Licence de mathématiques S5 — Algèbre générale 1
Université d'Avignon — Année 2021-22

3-ième feuille d'exercices - Arithmétique dans les anneaux principaux.

Exercice 1 : *Théorème des restes chinois.* 1. Soit $n, m \in \mathbb{N}^*$ tels que $n \wedge m = 1$

a) A quoi sont égaux les ensembles $n\mathbb{Z} + m\mathbb{Z}$ et $n\mathbb{Z} \cap m\mathbb{Z}$?

b) Pour $x \in \mathbb{Z}$ et $r \in \mathbb{N}$, on note $[x]_r \in \mathbb{Z}/r\mathbb{Z}$ la classe d'équivalence de x pour la relation de congruence modulo r (on a donc $[x]_r = x + r\mathbb{Z}$). Justifier que pour tous $x, y \in \mathbb{Z}$,

$$[x]_{nm} = [y]_{nm} \Longrightarrow [x]_n = [y]_n \text{ et } [x]_m = [y]_m \,.$$

En déduire qu'on peut définir une application

$$\Phi : \mathbb{Z}/(nm\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

telle que, pour tout $x \in \mathbb{Z}$, $\Phi([x]_{nm}) = ([x]_n, [x]_m)$. Montrer que Φ est un morphisme d'anneaux.

c) Montrer que Φ est injective. En déduire que Φ est un isomorphisme (pour la surjectivité, on pourra considérer le nombre d'éléments des anneaux $\mathbb{Z}/(nm\mathbb{Z})$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$).

d) En déduire que pour tous entiers a, b, le système d'équations

$$(*) \qquad \begin{cases} x \equiv a[n] \\ x \equiv b[m] \end{cases}$$

admet des solutions dans $\mathbb{Z}$, et que la différence de deux solutions est un multiple de nm.

e) Déterminer les solutions de $(*)$ lorsque $n = 21$, $m = 8$, $a = 5$, $b = 9$.

2. a) Plus généralement, on considère p entiers strictement positifs $n_1, \dots, n_p$ deux à deux premiers entre eux. On note ρ leur produit : $\rho = \prod_{i=1}^{p} n_i$. Montrer que l'application

$$\Phi : \mathbb{Z}/\rho\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_p\mathbb{Z}$$

définie par $\Phi([x]_\rho) = ([x]_{n_1}, \dots, [x]_{n_p})$ est un isomorphisme d'anneaux.

b) Résoudre (dans $\mathbb{Z}$) le système d'équations $\begin{cases} x \equiv 8[21] \\ x \equiv 6[8] \\ x \equiv 2[5] \end{cases}$

Exercice 2 : Soit $(A, +, \times)$ un anneau commutatif intègre. Cet anneau est dit *euclidien* s'il existe une application $d : A\backslash\{0\} \to \mathbb{N}$ (appelée stathme euclidien) telle que :

$$\forall (a,b) \in A \times A\backslash\{0\}\,,\ \exists (q,r) \in A \times A\,,\ \begin{cases} a = bq + r \\ r = 0 \text{ ou } d(r) < d(b) \end{cases}$$

a) Justifier que $(\mathbb{Z}, +, \times)$ et $(\mathbb{K}[x], +, \times)$ (avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$) sont des anneaux euclidiens.

b) Montrer que tout anneau euclidien est principal.

c) On considère le sous-anneau $\mathbb{Z}[i]$ de $(\mathbb{C}, +, \times)$ constitué des nombres complexes de parties réelle et imaginaire entières :

$$\mathbb{Z}[i] = \{a + ib \ ;\ a, b \in \mathbb{Z}\}$$

Montrer que l'application $d : \mathbb{Z}[i] \to \mathbb{N}$ définie, pour $a, b \in \mathbb{Z}$, par $d(a + ib) = |a + ib|^2 = a^2 + b^2$ est un stathme euclidien pour l'anneau $(\mathbb{Z}[i], +, \times)$. En déduire que cet anneau est principal.

Exercice 3 : a) Trouver deux polynômes $U, V \in \mathbb{R}[X]$ tels que

$$U(X)(X-1)^2 + V(X)(X+1)^2 = 2$$

b) On veut déterminer les polynômes $P \in \mathbb{R}[X]$ tels que

(E) $\qquad (X-1)^2$ divise $P(X)+1$ et $(X+1)^2$ divise $P(X)-1$

En utilisant a), trouver un polynôme P_0 solution de (E).

c) Si P est une autre solution de (E), que peut-on dire de $P - P_0$? En déduire toutes les solutions de (E).

Exercice 4 : On pose $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}\ ;\ a, b \in \mathbb{Z}\}$.

a) Montrer que $\mathbb{Z}[i\sqrt{5}]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

Pour $z = a + ib\sqrt{5}$ avec $a, b \in \mathbb{Z}$, on pose $N(z) = |z|^2 = a^2 + 5b^2$.

b) Trouver $z \in \mathbb{Z}[i\sqrt{5}]$, $z \neq \pm 3$, tel que $N(z) = 9$, et montrer que 3 n'est pas un élément premier de $\mathbb{Z}[i\sqrt{5}]$.

c) Montrer que 3 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$.

d) L'anneau $\mathbb{Z}[i\sqrt{5}]$ est-il principal ?

Exercice 5 : On se place dans l'anneau principal $(\mathbb{Z}[i], +, \times)$. On rappelle (voir TD2) que l'ensemble des unités de $\mathbb{Z}[i]$ est $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

a) Pour $z \in \mathbb{Z}[i]$, on pose $N(z) = |z|^2$. Montrer que si $N(z)$ est un nombre premier, alors z est un élément irréductible de $\mathbb{Z}[i]$.

b) Décomposer en facteurs irréductibles 7, 13, $2(3+i)$, $12+i$.

c) Quel est le pgcd de $11 + 7i$ et $3 + 7i$?

Exercices complémentaires.

Exercice 6 : Soit $(A, +, \times)$ un anneau commutatif et soit I_1, I_2, deux idéaux de A tels que $I_1 + I_2 = A$.

Montrer que les anneaux $A/(I_1 \cap I_2)$ et $A/I_1 \times A/I_2$ sont isomorphes (s'inspirer de l'exercice 1 pour définir un morphisme d'anneaux de $A/(I_1 \cap I_2)$ vers $A/I_1 \times A/I_2$).

Exercice 7 : *Théorème de Wilson.* Le but de l'exercice est de montrer l'équivalence suivante pour n entier, $n \geq 2$:

$$n \text{ est un nombre premier} \iff (n-1)! \equiv -1[n]$$

L'équivalence étant vraie pour $n = 2$, on supposera $n \geq 3$ dans la suite.

1. Soit $p \geq 3$ un nombre premier.

a) Quel est l'ensemble S des solutions dans $\mathbb{Z}/p\mathbb{Z}$ de l'équation $x^2 = \bar{1}$?

b) En remarquant que $(\mathbb{Z}/p\mathbb{Z})\backslash\{0\}$ est la réunion disjointe de paires d'éléments inverses l'un de l'autre pour la loi $\times$ et de S, montrer que le produit de tous les éléments de $(\mathbb{Z}/p\mathbb{Z})\backslash\{0\}$ est égal à $-\bar{1}$. En déduire que

$$(p-1)! \equiv -1[p]$$

2. Soit $n \geq 3$ un entier tel que $(n-1)! \equiv -1[n]$.

a) Montrer que

$$\forall a \in [\![1, n-1]\!]\,,\ a \wedge n = 1\,.$$

b) En déduire que n est un nombre premier.