{N}^*$. Montrer que les anneaux produits $\mathbb{Z}^r$ et $\mathbb{Z}^s$ ne sont isomorphes que si $r = s$.

Exercice 24. *Anneaux intègres finis.*

Montrer que tout anneau intègre fini est un corps.

Exercice 25. *Nombre fini d'idéaux.*

Soit A un anneau intègre possédant un nombre fini d'idéaux. Montrer que A est un corps.

⋆ **Exercice 26.** *Anneau fini réduit.*

Soit A un anneau fini *réduit* (c'est-à-dire que 0 est son seul élément nilpotent).

Montrer qu'il existe des corps $K_1, \dots, K_r$ tels que A soit isomorphe à l'anneau produit $K_1 \times \cdots \times K_r$.

Exercice 27. *Idéaux premiers et parties multiplicatives.*

Dans un anneau commutatif A, un idéal $I \trianglelefteq A$ différent de A est dit *premier* si

$$\forall x, y \in A, xy \in I \Rightarrow (x \in I \text{ ou } y \in I).$$

1. Déterminer les idéaux premiers de $\mathbb{Z}$.
2. Soit $f : A \to B$ un morphisme surjectif d'anneaux commutatifs. À quelle condition $\ker f$ est-il premier ?

Une partie non vide $S \subseteq A$ est dite *multiplicative* si elle ne contient pas 0 et que $\forall x, y \in S, xy \in S$.

3. Soit $S \subseteq A$ une partie multiplicative et $I \trianglelefteq A$ un idéal tel que $I \cap S = \emptyset$ et qui est maximal pour cette propriété. Montrer que I est un idéal premier de A.
4. Soit $S \subseteq \mathbb{Z}$ une partie multiplicative. Montrer qu'il existe un idéal vérifiant les hypothèses de la question précédente.

⋆⋆ **Exercice 28.** *Idéaux maximaux.*

1. Montrer que $\mathfrak{m}_0 = \{XP \,|\, P \in K[X]\}$ est un idéal de K[X], et qu'il n'existe pas d'idéal $\mathfrak{m}_0 \subsetneq I \subsetneq K[X]$. On dit que $\mathfrak{m}_0$ est un *idéal maximal* de K[X].
2. Déterminer les idéaux maximaux de $\mathbb{Z}$ et de K[X].
3. Soit $\mathscr{F} \subseteq C^0([0,1])$ un ensemble de fonctions tel que $\forall x \in [0,1], \exists f \in \mathscr{F} \,:\, f(x) \neq 0$. Montrer qu'il existe $n \in \mathbb{N}$ et $f_1, \dots, f_n \in \mathscr{F}$ tels que $\forall x \in [0,1], f_1^2(x) + \cdots + f_n^2(x) > 0$.
4. Soit $r \in \mathbb{N}$. Déterminer les idéaux maximaux de $C^r([0,1])$.
5. En s'intéressant aux idéaux $\mathfrak{m}^2 = \left\{\sum f_i g_i \,\middle|\, f_1, \dots, f_n, g_1, \dots, g_n \in \mathfrak{m}\right\}$, montrer que les anneaux $C^0([0,1])$ et $C^1([0,1])$ ne sont pas isomorphes.

Anneaux non commutatifs

⋆ **Exercice 29.** *Théorème de Jacobson-Kaplansky.*

Soit A un anneau et $a \in A$. On suppose que a n'est pas inversible, mais qu'il existe $b \in A$ tel que $ab = 1$ (un *inverse à droite* de a).

1. Pour tout $j \in \mathbb{N}$, on note $x_j := (1 - ba)a^j$. Montrer que les éléments x_j sont distincts.
2. En déduire que a possède une infinité d'inverses à droite.

⋆⋆ **Exercice 30.** *Vers un théorème de Jacobson.*

Le *centre* d'un anneau A est le sous-anneau $Z(A) = \left\{a \in A \,\middle|\, \forall x \in A, ax = xa\right\}$. Un élément de Z(A) est dit *central*.

1. Montrer que dans un anneau réduit, tout idempotent est central.
2. Soit A un anneau et $n \geq 2$ tel que $\forall x \in A, x^n = x$. Montrer $\left\{x^{n-1} \,\middle|\, x \in A\right\} \subseteq Z(A)$.
3. Soit A un anneau tel que $\forall x \in A, x^3 = x$. Montrer que A est commutatif.

Exercice 31. *Morphisme induit de groupes multiplicatifs.*

Soit A et B deux anneaux et $f : A \to B$ un morphisme d'anneaux.

1. Montrer que f induit un morphisme $f^\times : A^\times \to B^\times$ de groupes multiplicatifs.
2. Est-ce que $f^\times$ est surjectif à chaque fois que f l'est ?

Corps

Exemples

◦ **Exercice 32.** $\mathbb{F}_4$.

On admet l'existence d'un corps à quatre éléments $\mathbb{F}_4 = \{0, 1, a, b\}$.

1. Déterminer la caractéristique de $\mathbb{F}_4$.
2. En déduire les tables d'addition et de multiplication de $\mathbb{F}_4$.
3. À quels groupes connus sont isomorphes les groupes additif $(\mathbb{F}_4, +)$ et multiplicatif $(\mathbb{F}_4^\times, \cdot)$?

Exercice 33. *Corps de nombres.*

Soit $\tau \in \mathbb{C}$. On note $\mathbb{Q}[\tau] = \left\{P(\tau) \,\middle|\, P \in \mathbb{Q}[X]\right\}$.

Montrer que $\mathbb{Q}[\tau]$ est un corps si et seulement s'il s'agit d'un $\mathbb{Q}$-espace vectoriel de dimension finie.

⋆ **Exercice 34.** *Racines de l'unité dans $\mathbb{Q}[i]$.* *X*

1. Montrer que $\mathbb{Q}[i] = \{P(i) \mid P \in \mathbb{Q}[X]\}$ est un corps, et en donner une base en tant que $\mathbb{Q}$-espace vectoriel.
2. Déterminer le groupe $\mu_\infty(\mathbb{Q}[i]) = \{z \in \mathbb{Q}[i] \mid \exists n \in \mathbb{N}^* : z^n = 1\}$ des racines de l'unité dans $\mathbb{Q}[i]$.

Δ **Exercice 35.** *Corps quadratiques.*

Soit $d \in \mathbb{Z} \setminus \{0,1\}$ un entier *quadratfrei* (ou *sans facteur carré*, c'est-à-dire que le seul carré parfait divisant d est 1, ou encore que $|d|$ est un produit de nombres premiers tous différents).

On note alors $K_d = \{a + b\rho_d \mid a,b \in \mathbb{Q}\}$, où $\rho_d = \begin{cases} \sqrt{d} & \text{si } d > 0 \\ i\sqrt{|d|} & \text{si } d < 0. \end{cases}$

1. Montrer que K_d est un sous-corps de $\mathbb{C}$.
2. Soit $x \in K_d$. Montrer qu'il existe un unique couple $(a,b) \in \mathbb{Q}^2$ tel que $x = a + b\rho_d$.
3. Soit $\delta \in \mathbb{Z} \setminus \{0,1\}$ quadratfrei.
   Montrer que l'équation $x^2 = \delta$ possède une solution dans K_d si et seulement si $\delta = d$.
4. Soit $d \neq \delta \in \mathbb{Z} \setminus \{0,1\}$ deux entiers quadratfrei. Montrer que les corps K_d et K_δ ne sont pas isomorphes.
5. Montrer que K_d admet deux morphismes $K_d \to \mathbb{C}$, et deux automorphismes, que l'on précisera.

Exercice 36. *Un corps de nombres non galoisien.*

Soit $K = \mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a,b,c \in \mathbb{Q}\}$.

1. Montrer que K est un sous-corps de $\mathbb{C}$.
2. Montrer qu'il existe exactement trois morphismes de corps $K \to \mathbb{C}$, que l'on précisera.
3. Déduire de ce qui précède que id_K est le seul automorphisme de K.

⋆ **Exercice 37.** *Un corps biquadratique.*

1. Déterminer le plus petit sous-corps de $\mathbb{C}$ contenant $\sqrt{2}$ et $\sqrt{3}$: on le note K.
2. Montrer que K est aussi le plus petit sous-corps de $\mathbb{C}$ contenant $\sqrt{2} + \sqrt{3}$.
3. Déterminer les automorphismes de corps de K.

Morphismes

Exercice 38. *Morphismes de corps.*

Soit K et L deux corps de caractéristiques différentes.

Montrer qu'il n'existe pas de morphismes de corps $K \to L$.

♠ **Exercice 39.** *Morphisme de Frobenius.*

Soit p un nombre premier.

1. Montrer que, pour tout $k \in [\![1, p-1]\!]$, p divise le coefficient binomial $\binom{p}{k}$.
2. Soit K un corps de caractéristique p. Montrer que $x \mapsto x^p$ est un morphisme de corps $\mathrm{Fr} : K \to K$, appelé *morphisme de Frobenius*.
3. Montrer que si K est fini, Fr est un automorphisme.

Exercice 40. *Corps non isomorphes.*

Montrer que les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont deux à deux non isomorphes.

⋆ **Exercice 41.** *Groupes additif et multiplicatif.*

Soit K un corps. Montrer que les groupes $(K,+)$ et $(K^\times,\cdot)$ ne sont pas isomorphes.

Un peu de théorie

Exercice 42. *Extension entière.*

Soit B un anneau (commutatif) intègre et $A \subseteq B$ un sous-anneau. On suppose que B est *entier* sur A, c'est-à-dire que tout élément de B est racine d'un polynôme unitaire à coefficients dans A.

Montrer que A est un corps si et seulement si B est un corps.

⋆ **Exercice 43.** *Théorème de Pfister (1965).* *ÉNS*

Pour tout anneau commutatif et tout $n \in \mathbb{N}^*$, on note $\Sigma_n(A) = \left\{a_1^2 + \cdots + a_n^2 \,\middle|\, a_1, \dots, a_n \in A\right\}$.

1. Montrer que pour tout anneau commutatif A, $\Sigma_2(A)$ est stable par produit.
2. Ce résultat reste-t-il vrai pour $\Sigma_3(A)$?
3. Soit K un corps de caractéristique différente de 2 et n une puissance de 2.
   (a) Soit $a_1, \dots, a_n \in K$ et $x = \sum_{k=1}^{n} a_k^2 \in \Sigma_n(A)$. Montrer qu'il existe une matrice de $M_n(K)$ dont la première ligne est $\begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix}$ vérifiant $M M^T = M^T M = x I_n$.
   (b) En déduire que $\Sigma_n(K)$ est stable par produit.
4. On suppose que K est un corps dans lequel -1 est une somme de carrés et on note $s(K)$ l'entier $s \in \mathbb{N}^*$ minimal tel que $-1 \in \Sigma_s(K)$ (c'est la *Stufe*, ou le *niveau* du corps K).
   Montrer que $s(K)$ est une puissance de 2.

⋆ **Exercice 44.** *Valeurs absolues sur le corps des rationnels.*

Une *valeur absolue* sur un anneau commutatif A est la donnée d'une application $m : A \to \mathbb{R}_+$ telle que

(a) $m(0) = 0$ et $m(1) = 1$;
(b) $\forall a, b \in A, m(ab) = m(a)m(b)$;
(c) $\forall a, b \in A, m(a+b) \leq m(a) + m(b)$.

1. À quelle condition sur A la fonction $|\cdot|_{\text{triv}}$ définie par $\forall a \in A, |a|_{\text{triv}} = \mathbb{1}_{a \neq 0}$ est-elle une valeur absolue sur A ?
2. Montrer que pour tout p premier, la formule $|a|_p = p^{-v_p(a)}$ (convenablement étendue) définit une valeur absolue sur $\mathbb{Z}$. Mieux : montrer qu'il s'agit d'une valeur absolue *ultramétrique*, c'est-à-dire que
   (c_*) $\forall a, b \in \mathbb{Z}, |a+b|_p \leq \max\left(|a|_p, |b|_p\right)$.
3. Trouver une autre valeur absolue $|\cdot|_\infty$ sur $\mathbb{Z}$ telle que $\forall a \in \mathbb{Z}, |a|_\infty \prod_p |a|_p = |a|_{\text{triv}}$, où le produit court sur les nombres premiers et doit être correctement interprété.
4. On suppose que A est un sous-anneau d'un corps C, et que m est une valeur absolue sur A. Montrer que m s'étend de manière unique au *corps des fractions* $\text{Frac}(A) = \left\{\frac{a}{b} \,\middle|\, a \in A, b \in A \setminus \{0\}\right\} \subseteq C$.

Dans la suite, on étend les valeurs absolues déjà identifiées de $\mathbb{Z}$ à $\mathbb{Q}$.

On souhaite montrer qu'en un certain sens, on a trouvé toutes les valeurs absolues définies sur $\mathbb{Q}$. Fixons donc une valeur absolue m sur $\mathbb{Q}$.

5. Montrer que les assertions suivantes sont équivalentes :
   (i) la valeur absolue m est ultramétrique ;
   (ii) $\forall a \in \mathbb{Z}, m(a) \leq 1$;

(iii) la valeur absolue m est bornée en restriction aux entiers.

6. On suppose m ultramétrique et différente de $|\cdot|_{\text{triv}}$. Montrer qu'il existe un unique nombre premier p tel que $m(p) < 1$, et en déduire qu'il existe $s > 0$ tel que $m = |\cdot|_p^s$.
7. On suppose m non ultramétrique. On fixe un entier $a \geq 2$.
   (a) Justifier l'existence de $b \in \mathbb{N}$ tel que $b \geq 2$ et $m(b) > 1$.
   (b) En écrivant a^n en base b (pour tout $n \in \mathbb{N}$), montrer que $\dfrac{\ln(m(a))}{\ln a} \leq \dfrac{\ln(m(b))}{\ln b}$.
   (c) Montrer que l'inégalité précédente est une égalité si $m(a) > 1$.
   (d) En déduire $m(a) = a^{\ln m(b)/\ln b}$, d'abord sous l'hypothèse $m(a) > 1$, puis sans cette hypothèse.
8. Montrer le théorème d'Ostrowski (1916) : toute valeur absolue sur $\mathbb{Q}$ est de la forme $|\cdot|_{\text{triv}}$, $|\cdot|_\infty^s$ (pour un certain $s > 0$) ou $|\cdot|_p^s$ (pour un certain nombre premier p et un certain $s > 0$).

Algèbres

Exercice 45. *Représentation fidèle.*

Soit A une K-algèbre de dimension n. Montrer qu'il existe une sous-algèbre de $\mathrm{M}_n(\mathrm{K})$ isomorphe à A.

Exercice 46. *Algèbres intègres.*

Soit A une K-algèbre commutative, intègre, de dimension finie. Montrer que A est un corps.

Exercice 47. *Représentations matricielles des corps de nombres.*

1. Soit K un corps, et V un sous-espace vectoriel de $\mathrm{M}_n(\mathrm{K})$ tel que $\mathrm{V} \setminus \{0\} \subseteq \mathrm{GL}_n(\mathrm{K})$. Montrer que $\dim \mathrm{V} \leq n$.
2. Soit F un sous-corps de $\mathbb{C}$. On suppose F de dimension finie n en tant que $\mathbb{Q}$-espace vectoriel. Montrer qu'il existe un morphisme injectif de $\mathbb{Q}$-algèbres $\mathrm{F} \to \mathrm{M}_n(\mathbb{Q})$.
3. Soit $n \geq 2$. On admet que $\mathrm{X}^n - 2 \in \mathbb{Q}[\mathrm{X}]$ est irréductible. Construire une extension de degré n de $\mathbb{Q}$, c'est-à-dire une $\mathbb{Q}$-algèbre de dimension n qui est un corps.

Exercice 48. *Idéaux d'une* K*-algèbre.*

Soit A une K-algèbre.

1. Montrer que tout idéal de A en est un sous-K-espace vectoriel.
2. Montrer que, si tout sous-espace vectoriel de A en est un idéal, alors $\dim_{\mathrm{K}} \mathrm{A} \leq 1$.

Exercice 49. *Idéaux de* K^n.

Soit K un corps. Combien la K-algèbre K^n possède-t-elle d'idéaux ?

Exercice 50. *Algèbre quotient.*

Soit A une K-algèbre de dimension finie et I un idéal de A.

1. Justifier qu'il existe un projecteur π de noyau I.
2. On note $\mathrm{Q} = \operatorname{im} \pi$, et on considère désormais π comme une application linéaire $\pi : \mathrm{A} \to \mathrm{Q}$. Munir S d'une multiplication $\star$ telle que $(\mathrm{Q}, +, \cdot, \star)$ soit une K-algèbre et $\pi : \mathrm{A} \to \mathrm{Q}$ un morphisme d'algèbres.
3. On suppose l'idéal I *premier*, c'est-à-dire tel que $\forall x, y \in \mathrm{A}, xy \in \mathrm{I} \Rightarrow x \in \mathrm{I}$ ou $y \in \mathrm{I}$. Montrer que Q est intègre, et en déduire que c'est un corps.
4. Soit L un surcorps de K. Montrer qu'il existe un nombre fini de morphismes d'algèbres $\mathrm{A} \to \mathrm{L}$. Garde-t-on ce résultat sans hypothèse sur la dimension de A ?

⋆ **Exercice 51.** *Produit d'algèbres monogènes.*

Soit K un corps. Une K-algèbre A est dite *monogène* s'il existe $x \in A$ tel que $A = K[x]$.

1. On suppose le corps K infini. Montrer que le produit de deux algèbres monogènes est monogène.
2. Montrer que pour tout $n \in \mathbb{N}^*$, tout élément $a \in \mathbb{F}_p^n$ vérifie $a^p = a$ et en déduire que la question précédente ne s'étend pas aux corps finis.

Exemples

Exercice 52. *Cotangent de Zariski.*

1. Construire une K-algèbre $K[\varepsilon]$ possédant une base $(1, \varepsilon)$, où $\varepsilon^2 = 0$.
2. Soit $\varphi : K[X] \to K[\varepsilon]$ un morphisme d'algèbres.
Montrer qu'il existe $a, b \in K$ tel que $\forall P \in K[X], \varphi(P) = P(a) + bP'(a)\,\varepsilon$.

Exercice 53. *Normalisation.*

On considère l'ensemble A des polynômes $P \in K[X]$ dont le coefficient de degré 1 est nul.

1. Montrer que A est une sous-algèbre de K[X].
2. Montrer que A n'est pas isomorphe à K[X].

Exercice 54. *Sous-algèbres de* $C^0(\mathbb{R})$.

Trouver toutes les sous-algèbres de $C^0(\mathbb{R})$ de dimension finie.

Exercice 55. *Algèbres étales quadratiques.*

Soit K un corps de caractéristique nulle et $a \in K^*$.

1. Déterminer la plus petite sous-K-algèbre $R_a \subseteq M_2(K)$ contenant $\begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$ et calculer $\dim R_a$.
2. Soit B une K-algèbre. Montrer que les morphismes de K-algèbres $R_a \to B$ sont en bijection avec les éléments $b \in B$ tels que $b^2 = a\,1_B$.
3. Montrer que R_a est isomorphe à l'algèbre produit $K \times K$ si $\exists \alpha \in K : \alpha^2 = a$ et que R_a est un corps sinon.
4. Déterminer à isomorphisme près toutes les algèbres R_a dans les cas $K = \mathbb{C}$, puis $K = \mathbb{R}$.
5. Montrer que si $K = \mathbb{Q}$, il existe une infinité d'algèbres R_a deux à deux non isomorphes.
6. On revient à un sous-corps de $\mathbb{C}$ quelconque. Soit L une extension de K de degré 2, c'est-à-dire une K-algèbre de dimension 2 qui est un corps. Montrer qu'il existe $a \in K$ tel que L soit isomorphe à R_a.

Hors programme

⋆⋆ **Exercice 56.** *Centre de la catégorie des* $\mathbb{F}_p$*-algèbres commutatives.* *X*

Déterminer toutes les manières d'associer à une $\mathbb{F}_p$-algèbre commutative A un endomorphisme d'algèbres $\varphi_A : A \to A$ telles que, pour tout morphisme de $\mathbb{F}_p$-algèbres $f : A \to B$, on ait $\varphi_B \circ f = f \circ \varphi_A$.

Nombres algébriques et transcendants

Δ **Exercice 57.** *Nombre de Liouville.*

1. Soit $P \in \mathbb{Z}[X]$ de degré $n \geq 1$ et x une racine de P.
   (a) Montrer qu'il existe une constante $C > 0$ telle que, pour tous $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, on ait
   $$\left(P\left(\frac{a}{b}\right) \neq 0 \text{ et } \left|x - \frac{a}{b}\right| \leq 1\right) \Rightarrow \left|x - \frac{a}{b}\right| \geq \frac{C}{b^n}.$$
   (b) En déduire qu'il existe une constante $C' > 0$ telle que, pour tous $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, on ait
   $$\frac{a}{b} \neq x \Rightarrow \left|x - \frac{a}{b}\right| \geq \frac{C'}{b^n}.$$
2. Montrer que $\sum_{n=0}^{+\infty} 2^{-n!}$ est un nombre transcendant.
   Remarque. C'est historiquement le premier exemple de nombre transcendant (Liouville, 1844).

⋆ **Exercice 58.** *Extensions multiquadratiques.*

Soit $p_1, \dots, p_r$ des nombres premiers distincts.

1. On note pour tout $I \subseteq [\![1, n]\!]$, $r_I = \prod_{i \in I} \sqrt{p_i}$. Montrer que $K = \mathbb{Q}[\sqrt{p_1}, \dots, \sqrt{p_n}] := \mathrm{Vect}_{\mathbb{Q}}\left((r_I)_{I \subseteq [\![1,n]\!]}\right)$ est la plus petite sous-$\mathbb{Q}$-algèbre de $\mathbb{C}$ contenant les $\sqrt{p_i}$.
2. Montrer que K est un sous-corps de $\mathbb{C}$.
3. Montrer que $\dim_{\mathbb{Q}}(K) = 2^n$.
4. Montrer $\sqrt[3]{2} \notin K$.
5. Montrer que le groupe des automorphismes de $\mathbb{K}$ est de cardinal 2^n.

Exercice 59. *Extension purement transcendante.*

Montrer que les constantes sont les seuls éléments de K(X) algébriques sur K.

Indications

Exercice 1. On pourra chercher à appliquer certaines assertions à $1+x$ ou à $1+y$.

Exercice 2. On pourra constater que, pour tout $x \in \mathrm{A}$, les deux ensembles

$$\mathrm{C}^{\pm}(x) = \{y \in \mathrm{A} \mid xy = \pm yx\}$$

sont des sous-groupes de $(\mathrm{A}, +)$.

Exercice 3. Il s'agit de vérifier que la preuve du cours de première année s'étend à ce contexte.

Exercice 4. Dans $\mathbb{Z}$, la question est sans intérêt, mais on sait relier les générateurs de ces deux idéaux, grâce à une formule reliant PGCD et PPCM. Pour trouver les bonnes manipulations, on pourra commencer par supposer l'anneau intègre.

Pour la deuxième questions, les contre-exemples les plus classiques d'idéaux non principaux fournissent des réponses.

Exercice 6. Dans la première question, on pourra penser à la série géométrique, ou plutôt lui donner un sens dans ce contexte où les sommes infinies n'en ont pas. Pour la troisième question, on utilisera ce qui précède comme motivation heuristique.

Exercice 9. Essentiellement, cet exercice demande de montrer que tout morphisme d'anneaux de domaine $\mathbb{Z}[\mathrm{X}]$ est un morphisme d'évaluation.

Exercice 10. On pourra se demander ce que l'existence de tels morphismes entraîne sur l'unité 1_{A}.

Exercice 11. On pourra chercher un contre-exemple dont le domaine est $\mathbb{Z}$.

Exercice 12. On pourra commencer par s'intéresser à $\mathrm{A}_d \cap (\mathbb{Z} \times \{0\})$: quelle structure possède cette intersection ?

Exercice 13. Les deuxième et troisième questions ont un fort contenu géométrique. La dernière est plus difficile : on constatera que la démonstration du cours s'applique pour montrer que A possède un théorème d'existence et d'unicité de la décomposition en irréductibles. Ensuite, à l'aide d'un petit argument de parité, on peut montrer que si (x, y) est solution, alors les éléments $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entre eux dans A et en déduire que $x + i\sqrt{2}$ est alors le cube d'un élément A, ce que l'on peut ensuite analyser de façon élémentaire.

Exercice 14. Pour la troisième question, on pourra chercher l'ensemble des points fixes de c. Pour la dernière, on commencera par remarquer que l'on sait faire si le second membre est remplacé par ± 1.

Exercice 17. Les morphismes sont faciles à deviner. Pour montrer que ce sont les seuls, on pourra trouver des suites qui vérifient des équations polynomiales simples : leurs images devront alors vérifier les mêmes.

Exercice 18. Appliquer le théorème chinois.

Exercice 19. Quand deux anneaux sont isomorphes, les questions « de théorie des anneaux » ont les mêmes réponses de part et d'autre. Par exemple, les équations $x^d = 1$, d'inconnue x ont le même nombre de solutions.

Exercice 20. On pourra essayer de se ramener à $\mathbb{Z}$.

Exercice 21. Théorème chinois. Le cas où n est premier est à la fois facile (car $\mathbb{Z}/n\mathbb{Z}$ est alors un corps) et utile.

Exercice 22. Il y a une idée très classique qui permet de définir un élément inversible à l'aide de tout élément nilpotent.

Exercice 23. Dans un sens, il n'est pas très difficile de trouver des éléments idempotents dans un produit $\mathrm{R} \times \mathrm{S}$. Réciproquement, comment « retrouver » R à partir de $p = (1, 0) \in \mathrm{R} \times \mathrm{S}$?

Exercice 24. Une application $\mathrm{A} \to \mathrm{A}$ est injective si et seulement si elle est surjective.

Exercice 25. Voyez-vous comment un élément $a \in \mathrm{A}$ peut définir à lui tout seul une suite d'idéaux ?

Exercice 26. On pourra noter que dans un anneau fini, tout élément possède une puissance idempotente.

Exercice 27. Pour la troisième question, on pourra vérifier qu'étant donné un idéal I et un élément $x \notin \mathrm{I}$, l'ensemble $\mathrm{I} + (x) = \left\{ z + ax \,\middle|\, z \in \mathrm{I}, a \in \mathrm{A} \right\}$ est un idéal tel que $\mathrm{I} \subsetneq \mathrm{I} + (x)$.

Exercice 28. Pour la troisième question, constater que si la propriété était fausse, on aurait que, pour tout $n \in \mathbb{N}^*$, toutes les fonctions de $\mathscr{F}$ possèdent un zéro dans le même segment de la forme $\left[\frac{k}{n}, \frac{k+1}{n} \right]$.

Exercice 29. Que valent $a(1 - ba)$ et $(1 - ba)b$?

Exercice 30.

1. Étant donné $a \in \mathrm{A}$ idempotent et $x \in \mathrm{A}$, on pourra commencer par calculer $(axa - ax)^2$.
2. Application relativement directe.
3. Soit $x \in \mathrm{A}$. D'après la question précédente, $(x^2 + x)^2$ est central, donc...

Exercice 31. Un contre-exemple à la question 2 se trouve avec des anneaux jouant un rôle majeur dans le cours !

Exercice 32. On pourra par exemple montrer $ab = 1$.

Exercice 33. On montrera que les deux conditions équivalent à l'existence d'un polynôme non nul $\mathrm{P} \in \mathbb{Q}[\mathrm{X}]$ (que l'on pourra même choisir irréductible) tel que $\mathrm{P}(\tau) = 0$.

Exercice 34. Si $a + ib \in \mu_\infty(\mathbb{Q}[i])$, le polynôme $\mathrm{X}^2 - 2a\mathrm{X} + 1$ divise un certain polynôme $\mathrm{X}^n - 1$. Mais dans quel anneau, au juste ?

Exercice 35. Pour la dernière question, on pourra vérifier que les morphismes $\mathrm{K}_d \to \mathbb{C}$ sont déterminés par l'image de ρ_d, et s'interroger sur les images possibles.

Exercice 36. Pour montrer $\forall x \in \mathrm{K} \setminus \{0\}, x^{-1} \in \mathrm{K}$, un argument abstrait de dimension vaut mieux que des calculs explicites. Pour déterminer les morphismes $\rho : \mathrm{K} \to \mathbb{C}$, on s'interrogera sur ce que peut valoir $\rho(\sqrt[3]{2})$.

Exercice 37.

2. On pourra exprimer $\sqrt{2}$ ou $\sqrt{3}$ en fonction des premières puissances de $\sqrt{2} + \sqrt{3}$.
3. On pourra montrer qu'un morphisme de corps $\mathrm{K} \to \mathbb{C}$ est entièrement déterminé par l'image de $\sqrt[3]{2}$, et se demander quelles sont les images possibles.

Exercice 39. On rappelle qu'un morphisme de corps est juste un morphisme d'anneaux entre corps.

Exercice 40. Il y a plein de façons de faire. On peut par exemple montrer que le nombre de solutions de certaines équations ne change pas quand on passe d'un corps à un autre qui lui est isomorphe.

Exercice 41. Deux groupes isomorphes ont, pour tout $n \in \mathbb{N}^*$, le même nombre d'éléments vérifiant

$g^n = 1$. Cette remarque peut conclure, en faisant attention au fait que l'un des deux groupes est noté multiplicativement et en distinguant suivant la caractéristique du corps.

Exercice 42. Dans le sens direct, on pourra montrer que tout élément $x \in \mathrm{B} \setminus \{0\}$ annule un polynôme unitaire de $\mathrm{A}[\mathrm{X}]$ dont le coefficient constant est non nul.

Exercice 43. Pour la question 3(a), on pourra raisonner par récurrence, en cherchant dans la phase d'hérédité une matrice par blocs $\begin{pmatrix} \mathrm{A} & \mathrm{B} \\ \mathrm{U} & \mathrm{V} \end{pmatrix} \in \mathrm{M}_{2n}(\mathrm{K})$ avec $\mathrm{A}^{\mathrm{T}}\mathrm{A} = \mathrm{A}\mathrm{A}^{\mathrm{T}} = x\mathrm{I}_n$ et $\mathrm{B}^{\mathrm{T}}\mathrm{B} = \mathrm{B}\mathrm{B}^{\mathrm{T}} = y\mathrm{I}_n$. Le cas $x = y = 0$ nécessite un bidouillage particulier.

Exercice 44.

3. Ne pas se laisser impressionner par l'indice ∞...
5. Pour l'implication non triviale (iii) $\Rightarrow$ (i), on utilisera le binôme de Newton pour montrer une inégalité de la forme $\forall n \in \mathbb{N}, m(a+b)^n \leq \text{cte} \max\big(m(a), m(b)\big)^n$: reste à constater que cela suffit.
6. Pour l'unicité, on pourra utiliser le théorème de Bézout.
7. Pour la dernière sous-question, noter que $m(b^n a) > 1$ pour b assez grand.

Exercice 45. Il est peut-être plus facile de trouver un morphisme de A dans les endomorphismes d'un espace vectoriel de dimension n.

Exercice 46. En dimension finie, tout endomorphisme injectif est un automorphisme.

Exercice 47.

1. On cherchera à construire une application linéaire injective $\mathrm{V} \to \mathrm{K}^n$.
2. En fait, tout morphisme de $\mathbb{Q}$-algèbres $\mathrm{F} \to \mathrm{M}_n(\mathbb{Q})$ est automatiquement injectif.
3. On pourra chercher une matrice simple $\mathrm{A} \in \mathrm{M}_n(\mathbb{Q})$ telle que $\mathrm{A}^n = 2\mathrm{I}_n$.

Exercice 48. Que peut-on dire d'un idéal contenant un élément inversible ?

Exercice 49. Une erreur classique d'algèbre linéaire est de penser que, magiquement, les sous-espaces vectoriels d'un espace vectoriel donné « s'alignent » avec notre base préférée. Pour les idéaux de K^n, cette erreur devient réalité.

Exercice 50.

2. Ne pas faire preuve d'imagination : il faut définir la multiplication la plus naturelle possible. Votre travail est alors de montrer qu'elle est bien définie.
4. La réponse est évidemment non. Pour produire un contre-exemple, penser à une algèbre A pour laquelle il est très facile de définir des morphismes d'algèbres de domaine A.

Exercice 51. On pourra commencer par montrer le résultat pour un produit $\mathrm{K}[x]\times\mathrm{K}[y]$ avec deux éléments x, y dont les polynômes minimaux sont premiers entre eux. Ensuite, il faut être prêt à changer y sans changer $\mathrm{K}[y]$.

Exercice 52. Pour la première question, on pourra utiliser une matrice de $\mathrm{M}_2(\mathrm{K})$ de carré nul.

Exercice 54. Soit $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$. À quelle condition une fonction $f \in \mathrm{C}^0(\mathbb{R})$ est-elle annulée par le polynôme f?

Exercice 55.

3. On pourra utiliser la question précédente pour gérer le cas *scindé* (isomorphe à $\mathrm{K} \times \mathrm{K}$).
5. On pourra montrer que si $p \neq \ell$ sont premiers, R_p et R_ℓ ne sont pas isomorphes, là encore en utilisant

la deuxième question.

Exercice 56. On pourra commencer par montrer qu'il existe $P \in \mathbb{F}_p[X]$ tel que, pour tout élément a de toute $\mathbb{F}_p$-algèbre commutative A, on ait $\varphi_A(a) = P(a)$.

Exercice 57. Pour la première question, on pourra utiliser l'inégalité des accroissements finis et constater que le nombre $P\left(\frac{a}{b}\right)$ est un rationnel sur lequel on possède des informations.

Exercice 58.

2. Le fait que K soit (évidemment) de dimension finie doit suffire.
3. Procéder par récurrence, avec une assertion de récurrence soignement choisie : il est notamment important de montrer que dans $\mathbb{Q}[\sqrt{p_1}, \dots, \sqrt{p_k}]$, les premiers $p_{k+1}, \dots, p_n$ ne sont toujours pas des carrés.
4. La connaissance de $\dim_{\mathbb{Q}}(K)$ doit suffire.
5. On cherchera à définir ces automorphismes sur la base $(r_I)_{I \subseteq [\![1,n]\!]}$.

Exercice 59. On pourra se souvenir que α est algébrique sur K si et seulement si $K[\alpha]$ est un K-espace vectoriel de dimension finie.