HAX501X – Groupes et anneaux 1

Contrôle continu 1 – Correction

Clément Dupont

Questions diverses.

1) *L'élément $\overline{8}$ est-il inversible dans $\mathbb{Z}/39\mathbb{Z}$? Si oui, calculer son inverse.*

   Clairement, 8 et 39 sont premiers entre eux (car $8 = 2^3$ et $39 = 3 \cdot 13$), et donc par le cours, $\overline{8}$ est inversible dans $\mathbb{Z}/39\mathbb{Z}$. On peut calculer son inverse en utilisant l'algorithme d'Euclide étendu, ou en connaissant ses tables de multiplications : comme $8 \times 5 = 40$, on a $\overline{8} \times \overline{5} = \overline{1}$ et donc $\overline{8}^{-1} = \overline{5}$.

2) *Soient G et H deux groupes, et $f : G \to H$ un morphisme de groupes. Soit H' un sous-groupe de H. Montrer que l'image réciproque $f^{-1}(H')$ est un sous-groupe de G.*

   Voir le cours.

3) *Donner un exemple d'un groupe d'ordre 6 qui n'est pas cyclique. On justifiera brièvement.*

   Le groupe symétrique $\mathfrak{S}_3$ a 6 éléments mais n'est pas cyclique (parce que pas abélien, par exemple).

   Remarque : le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est cyclique, engendré par $(\overline{1}, \widetilde{1})$. (Ou, par le théorème chinois des restes, il est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ et donc cyclique.)

4) *On se place dans le groupe $G = \mathfrak{S}_4$. Trouver deux sous-groupes d'ordre 4 de G, l'un cyclique et l'autre non cyclique. On justifiera brièvement.*

   L'élément $(1\,2\,3\,4) \in \mathfrak{S}_4$ est d'ordre 4, et donc engendré un sous-groupe

   $$H = \langle\, (1\,2\,3\,4) \,\rangle = \{\mathrm{id}, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2)\}$$

   qui est un groupe cyclique d'ordre 4.

   Pour un groupe d'ordre 4 non cyclique, on sait qu'un tel groupe est engendré par deux éléments d'ordre 2 qui commutent. On choisit les éléments $(1\,2)$ et $(3\,4)$, et on voit facilement que le groupes qu'ils engendrent est

   $$H' = \langle\, (1\,2), (3\,4) \,\rangle = \{\mathrm{id}, (1\,2), (3\,4), (1\,2)(3\,4)\}$$

   qui est d'ordre 4 et non cyclique (car aucun de ses éléments n'est d'ordre 4).

Exercice : morphismes de groupes.

Le but de cet exercice est de classifier les morphismes de groupes de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, pour deux entiers $m, n \in \mathbb{N}^*$. Pour un entier relatif k, on note $\widetilde{k}$ sa classe dans $\mathbb{Z}/m\mathbb{Z}$, et $\overline{k}$ sa classe dans $\mathbb{Z}/n\mathbb{Z}$. On note $d = m \wedge n$ et on écrit $n = de$.

1) *Soit $u \in \mathbb{Z}$.*

a) *Montrer que l'application*

$$g_u : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\ ,\ k \mapsto \overline{uek}$$

passe au quotient par la relation de congruence modulo m.

Soient $k, k' \in \mathbb{Z}$ tels que $k \equiv k' \pmod m$. Alors il existe $l \in \mathbb{Z}$ tel que $k = k' + lm$. On a alors l'égalité dans $\mathbb{Z}/n\mathbb{Z}$:

$$g_u(k) = \overline{uek} = \overline{ue(k'+lm)} = \overline{uek' + uelm} = \overline{uek'} + \overline{uelm} = g_u(k') + \overline{uelm}.$$

Montrer que $g_u(k) = g_u(k')$ revient donc à montrer que $\overline{uelm} = \overline{0}$, c'est-à-dire que n divise le produit $uelm$. On calcule :

$$\frac{uelm}{n} = \frac{uelm}{de} = \frac{ulm}{d} = ul\frac{m}{d}\ .$$

Comme $d = m \wedge n$, on a que d divise m et donc $\frac{m}{d}$ est un entier. On en déduit que $\frac{uelm}{n}$ est un entier et donc que n divise $uelm$. On a donc bien montré que $g_u(k) = g_u(k')$. Donc g_u passe au quotient par la relation de congruence modulo m.

b) *On note*

$$h_u : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\ ,\ \widetilde{k} \mapsto \overline{uek}$$

l'application induite. Montrer que h_u est un morphisme de groupes.

On calcule, pour $\widetilde{k}, \widetilde{k'} \in \mathbb{Z}/m\mathbb{Z}$:

$$h_u(\widetilde{k} + \widetilde{k'}) = h_u(\widetilde{k+k'}) = \overline{ue(k+k')} = \overline{uek + uek'} = \overline{uek} + \overline{uek'} = h_u(\widetilde{k}) + h_u(\widetilde{k'}).$$

Donc h_u est un morphisme de groupes.

2) *Soit $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ un morphisme de groupes.*

a) *On note $\overline{a} = f(\widetilde{1})$. Montrer que $\overline{ma} = \overline{0}$.*

On a

$$\overline{ma} = \overline{\underbrace{a + a + \cdots + a}_{m}} = \underbrace{\overline{a} + \overline{a} + \cdots + \overline{a}}_{m} = \underbrace{f(\widetilde{1}) + f(\widetilde{1}) + \cdots + f(\widetilde{1})}_{m}$$

et donc, en utilisant le fait que f est un morphisme de groupes :

$$\overline{ma} = f(\underbrace{\widetilde{1} + \widetilde{1} + \cdots + \widetilde{1}}_{m}) = f(\widetilde{m}) = f(\widetilde{0}) = \overline{0}.$$

b) *En déduire que $\overline{a} \in \langle\, \overline{e}\, \rangle$.*

D'après la question précédente, $\overline{ma} = \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$, et donc n divise ma. Comme $d = m \wedge n$, on peut écrire $m = df$ avec $e \wedge f = 1$. On a alors que de divise dfa, et donc comme $d \neq 0$ (car sinon on aurait $m = n = 0$) on a que e divise fa. Or $e \wedge f = 1$ et donc par le lemme de Gauss, e divise a. Donc par définition $\overline{a} \in \langle\, \overline{e}\, \rangle$.

c) *En déduire qu'il existe $u \in \mathbb{Z}$ tel que $f = h_u$.*

D'après la question précédente, il existe $u \in \mathbb{Z}$ tel que $f(\widetilde{1}) = \overline{ue}$. On en déduit, comme f est un morphisme de groupes, que

$$f(\widetilde{2}) = f(\widetilde{1} + \widetilde{1}) = f(\widetilde{1}) + f(\widetilde{1}) = \overline{ue} + \overline{ue} = \overline{2ue}.$$

De même, $f(\widetilde{3}) = \overline{3ue}$, etc. Par une récurrence facile, on montre que pour tout $\widetilde{k} \in \mathbb{Z}/m\mathbb{Z}$ on a $f(\widetilde{k}) = \overline{kue}$, et donc que $f = h_u$.

3) *Faire la liste des morphismes de groupes de $\mathbb{Z}/110\mathbb{Z}$ vers $\mathbb{Z}/504\mathbb{Z}$.*

On pose $m = 110$ et $n = 504$. On calcule facilement, grâce à l'algorithme d'Euclide par exemple,

$$d = 110 \wedge 504 = 2 \qquad \text{et donc} \qquad e = \frac{504}{2} = 252.$$

Le bilan des questions 1) et 2) est que les morphismes de groupes de $\mathbb{Z}/110\mathbb{Z}$ vers $\mathbb{Z}/504\mathbb{Z}$ sont les h_u avec $u \in \mathbb{Z}$. On note que h_0 est le morphisme trivial : $h_0(\widetilde{k}) = \overline{0}$. Le morphisme de groupes h_1 est donné par $h_1(\widetilde{k}) = \overline{252k}$. Il n'est pas trivial car $h_1(\widetilde{1}) = \overline{252} \neq \overline{0}$.

Comme $\overline{252 \times 2} = \overline{0}$, on voit que h_0 et h_1 sont les seuls morphismes de groupes de $\mathbb{Z}/110\mathbb{Z}$ vers $\mathbb{Z}/504\mathbb{Z}$. En effet, $h_u = h_0$ si u est pair et $h_u = h_1$ si u est impair.