Sorbonne Université, Algèbre 2, année 2025-2026

Corrigé de la feuille de TD numéro 2

Exercice 1.

(1) On vérifie que $(\mathrm{M}_2(\mathbb{R}), +)$ est un groupe, que $(\mathrm{M}_2(\mathbb{R}), \times)$ est un monoïde et que $\times$ est distributive par rapport à $+$.

(2) Il existe des matrices A, B telles que $AB \neq BA$, donc l'anneau n'est pas commutatif. Il existe des matrices A, B non nulles telles que AB est la matrice nulle, donc l'anneau n'est pas intègre.

Exercice 2.

(1) $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$ mais pas un idéal, $\mathbb{Q}$ est un sous-anneau de $\mathbb{R}$ mais pas un idéal, l'ensemble $D_n(\mathbb{R})$ des matrices diagonales à coefficients réels est un sous-anneau de $M_n(\mathbb{R})$ mais ce n'est pas un idéal.

(2) $n\mathbb{Z}$ pour $n \geq 2$ est un idéal de $\mathbb{Z}$, mais ce n'est pas un sous-anneau puisqu'il ne contient pas le neutre multiplicatif.

(3) Les sous-groupes de $(\mathbb{Z}, +, \times)$ sont les $n\mathbb{Z}$. Ce sont aussi ses idéaux. Si A est un sous-anneau de $\mathbb{Z}$, alors il contient 1, donc $A = \mathbb{Z}$.

(4) Tout idéal non nul d'un corps contient 1, donc est égal au corps entier.

Exercice 3.

(1) On vérifie qu'il s'agit d'un sous-anneau de $(\mathbb{Q}, +, \times)$: c'est un sous-groupe de $(\mathbb{Q}, +)$, stable par multiplication interne et qui contient le neutre multiplicatif.

(2) Soit $n/10^k$ un élément de $\mathbb{D}$. S'il existe $n'/10^{k'}$ dans $\mathbb{D}$ tel que $(n/10^k)(n'/10^{k'}) = 1$ alors les seuls diviseurs premiers de n sont 2 et 5, donc n est de la forme $2^a 5^b$. Réciproquement, le décimal $(2^a 5^b)/10^k$ est bien inversible, d'inverse $10^k/(2^a 5^b)$ que l'on peut écrire, en supposant par exemple $b \geq a$, sous la forme $10^k 2^{b-a}/(2^b 5^b) = 10^k 2^{b-a}/10^b$.

Exercice 4. Il est clair que $Z(A)$ contient 0_A et 1_A. Si a, a' sont dans $Z(A)$ alors pour tout $b \in A$ on a $b(a - a') = (a - a')b$ et $baa' = aa'b$, donc $Z(A)$ est stable par addition, soustraction et multiplication. C'est bien un sous-anneau.

Exercice 5. Si A est un corps, il est intègre. Réciproquement, supposons que A est intègre. On commence par observer que l'application φ_a est injective : si $\varphi_a(x) = \varphi(y)$ alors $ax = ay$ donc $a(x - y) = 0_A$ donc $x - y = 0_A$ (car $a \neq 0_A$ et A est intègre). L'anneau A étant fini, φ_a est aussi surjective, donc il existe $b \in A$ tel que $\varphi_a(b) = 1_A$, d'où $ab = 1_A$. Ainsi, a est inversible à droite. En considérant $\psi_a : x \mapsto xa$, on démontre de même que a est inversible à gauche.

Exercice 6. Soit $\mathbb{K}$ un sous-corps de $\mathbb{Q}$. Par définition, $\mathbb{K}$ contient 1 et $(\mathbb{K}, +)$ est un groupe, donc $\mathbb{K}$ contient $\mathbb{Z}$. Comme $\mathbb{K}$ est un sous-corps, $(\mathbb{K}, \times)$ est un groupe, donc $\mathbb{K}$ est stable par produit et division, d'où $\mathbb{K}$ contient $\mathbb{Q}$.

Exercice 7.

(1) Par définition, un morphisme d'anneaux envoie 1 sur 1_A, donc k sur $k1_A$. Ce morphisme est bien unique.

(2) Le noyau de φ est un idéal de A, donc il existe un entier $n \geq 0$ tel que $\ker(\varphi) = n\mathbb{Z}$. Supposons maintenant que A est intègre et que $n \geq 1$. Si $n = ab$ avec $a, b \in \mathbb{N}^*$ alors $\varphi(ab) = 0_A = \varphi(a)\varphi(b)$, donc $\varphi(a) = 0_A$ ou $\varphi(b) = 0_A$. Supposons par exemple que $\varphi(a) = 0_A$, alors a appartient à $\ker(\varphi) = n\mathbb{Z}$, donc $a = n$ et $b = 1$. De même, si $\varphi(b) = 0_A$, alors $b = n$ et $a = 1$. Les seuls diviseurs de n sont donc 1 et lui-même, ce qui démontre la primalité de n.

(3) Si $n = 0$, alors φ est injectif, donc $\mathrm{Im}(\varphi)$ est un sous-anneau de A isomorphe à $\mathbb{Z}$. Comme on suppose que A est un corps (commutatif par définition), chaque $\varphi(k)$ avec $k \neq 0$ possède un inverse $\varphi(k)^{-1}$. Considérons l'application $\psi : \mathbb{Q} \to A$ qui envoie 0 sur 0_A et qui envoie $p/q \in \mathbb{Q}$ avec $p \in \mathbb{Z}, q \in \mathbb{N}^*$ et $p \wedge q = 1$ sur $\varphi(p)\varphi(q)^{-1}$. On vérifie aisément qu'il s'agit d'un morphisme de corps : $\psi(p/q + p'/q') = \psi((pq' + qp')/qq') = \varphi(pq' + qp')\varphi(qq')^{-1} = (\varphi(p)\varphi(q') + \varphi(q)\varphi(p'))\varphi(q)^{-1}\varphi(q')^{-1} = \cdots = \psi(p/q) + \psi(p'/q')$ et de même $\psi((p/q)(p'/q')) = \psi(p/q)\psi(p'/q')$. Il reste à vérifier l'injectivité de ψ : si $\psi(p/q) = 0_A$ alors $\varphi(p)\varphi(q)^{-1} = 0_A$ donc $\varphi(p) = 0_A$ par intégrité, donc $p = 0$ par injectivité de φ.

Exercice 8. Le noyau de φ est un idéal. Il n'est pas égal à K tout entier car φ envoie le neutre multiplicatif sur le neutre multiplicatif, donc il est trivial (voir l'exercice 2). Ainsi, φ est injectif.

Exercice 9. Les inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{k}$ avec $1 \leq k \leq n$ vérifiant $k \wedge n = 1$. Si n est premier, tout élément non trivial est donc inversible, donc $\mathbb{Z}/n\mathbb{Z}$ est un corps, donc intègre. Si n n'est pas premier, alors $n = ab$ avec $1 < a, b < n$, et $\bar{a}\bar{b} = \bar{0}$ avec $\bar{a}, \bar{b}$ non nuls, donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

Exercice 10. Soit A un anneau intègre et $a \in A$. Si x_0 est une solution de l'équation $x^2 = a$ alors $(x - x_0)(x + x_0) = 0$ donc $x = \pm x_0$ par intégrité. Voici un contre-exemple sans intégrité : $A = M_n(\mathbb{R})$ et $a = I_n$, il y a 2^n solutions évidentes (matrices diagonales avec ± 1 sur la diagonale), ou encore $A = \mathbb{Z}/8\mathbb{Z}$ avec $a = \bar{1}$ et $x = \bar{1}, \bar{3}, \bar{5}, \bar{7}$.

Exercice 11.

(1) L'ensemble $\mathbb{Q}[\sqrt{2}]$ contient clairement 0 et 1, et on vérifie sans peine qu'il est stable par addition, soustraction, multiplication, inversion (d'un élément non nul).

(2) On vérifie que $\varphi(u + u') = \varphi(u) + \varphi(u')$ et que $\varphi(uu') = \varphi(u)\varphi(u')$ pour tous $u, u' \in \mathbb{Q}[\sqrt{2}]$, donc φ est bien un morphisme de corps. Il est clairement surjectif, et il est injectif car si $\varphi(x + y\sqrt{2}) = 0$ alors $x - y\sqrt{2} = 0$, donc $x = y = 0$ (car $\sqrt{2}$ est irrationnel). C'est donc bien un automorphisme de corps.

(3) On considère l'application $\psi : \mathbb{Q}[X] \to \mathbb{Q}[\sqrt{2}] : P \mapsto P(\sqrt{2})$. Il s'agit d'un morphisme d'anneaux, et il est surjectif. Calculons son noyau : si $\psi(P) = 0$ alors $P(\sqrt{2}) = 0$. On a aussi $\varphi(P(\sqrt{2})) = 0 = P(\varphi(\sqrt{2})) = P(-\sqrt{2}) = 0$. Donc $(X - \sqrt{2})(X + \sqrt{2})$ divise P, i.e., $X^2 - 2$ divise P. Ainsi, $\ker(\psi)$ est l'idéal engendré par $X^2 - 2$.

(4) D'après le cours, $\mathbb{Q}[X]/(X^2 - 2)$ est un $\mathbb{Q}$-espace vectoriel de dimension $\deg(X^2 - 2) = 2$. Alternativement, on peut vérifier à la main que $\mathbb{Q}[\sqrt{2}]$ est un $\mathbb{Q}$-espace vectoriel de dimension 2 dont une base est $(1, \sqrt{2})$.

Exercice 12.

(1) Voir la question (1) de l'exercice précédent. Ce n'est pas un sous-corps : par exemple, l'élément $2+\sqrt{2}$ a pour inverse dans $\mathbb{Q}[\sqrt{2}]$ l'élément $(-2+\sqrt{2})/4$, qui n'appartient pas à $\mathbb{Z}[\sqrt{2}]$.

(2) Il s'agit d'un calcul qui ne devrait pas poser problème.

(3) Si $u \in \mathbb{Z}[\sqrt{2}]$ est inversible, il existe $v \in \mathbb{Z}[\sqrt{2}]$ tel que $uv = 1$, donc $N(u)N(v) = N(uv) = N(1) = 1$. Or $N(u)$ et $N(v)$ sont des entiers, donc $N(u) = \pm 1$. Réciproquement, si $N(u) = \pm 1$ alors $u\bar{u} = \pm 1$ donc u est inversible, d'inverse $\pm\bar{u}$.

(4) Le groupe des inversibles contient, par exemple, $1+\sqrt{2}$. Il contient donc $(1+\sqrt{2})^n$ pour tout $n \in \mathbb{Z}$.

(5) Comme u est inversible, on a $\bar{u} = 1/u$ ou $\bar{u} = -1/u$. Dans le premier cas, on a $0 < \bar{u} < 1$ et dans le second cas on a $-1 < \bar{u} < 0$. Ainsi, on a bien $-1 < \bar{u} < 1$, i.e., $-1 < x - y\sqrt{2} < 1$. Comme d'autre part $x + y\sqrt{2} > 1$, on obtient $2x > 0$ et donc $x > 0$, donc $x \geq 1$, puis $x - y\sqrt{2} < 1$ donne $-1 \leq x - 1 \leq y\sqrt{2}$, d'où $y \geq 0$. Si $y = 0$ alors u doit être égal à 1, ce qui contredit notre hypothèse, donc $y \geq 1$.

(6) D'après la question précédente, l'ensemble $E = \mathbb{Z}[\sqrt{2}]^\times \cap]1, +\infty[$ possède un plus petit élément, à savoir $\rho = 1+\sqrt{2}$. Soit u un élément de E. Puisque la suite $(\rho^n)_{n\in\mathbb{N}}$ tend vers l'infini, il existe un entier $n \geq 1$ tel que $\rho^n \leq u < \rho^{n+1}$, d'où $1 \leq u\rho^{-n} < \rho$. Comme $\mathbb{Z}[\sqrt{2}]^\times$ muni de la multiplication est un groupe, l'élément $u\rho^{-n}$ appartient à $\mathbb{Z}[\sqrt{2}]^\times$ et donc à E. Par minimalité de ρ, on obtient $u\rho^{-n} = 1$, d'où $u = \rho^n$.

Considérons maintenant l'application $\varphi : \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}[\sqrt{2}]^\times$ qui envoie $(1, \bar{0})$ sur ρ et $(0, \bar{1})$ sur -1. Il s'agit clairement d'un morphisme de groupes, et on voit facilement qu'il est injectif. Pour la surjectivité, prenons $u \in \mathbb{Z}[\sqrt{2}]^\times$. Si $u = \pm 1$, il est bien dans l'image de φ. Supposons maintenant que $u \neq \pm 1$. Alors quitte à remplacer u par $-u$ on peut supposer $u > 0$, et quitte à remplacer u par $1/u$ on peut supposer que $u > 1$, et donc que $u = \rho^n$ pour un certain $n \geq 1$ (en vertu de ce qui a été démontré plus haut).

(7) Posons $u = x + y\sqrt{2}$. Commençons par observer que (x, y) est solution de $x^2 - 2y^2 = 1$ si et seulement si $N(u) = 1$, et que (x, y) est solution de $x^2 - 2y^2 = -1$ si et seulement si $N(u) = -1$. D'après la question précédente, tout u qui vérifie $N(u) = \pm 1$ est de la forme $u = \pm(1+\sqrt{2})^n$ avec $n \in \mathbb{Z}$. Notons que $N(1+\sqrt{2}) = -1$, donc $N(\pm(1+\sqrt{2})^n) = N(1+\sqrt{2})^n = (-1)^n$, d'où le résultat.

Exercice 13. Ici $N(x+iy) = x^2+y^2$ et $x+iy$ est inversible si et seulement si $N(x+iy) = \pm 1$, i.e., $x^2 + y^2 = \pm 1 = 1$. Il y a donc quatre couples (x, y) possibles : $(\pm 1, 0)$ et $(0, \pm 1)$.

Exercice 14.

(1) Comme $\varphi(1) = 1$, on a bien $\varphi(x) = x$ pour tout $x \in \mathbb{Z}$. Ensuite, si $x = p/q$ est dans $\mathbb{Q}$, on a $\varphi(p/q) = \varphi(p)/\varphi(q) = p/q$.

(2) On écrit $y - x = \sqrt{y-x}^2$. On en déduit que $\varphi(y) - \varphi(x) = \varphi(y-x) = \varphi(\sqrt{y-x}^2) = \varphi(\sqrt{y-x})^2 \geq 0$, d'où $\varphi(y) \geq \varphi(x)$.

(3) Supposons qu'il existe un réel x tel que $x \neq \varphi(x)$, par exemple $x < \varphi(x)$ (l'autre cas étant similaire). Par densité de $\mathbb{Q}$ dans $\mathbb{R}$, il existe un rationnel r tel que $x < r < \varphi(x)$. En appliquant φ à l'inégalité $x < r$, on obtient $\varphi(x) < \varphi(r) = r$, donc $\varphi(x) < r < \varphi(x)$, absurde !

(4) On note pour commencer que α est nécessairement différent de $-\alpha$, sinon $2\alpha = 0$, donc $\alpha = 0$. De façon analogue à la question (1) de l'exercice 12, on montre que $K[\alpha]$ est un sous-corps de $\mathbb{R}$, et de façon analogue à la question (2) de ce même exercice, l'application $x + y\alpha \mapsto x - y\alpha$ est un automorphisme de corps non trivial. Il découle donc de la question précédente que $K[\alpha]$ est un sous-corps propre de $\mathbb{R}$. Plus généralement, $\mathbb{R}$ n'est pas un espace de dimension finie ≥ 2 sur un sous-corps (Artin).

Exercice 15.

(1) Le morphisme d'évaluation $P(X) \mapsto P(a)$ est surjectif et de noyau $(X - a)$.

(2) Dans $K[X]/(X^n)$, on a $\overline{X} \neq 0$ mais $\overline{X}^n = 0$, donc $\overline{X}$ est un diviseur de zéro.

(3) Tout élément de $K[X]/(X^2)$ s'écrit $a + b\overline{X}$. Observons que $(a + b\overline{X})(a - b\overline{X}) = a^2 - b^2\overline{X}^2 = a^2$. Ainsi, si a est non nul, $a+b\overline{X}$ est inversible. Récirproquement, s'il existe $u+v\overline{X}$ tel que $(a + b\overline{X})(u + v\overline{X}) = 1$, alors $au + (av + bu)\overline{X} = 1$ donc $au = 1$ donc a est non nul.

Exercice 16.

(1) On suppose que I est maximal. Soit $a \in A$, $a \neq 0$. Si a n'appartient pas à I, alors l'idéal de A engendré par a et I est A tout entier (par maximalité de I), donc contient 1. Donc il existe $x, y \in A$ et $z \in I$ tels que $xa + yz = 1$, donc x est l'inverse de a modulo I. Ainsi, tout élément non trivial de A/I est inversible, ce qui démontre que A/I est un corps.

(2) On suppose que A/I est un corps. Soit J un idéal de A contenant I. S'il existe un élément $a \in J$ qui n'est pas dans I, alors $\bar{a}$ est inversible, donc il existe $x \in A$ tel que $\bar{x}\bar{a} = \bar{1}$. Ainsi, $xa - 1 = z$ pour un certain $z \in I$, donc $1 = xa - z$. Comme a appartient à J et I est contenu dans J, 1 appartient à J, donc $J = A$, ce qui prouve la maximalité de I.

Exercice 17. On définit $\varphi : A \to A/I \times A/J$ par $\varphi(a) = (\overline{a}, \overline{a})$. Son noyau est $I \cap J$, et elle est surjective car $I + J = A$. On conclut grâce à la propriété universelle du quotient.