DEVOIR MAISON N°4

DM4 : ANNEAUX $\mathbb{Z}/n\mathbb{Z}$ – CORRIGÉ

1) Soit $a,b \in \mathbb{Z}$. Montrer que $\overline{a} = \overline{b}$ si et seulement si $a \equiv b \quad [n]$.

On procède par double implication. Supposons $\overline{a} = \overline{b}$. Comme $b \equiv b \quad [n]$, on a $b \in \overline{b}$ donc $b \in \overline{a}$. Ainsi, $b \equiv a \quad [n]$. Réciproquement, supposons $a \equiv b \quad [n]$ et montrons que $\overline{a} = \overline{b}$. Montrons d'abord que $\overline{a} \subset \overline{b}$. Soit $y \in \overline{a}$. Alors $y \equiv a \equiv b \quad [n]$. On en déduit que $y \in \overline{b}$, si bien que $\overline{a} \subset \overline{b}$. On montrerait de même que $\overline{b} \subset \overline{a}$. Finalement, on a bien équivalence.

2) Montrer que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif. *On admettra que $+$ et $\cdot$ sont des l.c.i. et des applications bien définies.*

Soit $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$.

- Montrons d'abord que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.
  - $+$ est commutative car
  $$\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$$
  (On a le droit de commuter sous la barre car $a, b \in \mathbb{Z}$ et que $+$ est commutative sur $\mathbb{Z}$).
  - $+$ est associative car
  $$\begin{aligned}\overline{a} + \left(\overline{b} + \overline{c}\right) &= \overline{a} + \overline{b+c} = \overline{a + (b+c)} = \overline{(a+b)+c} \\ &= \overline{a+b} + \overline{c} = (\overline{a} + \overline{b}) + \overline{c}\end{aligned}$$
  - $\overline{0} \in \mathbb{Z}/n\mathbb{Z}$ est élément neutre pour $+$ car
  $$\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$$
  et par commutativité, $\overline{0+a} = \overline{a}$.
  - $\overline{a}$ admet $\overline{-a}$ pour opposé : tout d'abord $\overline{-a} \in \mathbb{Z}/n\mathbb{Z}$ puisque si $a = 0$, c'est clair, et sinon $\overline{-a} = \overline{n-a} \in \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\} = \mathbb{Z}/n\mathbb{Z}$. Ensuite,
  $$\overline{a} + \overline{-a} = \overline{a + (-a)} = \overline{0}$$
  et de même $\overline{-a} + \overline{a} = \overline{0}$. Ainsi, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.
- Montrons que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif (on évite d'écrire le terme « monoïde »).
  - $\cdot$ est commutative car
  $$\overline{a}\overline{b} = \overline{ab} = \overline{ba} = \overline{b}\overline{a}$$
  - $\cdot$ est associative car
  $$(\overline{a}\overline{b})\overline{c} = \overline{ab}\overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}\overline{bc} = \overline{a}(\overline{b}\overline{c})$$
  - Comme $n \geq 2$, on a $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$. $\overline{1}$ est élément neutre pour $\cdot$ car
  $$\overline{1}\overline{a} = \overline{1a} = \overline{a}$$
  et de même $\overline{a}\overline{1} = \overline{a}$.
  - $\cdot$ est distributive sur $+$ car
  $$\overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b+c} = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac} = \overline{a}\overline{b} + \overline{ac}$$
  et on montrerait de même que $(\overline{b} + \overline{c})\overline{a} = \overline{b}\overline{a} + \overline{c}\overline{a}$. Finalement, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif.

3) Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Montrer que $\overline{a}$ est inversible si et seulement si $a \wedge n = 1$.

Supposons que $a \wedge n = 1$. Par le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que

$$au + nv = 1$$

ainsi, $au \equiv 1 \quad [n]$. Cela entraine par la question 1 que $\overline{au} = \overline{1}$. Ainsi, $\overline{a} \cdot \overline{u} = \overline{1}$. On note r le reste de la division euclidienne de u par n. Alors $\overline{u} = \overline{r}$ et comme $r \in [\![0, n-1]\!]$, on en déduit que $\overline{r} \in \mathbb{Z}/n\mathbb{Z}$. Ainsi, $\overline{u} \in \mathbb{Z}/n\mathbb{Z}$, si bien que $\overline{a}$ est inversible (d'inverse $\overline{u}$).

Réciproquement, supposons que $\overline{a}$ soit inversible. Alors il existe $\overline{u} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{a} \cdot \overline{u} = \overline{1}$. On en déduit que $\overline{au} = \overline{1}$, c'est-à-dire que $au \equiv 1 \quad [n]$. Cela signifie que a est inversible modulo n (d'inverse u). Or, on a vu que cela était équivalent à $a \wedge n = 1$. D'où le résultat

(Note : on aurait presque pu procéder par équivalence en se basant sur le sens direct ci-dessus. Cependant, il faudrait pouvoir justifier que l'inverse modulo n de a, à savoir u, peut toujours être pris dans $[\![0, n-1]\!]$, afin d'assurer que $\overline{u} \in \mathbb{Z}/n\mathbb{Z}$. Cela étant, on a presque déjà prouvé ce résultat dans le cours donc ce n'est pas bien grave.)

4) En déduire que si n n'est pas premier, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. De plus, donner un contre-exemple lorsque $n = 14$.

Si n n'est pas premier [1], alors il existe $a, b \in [\![2, n-1]\!]$ tels que $n = ab$. Ainsi, $ab \equiv 0 \quad [n]$, ou encore

$$\overline{0} = \overline{ab} = \overline{a}\overline{b}$$

Cependant, comme $a, b \in [\![2, n-1]\!]$, on a $a \not\equiv 0 \quad [n]$ donc $\overline{a} \neq \overline{0}$ et de même pour $\overline{b}$. Ainsi, $\overline{a}$ et $\overline{b}$ sont des diviseurs de zéro. Finalement, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

Si $n = 14$, alors $\overline{7} \cdot \overline{2} = \overline{14} = \overline{0}$ montre que $\overline{7}$ et $\overline{2}$ sont des diviseurs de zéro.

5) Déduire de la question 3 que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si et seulement si n est premier. De plus, lorsque $n = 7$, donner un inverse de tous les éléments inversibles de $\mathbb{Z}/7\mathbb{Z}$.

On procède par double implication. Pour le sens direct, si $\mathbb{Z}/n\mathbb{Z}$ est un corps, alors $\mathbb{Z}/n\mathbb{Z}$ est intègre. Or, en prenant la contraposée du résultat de la question 4, cela entraine que n est premier.

Pour le sens réciproque, supposons que n soit premier. Par la question 2, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif. De plus comme $n \geq 2$, on a clairement $\mathbb{Z}/n\mathbb{Z} \neq \{\overline{0}\}$. Enfin, soit $\overline{a} \in (\mathbb{Z}/n\mathbb{Z}) \setminus \{\overline{0}\}$: montrons que $\overline{a}$ est inversible. Comme $\overline{a} \neq \overline{0}$, on a $a \in [\![1, n-1]\!]$. n étant premier, on a donc $a \wedge n = 1$. Par la question 3, on en déduit que $\overline{a}$ est inversible. Finalement, tout élément différent de $\overline{0}$ est inversible : $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Enfin, si $n = 7$, tout élément de $(\mathbb{Z}/7\mathbb{Z})^*$ est inversible et

$$\overline{1} \cdot \overline{1} = \overline{1} \quad \text{donc } \overline{1}^{-1} = \overline{1}$$

$$\overline{2} \cdot \overline{4} = \overline{8} = \overline{1} \quad \text{donc } \overline{2}^{-1} = \overline{4} \text{ et } \overline{4}^{-1} = \overline{2}$$

$$\overline{3} \cdot \overline{5} = \overline{15} = \overline{1} \quad \text{donc } \overline{3}^{-1} = \overline{5} \text{ et } \overline{5}^{-1} = \overline{3}$$

$$\overline{6} \cdot \overline{6} = \overline{36} = \overline{1} \quad \text{donc } \overline{6}^{-1} = \overline{6}$$

1. Cela implique en particulier que $n \geq 4$ donc $[\![2, n-1]\!]$ est non vide.