Anneaux

Exercice 48
Dans un anneau A, on dit qu'un élément a est un *diviseur de zéro* lorsque $a \neq 0$ et il existe un $b \neq 0$ tel que $ab = 0$ ou que $ba = 0$.
Montrer que dans un anneau sans diviseur de zéro, on peut simplifier par un élément non nul, au sens suivant :

$$\text{Pour tout } a \text{ non nul et tous } b, c, \quad ab = ac \Rightarrow b = c.$$

Exercice 49
On dit qu'un élément a d'un anneau A est *nilpotent* lorsqu'il existe un entier $n \geq 1$ tel que $a^n = 0$.

1) Montrer que tout nilpotent non nul est un diviseur de zéro.

2) On suppose l'anneau A commutatif. Montrer que l'ensemble des nilpotents de A est un idéal de A.

Exercice 50
Soit A un anneau dans lequel pour tout élément a, l'identité $a^2 = a$ est vérifiée.

1) Montrer que pour tout $a \in A$, $a + a = 0$.

2) Montrer que A est un anneau commutatif.

Corps commutatifs

Exercice 51

1) Citer un exemple de sous-corps de $\mathbf{R}$ autre que $\mathbf{R}$ lui-même.

2) Montrer que $\{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ est un sous-corps de $\mathbf{R}$.

3) Montrer que le seul sous-corps de $\mathbf{Q}$ est $\mathbf{Q}$ lui-même.

4) Quels sont les sous-corps de $\mathbf{Z}/p\mathbf{Z}$ (p premier) ?

Exercice 52
Soit k et l deux corps commutatifs. On appelle *morphisme de corps* toute application f non identiquement nulle de k vers l qui vérifie pour tous x et y de k les deux conditions :

$$f(x + y) = f(x) + f(y) \qquad \text{et} \qquad f(xy) = f(x)f(y).$$

1) Citer un exemple intéressant de morphisme de corps de $\mathbf{C}$ vers $\mathbf{C}$.
Dans les deux questions qui suivent, f désigne un morphisme de corps.

2) Montrer que f est une injection.

3) Montrer que $f(1) = 1$.

L'anneau commutatif $\mathbf{Z}/n\mathbf{Z}$

Exercice 53
Déterminer les diviseurs de zéro et les nilpotents dans $\mathbf{Z}/5\mathbf{Z}$, puis $\mathbf{Z}/6\mathbf{Z}$, $\mathbf{Z}/125\mathbf{Z}$, $\mathbf{Z}/20\mathbf{Z}$ et en toute généralité $\mathbf{Z}/n\mathbf{Z}$ où n est un entier supérieur ou égal à 2.

Exercice 54
Pour $a \geq 2$, on note π_a la projection de $\mathbf{Z}$ sur $\mathbf{Z}/a\mathbf{Z}$, qui associe à un entier sa classe modulo a.

1) Montrer qu'il existe une application φ et une seule de $\mathbf{Z}/6\mathbf{Z}$ vers $\mathbf{Z}/2\mathbf{Z}$ qui vérifie la condition :

$$\varphi \circ \pi_6 = \pi_2.$$

Généraliser en remplaçant 2 et 6 par des entiers m et n tels que $2 \leq m$ et m divise n.

2) Soit a et b supposés **premiers entre eux**. On note φ l'application de $\mathbf{Z}/ab\mathbf{Z}$ vers $\mathbf{Z}/a\mathbf{Z}$ et ψ l'application de $\mathbf{Z}/ab\mathbf{Z}$ vers $\mathbf{Z}/b\mathbf{Z}$ construites à la première question.

On note ensuite :

$$\begin{array}{rccc} F: & \mathbf{Z}/ab\mathbf{Z} & \to & \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z} \\ & \alpha & \mapsto & (\varphi(\alpha), \psi(\alpha)) \,. \end{array}$$

a) Expliciter F quand $a = 2$ et $b = 3$ (écrire l'image de chacun des éléments de $\mathbf{Z}/6\mathbf{Z}$).

b) Dans le cas général, montrer que F est injective, puis qu'elle est bijective.

c) En déduire que :

$$\begin{array}{rccc} G: & \mathbf{Z} & \to & \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z} \\ & k & \mapsto & (\pi_a(k), \pi_b(k)) \end{array}$$

est une surjection.

d) En déduire qu'il existe des entiers n tels que : $n \equiv 11$ modulo 40 et $n \equiv 15$ modulo 19. Connaissez-vous une technique pour les trouver ?

Exercice 55

(Le "théorème de Wilson")

1) Soit n un entier supérieur ou égal à 2. Montrer que si

$$(n-1)\,! \equiv -1 \text{ modulo } n,$$

alors n est premier. (On pourra raisonner par contraposition).

2) Réciproquement, soit p un nombre premier. Le but est de prouver que :

$$(p-1)\,! \equiv -1 \text{ modulo } p.$$

a) Remarquer que l'égalité souhaitée équivant à la relation suivante, à comprendre comme écrite dans $\mathbf{Z}/p\mathbf{Z}$:

$$\overline{(p-1)\,!} = -\overline{1}.$$

b) Dans $\mathbf{Z}/p\mathbf{Z}$, résoudre l'équation $x^2 = 1$, d'inconnue x.

c) Déduire de la question précédente qu'il y a deux éléments dans $\mathbf{Z}/p\mathbf{Z}$ (un seul si $p = 2$) qui sont égaux à leur propre inverse, et les expliciter.

d) En rapprochant les facteurs de leurs inverses, montrer que dans $\mathbf{Z}/p\mathbf{Z}$, on a :

$$\overline{2} \times \cdots \times \overline{p-2} = \overline{1}.$$

e) Conclure.