ÉNS de Lyon
M2 FEADEP

Cours d'algèbre
2018-2019

Feuille d'exercices n°7 : Anneaux

Dans toute cette feuille K est un corps et A est un anneau commutatif unitaire.

À faire

Exercice 1. Trouvez les éléments inversibles, irréductibles, premiers, diviseurs de 0, nilpotents, idempotents des anneaux suivants :

$$\mathbb{Z}/n\mathbb{Z}, \qquad K, \qquad K[X], \qquad \mathcal{M}_2(K).$$

Exercice 2.

1. Soit I un idéal de A. Montrer que :
   (a) I est premier $\iff A/I$ est intègre.
   (b) I est maximal $\iff A/I$ est un corps.
2. Soit $J = (a)$ un idéal principal de A engendré par $a \in A$. Montrer que :
   (a) $J = (a)$ est un idéal premier $\iff a$ est un élément premier.
   (b) $J = (a)$ est un idéal maximal parmi les idéaux propres principaux $\iff a$ est un élément irréductible.
3. En déduire qu'un anneau est intègre (resp. un corps) si, et seulement si, 0 est premier (resp. maximal).

Exercice 3. Montrer qu'un anneau fini intègre est un corps.

Exercice 4. ***(Quotients d'un anneau)***
Soient I, J deux idéaux de A.

1. Montrer que l'image réciproque d'un idéal par un morphisme d'anneaux est un idéal.
2. Décrire les idéaux de l'anneau A/I.
3. Parmi eux, lesquels sont premiers ? maximaux ?
4. Déterminer un isomorphisme naturel entre $A/(I+J)$ et un quotient de A/I.
5. Soit $\varphi : A \to B$ un morphisme d'anneaux. Trouver une condition suffisante sur φ pour que l'image de tout idéal de A soit un idéal de B. Donner un contre-exemple lorsque celle-ci n'est pas satisfaite.

Exercice 5. ***(Double quotient d'un anneau)***

1. Soient I, J deux idéaux de A. On note $\pi_I : A \to A/I$ et $\pi_J : A \to A/J$ les projections canoniques. Montrer que les anneaux $(A/I)/\pi_I(J)$ et $(A/J)/\pi_J(I)$ sont canoniquement isomorphes.
2. Soit $P \in \mathbb{Z}[X]$ unitaire irréductible et α une racine de P dans $\mathbb{C}$. Donner un critère pour qu'un nombre premier p soit toujours premier dans $\mathbb{Z}[\alpha]$.
3. Pour un entier $n \geq 3$, montrer que 2 est toujours irréductible dans $\mathbb{Z}[i\sqrt{n}]$.
4. En déduire que $\mathbb{Z}[i\sqrt{n}]$ n'est pas factoriel.
   Indication : on pourra distinguer les cas n pair et n impair.

Exercice 6. ***(Relations de Bézout explicites)***

1. Soient $a, b \in \mathbb{N}^*$ premiers entre eux. Déterminer explicitement l'application réciproque $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/35\mathbb{Z}$ de l'application canonique $\mathbb{Z}/35\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.
2. Déterminer toutes les racines carrées de -1 dans $\mathbb{Z}/5\mathbb{Z}$ et de 2 dans $\mathbb{Z}/7\mathbb{Z}$. En déduire la liste des entiers dans $\mathbb{Z}$ dont le carré est congru à 9 modulo 35.
3. Dans l'anneau euclidien $\mathbb{Z}[i]$, déterminer un PGCD et une relation de Bézout du couple $(3+i, 1+3i)$.

Exercice 7. ***(Stabilité des propriétés d'anneaux)***

1. Montrer que l'anneau $A[X]$ est principal si, et seulement si, A est un corps.
2. Plus généralement, parmi les propriétés euclidien/principal/factoriel/noethérien, lesquelles sont stables par sous-anneau ? anneau quotient ?
3. Montrer qu'un anneau factoriel dans lequel tout couple de nombres premiers entre eux admet une relation de Bézout est principal.

Exercice 8.

1. Soit $u \in A^\times$ et $n \in A$ un élément nilpotent. Montrer que $u+n$ est inversible.
2. Décrire l'inverse de $1-n$ lorsque n est nilpotent, puis calculer $8^{-1} \mod 243$.
3. Soit $P = \sum_{k=0}^{n} a_k X^k \in A[X]$. Montrer que P est inversible si, et seulement si, a_0 est inversible et $a_1, \dots, a_n$ sont nilpotents.

Exercice 9. ***(Morphismes d'anneaux)***

1. Soit $f : A \to B$ un morphisme d'anneaux.
   (a) Montrer que f induit un morphisme de groupes $f' : A^\times \to B^\times$.
   (b) On suppose que f est surjective. Á-t-on f' également surjective ?
2. Soient $m, n \in \mathbb{N}^*$.
   (a) Déterminer l'ensemble des morphismes de groupes, et d'anneaux $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.
   (b) Déterminer l'ensemble des morphismes de groupes, et d'anneaux $\mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$.

Exercice 10. ***(Éléments irréductibles de*** $\mathbb{Z}[i]$***)***

1. Justifier que l'anneau $\mathbb{Z}[i]$ est euclidien.
2. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?
3. Montrer que tout élément irréductible de $\mathbb{Z}[i]$ divise dans $\mathbb{Z}[i]$ un élément irréductible de $\mathbb{Z}$.
4. Soit p un nombre premier dans $\mathbb{Z}$ qui est réductible dans $\mathbb{Z}[i]$.
   (a) Montrer que p est le produit de deux irréductibles de $\mathbb{Z}[i]$ complexes conjugués l'un de l'autre.
   (b) Á quelle condition sont-ils associés dans $\mathbb{Z}[i]$?
5. Décrire les éléments irréductibles de $\mathbb{Z}[i]$.

Exercice 11. ***(Un exemple d'anneau ni factoriel, ni noethérien)***

1. Montrer que pour un corps K quelconque, $K[X^2, X^3] \subset K[X]$ n'est pas factoriel malgré l'existence d'une décomposition en irréductibles. Que peut-on même remarquer sur cette décomposition en irréductibles ?
2. Soit $\mathcal{H}(\mathbb{C})$ l'anneau des fonctions entières sur $\mathbb{C}$ (i.e. fonctions holomorphes définies sur $\mathbb{C}$ entier).
   (a) Montrer que $\mathcal{H}(\mathbb{C})$ est intègre, et trouver ses inversibles.
   (b) Montrer que les irréductibles de $\mathcal{H}(\mathbb{C})$ sont, à inversible près, les fonctions affines $z \mapsto z - z_0$ pour $z_0 \in \mathbb{C}$.
   (c) En déduire que $\mathcal{H}(\mathbb{C})$ n'est ni factoriel, ni noethérien.

Exercice 12. ***(Exemple d'équation de Mordell)***
Dans cet exercice, on cherche à résoudre dans $\mathbb{Z}$ l'équation de Mordell $y^2 = x^3 - 2$.

1. Rappeler pourquoi $\mathbb{Z}[i\sqrt{2}]$ est factoriel.
2. Soit A un anneau factoriel et $a, b \in A$ premiers entre eux tels que $ab = c^n$ pour un certain $n \geq 1$, montrer qu'il existe $u, v \in A^\times$ et $\alpha, \beta \in A$ tels que $a = u\alpha^n$ et $b = v\beta^n$.
3. Soit (x, y) une solution de l'équation de Mordell. Montrer que $(y + i\sqrt{2})$ et $(y - i\sqrt{2})$ sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$ et que ce sont des cubes dans cet anneau.
4. En écrivant explicitement le fait d'être un cube, en déduire que les seules solutions de l'équation dans $\mathbb{Z}$ sont $(3, 5)$ et $(3, -5)$.

Exercice 13. ***(Propriétés de l'indicatrice d'Euler)***

1. Démontrer les propriétés suivantes sur l'indicatrice d'Euler :
   (a) Si $p \in \mathcal{P}$ et $\alpha \in \mathbb{N}^*$, alors $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.
   (b) Si $a \wedge b = 1$, alors $\varphi(ab) = \varphi(a)\varphi(b)$.
   (c) On a $\varphi(n) = n \prod_{\substack{p \in \mathcal{P} \\ p|n}} \left(1 - \frac{1}{p}\right)$.
   (d) On a $n = \sum_{d|n} \varphi(d)$.
2. En déduire les théorèmes suivants :
   (a) (Théorème d'Euler) Pour tout $a \wedge n = 1$, on a $a^{\varphi(n)} \equiv 1 \mod n$.
   (b) (Théorème de Fermat) Pour tout $p \in \mathcal{P}$ et tout $a \wedge p = 1$, on a $a^{p-1} \equiv 1 \mod p$.
   (c) (Théorème de Wilson) Pour $a \in \mathbb{N}^*$, on a $(a-1)! \equiv -1 \mod a \iff a$ est premier.
   (d) (Théorème RSA) Soient $p, q \in \mathcal{P}$ tels que $p \neq q$ et $n = pq$. Alors pour tous $d, e \in \mathbb{Z}$, on a $de \equiv 1 \mod \varphi(n) \Longrightarrow \forall m \in \mathbb{Z},\ m^{de} = m \mod n$.

Problèmes

Exercice 14. ***(Structure des*** $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$***)***
Soit p un nombre premier dans $\mathbb{Z}$ et $\alpha \in \mathbb{N}^*$.

1. On suppose que p est impair.
   (a) Montrer que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.
   (b) Montrer que pour tout $\beta \in \mathbb{N}^*$, il existe $m \in \mathbb{Z}$ tel que $m \wedge p = 1$ et $(1+p)^{p^\beta} = 1 + mp^{\beta+1}$.
   (c) En l'ordre de $\overline{p+1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.
   (d) Montrer que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ contient un élément d'ordre $p-1$.
   Indication : On pourra considérer un antécédent d'un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ *par la surjection canonique* $\psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$.
   (e) En déduire que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.
2. On suppose désormais $p = 2$. Décrire $(\mathbb{Z}/2\mathbb{Z})^\times$ et $(\mathbb{Z}/4\mathbb{Z})^\times$.
3. On suppose $\alpha \geq 3$. Soit $\psi : (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ et $U(\alpha)$ le noyau de ψ.
   (a) Montrer que pour tout $\beta \in \mathbb{N}^*$, il existe $m \in \mathbb{Z}$ impair tel que $5^{2^\beta} = 1 + m2^{\beta+1}$.
   (b) En déduire $U(\alpha)$ est un groupe cyclique d'ordre $2^{\alpha-2}$ engendré par $\overline{5}$.
   (c) Justifier l'isomorphisme de groupes $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/4\mathbb{Z})^\times \times U(\alpha)$.

Exercice 15. ***(Un exemple d'anneau principal non euclidien)***
On démontre d'abord le critère suivant de caractérisation de non-euclidiennité.

1. Soit A un anneau euclidien Montrer qu'il existe un élément non inversible $x \in A$ tel que la restriction à $A^\times \cup \{0\}$ de la projection canonique $A \to A/(x)$ est surjective.

Soit $\alpha = \frac{1+i\sqrt{19}}{2} \in \mathbb{C}$ et $A = \mathbb{Z}[\alpha]$.

2. Calculer $A^\times$.
3. Montrer que A n'est pas euclidien.
4. Soient $a, b \in A \setminus \{0\}$. Montrer qu'il existe des éléments $q, r \in A$ tels que $r = 0$ ou $|r| < |b|$ choisis de sorte que $a = bq + r$ ou $2a = bq + r$.
5. Montrer que $A/(2)$ est un corps.
6. Montrer que A est principal.

Exercice 16. ***(Anneaux d'entiers quadratiques)***
Soit $d \geq 2$ un entier sans facteur carré. On note $\sqrt{d}$ un choix de racine carrée de d dans $\mathbb{C}$ (imaginaire pur si $d < 0$) et $K = \mathbb{Q}(\sqrt{d})$ et $\mathcal{O}_K$ l'ensemble des entiers algébriques de K.

1. Si $d \equiv 2, 3 \mod 4$, montrer que $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.
2. Si $d \equiv 1 \mod 4$, montrer que $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ et trouver le polynôme minimal sur $\mathbb{Z}$ de cet élément.
3. Supposons que $d < 0$. Montrer que $N : z \mapsto |z|^2$ est à valeurs entières sur $\mathcal{O}_K$, et que c'est un stathme euclidien sur $\mathcal{O}_K$ si, et seulement si, $d \in \{-1, -2, -3, -7, -11\}$.
4. Trouver les inversibles de $\mathcal{O}_K$ pour tout $d < 0$.
5. Déterminer les irréductibles de $\mathbb{Z}[i]$, et en déduire quels nombres premiers s'écrivent comme somme de deux carrés d'entiers.
   Indication : On pourra utiliser le fait que $\mathbb{Z}[i]$ est euclidien.
6. Montrer que $\mathbb{Z}[\sqrt{2}]$ a une infinité d'inversibles.

Pour aller plus loin

Exercice 17. ***(Radical d'un idéal)***

1. Montrer que l'ensemble des éléments nilpotents de A forme un idéal de A.
2. Soit I un idéal de A. Soit $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N}; x^n \in I\}$. Montrer que $\sqrt{I}$ est un idéal de A contenant I.
3. Décrire $\sqrt{(0)}$ et calculer $\sqrt{\sqrt{I}}$.
4. Décrire $\sqrt{(\bar{a})}$ dans $\mathbb{Z}/b\mathbb{Z}$ pour $a, b \in \mathbb{N}^*$.
5. Calculer $\sqrt{(X)}$ et $\sqrt{(X^3, Y)}$ dans $\mathbb{C}[X, Y]$.
6. Décrire l'image de $\sqrt{I}$ dans A/I par la projection canonique.
7. Montrer que l'intersection de tous les idéaux premiers de A contenant I est $\sqrt{I}$.
   Indication : montrer que si $x \notin \sqrt{I}$, alors l'ensemble des idéaux contenant I qui n'intersectent pas l'ensemble $\{x^n \mid n \in \mathbb{N}\}$ est non vide, puis que tout élément maximal de cet ensemble est un idéal premier de A.
8. Déterminer les éléments nilpotents de l'anneau $A/\sqrt{(0)}$.

Anneaux locaux

Un anneau est dit *local* s'il admet un unique idéal maximal.

Exercice 18.

1. Pour quels $n \in \mathbb{N}^*$ l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il local ?
2. Tout sous-anneau d'un anneau local est-il un anneau local ?
3. Tout quotient d'un anneau local est-il un anneau local ?
4. Soit $\mathfrak{m}$ un idéal maximal de A et $n \in \mathbb{N}^*$. Montrer que l'anneau $A/\mathfrak{m}^n$ est local.
5. Montrer que s'équivalent :
   (i) l'anneau A est local ;
   (ii) l'ensemble $A \setminus A^\times$ est un idéal de A ;
   (iii) pour tous $a, b \in A$ tels que $a + b = 1$, on a $a \in A^\times$ ou $b \in A^\times$.
6. Si vous connaissez $\mathbb{Z}_p$, montrez que pour tout nombre premier $p \in \mathbb{N}$, l'anneau $\mathbb{Z}_p$ est local.

Exercice 19. On appelle *série formelle* à coefficients dans K la donnée d'une suite dénombrable d'éléments de K. On note $K[[X]]$ l'ensemble des séries formelles à coefficients dans K.

1. Munir $K[[X]]$ d'une structure d'anneau commutatif pour laquelle il existe une injection naturelle de $K[X]$ dans $K[[X]]$.
2. Montrer que l'anneau $K[[X]]$ est intègre et que ses inversibles sont les suites $(x_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$ telles que $x_0 \neq 0$.
3. Soit $K((X))$ le corps des fractions de $K[[X]]$. Montrer que les éléments de $K((X))$ sont les suites $(x_n)_{n\in\mathbb{Z}}$ d'éléments de K pour lesquelles il existe un entier $n_0 \in \mathbb{N}$ tel que $a_n = 0$ pour tout $n < -n_0$.
4. Montrer que l'anneau $K[[X]]$ est local et préciser son idéal maximal.