MAT35B - L3A ALGÈBRE
Premier semestre — 2022-2023

Fiche 6: Anneaux commutatifs

Dans cette fiche, tous les anneaux seront unifères et commutatifs.

1. Soit A un anneau. On rappelle que la **caractéristique** de A est l'entier naturel $\mathrm{car}(A)$ tel que $\mathrm{car}(A)\mathbb{Z}$ soit le noyau du morphisme $\Theta_A : \mathbb{Z} \to A$ défini par $\Theta_A(k) = k1_A$ pour $k \in \mathbb{Z}$.

(a) Quel est le plus petit sous-anneau de A ? À quoi est-il isomorphe ? Distinguer selon que 1_A est ou non d'ordre fini dans le groupe $(A, +)$.

(b) Montrer si A est intègre, $\mathrm{car}(A)$ est 0 ou un nombre premier.

(c) Soit $p \in \mathbb{N}$ un nombre premier. Quels sont les anneaux de cardinal p à isomorphisme près ?

2. Pour a et b dans $\mathbb{N}^*$, à quelle condition existe-t-il un morphisme d'anneaux de $\mathbb{Z}/a\mathbb{Z}$ dans $\mathbb{Z}/b\mathbb{Z}$?

3. Soit A un anneau non nul.

(a) On suppose que A est fini. Soit $a \in A \setminus \{0\}$. Montrer que a est soit inversible, soit diviseur de zéro dans A. En déduire que A est un corps si et seulement si A est intègre.

(b) Cela reste-t-il toujours vrai pour un anneau infini ?

(c) Soit $a \in A$. Montrer que si a est nilpotent, alors $1_A - a$ est inversible.

4. Soit K un corps. Soit G un sous-groupe fini de $K^\times$. Le but de l'exercice est de montrer que le groupe G est cyclique. On note $|G| = n$.

(a) On note e l'exposant de G, *i.e.* le plus petit des entiers d tel que $g^d = 1$ pour tout $g \in G$. En utilisant le polynôme $X^e - 1$ montrer que $n \leq e$.

(b) Montrer que $e = n$.
Indication : e est le PPCM des ordres des éléments de G.

(c) Montrer que le groupe G contient un élément d'ordre e et conclure.

5. Soient A un anneau et $S \in A[X]$.

(a) Vérifier que $(S) = SA[X]$ est un sous-groupe de $(A[X], +)$ et que $A[X]/(S)$ possède une structure d'anneau déduite de celle de $A[X]$, faisant de la projection canonique $\pi : A[X] \to A[X]/(S)$ un morphisme d'anneaux.

(b) Montrer que si le polynôme S est unitaire de degré d, la restriction de π à $A[X]_{\leq d-1}$ est bijective, *i.e.* $A[X]_{\leq d-1}$ est un système de représentants de $A[X]/(S)$.

6. On considère les polynômes $P_1 = X^2$, $P_2 = X^2 + X$, $P_3 = X^2 + 1$ et $P_4 = X^2 + X + 1$ dans $(\mathbb{Z}/2\mathbb{Z})[X]$. Pour tout $i \in [\![1, 4]\!]$, on note $A_i = (\mathbb{Z}/2\mathbb{Z})[X]/(P_i)$.

(a) Montrer que ces anneaux ont exactement 4 éléments.

(b) Parmi les anneaux A_1, A_2, A_3, A_4, $(\mathbb{Z}/2\mathbb{Z})^2$ et $\mathbb{Z}/4\mathbb{Z}$, lesquels sont isomorphes ? Lesquels sont des corps ?

7. Soit A un anneau de cardinal 4 non isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

(a) Montrer que la caractéristique de A est 2.

(b) Montrer qu'il existe un élément a de A tel que $A = \{0_A, 1_A, a, a + 1_A\}$.

(c) Montrer qu'il existe un unique morphisme d'anneau $\phi : (\mathbb{Z}/2\mathbb{Z})[X] \to A$ tel que $\phi(X) = a$.

(d) Montrer que $\mathsf{Ker}(\phi)$ contient un unique polynôme S de degré 2.

(e) En déduire un isomorphisme $\bar{\phi} : (\mathbb{Z}/2\mathbb{Z})[X]/(S) \to A$.

(f) Combien y a-t-il d'anneaux de cardinal 4 à isomorphisme près ?

8. On considère les polynômes $P_1 = X^2 - 1$, $P_2 = X^2 + X + 1$, $P_3 = X^2 + 1$, $P_4 = X^2 - 5X + 6$ et $P_5 = X^2 + 2X + 1$ dans $\mathbb{R}[X]$. Pour tout $i \in [\![1, 5]\!]$, on note $A_i = \mathbb{R}[X]/(P_i)$. Parmi ces anneaux, lesquels sont isomorphes entre eux ?

9. Étant donné un élément $\alpha \in \mathbb{R}$ et un sous-anneau $A \subseteq \mathbb{R}$, on définit l'application $\mathsf{ev}_\alpha^A : A[X] \to \mathbb{R}$ qui associe $P(\alpha) \in \mathbb{R}$ à $P \in A[X]$.

(a) Montrer que $\mathsf{ev}_{A,\alpha}$ est un morphisme d'anneaux.

(b) On fixe désormais $\alpha = \sqrt{2}$. Déterminer le noyau I_1 du morphisme $\mathsf{ev}_\alpha^{\mathbb{R}}$. L'idéal I_1 est-il premier ? maximal ?

(c) Déterminer le noyau I_2 du morphisme $\mathsf{ev}_\alpha^{\mathbb{Q}}$. L'idéal I_2 est-il premier ? maximal ?

(d) (i) Déterminer le noyau I_3 du morphisme $\mathsf{ev}_\alpha^{\mathbb{Z}}$. L'idéal I_3 est-il premier ? maximal ?

(ii) Donner un idéal maximal de $\mathbb{Z}[X]$ qui contient I_3.

(iii) Existe-t-il un idéal maximal de $\mathbb{Z}[X]$ contenant $X + 1$ et I_3 ?

(iv) Existe-t-il un idéal maximal de $\mathbb{Z}[X]$ qui contient $X + 4$ et I_3 ?

10. Soient K un corps et $P \in K[X]$ un polynôme de degré 2 ou 3 sans racine dans K. Montrer que P est irréductible dans $K[X]$. Donner un contre-exemple avec un polynôme de degré 4.

11. On considère les polynômes suivants dans $\mathbb{Z}[X]$:

(a) $P_1 = X^4 - 6X^2 + X - 1$,

(b) $P_2 = X^4 + X^3 - X^2 + 7X - 1$,

(c) $P_3 = 2X^5 + 3X^4 + 8X^3 - 2X^2 + 5X - 1$,

(d) $P_4 = X^5 - 6X^3 + 2X^2 - 4X + 5$.

Lequels sont irréductibles ?

Indication : on pourra utiliser le morphisme d'anneau de $\mathbb{Z}[X]$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$ qui envoie X sur X, où $p \in \mathbb{N}^*$ est premier.

12. Soient A anneau intègre et deux éléments non nuls de A. On suppose que a et b possèdent un PPCM m dans A.

(a) Montrer qu'il existe un unique $d \in A$ tel que $ab = md$.

(b) Montrer que d est un PGCD de a et b.

13. (a) Soit A un anneau principal. Soient a et b deux éléments non nuls de A et d un diviseur commun d de a et b. Montrer que d est un PGCD de a et b si et seulement s'il existe deux éléments u et v de A tels que $d = au + bv$.

(b) Dans $\mathbb{Z}[X]$, quel est le PGCD de 2 et X ? L'anneau $\mathbb{Z}[X]$ est-il principal ?

(c) Dans $\mathbb{R}[X, Y]$, quel est le PGCD de X et Y ? L'anneau $\mathbb{R}[X, Y]$ est-il principal ?

14. (*a*) Dans l'anneau $\mathbb{Z}[X]$ existe-t-il des idéaux premiers non nuls et non maximaux ?

(*b*) Mêmes questions dans l'anneau $\mathbb{R}[X, Y]$.

15. Soit A un anneau. Montrer que $A[X]$ est principal si et seulement si A est un corps. On pourra considérer le morphisme d'évaluation en 0 de $A[X]$ dans A ou bien regarder pour chaque $a \in A \setminus \{0\}$ l'idéal $I_a = aA[X] + XA[X]$.

16. Soit K un corps. On considère l'anneau $A = K[X, Y]/(Y^2 - X^3)$ et on considère le morphisme d'anneaux $f : K[X, Y] \to K[T]$ défini par $f(P(X, Y)) = P(T^2, T^3)$.

(*a*) (i) Le morphisme f est-il surjectif ?

(ii) Montrer que f fournit un morphisme $\bar{f} : A \to K[T]$ par passage au quotient.

(iii) Montrer que le morphisme $\bar{f}$ est injectif.

(*b*) L'anneau quotient $A = K[X, Y]/(Y^2 - X^3)$ est-il intègre ?

(*c*) Montrer que $(\bar{X}, \bar{Y})$ est un idéal premier de A.

(*d*) Montrer que $\bar{X}$ et $\bar{Y}$ ont un PGCD mais pas de PPCM dans l'anneau A.

17. *Une construction du corps des nombres réels à partir du corps des rationnels.* Soient A l'ensemble des suites de Cauchy de rationnels et I l'ensemble des suites de rationnels convergeant vers 0. On admet que A est un sous-anneau de $\mathbb{Q}^{\mathbb{N}}$ et que toute suite de Cauchy est bornée. Montrer que I est un idéal maximal de A et que $\mathbb{Q}$ est isomorphe à un sous-corps de A/I.

Indication : montrer que si $u \in A \setminus I$, alors u n'a qu'un nombre fini de termes nuls et la suite v définie par $v_n = 1/u_n$ si $u_n \neq 0$ et $v_n = 0$ si $u_n = 0$ appartient à A.