DM6 – Structures algébriques

À rendre pour le 24/01/2025.
Consignes de présentation : cf. DM1

Exercice 1. L'anneau $\mathbb{Z}/n\mathbb{Z}$

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

1. Montrer que $\left\{\overline{k},\ k \in \mathbb{Z}\right\} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$.

Dans la suite cet ensemble est 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 2b). 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 2c). 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. (c) Montrer que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.

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

5. (a) Soit $k \in [\![2, n-1]\!]$ tel que $k \mid n$. 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 $\overline{143}$).