UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Feuille n°2 : anneaux, quotients, $\mathbf{Z}/n\mathbf{Z}$

Exercices à savoir faire chez soi

Exercice 1

Chercher quelques-uns des exercices proposés sur la page
`http://wims.unice.fr/wims/fr_U1~algebra~oefintrogroupe.fr.html`

Exercice 2

1 21026 appartient-il à $12756 + 2067\mathbf{Z}$?

2 Calculer l'image de 2099 dans $\mathbf{Z}/17\mathbf{Z}$ sous la forme $[n]_{17}$ où n est un entier compris entre 0 et 16.

Exercice 3

1 Écrire les tables d'opération dans l'anneau $\mathbf{Z}/6\mathbf{Z}$. Même question avec $\mathbf{Z}/8\mathbf{Z}$.

2 Considérons l'application $f : \mathbf{Z}/8\mathbf{Z} \to \mathbf{Z}/8\mathbf{Z}$ qui envoie x sur x^3. Calculer les images de tous les éléments de $\mathbf{Z}/8\mathbf{Z}$ par f sous la forme $[n]_8$ où n est un entier compris entre 0 et 7. L'application f est-elle injective ?

3 $[2]_{26}$ est-il un diviseur de zéro dans $\mathbf{Z}/26\mathbf{Z}$?

Exercice 4

Vrai ou faux ?

1 Soit G un groupe, d'élément neutre e. Soit $g \in G$. S'il existe un entier positif n tel que $g^n = e$, alors g est d'ordre fini.

2 Soit n un entier strictement positif. L'ordre d'une racine n-ème de l'unité, vue comme élément du groupe $(\mathbf{C}^\times, \times)$, est n.

Exercice 5

Soit $(G, \star)$ et $(H, \otimes)$ des groupes, $\varphi : G \to H$ un morphisme. Montrer

$$\forall g \in G, \quad \forall n \in \mathbf{Z}, \quad \varphi(g^{\star n}) = \varphi(g)^{\otimes n}$$

(par récurrence sur n quand n est positif, puis en utilisant le fait que l'image du symétrique est le symétrique de l'image).

Réécrire cette relation quand G et H sont notés tous les deux multiplicativement, puis tous les deux additivement, puis quand G est noté multiplicativement et H additivement, puis quand G est noté additivement et H multiplicativement.

Exercice 6

Soit $\mathbf{U}$ l'ensemble des nombres complexes de module 1.

1 Montrer que $\mathbf{U}$ est un sous-groupe de $(\mathbf{C}^\times, \times)$.

2 Soit $f : \mathbf{C}^\times \to \mathbf{U}$ définie par $f(z) = \frac{z}{|z|}$. Vérifier que f est bien définie. Montrer que f est un morphisme de groupes surjectif. Quel est son noyau ?

3 Soit $f : \mathbf{U} \to \mathbf{U}$ définie par $g(z) = z^2$. Vérifier que g est bien définie. Montrer que g est un morphisme de groupes surjectif. Quel est son noyau ?

4 Soit n un entier strictement positif. Montrer que $\mathbf{U}_n = \{z \in \mathbf{C}, \quad z^n = 1\}$ est un sous-groupe de $\mathbf{U}$. Le groupe $\mathbf{U}_n$ est-il cyclique ?

Exercices à savoir faire

Exercice 7

1 Soit p un nombre premier, et $(G, \star)$ un groupe d'ordre p. Montrer que G est cyclique. *Indication :* Soit g un élément de G différent de l'élément neutre. Que peut-on dire de l'ordre du sous-groupe de G engendré par g ?

2 Démontrer que le noyau d'un morphisme de groupes $G \to H$ est un sous-groupe de G. *Indication :* écrire...

3 Démontrer que le noyau d'un morphisme d'anneaux commutatifs $A \to B$ est un idéal de A. *Indication :* écrire...

4 Soit $f : G \to H$ un morphisme de groupes. On suppose f bijectif. Montrer que $f^{-1} : H \to G$ est un morphisme de groupes. Même question avec un morphisme d'anneaux.

5 Vérifier que $(\mathbf{R}[X], +, \times)$ est un anneau commutatif, que pour tout $P \in \mathbf{R}[X]$, l'ensemble

$$P.\mathbf{R}[X] = \{P.Q, \quad Q \in \mathbf{R}[X]\}$$

est un idéal de $\mathbf{R}[X]$ et que pour tout $a \in \mathbf{R}$, l'ensemble

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

est un idéal de $\mathbf{R}[X]$. Existe-t-il d'autres idéaux de $\mathbf{R}[X]$ que ceux de la forme I_a ? Déterminer $\mathbf{R}[X]^\times$.

6 Soit $f : A \to B$ un morphisme d'anneaux commutatifs. Montrer la relation $f(A^\times) \subset B^\times$. Donner un exemple où il n'y a pas égalité.

7 Soit A un anneau commutatif. Pour a élément non nul de A, on considère l'application de A dans A définie par $x \mapsto a\,x$. Montrer que cette application est injective si et seulement si a n'est pas diviseur de zéro, et surjective si et seulement si a est inversible. En déduire que si A est fini, tout élément non nul de A est soit inversible, soit diviseur de zéro.

Exercice 8

1 Sachant que $187489 = 433^2$ et que 433 est un nombre premier, combien de diviseurs de zéro y a-t-il dans $\mathbf{Z}/187489\mathbf{Z}$?

2 Déterminer les puissances de 2 modulo 9. Que peut-on en conclure sur le groupe $(\mathbf{Z}/9\mathbf{Z})^\times$?

Exercice 9

1 Déterminer l'ordre de $[2]_{14}$ dans le groupe additif $(\mathbf{Z}/14\mathbf{Z}, +)$.

2 Montrer que $\{[0]_{20}, [5]_{20}, [10]_{20}, [15]_{20}\}$ est un sous-groupe de $(\mathbf{Z}/20\mathbf{Z}, +)$, dont on déterminera un générateur.
3 Expliciter un sous-groupe d'ordre 10 de $(\mathbf{Z}/20\mathbf{Z}, +)$.
4 Quels sont les ordres possibles des sous-groupes de $(\mathbf{Z}/10\mathbf{Z}, +)$?
5 Soient n un entier naturel non nul. Le but de cette question est de déterminer tous les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$.

a) Soit d un diviseur de n. Expliciter un sous-groupe G_d de $\mathbf{Z}/n\mathbf{Z}$ d'ordre d (on pourra s'inspirer des exemples numériques précédents).

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

c) Conclure quant à la description de tous les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$.

6 Application numérique : donner la liste de tous les sous-groupes de $(\mathbf{Z}/10\mathbf{Z}, +)$.

Exercice 10
1 L'équation $X^2 + Y^2 = [3]_4$ a-t-elle des solutions $(X, Y) \in (\mathbf{Z}/4\mathbf{Z})^2$?
2 Soit n un entier congru à 3 modulo 4. L'équation $x^2+y^2 = n$ a-t-elle des solutions $(x, y) \in \mathbf{Z}^2$?
Indication : utiliser la question précédentes et le morphisme d'anneaux $\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z}$.

Exercice 11
1 Que pensez-vous de la construction suivante : « Définissons une application $f : \mathbf{Z}/10\mathbf{Z} \to \mathbf{Z}/3\mathbf{Z}$ de la manière suivante : soit c un élément de $\mathbf{Z}/10\mathbf{Z}$; on choisit un représentant x de c dans $\mathbf{Z}$ et on pose $f(c) := [x]_3$ ».
2 Quels sont les morphismes de groupes $\mathbf{Z}/10\mathbf{Z} \to \mathbf{Z}/3\mathbf{Z}$? *Indication :* remarquant que $10.[1]_{10} = [0]_{10}$, déterminer l'image de $[1]_{10}$, puis conclure.

Exercice 12
1 Soit m et n deux entiers naturels non nuls premiers entre eux. Rappeler comment trouver une relation de Bézout $um + vn = 1$. Soit x et y des entiers relatifs. Vérifier que l'élément $[umy + vnx]_{mn} \in \mathbf{Z}/(mn)\mathbf{Z}$ ne dépend que de $[x]_m$ et $[y]_n$. Vérifier que l'application

$$\begin{array}{rcl} (\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z}) & \longrightarrow & \mathbf{Z}/(mn)\mathbf{Z} \\ ([x]_m, [y]_n) & \longmapsto & [umy + vnx]_{mn} \end{array}$$

est bien définie. Montrer que c'est un isomorphisme d'anneaux, dont on explicitera l'isomorphisme réciproque.
2 Déterminer les entiers compris entre 0 et 100 qui sont congrus à 9 modulo 11 et à 3 modulo 13.

Exercices à chercher

Exercice 13
Soit E un ensemble muni d'une loi de composition interne $\star$ associative qui vérifie la propriété suivante

$$\exists e \in E, \quad \left\{ \begin{array}{ll} \forall x \in E, & e \star x = x \\ \forall x \in E, & \exists y \in E, \quad y \star x = e \end{array} \right.$$

Montrer que $(E, \star)$ est un groupe. *Indication :* soit $x \in E$, y vérifiant $y \star x = e$ et z vérifiant $z \star y = e$; vérifier l'égalité $y \star x \star e = y \star x$ et en utilisant z en déduire que $x \star e = x$; puis en considérant $z \star y \star x$, montrer que $z = x$, et conclure.

Exercice 14

Il est souvent important (notamment pour les applications cryptographiques du type RSA) de pouvoir calculer rapidement a^t modulo n avec a, t, n grands. Une méthode naïve serait de d'abord calculer a^t, puis son reste modulo n en utilisant la division euclidienne. Dans la pratique, ce calcul est *absolument irréalisable*, même en utilisant des ordinateurs surpuissants. En effet l'exposant t pourra typiquement avoir plusieurs centaines de chiffres, si bien que le seul *nombre de chiffres* de a^t (ne parlons même pas de sa valeur...), qui est de l'ordre de grandeur de t, sera supérieur au nombre d'atomes dans l'univers, ce qui va déjà poser quelques problèmes pour le représenter dans la mémoire de l'ordinateur... Une méthode déjà plus raisonnable consisterait à calculer les puissances successives de a en réduisant modulo n à chaque multiplication. Le fait de toujours travailler modulo n assure qu'on manipulera toujours ainsi des nombres de taille raisonnable. Par contre cette méthode nécessite a priori t multiplications modulo n, ce qui risque de prendre un temps prohibitif si t est grand.

Voici une méthode beaucoup moins gourmande en multiplications : on écrit t en binaire : $t = \sum_{i=1}^{N} t_i 2^i$ (où $t_i \in \{0, 1\}$). Pour $i \in \{1, \ldots, N\}$ on calcule les a^{2^i} par élévations successives au carré modulo n ; on calcule alors a^t modulo n en effectuant le produit (modulo n) des a^{2^i} pour lesquels $t_i = 1$. Calculer avec cette méthode 3^{2010} modulo 50. Montrer que cette méthode utilise un nombre de multiplications modulo n de l'ordre de $\log(t)$ (ce qui est tout à fait raisonnable, même si t a plusieurs centaines du chiffres, car $\log(t)$ est de l'ordre de grandeur du nombre de chiffres de t).

Exercice 15

1 Soient a et b des éléments de $\mathbf{Z}/3\mathbf{Z}$; calculer $(a+b)^3$

2 Soient a et b des éléments de $\mathbf{Z}/6\mathbf{Z}$; calculer $(a+b)^6$.

3 Soient a et b des éléments de $\mathbf{Z}/7\mathbf{Z}$; calculer $(a+b)^7$.

Exercice 16

Soit $n \geqslant 2$ un entier naturel. Le but de cet exercice est de déterminer tous les morphismes d'anneaux de $\mathbf{Z}/10\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$.

1 Montrer que tout morphisme de groupes de $\mathbf{Z}/10\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ est déterminé par l'image de $[1]_{10}$.

2 Soit $\varphi : \mathbf{Z}/10\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ un morphisme d'anneaux. En appliquant φ à l'égalité $10.[1]_{10} = [0]_{10}$, trouver une relation entre 10 et n.

3 En déduire tous les morphismes d'anneaux de $\mathbf{Z}/10\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ (on discutera suivant les valeurs de n).

4 Reprendre les questions précédentes en remplaçant 10 par un entier naturel $m \geqslant 2$ quelconque.

Exercice 17

1 On considère le groupe $\mathbf{Q}/\mathbf{Z}$, quotient de $(\mathbf{Q}, +)$ par le sous-groupe $\mathbf{Z}$. Décrire la loi de groupe sur $\mathbf{Q}/\mathbf{Z}$.

2 $\mathbf{Q}/\mathbf{Z}$ 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 18

Soit p un nombre premier impair.
1 Quels éléments de $(\mathbf{Z}/p\mathbf{Z})^\times$ sont leur propre inverse ?
2 Déduire de la question précédente le théorème de Wilson : soit n un entier naturel supérieur à 3 ; alors n est premier si et seulement si on a $(n-1)! \equiv -1 \mod n$.