UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Feuille n°2 : Anneaux et structure d'anneaux sur $\mathbf{Z}/n\mathbf{Z}$

Dans tout le cours les anneaux sont munis d'une unité pour la multiplication et les morphismes d'anneaux respectent les unités.

Exercices à savoir faire

Questions de cours

1 Ecrire les tables d'opération dans l'anneau $\mathbf{Z}/6\mathbf{Z}$.
2 Soit p un nombre premier, et soit $(G, \star)$ un groupe d'ordre p. Montrer que G est cyclique.
3 Démontrer que le noyau d'un morphisme d'anneaux commutatifs est un idéal.
4 L'application $f\;:\mathbf{Z}/10\mathbf{Z} \to \mathbf{Z}/3\mathbf{Z}$ construite de la manière suivante est-elle bien définie ? Pour un élément c de $\mathbf{Z}/10\mathbf{Z}$, on choisit un représentant x et on pose $f(c) := [x]_3$.

Exercice 1

1 Montrer que $\mathbf{Z} \times \mathbf{Z}$ peut être muni d'une structure naturelle d'anneau.
2 Montrer que $\mathbf{R}[X]$ est un anneau, et que pour tout $a \in \mathbf{R}$, l'ensemble

$$I_a = \{P \in \mathbf{R}[X] \;/\; P(a) = 0\}$$

est un idéal de $\mathbf{R}[X]$.

Exercice 2

1 Déterminer l'ordre de $\overline{2}$ dans $(\mathbf{Z}/10\mathbf{Z}, +)$.
2 Montrer que $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ est un sous-groupe de $(\mathbf{Z}/12\mathbf{Z}, +)$.
3 Expliciter un sous-groupe d'ordre 6 de $(\mathbf{Z}/12\mathbf{Z}, +)$.
4 Quels sont les ordres possibles des sous-groupes de $(\mathbf{Z}/6\mathbf{Z}, +)$?
5 Soient n un entier naturel non nul. Le but de cette question est de déterminer tous les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$. Soit d un diviseur de n.

a) Expliciter un sous-groupe G_d de $\mathbf{Z}/n\mathbf{Z}$ d'ordre d.

b) Soit H un sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ d'ordre d. Montrer que pour tout $\overline{x} \in H$, $d \cdot \overline{x} = 0$. Combien d'éléments de $\mathbf{Z}/n\mathbf{Z}$ vérifient cette équation ? En déduire que $H = G_d$.

c) Conclure.

6 Donner la liste de tous les sous-groupes de $(\mathbf{Z}/6\mathbf{Z}, +)$.

Exercice 3

Déterminer les puissances de 2 modulo 9. Que dire du groupe $(\mathbf{Z}/9\mathbf{Z})^\times$?

Exercice 4

1 Soit m et n deux entiers naturels non nuls premiers entre eux. On a vu comment trouver une relation de Bézout $um + vn = 1$. Montrer alors que l'application

$$\begin{array}{ccc} (\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z}) & \to & \mathbf{Z}/(mn)\mathbf{Z} \\ (x, y) & \mapsto & umy + vnx \end{array}$$

est bien définie, est un isomorphisme. Déterminer son isomorphisme réciproque.
2 Trouver l'entier entre 0 et 100 congru à 9 modulo 11 et à 3 modulo 13.

Exercice 5

Il est souvent important de calculer a^t modulo n avec a, t, n grands (calculer a^t dans $\mathbf{Z}$ n'est pas envisageable). Méthode : Ecrire t en binaire : $t = \Sigma t_i 2^i$ (où $t^i \in \{0, 1\}$). Les a^{2^i} se calculent facilement par élévations au carré successives modulo n, et a^t modulo n est le produit (modulo n) des a^{2^i} pour lesquels $t^i = 1$.

Calculer 3^{2010} modulo 50.

Exercices à chercher

Exercice 6

Le but de cet exercice est de déterminer tous les morphismes d'anneaux de $\mathbf{Z}/10\mathbf{Z}$ dans un $\mathbf{Z}/n\mathbf{Z}$.
1 Montrer que tout morphisme de groupes de $\mathbf{Z}/10\mathbf{Z}$ dans un $\mathbf{Z}/n\mathbf{Z}$ est déterminé par l'image de $[1]_{10}$.
2 Quelles sont les valeurs possibles pour l'image de $[1]_{10}$ par un morphisme d'anneaux de $\mathbf{Z}/10\mathbf{Z}$ dans un $\mathbf{Z}/n\mathbf{Z}$?
3 Déterminer tous les morphismes d'anneaux de $\mathbf{Z}/10\mathbf{Z}$ dans un $\mathbf{Z}/n\mathbf{Z}$.

Exercice 7

1 L'équation $x^3 + x + 1 = 0$ a-t-elle des solutions dans $\mathbf{Z}/2\mathbf{Z}$.
2 L'équation $x^3 + x + 1 = 0$ a-t-elle des solutions dans $\mathbf{Z}$?

Exercice 8

1 Quelle opération fait de $\mathbf{Q}/\mathbf{Z}$ un groupe ?
2 Ce groupe est-il fini ?
3 Quel est l'ordre de $7/12$ dans ce groupe ?
4 Montrer que tous les éléments de $\mathbf{Q}/\mathbf{Z}$ sont d'ordre fini.

Exercice 9

Soit p un nombre premier impair.
1 Quels éléments de $(\mathbf{Z}/p\mathbf{Z})^{\times}$ sont leur propre inverse ?
2 Démontrer le théorème de Wilson, Théorème de Wilson : Soit n un entier naturel supérieur à 3. Alors n est premier si, et seulement si, $(n-1)! = -1 \pmod{n}$.