Devoir à la maison n° 12

À rendre le 20 janvier

Dans ce problème vous pourrez utiliser librement le résultat suivant :

Théorème : Si f est une injection entre deux ensembles finis ayant le même nombre d'éléments, alors f est une bijection.

I – L'anneau $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}$, $n \geqslant 2$. Pour tout $k \in \mathbb{Z}$, on note $\overline{k}$ le reste de la division euclidienne de k par n.

1) Montrer que $\left\{ \overline{k} \;\middle|\; k \in \mathbb{Z} \right\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Cet ensemble est alors noté $\mathbb{Z}/n\mathbb{Z}$.

2) **a)** Soient $k, \ell \in \mathbb{Z}$. Montrer que $\overline{k} = \overline{\ell}$ si et seulement si $k \equiv \ell[n]$.

b) Soient $k, k', \ell, \ell' \in \mathbb{Z}$ tels que $\overline{k} = \overline{k'}$ et $\overline{\ell} = \overline{\ell'}$. Montrer que $\overline{k+\ell} = \overline{k'+\ell'}$.
*Ceci permet de définir une addition $\oplus$ sur $\mathbb{Z}/n\mathbb{Z}$: soient $a, b \in \mathbb{Z}/n\mathbb{Z}$. Alors il existe $k, \ell \in \mathbb{Z}$ tels que $a = \overline{k}$ et $b = \overline{\ell}$. On pose alors $a \oplus b = \overline{k+\ell}$, c'est-à-dire $\overline{k} \oplus \overline{\ell} = \overline{k+\ell}$, ce qui est défini sans ambiguité grâce à la question **2)b)**. Pour plus de commodités, $\oplus$ sera aussi notée $+$.*

c) Soient $k, k', \ell, \ell' \in \mathbb{Z}$ tels que $\overline{k} = \overline{k'}$ et $\overline{\ell} = \overline{\ell'}$. Montrer que $\overline{k \times \ell} = \overline{k' \times \ell'}$.
*Ceci permet de définir une multiplication $\otimes$ sur $\mathbb{Z}/n\mathbb{Z}$: soient $a, b \in \mathbb{Z}/n\mathbb{Z}$. Alors il existe $k, \ell \in \mathbb{Z}$ tels que $a = \overline{k}$ et $b = \overline{\ell}$. On pose alors $a \otimes b = \overline{k \times \ell}$, c'est-à-dire $\overline{k} \otimes \overline{\ell} = \overline{k \times \ell}$, ce qui est défini sans ambiguité grâce à la question **2)c)**. Pour plus de commodités, $\otimes$ sera aussi notée $\times$.*

3) Pour vérifier que vous avez bien compris :

a) Donner les éléments de $\mathbb{Z}/6\mathbb{Z}$.

b) Dans $(\mathbb{Z}/6\mathbb{Z}, +, \times)$, calculer $\overline{2} + \overline{3}$, $\overline{3} + \overline{5}$, $\overline{1} + \overline{5}$, $\overline{3} \times \overline{5}$ et $\overline{2} \times \overline{3}$.

4) **a)** Montrer que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.

b) Montrer que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau. Est-il commutatif ?

5) **a)** Soit $k \in [\![2, n-1]\!]$ tel que $k|n$. Montrer alors qu'il existe $a \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \neq 0$ et $\overline{k} \times a = \overline{0}$.

b) Soit $k \in [\![2, n-1]\!]$ tel que k et n ne soient pas premiers entre eux. Montrer alors qu'il existe $a \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \neq 0$ et $\overline{k} \times a = \overline{0}$.

c) Soit $k \in [\![1, n-1]\!]$ tel que $k \wedge n = 1$. En utilisant le théorème de Bézout, montrer qu'il existe $m \in \mathbb{Z}$ tel que $\overline{k \times m} = \overline{1}$. En déduire que $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ pour la loi $\times$.

6) Montrer que $(\mathbb{Z}/n\mathbb{Z}, +\times)$ est un corps si et seulement si n est premier.

7) Pour vérifier que vous avez bien compris : dans $\mathbb{Z}/150\mathbb{Z}$, dire si 81 et 143 sont inversibles. Pour chacun d'eux, donner son inverse s'il existe, sinon donner un élément non nul a de $\mathbb{Z}/150\mathbb{Z}$ tel que $a \times b = \overline{0}$ (avec $b = \overline{81}$ ou $\overline{143}$).

II – Le théorème chinois

L'objectif de cette partie est de montrer que si $n, m \in \mathbb{N}\setminus\{0,1\}$ sont premiers entre eux, les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes.
Les lois $+$ et $\times$ de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont telles que si $(a,b),(c,d) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, alors $(a,b)+(c,d) = (a+b, c+d)$ et $(a,b)\times(c,d) = (a\times c, b\times d)$, et on admettra que muni de ces lois, $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est un anneau (ces sont les *lois produit* définies en TD).

Si $n \in \mathbb{Z}$ et $x \in \mathbb{Z}$, on notera désormais $\overline{x}^{[n]}$ le reste de la division euclidienne de x par n.

8) Soit $n, m \in \mathbb{N}\setminus\{0,1\}$ deux entiers premiers entre eux et $\varphi : \left\{ \begin{array}{ccc} \mathbb{Z}/nm\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ x & \mapsto & \left(\overline{x}^{[n]}, \overline{x}^{[m]}\right) \end{array} \right.$.

a) Montrer que pour tout $x \in \mathbb{Z}$, $\varphi(\overline{x}^{[nm]}) = \left(\overline{x}^{[n]}, \overline{x}^{[m]}\right)$.

b) Montrer que φ est un morphisme d'anneaux.

c) Montrer que φ est un isomorphisme d'anneaux.

9) **Application :** Soit $n, m \in \mathbb{N}^*$ premiers entre eux et soit $a \in [\![0, n-1]\!]$, $b \in [\![0, m-1]\!]$. On cherche à résoudre le système de congruences

$$\left\{ \begin{array}{rcll} x & \equiv & a & [n] \\ x & \equiv & b & [m] \end{array} \right. .$$

a) Montrer qu'il existe une unique solution $x_0 \in [\![0, nm-1]\!]$.

b) Exprimer l'ensemble des solutions en fonction de x_0.

c) Donner l'expression d'une solution particulière (on pourra utiliser un entier u tel que $nu \equiv 1\,[m]$).

10) Résoudre $\left\{ \begin{array}{rcll} x & \equiv & 10 & [47] \\ x & \equiv & 5 & [111] \end{array} \right.$.

— FIN —