Université de Rennes 1 — Année universitaire 2019-2020
Licence de mathématiques
Module Anneaux et Arithmétique

Feuille de TD n°2

Exercice 2.1

Soit A un anneau et a un élément de A. Montrer que le sous-anneau de A engendré par $\{a\}$ est $\mathbf{Z}[a]$ (image de $\mathbf{Z}[X]$ par l'unique morphisme d'anneaux $\mathbf{Z}[X] \to A$ qui envoie X sur a). Généraliser au sous-anneau engendré par une partie finie S de A.

Exercice 2.2

Soit E un ensemble et $(A_e)_{e\in E}$ une famille d'anneaux indexée par E, $B := \prod_{e\in E} A_e$ l'anneau produit. Pour tout $e \in E$, on note $\pi_e\colon B \to A_e$ le morphisme d'anneaux (*cf.* cours ou exercice 1.3.2) donné par la projection sur A_e. Soit C un anneau. Montrer que l'application suivante est bijective :

$$\begin{array}{ccc} \mathrm{Hom}_{\mathrm{anneaux}}(C,B) & \longrightarrow & \prod_{e\in E} \mathrm{Hom}_{\mathrm{anneaux}}(C,A_e) \\ \varphi & \longmapsto & (\pi_e \circ \varphi)_{e\in E} \end{array}.$$

Exercice 2.3

1. Soit n un entier positif. Décrire tous les idéaux de $\mathbf{Z}/n\mathbf{Z}$ et les relations d'inclusion entre ces idéaux.
2. Soit $\mathbf{K}$ un corps. Décrire tous les idéaux de $\mathbf{K}[X]/\langle X^4 + 3\,X^3 + 2\,X^2\rangle$ et les relations d'inclusion entre ces idéaux.

Exercice 2.4

On note $\mathcal{C}^\infty(\mathbf{R},\mathbf{R})$ l'ensemble des fonctions de classe $\mathcal{C}^\infty$ sur $\mathbf{R}$.

1. Montrer que cet ensemble, muni de l'addition et de la multiplication ponctuelles, est un anneau.
2. Soit $x_0 \in \mathbf{R}$. Montrer que $\{f \in \mathcal{C}^\infty(\mathbf{R},\mathbf{R}), f(x_0) = 0\}$ est un idéal maximal de $\mathcal{C}^\infty(\mathbf{R},\mathbf{R})$.
3. Soit
$$\mathcal{I} = \{f \in \mathcal{C}^\infty(\mathbf{R},\mathbf{R}), \forall n \in \mathbf{N}, f^{(n)}(x_0) = 0\}$$
Montrer que $\mathcal{I}$ est un idéal premier non nul de $\mathcal{C}^\infty(\mathbf{R},\mathbf{R})$ (idéal des fonctions « plates » en x_0), et construire un morphisme injectif de $\mathcal{C}^\infty(\mathbf{R},\mathbf{R})/\mathcal{I}$ vers $\mathbf{R}[[X]]$. *Note :* on peut en fait construire un isomorphisme de $\mathcal{C}^\infty(\mathbf{R},\mathbf{R})/\mathcal{I}$ sur $\mathbf{R}[[X]]$ (théorème de Borel). On obtient ainsi une interprétation fonctionnelle de l'anneau de séries formelles $\mathbf{R}[[X]]$: c'est l'anneau des fonctions $\mathcal{C}^\infty$ sur $\mathbf{R}$ modulo les fonctions plates en un point fixé.
4. (si vous connaissez la notion de fonction holomorphe) Que se passe-t-il si on s'intéresse aux objets analogues quand on remplace $\mathcal{C}^\infty(\mathbf{R},\mathbf{R})$ par l'anneau des fonctions holomorphes sur $\mathbf{C}$?

Exercice 2.5

On désigne par i un élément de $\mathbf{C}$ tel que $i^2 = -1$. Soit $\mathbf{Z}[i\sqrt{3}]$ l'image dans $\mathbf{C}$ de l'unique morphisme d'anneaux $\mathbf{Z}[X] \to \mathbf{C}$ qui envoie X sur $i\sqrt{3}$.

1. Montrer que $\mathbf{Z}[i\sqrt{3}]$ est un anneau intègre isomorphe à $\mathbf{Z}[X]/\langle X^2+3\rangle$ et que
$$\mathbf{Z}[i\sqrt{3}] = \{a + i\,b\,\sqrt{3}\}_{(a,b)\in\mathbf{Z}^2}.$$
2. Montrer que l'application
$$N\colon \begin{array}{ccc} \mathbf{Z}[i\sqrt{3}] & \longrightarrow & \mathbf{N} \\ z & \longmapsto & z\bar{z} \end{array}$$
est bien définie et vérifie
$$\forall (z_1, z_2) \in \mathbf{Z}[i\sqrt{3}]^2, \quad N(z_1 z_2) = N(z_1)N(z_2).$$
En déduire les éléments de $\mathbf{Z}[i\sqrt{3}]^\times$.
3. Montrer que l'équation
$$a^2 + 3b^2 = 2, \quad (a, b) \in \mathbf{Z}^2$$
n'a pas de solution. En déduire que 2 est un élément irréductible de $\mathbf{Z}[i\sqrt{3}]$.
4. Montrer que $2\mathbf{Z}[i\sqrt{3}]$ n'est pas un idéal premier de $\mathbf{Z}[i\sqrt{3}]$ de deux façons différentes :
   (a) en calculant le quotient $\mathbf{Z}[i\sqrt{3}]/2\mathbf{Z}[i\sqrt{3}]$;
   (b) en utilisant la relation $4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$.

Exercice 2.6

Soit p un nombre premier et $\mathbf{Z}_{(p)} = \left\{\frac{a}{b}\right\}_{a\in\mathbf{Z},\, b\in\mathbf{Z}\setminus p\mathbf{Z}}$ (*cf.* l'exercice 1.7.3). Décrire l'ensemble des éléments irréductibles de $\mathbf{Z}_{(p)}$. Combien y a-t-il de classes d'éléments irréductibles pour la relation d'association ? Énoncer et démontrer un théorème de « factorisation unique » dans $\mathbf{Z}_{(p)}$.

Exercice 2.7

Soit x un entier non nul et $\mathbf{Z}\left[\frac{1}{x}\right]$ l'image de $\mathbf{Z}[X]$ par l'unique morphisme d'anneaux de $\mathbf{Z}[X]$ vers $\mathbf{Q}$ envoyant X sur $\frac{1}{x}$ (*cf.* l'exercice 1.7.2). Décrire l'ensemble des classes d'éléments irréductibles pour la relation d'association. Énoncer et démontrer un théorème de « factorisation unique » dans $\mathbf{Z}\left[\frac{1}{x}\right]$

Exercice 2.8

Résoudre l'équation $x^3 = 2, \quad x \in A$ où A désigne successivement l'un des anneaux suivants (et 2 désigne l'image de 2 dans A par l'unique morphisme d'anneaux $\mathbf{Z} \to A$) :
$$\mathbf{R}, \quad \mathbf{Q}, \quad \mathbf{Q}[X]/\langle X^3 - 2\rangle, \quad \mathbf{C}, \quad \mathbf{Z}/n\mathbf{Z} \quad (n \in \{5, 10, 35, 25, 125\})$$

Exercice 2.9

Pour tout anneau A, on note $\mathrm{car}(A) \in \mathbf{N}$ la caractéristique de A.

1. Soit A un anneau et n un entier positif. Montrer que les conditions suivantes sont équivalentes :

   (a) A est de caractéristique n ;
   (b) (si $n > 0$) 1_A est d'ordre n en tant qu'élément du groupe $(A, +)$;
   (c) A contient un sous-anneau isomorphe à $\mathbf{Z}/n\mathbf{Z}$.
2. Donner les caractéristiques de l'anneau nul, de $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ et $\mathbf{Z}/n\mathbf{Z}$ ($n \in \mathbf{N}$).
3. Montrer que la caractéristique d'un anneau intègre est soit nulle, soit un nombre premier.
4. Soit A un anneau et B un sous anneau de A. Montrer que $\mathrm{car}(A) = \mathrm{car}(B)$.
5. Soit $\varphi\colon A \to B$ un morphisme d'anneaux. Montrer que $\mathrm{car}(B)$ divise $\mathrm{car}(A)$.
6. Soit A un anneau. Exprimer $\mathrm{car}(A[X])$ en fonction de $\mathrm{car}(A)$.
7. Soit A et B des anneaux. Exprimer $\mathrm{car}(A \times B)$ en fonction de $\mathrm{car}(A)$ et $\mathrm{car}(B)$.
8. Soit E un ensemble et A un anneau. Exprimer $\mathrm{car}(A^E)$ en fonction de $\mathrm{car}(A)$.
9. Soit E un ensemble et $(A_e)_{e\in E}$ une famille d'anneaux indexée par E. Exprimer $\mathrm{car}(\prod_{e\in A} A_e)$ en fonction des $\mathrm{car}(A_e)$.
10. Soit p un nombre premier et A un anneau de caractéristique p. Montrer que $x \mapsto x^p$ est un morphisme d'anneaux. Donner un exemple d'un anneau de caractéristique 4 pour lequel $x \mapsto x^4$ n'est pas un morphisme d'anneaux.

Exercice 2.10

On désigne par i un élément de $\mathbf{C}$ tel que $i^2 = -1$. Soit $\mathbf{Z}[i]$ l'image de l'unique morphisme d'anneaux $\mathbf{Z}[X] \to \mathbf{C}$ qui envoie X sur i (*cf.* l'exercice 1.7.1).

1. Soit p un nombre premier. Montrer que les conditions suivantes sont équivalentes, et qu'elles sont entraînées par la condition « p n'est pas un élément irréductible de $\mathbf{Z}[i]$ ».
   (a) $p\mathbf{Z}[i]$ n'est pas un idéal premier de $\mathbf{Z}[i]$;
   (b) -1 est un carré modulo p.
2. Soit $z \in \mathbf{Z}[i]$. Montrer que $z \in \mathbf{Z}[i]^\times$ si et seulement si $N(z) = 1$ (*cf.* l'exercice 1.7.1).
3. Soit $z_1, z_2 \in \mathbf{Z}[i]$ tels que $N(z_1) = N(z_2)$ et z_1 divise z_2. Montrer que z_1 et z_2 sont associés.
4. Soit $z \in \mathbf{Z}[i]$ tel que $N(z)$ est un nombre premier. Montrer que z est un élément irréductible de $\mathbf{Z}[i]$.
5. Soit p un nombre premier tel que p est une somme de deux carrés, c'est-à-dire qu'il existe $(a, b) \in \mathbf{Z}^2$ tel que $p = a^2 + b^2$. Montrer que -1 est un carré modulo p, et que p n'est pas un élément irréductible de $\mathbf{Z}[i]$.
6. On admet (provisoirement) la propriété $(\mathcal{P})$ suivante : soit $(a, b, c) \in \mathbf{Z}[i]^3$; on suppose que a et b sont irréductibles, non associés, et divisent c ; alors ab divise c. Soit p un nombre premier. Montrer que les conditions suivantes sont équivalentes :
   (a) p n'est pas un élément irréductible de $\mathbf{Z}[i]$;
   (b) $p\mathbf{Z}[i]$ n'est pas un idéal premier de $\mathbf{Z}[i]$;
   (c) -1 est un carré modulo p ;
   (d) p est une somme de deux carrés.
7. Montrer que l'analogue de la propriété $(\mathcal{P})$ pour $\mathbf{Z}[i\sqrt{3}]$ est fausse (*cf.* exercice 2.5).

Exercice 2.11

1. Soit A un anneaux et $\mathcal{I}_1$, $\mathcal{I}_2$, $\mathcal{I}_3$ trois idéaux de A, supposé deux à deux étrangers. Montrer que les idéaux $\mathcal{I}_1$ et $\mathcal{I}_2 \cdot \mathcal{I}_3$ sont étrangers. En déduire que $\mathcal{I}_1 \cdot \mathcal{I}_2 \cdot \mathcal{I}_3 = \mathcal{I}_1 \cap \mathcal{I}_2 \cap \mathcal{I}_3$ et que le morphisme naturel
$$A \to A/\mathcal{I}_1 \times A/\mathcal{I}_2 \times A/\mathcal{I}_3$$
est surjectif.
2. Démontrer la version générale du théorème chinois énoncée en cours.
3. Résoudre les systèmes de congruences suivants d'inconnue $x \in \mathbf{Z}$:

$$(1)\left\{\begin{array}{rcl} x & \equiv & 3\ [12] \\ x & \equiv & 3\ [21] \end{array}\right. \qquad (2)\left\{\begin{array}{rcl} x & \equiv & 5\ [15] \\ x & \equiv & 4\ [14] \\ x & \equiv & 3\ [13] \end{array}\right.$$

$$(3)\left\{\begin{array}{rcl} 2x & \equiv & 1\ [25] \\ x & \equiv & 5\ [13] \end{array}\right. \qquad (4)\left\{\begin{array}{rcl} x & \equiv & 1\ [10] \\ x & \equiv & 5\ [15] \end{array}\right.$$

$$(5)\left\{\begin{array}{rcl} x & \equiv & 17\ [21] \\ x & \equiv & 2\ [6] \end{array}\right. \qquad (6)\left\{\begin{array}{rcl} 9x & \equiv & 2\ [15] \\ x & \equiv & 6\ [17] \end{array}\right.$$

Exercice 2.12

1. Soit A un anneau. On note $\iota\colon A \to A[X]$ le morphisme d'anneaux injectif naturel. Soit C un anneau, $\theta \in \mathrm{Hom}_{\mathrm{anneaux}}(A, C)$ et $c \in C$. On suppose que le triplet (C, θ, c) vérifie la propriété suivante : pour tout anneau B, l'application
$$\begin{array}{rcl} \mathrm{Hom}_{\mathrm{anneaux}}(C, B) & \longrightarrow & \mathrm{Hom}_{\mathrm{anneaux}}(A, B) \times B \\ \varphi & \longmapsto & (\varphi \circ \theta, \varphi(c)) \end{array}$$
est une bijection. Montrer qu'il existe un unique isomorphisme d'anneaux $\psi\colon A[X] \to C$ tel que $\psi \circ \iota = \theta$ et qui envoie X sur c.
2. Soit A un anneau, C une A-algèbre et $c \in C$. On suppose que le couple (C, c) vérifie la propriété suivante : pour toute A-algèbre B, l'application
$$\begin{array}{rcl} \mathrm{Hom}_{A-\mathrm{alg\grave{e}bres}}(C, B) & \longrightarrow & B \\ \varphi & \longmapsto & \varphi(c) \end{array}$$
est une bijection. Montrer qu'il existe un unique isomorphisme de A-algèbres de $A[X]$ vers C qui envoie X sur c.
3. Comparer les deux énoncés.

Exercice 2.13

Cet exercice vise à mettre en lumière un certain nombre de résultats illustrant le fait que toutes les notions relatives à la théorie des anneaux développées dans le cours sont (et c'est heureux)

« invariantes par isomorphisme d'anneaux ». Certaines définitions utilisées dans cet exercice seront données plus tard dans le cours ; si vous ne les connaissez pas, vous pouvez attendre qu'elles soient données pour revenir ensuite sur les propriétés correspondantes à démontrer dans cet exercice.

Dans tous les énoncés, A et B sont des anneaux supposés isomorphes, et $\varphi\colon A \to B$ est un isomorphisme d'anneaux de A sur B. On demande de montrer les propriétés suivantes.

1. Pour tout a dans A, on a $a \in A^{\times}$ si et seulement si $\varphi(a) \in A^{\times}$; en outre φ induit un isomorphisme de groupes de $A^{\times}$ sur $B^{\times}$.
2. Pour tout a dans A, a est irréductible si et seulement si $\varphi(a)$ est irréductible.
3. Pour tout a dans A, a est diviseur de zéro si et seulement si $\varphi(a)$ est diviseur de zéro.
4. Pour tout a dans A, a est nilpotent si et seulement si $\varphi(a)$ est nilpotent ; pour la définition de « nilpotent », se reporter à l'exercice 1.10.
5. Pour tout idéal $\mathcal{I}$ de A, $\varphi(\mathcal{I})$ est un idéal de B, et $\mathcal{I}$ est premier (respectivement maximal) si et seulement si $\varphi(\mathcal{I})$ est premier (respectivement maximal).
6. A est intègre si et seulement si B est intègre.
7. A est réduit si et seulement si B est réduit ; pour la définition de « réduit », se reporter à l'exercice 1.10.
8. A est un corps si et seulement si B est un corps.
9. A est euclidien si et seulement si B est euclidien.
10. A est factoriel si et seulement si B est factoriel.
11. A et B ont même caractéristique.