# HAX501X – Groupes et anneaux 1

# Contrôle continu 1 – Correction

Clément Dupont

### Questions de cours (7 pts).

1) *(1 pt) Est-ce que* $\overline{17}$ *est inversible dans* $\mathbb{Z}/140\mathbb{Z}$ *? Si oui, calculer son inverse.*

Comme 17 et 140 sont premiers entre eux (par exemple parce que 17 est premier et que 140 n'est pas un multiple de 17), on déduit que $\overline{17}$ est inversible dans $\mathbb{Z}/140\mathbb{Z}$. On calcule son inverse grâce à une relation de Bézout entre 17 et 140, trouvée par l'algorithme d'Euclide étendu :

$$140 = 17 \times 8 + 4 \ \ , \ \ 17 = 4 \times 4 + 1,$$

donc

$$1 = 17 - 4 \times 4 = 17 - (140 - 17 \times 8) \times 4 = 17 \times 33 - 140 \times 4,$$

d'où

$$\overline{17} \times \overline{33} = \overline{1}.$$

Donc l'inverse de $\overline{17}$ dans $\mathbb{Z}/140\mathbb{Z}$ est $\overline{33}$.

2) *(1 pt) Calculer, en justifiant,* $\varphi(140)$.

On a $140 = 4 \times 5 \times 7$, et donc en utilisant la multiplicativité de l'indicatrice d'Euler :

$$\varphi(140) = \varphi(4) \times \varphi(5) \times \varphi(7) = 2 \times 4 \times 6 = 48.$$

3) *(1 pt) Dans le groupe* $\mathbb{Z}/140\mathbb{Z}$*, quel est l'ordre du sous-groupe engendré par* $\overline{119}$ *? On justifiera.*

Par le cours, on a

$$\langle \overline{119} \rangle = \langle \overline{119 \wedge 140} \rangle.$$

On calcule donc $119 \wedge 140$ par l'algorithme d'Euclide :

$$140 = 119 \times 1 + 21 \ \ , \ \ 119 = 21 \times 5 + 14 \ \ , \ \ 21 = 14 \times 1 + 7 \ \ , \ \ 14 = 7 \times 2 + 0.$$

Donc $119 \wedge 140 = 7$ et donc

$$\langle \overline{119} \rangle = \langle \overline{7} \rangle$$

qui par le cours est d'ordre

$$\frac{140}{7} = 20.$$

4) *(1 pt) Soit* $f : G \to H$ *un morphisme de groupes. Démontrer que, si l'on note* $e_G$ *et* $e_H$ *les éléments neutres respectifs de* $G$ *et* $H$*, on a* $f(e_G) = e_H$.

Voir le cours.

5) *(1,5 pt) Soit $G$ un groupe, et soient $H, H'$ deux sous-groupes de $G$. Montrer que $H \cap H'$ est un sous-groupe de $G$.*

Voir le cours.

6) *(0,5 pt) Énoncer le théorème de Lagrange.*

Voir le cours.

7) *(1 pt) En utilisant le théorème de Lagrange, démontrer qu'un groupe $G$ d'ordre $p$ premier est nécessairement cyclique.*

Voir le cours.

## Exercice 1 : des congruences (4 pts).

1) *(0,5 pt) Déterminer, suivant les valeurs de l'entier naturel $n$, le reste de la division euclidienne de $3^n$ par 5.*

On voit facilement que $3^4 \equiv 1 \pmod 5$. (Par le calcul ou par application du petit théorème de Fermat.) Le reste dans la division euclidienne de $3^n$ par 5 dépend donc du reste dans la division euclidienne de $n$ par 4 :

▷ si $n \equiv 0 \pmod 4$ alors $3^n \equiv 1 \pmod 5$ ;

▷ si $n \equiv 1 \pmod 4$ alors $3^n \equiv 3 \pmod 5$ ;

▷ si $n \equiv 2 \pmod 4$ alors $3^n \equiv 4 \pmod 5$ ;

▷ si $n \equiv 3 \pmod 4$ alors $3^n \equiv 2 \pmod 5$.

2) *(1,5 pt) Pour quels entiers naturels $n$ a-t-on à la fois $n \equiv 2 \pmod 5$ et $3^n \equiv 2 \pmod 5$ ? Justifier.*

D'après la question précédente on a l'équivalence :

$$(n \equiv 2 \pmod 5 \text{ et } 3^n \equiv 2 \pmod 5) \iff (n \equiv 2 \pmod 5 \text{ et } n \equiv 3 \pmod 4).$$

Comme $5 \wedge 4 = 1$ on peut appliquer le théorème chinois au système de congruences :

$$\begin{cases} n \equiv 2 \pmod 5 \\ n \equiv 3 \pmod 4 \end{cases}$$

On voit que 7 est une solution particulière. Le système est donc équivalent à :

$$n \equiv 7 \pmod{20}.$$

Conclusion : les entiers naturels $n$ tels qu'on a à la fois $n \equiv 2 \pmod 5$ et $3^n \equiv 2 \pmod 5$ sont ceux qui sont congrus à 7 modulo 20.

3) *(2 pts) Déterminer l'ensemble des entiers naturels $n$ qui vérifient :*

$$3^n \equiv n \pmod 5.$$

On fait une disjonction de cas selon le reste dans la division euclidienne de $n$ (et donc de $3^n$) modulo 5. On remarque que par la question 1) on ne peut pas avoir $3^n \equiv 0 \pmod 5$. On a donc 4 cas à traiter, dont un a déjà été traité. Les 3 autres se traitent de la même manière.

▷ $(n \equiv 1 \pmod 5$ et $3^n \equiv 1 \pmod 5) \iff (n \equiv 1 \pmod 5$ et $n \equiv 0 \pmod 4)$. Par le théorème chinois, c'est équivalent à $n \equiv 16 \pmod{20}$.

- ▷ ($n \equiv 2 \pmod 5$ et $3^n \equiv 2 \pmod 5$) $\iff n \equiv 7 \pmod{20}$ par la question 2).
- ▷ ($n \equiv 3 \pmod 5$ et $3^n \equiv 3 \pmod 5$) $\iff$ ($n \equiv 3 \pmod 5$ et $n \equiv 1 \pmod 4$). Par le théorème chinois, c'est équivalent à $n \equiv 13 \pmod{20}$.
- ▷ ($n \equiv 4 \pmod 5$ et $3^n \equiv 4 \pmod 5$) $\iff$ ($n \equiv 4 \pmod 5$ et $n \equiv 2 \pmod 4$). Par le théorème chinois, c'est équivalent à $n \equiv 14 \pmod{20}$.

Conclusion : on a $3^n \equiv n \pmod 5$ si et seulement si le reste dans la division euclidienne de $n$ par 20 est parmi 7, 13, 14, 16.

## Exercice 2 : 24 heures chrono (4 pts)

1) *(1 pt) Montrer que le groupe $\mathbb{Z}/24\mathbb{Z}$ a autant de générateurs que de sous-groupes. Faire la liste des générateurs. Faire la liste des sous-groupes, en décrivant chaque sous-groupe de la manière la plus explicite possible.*

- ▷ Les générateurs de $\mathbb{Z}/24\mathbb{Z}$ sont les éléments $\overline{a}$ avec $a \wedge 24 = 1$. On remarque que comme $24 = 2^3 \times 3$, cela revient à demander que $a$ ne soit divisible ni par 2 ni par 3. On obtient donc la liste des générateurs :

$$\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{-11}, \overline{-7}, \overline{-5}, \overline{-1}.$$

- ▷ Les sous-groupes de $\mathbb{Z}/24\mathbb{Z}$ sont les $\langle \overline{d} \rangle$, avec $d$ un diviseur positif de 24, et ces sous-groupes sont deux à deux distincts. On obtient donc les sous-groupes :

$$\begin{aligned}
\langle \overline{1} \rangle &= \mathbb{Z}/24\mathbb{Z};\\
\langle \overline{2} \rangle &= \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}\};\\
\langle \overline{3} \rangle &= \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}\};\\
\langle \overline{4} \rangle &= \{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}, \overline{20}\};\\
\langle \overline{6} \rangle &= \{\overline{0}, \overline{6}, \overline{12}, \overline{18}\};\\
\langle \overline{8} \rangle &= \{\overline{0}, \overline{8}, \overline{16}\};\\
\langle \overline{12} \rangle &= \{\overline{0}, \overline{12}\};\\
\langle \overline{24} \rangle &= \{\overline{0}\}.
\end{aligned}$$

2) *(1 pt) Montrer que le groupe $(\mathbb{Z}/24\mathbb{Z})^\times$ peut être engendré par 3 de ses éléments.*

Par la question précédente on a :

$$(\mathbb{Z}/24\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{-11}, \overline{-7}, \overline{-5}, \overline{-1}\}.$$

Les égalités suivantes montrent qu'il peut être engendré par $\overline{5}, \overline{7}, \overline{-1}$ :

$$\begin{aligned}
\overline{11} &= \overline{5} \times \overline{7};\\
\overline{-11} &= \overline{5} \times \overline{7} \times \overline{-1};\\
\overline{-7} &= \overline{7} \times \overline{-1};\\
\overline{-5} &= \overline{5} \times \overline{-1}.
\end{aligned}$$

(Il y a d'autres systèmes de générateurs possibles.)

3) *(1 pt) Lister les sous-groupes d'ordre 2 du groupe $(\mathbb{Z}/24\mathbb{Z})^\times$.*

Un sous-groupe d'ordre 2 de $(\mathbb{Z}/24\mathbb{Z})^\times$ est de la forme $\{\overline{1}, \overline{a}\}$ avec $\overline{a} \neq \overline{1}$ et $\overline{a}^2 = \overline{1}$, c'est-à-dire $\overline{a}$ un élément d'ordre 2 de $(\mathbb{Z}/24\mathbb{Z})^\times$. Un calcul rapide montre que tous les éléments $\neq \overline{1}$ sont d'ordre 2 dans $(\mathbb{Z}/24\mathbb{Z})^\times$, et donc il y a 7 sous-groupes d'ordre 2 de $(\mathbb{Z}/24\mathbb{Z})^\times$ :

$$\{\overline{1}, \overline{5}\}, \{\overline{1}, \overline{7}\}, \{\overline{1}, \overline{11}\}, \{\overline{1}, \overline{-11}\}, \{\overline{1}, \overline{-7}\}, \{\overline{1}, \overline{-5}\}, \{\overline{1}, \overline{-1}\}.$$

4) *(1 pt) Donner un exemple de sous-groupe d'ordre 4 du groupe $(\mathbb{Z}/24\mathbb{Z})^\times$. (Bonus : lister tous les sous-groupes d'ordre 4.)*

On montre que $\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ est un sous-groupe de $(\mathbb{Z}/24\mathbb{Z})^\times$ :

- ▷ il contient $\overline{1}$ ;
- ▷ il est stable par produit car $\overline{5}^2 = \overline{7}^2 = \overline{11}^2 = \overline{1}$, et $\overline{5} \times \overline{7} = \overline{11}$, $\overline{5} \times \overline{11} = \overline{7}$, $\overline{7} \times \overline{11} = \overline{5}$ ;
- ▷ il est stable par passage à l'inverse car $\overline{5}^{-1} = \overline{5}$, $\overline{7}^{-1} = \overline{7}$, $\overline{11}^{-1} = \overline{11}$.

Pour le bonus : les sous-groupes d'ordre 4 de $(\mathbb{Z}/24\mathbb{Z})^\times$ sont

$$\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}, \{\overline{1}, \overline{5}, \overline{-7}, \overline{-11}\}, \{\overline{1}, \overline{-5}, \overline{7}, \overline{-11}\}, \{\overline{1}, \overline{-5}, \overline{-7}, \overline{11}\},$$

$$\{\overline{1}, \overline{5}, \overline{-1}, \overline{-5}\}, \{\overline{1}, \overline{7}, \overline{-1}, \overline{-7}\}, \{\overline{1}, \overline{11}, \overline{-1}, \overline{-11}\}.$$

## Exercice 3 : transformations affines (4 pts).

1) *Pour $(a, b)$ et $(a', b')$ deux éléments de $\mathbb{R}^* \times \mathbb{R}$, on définit*

$$(a, b)\#(a', b') = (aa', b + ab').$$

a) *(1,5 pt) Montrer que $\mathbb{R}^* \times \mathbb{R}$, muni de la loi de composition interne $\#$, est un groupe.*

On vérifie les axiomes du cours.

▷ Associativité. Soient $(a, b), (a', b'), (a'', b'') \in \mathbb{R}^* \times \mathbb{R}$. On calcule :

$$\big((a, b)\#(a', b')\big)\#(a'', b'') = (aa', b + ab')\#(a'', b'') = (aa'a'', b + ab' + aa'b'')$$

et

$$(a, b)\#\big((a', b')\#(a'', b'')\big) = (a, b)\#(a'a'', b' + a'b'') = (aa'a'', b + ab' + aa'b'').$$

On a donc l'égalité : $((a, b)\#(a', b'))\#(a'', b'') = (a, b)\#((a', b')\#(a'', b''))$.

▷ Existence d'un élément neutre. On vérifie que $(1, 0)$ est neutre pour $\#$ : pour tout $(a, b) \in \mathbb{R}^* \times \mathbb{R}$ on a :

$$(1, 0)\#(a, b) = (1 \times a, 0 + 1 \times b) = (a, b) \quad \text{et} \quad (a, b)\#(1, 0) = (a \times 1, b + a \times 0) = (a, b).$$

▷ Existence d'inverses. Soit $(a, b) \in \mathbb{R}^* \times \mathbb{R}$. On cherche un inverse $(a', b')$ de $(a, b)$ pour la loi $\#$. En écrivant l'égalité $(a, b)\#(a', b') = (1, 0)$, on voit qu'on doit avoir $aa' = 1$ et $b + ab' = 0$. Cela pousse donc à poser $a' = \frac{1}{a}$ et $b' = -\frac{b}{a}$. On calcule alors

$$(a, b)\#(\tfrac{1}{a}, -\tfrac{b}{a}) = (a \times \tfrac{1}{a}, b + a \times (-\tfrac{b}{a})) = (1, 0)$$

et

$$(\tfrac{1}{a}, -\tfrac{b}{a})\#(a, b) = (\tfrac{1}{a} \times a, -\tfrac{b}{a} + \tfrac{1}{a} \times b) = (1, 0).$$

Donc $(a, b)$ est inversible pour $\#$ et son inverse est $(\frac{1}{a}, -\frac{b}{a})$.

b) *(0,5 pt) Ce groupe est-il abélien ? On justifiera.*

Le groupe $(\mathbb{R}^* \times \mathbb{R}, \#)$ n'est pas abélien. Par exemple on peut calculer :

$$(1,1)\#(2,0) = (1\times 2, 1+1\times 0) = (2,1) \quad \text{et} \quad (2,0)\#(1,1) = (2\times 1, 0+2\times 1) = (2,2).$$

2) *Pour $(a,b) \in \mathbb{R}^* \times \mathbb{R}$ on considère l'application*

$$f_{a,b} : \mathbb{R} \longrightarrow \mathbb{R}\ ,\ x \mapsto ax+b.$$

*On remarque (on ne demande pas de justification) que c'est une application bijective. On rappelle la notation $\mathrm{Bij}(E)$ pour le groupe des permutations d'un ensemble $E$.*

a) *(1 pt) Montrer que l'application*

$$\Phi : \mathbb{R}^* \times \mathbb{R} \longrightarrow \mathrm{Bij}(\mathbb{R})\ ,\ (a,b) \mapsto f_{a,b}$$

*est un morphisme de groupes, où la structure de groupe de $\mathbb{R}^* \times \mathbb{R}$ est celle de la question précédente.*

Soient $(a,b),(a',b') \in \mathbb{R}^* \times \mathbb{R}$. On veut montrer l'égalité :

$$\Phi\left((a,b)\#(a',b')\right) \stackrel{?}{=} \Phi(a,b) \circ \Phi(a',b'),$$

c'est-à-dire :

$$f_{aa',b+ab'} \stackrel{?}{=} f_{a,b} \circ f_{a',b'}.$$

On calcule donc la composée $f_{a,b} \circ f_{a',b'}$ : pour $x \in \mathbb{R}$ on a

$$f_{a,b}(f_{a',b'}(x)) = f_{a,b}(a'x+b') = a(a'x+b')+b = (aa')x + (b+ab') = f_{aa',b+ab'}(x).$$

Donc $f_{aa',b+ab'} = f_{a,b} \circ f_{a',b'}$ et on a montré que $\Phi$ est un morphisme de groupes.

b) *(1 pt) Montrer que ce morphisme de groupes est injectif.*

On montre que $\ker(\Phi) = \{(1,0)\}$. Soit $(a,b) \in \mathbb{R}^* \times \mathbb{R}$ tel que $\Phi(a,b) = \mathrm{id}_{\mathbb{R}}$. Cela veut dire que $f_{a,b} = \mathrm{id}_{\mathbb{R}}$ ou encore que :

$$\forall x \in \mathbb{R},\ ax+b = x.$$

En spécifiant $x=0$, on obtient $b=0$. En spécifiant $x=1$, on obtient $a+b=1$, et donc $a=1$. Donc $(a,b)=(1,0)$. On a donc montré que $\ker(\Phi) = \{(1,0)\}$ et donc que $\Phi$ est un morphisme de groupes injectif.

## Exercice 4 : union de sous-groupes (3 pts).

1) *(2 pts) Soit $G$ un groupe et $H$, $K$ deux sous-groupes de $G$. Montrer que $H \cup K$ est un sous-groupe de $G$ si et seulement si $H \subset K$ ou $K \subset H$.*

On procède (évidemment) par double implication.

- ▷ Si $H \subset K$ alors $H \cup K = K$ qui est un sous-groupe de $G$ par hypothèse. Si $K \subset H$ alors $H \cup K = H$ qui est un sous-groupe de $G$ par hypothèse.
- ▷ On suppose que $H \cup K$ est un sous-groupe de $G$ et on montre que $H \subset K$ ou $K \subset H$. On procède par l'absurde : supposons que $H \not\subset K$ et $K \not\subset H$. Cela veut dire qu'il existe $h \in H$ tel que $h \notin K$ et qu'il existe $k \in K$ tel que $k \notin H$. Comme $h$ et $k$ sont tous les deux des éléments de $H \cup K$ et que $H \cup K$ est un sous-groupe de $G$, on en déduit que $hk \in H \cup K$, c'est-à-dire que $hk \in H$ ou $hk \in K$. On fait une disjonction de cas.

- Supposons que $hk \in H$. Comme $H$ est un sous-groupe de $G$ et que $h \in H$, on en déduit que $h^{-1}(hk) \in H$, c'est-à-dire que $k \in H$, ce qui est faux.
- Supposons que $hk \in K$. Comme $K$ est un sous-groupe de $G$ et que $k \in K$, on en déduit que $(hk)k^{-1} \in K$, c'est-à-dire que $h \in K$, ce qui est faux.

On obtient donc une contradiction dans tous le cas. Fin de la preuve par l'absurde : on a montré que $H \subset K$ ou $K \subset H$.

2) *(1 pt) Donner un exemple de groupe $G$ et de trois sous-groupes $H$, $K$, $L$ qui sont tous les trois différents de $G$ et tels que $G = H \cup K \cup L$.*

Le groupe $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est l'union de ses trois sous-groupes d'ordre 2, qui sont

$$H = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{0})\} \ \ , \ \ K = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1})\} \ \ , \ \ L = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{1})\}.$$