Université de Strasbourg
Adriano Marmora, marmora@math.unistra.fr

Master 1 Semestre 1, 2026-2027
Feuille de TD

Algèbre I

Anneaux

Exercice 1. Soit A un anneau unitaire. Alors $1_A = 0_A$ si et seulement si $A = \{0_A\}$.

Exercice 2. Soit V un k-espace vectoriel, en particulier V est un groupe abélien. On note $\mathrm{End}_{\mathbb{Z}}(V)$ l'anneau des homomorphismes de groupes de V dans V et on note $\mathrm{End}_k(V)$ l'anneau des applications k-linéaires de V dans V. Alors $\mathrm{End}_k(V)$ est un sous-anneau de $\mathrm{End}_{\mathbb{Z}}(V)$. Est-ce un idéal ? Et si k est $\mathbb{Q}$? un corps fini ? un corps $\mathbb{F}_p$ (p premier) ?

Exercice 3. (exercice fleuve) Calculer l'anneau $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z})$ et l'anneau $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z})$. Puis l'anneau $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ (n premier puis n puissance d'un nombre premier). Calculer $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}\times\mathbb{Z})$. Si p est premier, calculer $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}\times \mathbb{Z}/p\mathbb{Z})$, $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z})$, $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/p^k\mathbb{Z} \times \mathbb{Z}/p^\ell\mathbb{Z})$. Si n et m sont permiers entre eux, alors $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$ est « naturellement » isomorphe à $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z})$. Étudier encore l'anneau $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$ lorsque n divise m. Continuer autant que vous le pouvez afin de pouvoir répondre à la question suivante : pour G un groupe abélien de type fini, quand est-ce que $\mathrm{End}_{\mathbb{Z}}(G)$ est commutatif ?

Exercice 4. Décrire, « le plus possible », les anneaux $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$, $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}]$, $\mathbb{C}[\mathfrak{S}_3]$, etc.

Exercice 5. L'ensemble R des nombres rationels de la forme a/b où b n'est *pas* un multiple de 6 est-il un sous-anneau de $\mathbb{Q}$?

Exercice 6. Soient A un anneau unitaire et I un idéal à gauche et S un sous-ensemble de A. Alors l'ensemble, noté IS, égal au sous-groupe additif engendré par $\{xs\}_{x\in I, s\in S}$, est un idéal à gauche. Si S est un idéal à droite, alors IS est un idéal bilatère.

Exercice 7. Soit A un anneau non nul (commutatif et unitaire). Soit $S \subset A$ un sous-ensemble stable par multiplication et ne contenant pas 0. Il existe alors $\mathfrak{p}$ un idéal maximal parmi les idéaux ayant une intersection vide avec S. Tout tel idéal est premier.

Exercice 8. Soit A un anneau intègre (commutatif et unitaire) et soit S un sous-ensemble de $A \smallsetminus \{0_A\}$ stable par multiplication. Alors l'ensemble $S^{-1}A$ des éléments du corps des fractions de A qui s'écrivent a/s avec $a \in A$ et $s \in S$ est un anneau.

Exercice 9. Soit A un anneau principal (intègre, commutatif est unitaire) et soit $S \subset A \smallsetminus \{0_A\}$ un sous-ensemble stable par multiplication. Alors l'anneau $S^{-1}A$ est principal.

Exercice 10. Soit A un anneau factoriel (intègre, commutatif est unitaire) et soit $S \subset A \smallsetminus \{0_A\}$ un sous-ensemble stable par multiplication. Alors l'anneau $S^{-1}A$ est factoriel ; ses éléments irréductibles sont les $p \in A$ tel que $(p) \cap S = \emptyset$.

Exercice 11. Soit A un anneau factoriel et $p \in A$ irréductible. Alors $S = A \smallsetminus (p)$ est stable par multiplication et l'anneau $S^{-1}A$ est principal.

Exercice 12. Dans un anneau principal A, soient $a_1, \ldots, a_n$ des éléments de A et soit d tel que $(d) = (a_1, \ldots, a_n)$ alors d est le plus grand diviseur commun à $a_1, \ldots, a_n$.

Exercice 13. Le groupe des inversibles de l'anneau $\mathbb{Z}/p^r\mathbb{Z}$ est cyclique si $p \geq 3$ est premier et est $\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$ si $p = 2$. (Si $p \geq 3$, alors ce groupe est engendré par $1 + p$ et un groupe cyclique d'ordre $p - 1$; si $p = 2$ alors il est le produit du groupe engendré par 5 et du groupe engendré par -1.)

Exercice 14. Soit K un anneau commutatif (unitaire) et soit R l'ensemble des fonctions de $\mathbb{N}^*$ dans K (pas nécessairement à support fini). On munit R de l'addition usuelle des fonctions et du produit de convolution : si $f, g \in R$ et si $m \in \mathbb{N}^*$

$$f * g(m) = \sum_{xy=m} f(x)g(y).$$

Alors R est un anneau commutatif dont l'unité est la fonction $\delta : \mathbb{N}^* \to K$ telle que $\delta(1) = 1_K$ et $\delta(m) = 0_K$ pour tout $m \geq 2$. Si K est intègre alors R l'est aussi.
Une fonction $f : \mathbb{N}^* \to K$ est dite *multiplicative* si $f(mn) = f(m)f(n)$ pour tous $m, n \in \mathbb{N}^*$ *premiers entre eux*. Si f et g sont multiplicatives, alors $f * g$ est multiplicative. Deux fonctions multiplicatives sont égales si et seulement si elles coïncident sur les puissances des nombres premiers.
La *fonction de Möbius* est la fonction $\mu : \mathbb{N}^* \to K$ tel que $\mu(1) = 1_K$, $\mu(n) = (-1_K)^r$ si n est le produit de r nombres premiers deux à deux distincts et $\mu(n) = 0$ sinon (c'est-à-dire s'il existe p premier tel que p^2 divise n). Alors μ est multiplicative. Soit $\phi \in R$ la fonction constante égale à 1_K. Alors $\mu * \phi = \delta$ (le vérifier d'abord sur les puissances des nombres premiers). Expliciter l'égalité $\mu * (\phi * f) = f$ (« formule d'inversion de Möbius »).

Exercice 15. Lorsque A est un anneau commutatif unitaire (pas nécessairement intègre), calculer $A[X]^*$.

Exercice 16. Soit B un anneau et A un sous-anneau de B. On dit qu'un élément $b \in B$ est *entier sur* A s'il existe $n \in \mathbb{N}^*$ et $a_0, \ldots, a_{n-1}$ dans A tels que

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

Un anneau intègre A (commutatif et unitaire) est dit *intégralement clos* si tout élément de $K = \mathrm{Frac}(A)$ qui est entier sur A appartient à A.

— Un anneau factoriel est intégralement clos.
— Soit $d \in \mathbb{Z} \setminus \{0\}$ est un entier sans facteur carré, on pose $\mathbb{Z}[\sqrt{d}] = \{x \in \mathbb{C} \mid \exists a, b \in \mathbb{Z}, x = a + b\sqrt{d}\}$. Si $d = 1 \mod 4$, alors $\mathbb{Z}[\sqrt{d}]$ n'est pas intégralement clos.

Exercice 17. Dans un anneau factoriel A, on a, pour tous a, $b \in A$, $ab = \mathrm{pgcd}(a, b)\,\mathrm{ppcm}(a, b)$.

Exercice 18. Soit A un anneau euclidien relativement à v. Soit $K = \mathrm{Frac}(A)$ et soit $s \in A \setminus \{0\}$. Alors $A_s = \{x \in K \mid \exists a \in A, n \in \mathbb{N}, x = \frac{a}{s^n}\}$ est un anneau euclidien.

Exercice 19. Soit k un corps. Étudier l'irréductibilité des polynômes suivant dans $k[X, Y]$: $Y - X^2$, $X^2 + Y^2 + 1$, $X^2 + Y^2 - 1$, $X^2 - Y^2 - 1$, $Y^2 - X^3$, $X^3 - Y^2 - X$, $XY^3 - X^2Y - Y^2 + X$.

Exercice 20. Soit A l'anneau $\mathbb{C}[X, Y]/(Y^2 - X^3)$, notons x et y les images de X et Y dans A.
— Montrer qu'on définit un morphisme de A dans $\mathbb{C}[T]$ en posant $\phi(x) = T^2$ et $\phi(y) = T^3$. Montrer que ϕ est injectif. Quel est son image ?
— Montrer que $\mathrm{Frac}(A)$ est isomorphe à $\mathbb{C}(T)$. En déduire que A n'est pas intégralement clos (utiliser **Exercice 16** et considérer l'élément T de $\mathrm{Frac}(A)$).

Exercice 21. L'anneau $\mathbb{C}[X, Y]/(X^3 - Y^2 - X)$ n'est pas factoriel (si x, y sont les images de X et Y, montrer que y est irréductible mais que (y) n'est pas premier car $y^2 = x(x - 1)(x + 1)$).

Exercice 22. Les anneaux $\mathbb{C}[X, Y]/(Y - X^2)$ et $\mathbb{C}[X, Y]/(XY - 1)$ sont factoriels et même principaux (trouver des anneaux plus simples auquel ils sont isomorphes).

Exercice 23. Soient P et Q dans $\mathbb{C}[X, Y]$ sans facteur commun.
— Il existe A, B dans $\mathbb{C}[X, Y]$ et D dans $\mathbb{C}[X]$ avec $D \neq 0$ et $D = AP + BQ$ (travailler dans l'anneau $\mathbb{C}(X)[Y]$).
— En déduire que $V = \{(x, y) \in \mathbb{C}^2 \mid P(x, y) = Q(x, y) = 0\}$ est fini.

Exercice 24. Montrer que $\mathbb{C}[X, Y]/(X^2 + Y^2 + \varepsilon)$ est principal pour $\varepsilon = \pm 1$ (par un changement de variables se ramener à $XY - 1$, voir **Exercice 22**)

Exercice 25. Montrer que $\mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ n'est pas factoriel.

Corps

Exercice 26. Soit α la classe de X dans $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$. Alors $(1, \alpha)$ est une base du $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_4$. Les éléments de $\mathbb{F}_4$ sont $\{0, 1, \alpha, 1 + \alpha\}$. Donner leurs polynômes minimaux.

Exercice 27. Identifier le sous-groupe additif sous-jacent au corps $\mathbb{F}_4$.

Exercice 28. Écrire les tables d'addition et de multiplication de $\mathbb{F}_4$ et de $\mathbb{Z}/4\mathbb{Z}$; les comparer.

Exercice 29. Trouver une racine treizième de 3 dans le corps $\mathbb{F}_{13}$.

Exercice 30.

(1) Vérifier que le polynôme $P = X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.
(2) Soit β la classe de X dans le corps $\mathbb{F}_8 = \mathbb{F}_2[X]/(P)$; alors $(1, \beta, \beta^2)$ est une base du $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_8$.
(3) Les éléments de $\mathbb{F}_8$ sont alors
$$\{0, 1, \beta, 1 + \beta, \beta^2, 1 + \beta^2, \beta + \beta^2, 1 + \beta + \beta^2\}.$$
(4) Donner le polynôme minimal de chacun de ces éléments.

Exercice 31. Déterminer le nombre de polynômes irréductibles (et unitaires) de degré 3 dans le corps $\mathbb{F}_3$.

Exercice 32. Trouver des factorisations de $X^9 - X$ et de $X^{27} - X$ dans $\mathbb{F}_3$. Montrer que les facteurs de vos factorisations sont irréductibles.

Exercice 33. Factoriser $X^{16} - X$ dans $\mathbb{F}_4$ puis dans $\mathbb{F}_8$.

Exercice 34. Soit K un corps fini. Le produit des éléments non nuls de K est égal à -1.

Exercice 35. Tout élément de $\mathbb{F}_p$ a exactement une racine p-ième.

Exercice 36. Faire ces questions *sans* utiliser les résultats sur les corps finis.

(1) Soit $F = \mathbb{F}_p$, quel est le nombre de polynômes irréductibles et unitaires de degré 2 à coefficients dans F ?
(2) Soit $f(X)$ l'un de ces polynômes (le nombre trouvé à la question précédente est strictement positif !). Montrer que $K = F[X]/(f)$ est un corps à p^2 éléments et que tous ses éléments s'écrivent d'une seule manière sous la forme $a + b\alpha$ où a, b sont dans F et α est la classe de X dans K. Montrer que tout élément de la forme $a + b\alpha$ avec $b \neq 0$ est la racine d'un polynôme irréductible de degré 2 dans $F[X]$.
(3) Montrer que tout polynôme de degré 2 dans $F[X]$ a une racine dans $\mathbb{K}$.
(4) Montrer que tous les corps K obtenus par la construction des questions précédentes sont isomorphes.