HAX501X – Groupes et anneaux 1

Examen (session 1) – Correction

Questions diverses (5 pts).

1) *Dans le groupe $\mathbb{Z}/1200\mathbb{Z}$, quel est l'ordre du groupe engendré par $\overline{486}$? On justifiera.*

   Par le cours, ce groupe est d'ordre
   $$\frac{1200}{486 \wedge 1200}.$$
   Pour calculer le PGCD de 486 et 1200, on peut décomposer en produit de nombres premiers, ou utiliser l'algorithme d'Euclide. On trouve $486 \wedge 1200 = 6$, et donc l'ordre recherché est $\frac{1200}{6} = 200$.

2) *Dans le groupe $\mathbb{C}^*$, lister les éléments d'ordre 6. (Sans démonstration.)*

   Les nombres complexes $z \in \mathbb{C}^*$ qui vérifient $z^6 = 1$ sont les 6 racines 6-èmes de l'unité $e^{\frac{2i\pi k}{6}}$ avec $k = 0, 1, 2, 3, 4, 5$. Si l'on note $\xi = e^{\frac{2i\pi}{6}}$, ce sont les éléments ξ^k avec $k = 0, 1, 2, 3, 4, 5$. Parmi ceux-ci, seuls ξ et ξ^5 sont d'ordre 6. En effet, $\xi^0 = 1$ est d'ordre 1, ξ^3 est d'ordre 2 et ξ^2 et ξ^4 sont d'ordre 3. Conclusion : les éléments d'ordre 6 dans le groupe $\mathbb{C}^*$ sont
   $$e^{\frac{2i\pi}{6}} = e^{\frac{i\pi}{3}} \quad \text{et} \quad e^{\frac{2i\pi\cdot 5}{6}} = e^{\frac{5i\pi}{3}} = e^{-\frac{i\pi}{3}}.$$

3) *Dans $\mathbb{R}^2$, soit r la rotation d'angle $\frac{\pi}{3}$ et soit s la réflexion par rapport à l'axe des ordonnées $\mathbb{R}(0,1)$. Décrire précisément la composée $s \circ r$. (Sans démonstration.)*

   Notons Δ l'axe des ordonnées. D'après le cours, la composée $s \circ r$ est la réflexion par rapport à la droite $r_{-\pi/6}(\Delta)$, qui est la droite qui forme un angle orienté $\frac{\pi}{3}$ en partant de l'axe des abscisses.

4) *Dans l'anneau $\mathbb{R}[X]$, décrire concrètement l'idéal $(X^2, X^2 - 2X + 1)$. On justifiera.*

   D'après le cours, l'idéal de $\mathbb{R}[X]$ engendré par deux polynômes f, g est égal à l'idéal engendré par le PGCD $f \wedge g$. Ici on voit facilement que X^2 et $X^2 - 2X + 1$ sont premiers entre eux, soit grâce à l'algorithme d'Euclide, soit en factorisant $X^2 - 2X + 1 = (X-1)^2$. Donc l'idéal qu'ils engendrent est l'idéal engendré par 1, c'est-à-dire $\mathbb{R}[X]$.

5) *Soient A, B des anneaux commutatifs, $f : A \to B$ un morphisme d'anneaux, et J un idéal de B. Montrer que l'image réciproque $f^{-1}(J)$ est un idéal de A. (On montrera notamment que c'est un sous-groupe de A.)*

   ▷ On a $f(0_A) = 0_B$ (parce que f est un morphisme de groupes) et $0_B \in J$ (car J est un sous-groupe de B), et donc $0_A \in f^{-1}(J)$.

   ▷ Soient $x, x' \in f^{-1}(J)$, c'est-à-dire x, x' sont des éléments de A tels que $f(x), f(x') \in J$. Comme f est un morphisme de groupes on a que $f(x + x') = f(x) + f(x')$, qui est dans J car J est un sous-groupe de B. Donc $x + x' \in f^{-1}(J)$.

▷ Soit $x \in f^{-1}(J)$, c'est-à-dire x est un élément de A tel que $f(x) \in J$. Comme f est un morphisme de groupes on a que $f(-x) = -f(x)$, qui est dans J car J est un sous-groupe de B. Donc $-x \in f^{-1}(J)$.

▷ Soit $x \in J$, c'est-à-dire x est un élément de A tel que $f(x) \in J$; soit $a \in A$ un autre élément. Comme f est un morphisme d'anneaux, on a que $f(ax) = f(a)f(x)$, qui est un élément de J car J est un idéal de B. Donc $ax \in f^{-1}(J)$.

Exercice 1 : autour du groupe produit (6 pts). *Pour un groupe G et deux sous-groupes H, K de G, on considère les conditions suivantes.*

(i) Pour tout $x \in G$, il existe $y \in H$ et $z \in K$ tels que $x = yz$.

(ii) $H \cap K = \{e\}$.

(iii) Les éléments de H et K commutent entre eux : $\forall y \in H$, $\forall z \in K$, $yz = zy$.

Les quatre questions sont indépendantes.

1) *Soit $G = (\mathbb{Z}/11\mathbb{Z})^\times$, soit H le sous-groupe engendré par $\overline{3}$, et K le sous-groupe engendré par $\overline{10}$. Lister les éléments de H et K, et démontrer que H et K vérifient les conditions (i), (ii), (iii).*

Listons d'abord les éléments de G :

$$G = \{\overline{1}, \overline{2}, \dots, \overline{10}\}.$$

Puis les éléments de H :

$$H = \{\overline{1}, \overline{3}, \overline{3}^2, \dots\} = \{\overline{1}, \overline{3}, \overline{9}, \overline{5}, \overline{4}\} = \{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\}.$$

Et enfin les éléments de K :

$$K = \{\overline{1}, \overline{10}, \overline{10}^2, \dots\} = \{\overline{1}, \overline{10}\} = \{\overline{1}, \overline{-1}\}.$$

(i) La condition est clairement vérifiée pour les x qui sont dans H ou K, et il suffit donc de traiter le cas des x restants : $\overline{2} = \overline{-9} = \overline{9} \times \overline{-1}$; $\overline{6} = \overline{-5} = \overline{5} \times \overline{-1}$; $\overline{7} = \overline{-4} = \overline{4} \times \overline{-1}$; $\overline{8} = \overline{-3} = \overline{3} \times \overline{-1}$.

(ii) On voit clairement que $H \cap K = \{\overline{1}\}$.

(iii) C'est évident car G est un groupe abélien (car la loi $\times$ dans $\mathbb{Z}/11\mathbb{Z}$ est commutative).

2) *Soient G_1, G_2 deux groupes, et soit $G = G_1 \times G_2$ leur produit. On note e_1 et e_2 les éléments neutres respectifs de G_1 et G_2. Montrer que les ensembles $H = G_1 \times \{e_2\}$ et $K = \{e_1\} \times G_2$ sont deux sous-groupes de G qui vérifient les conditions (i), (ii), (iii).*

On montre que H est un sous-groupe de G, le cas de K étant similaire :

▷ Le neutre (e_1, e_2) de G est clairement dans H.

▷ Soient deux éléments $(x_1, e_2), (x_1', e_2) \in H$ (avec $x_1, x_1' \in G_1$). Alors leur produit dans G est

$$(x_1, e_2)(x_1', e_2) = (x_1 x_1', e_2 e_2) = (x_1 x_1', e_2),$$

qui est dans H. Donc H est stable par produit.

▷ Soit un élément $(x_1, e_2) \in H$ (avec $x_1 \in G_1$). Son inverse dans G est

$$(x_1, e_2)^{-1} = (x_1^{-1}, e_2^{-1}) = (x_1^{-1}, e_2)$$

qui est dans H. Donc H est stable par passage à l'inverse.

On montre maintenant que H, K vérifient les conditions (i), (ii), (iii) :

(i) Un élément $x \in G$ s'écrit (x_1, x_2) avec $x_1 \in G_1$ et $x_2 \in G_2$. Or, on peut écrire

$$(x_1, x_2) = (x_1 e_1, e_2 x_2) = (x_1, e_2)(e_1, x_2),$$

qui est donc le produit d'un élément de H et d'un élément de K.

(ii) Clairement, le seul élément de G qui est à la fois dans H et K est (e_1, e_2), qui est l'élément neutre de G.

(iii) Soient deux éléments $(x_1, e_2) \in H$ (avec $x_1 \in G_1$) et $(e_1, x_2) \in K$ (avec $x_2 \in G_2$). On calcule :

$$(x_1, e_2)(e_1, x_2) = (x_1 e_1, e_2 x_2) = (x_1, x_2)$$

et

$$(e_1, x_2)(x_1, e_2) = (e_1 x_1, x_2 e_2) = (x_1, x_2),$$

et donc (x_1, e_2) et (e_1, x_2) commutent.

3) *Soit G un groupe et H, K deux sous-groupes qui vérifient les conditions (i), (ii), (iii).*

a) *Démontrer que pour un élément $x \in G$, l'écriture $x = yz$ avec $y \in H$ et $z \in K$ est unique.*

Supposons qu'on ait deux écritures $x = yz$ et $x = y'z'$ avec $y, y' \in H$ et $z, z' \in K$. On a donc l'égalité $yz = y'z'$, qu'on peut réécrire sous la forme :

$$(y')^{-1} y = z' z^{-1}.$$

Or, H et K sont des sous-groupes de G, et donc $(y')^{-1} y \in H$ et $z' z^{-1} \in K$. Comme ces deux éléments sont égaux et que par la condition (ii), $H \cap K = \{e\}$, on en conclut que $(y')^{-1} y = e$ et $z' z^{-1} = e$. Cela implique que $y = y'$ et $z = z'$. Donc l'écriture $x = yz$ avec $y \in H$ et $z \in K$ est bien unique.

b) *Démontrer qu'il existe un isomorphisme entre le groupe produit $H \times K$ et G.*

On définit une application

$$f : H \times K \longrightarrow G \quad , \quad (y, z) \mapsto yz.$$

La condition (i) et la question précédente disent exactement que f est une bijection. Il reste à montrer que c'est un morphisme de groupes. Soient $(y, z), (y', z') \in H \times K$, On calcule :

$$f((y, z)(y', z')) = f(yy', zz') = yy'zz'$$

et

$$f(y, z) f(y', z') = yzy'z'.$$

Par la condition (iii) on a $y'z = zy'$ et donc $f((y, z)(y', z')) = f(y, z) f(y', z')$. Donc f est un morphisme de groupes, et donc un isomorphisme de groupes.

4) *On pose $G = D_4$, le groupe diédral à 8 éléments. Trouver deux sous-groupes H, K de G, différents de $\{e\}$ et G, pour lesquels (i) et (ii) sont vrais mais pas (iii). On justifiera soigneusement ces faits.*

Écrivons, comme dans le cours, $D_4 = \{\mathrm{id}, r, r^2, r^3, s, rs, r^2 s, r^3 s\}$. On définit

$$H = \langle r \rangle = \{\mathrm{id}, r, r^2, r^3\} \quad \text{et} \quad K = \langle s \rangle = \{\mathrm{id}, s\}.$$

Il est clair que les conditions (i) et (ii) sont vérifiées, vu la manière dont a représenté les éléments de D_4. Mais (iii) n'est pas vérifiée car $rs \neq sr$. En effet, $sr = r^{-1}s = r^3 s$.

Exercice 2 : sous-anneaux de $\mathbb{Z}^2$ (6 pts). *On se place dans l'anneau $\mathbb{Z}^2$. Pour tout $n \in \mathbb{N}$ on définit*

$$A_n = \{(x, y) \in \mathbb{Z}^2 \mid x \equiv y \pmod{n}\}.$$

1) *Montrer que A_n est un sous-anneau de $\mathbb{Z}^2$.*

   On vérifie les axiomes un par un :

   - ▷ $(0, 0) \in A_n$ car $0 \equiv 0 \pmod{n}$.
   - ▷ Soient $(x, y), (x', y') \in A_n$. Alors $x \equiv y \pmod{n}$ et $x' \equiv y' \pmod{n}$, et donc $x + x' \equiv y + y' \pmod{n}$ d'où $(x + x', y + y') \in A_n$, c'est-à-dire $(x, y) + (x', y') \in A_n$.
   - ▷ Soit $(x, y) \in A_n$, c'est-à-dire $x \equiv y \pmod{n}$. Alors $-x \equiv -y \pmod{n}$, et donc $(-x, -y) \in A_n$, d'où $-(x, y) \in A_n$.
   - ▷ $(1, 1) \in A_n$ car $1 \equiv 1 \pmod{n}$.
   - ▷ Soient $(x, y), (x', y') \in A_n$. Alors $x \equiv y \pmod{n}$ et $x' \equiv y' \pmod{n}$, et donc $xx' \equiv yy' \pmod{n}$ d'où $(xx', yy') \in A_n$, c'est-à-dire $(x, y)(x', y') \in A_n$.

2) *Soit A un sous-anneau de $\mathbb{Z}^2$. On veut montrer qu'il existe $n \in \mathbb{N}$ tel que $A = A_n$.*

   a) *Montrer que pour $k \in \mathbb{Z}$ on a : $(k, k) \in A$.*

   Comme A est un sous-anneau de $\mathbb{Z}^2$, on a que $(1, 1) \in A$. Or A est un sous-groupe de $\mathbb{Z}^2$, donc pour tout $k \in \mathbb{Z}$, $k(1, 1) \in A$, c'est-à-dire $(k, k) \in A$.

   b) *Montrer que pour $k \in \mathbb{Z}$ on a : $(k, 0) \in A \iff (0, k) \in A$.*

   On montre $\Longrightarrow$, la réciproque étant prouvée de la même manière. Soit $k \in \mathbb{Z}$ tel que $(k, 0) \in A$. Comme A est un sous-groupe de $\mathbb{Z}^2$ et que $(k, k) \in A$ par la question précécente, on a donc que $(k, k) - (k, 0) \in A$, c'est-à-dire $(0, k) \in A$.

   c) *On suppose qu'il n'existe pas d'élément de A de la forme $(0, y)$ avec $y \neq 0$. Montrer que $A = A_0$. (Avant cela il est conseillé de réfléchir quelques instants à ce qu'est le sous-anneau A_0.)*

   Le sous-anneau A_0 est l'ensemble des $(x, y) \in \mathbb{Z}^2$ tels que $x \equiv y \pmod{0}$, ce qui revient à dire que $x - y$ est un multiple de 0, c'est-à-dire $x = y$. Donc :

$$A_0 = \{(k, k),\ k \in \mathbb{Z}\}.$$

   La question 2)a) a donc montré que pour tout sous-anneau A de $\mathbb{Z}^2$, on a $A_0 \subset A$. On suppose maintenant qu'il n'existe pas d'élément de A de la forme $(0, y)$ avec $y \neq 0$, et on veut montrer que $A \subset A_0$. Soit $(x, y) \in A$. Comme A est un sous-groupe de $\mathbb{Z}^2$ et que $(x, x) \in A$ par la question 2)a), on en conclut que $(x, y) - (x, x) \in A$, c'est-à-dire $(0, y - x) \in A$. Par l'hypothèse, on ne peut pas avoir $y - x \neq 0$, et donc $y - x = 0$ d'où $y = x$. Donc $(x, y) = (x, x) \in A_0$.

   d) *On suppose qu'il existe un élément de A de la forme $(0, y)$ avec $y \neq 0$. Soit n le plus petit entier $\geqslant 1$ tel que $(0, n) \in A$. Montrer que $A = A_n$.*

   - ▷ On montre que $A_n \subset A$. Soit $(x, y) \in A_n$, alors $x \equiv y \pmod{n}$, et donc il existe $k \in \mathbb{Z}$ tel que $y = x + kn$. On a donc

$$(x, y) = (x, x + kn) = (x, x) + k(0, n).$$

     Or, $(x, x) \in A$ par la question 2)a), et $(0, n) \in A$; comme A est un sous-groupe de $\mathbb{Z}^2$, on en conclut que $(x, y) \in A$.

- ▷ On montre que $A \subset A_n$. Soit $(x, y) \in A$. Comme $(x, x) \in A$ par la question 2)a) et que A est un sous-groupe de $\mathbb{Z}^2$, on a que $(x, y) - (x, x) \in A$, c'est-à-dire $(0, y - x) \in A$. Effectuons la division euclidienne de $y - x$ par n :

$$y - x = qn + r \qquad \text{avec } q, r \in \mathbb{Z} \text{ et } 0 \leqslant r < n.$$

On a donc

$$(0, y - x) - q(0, n) = (0, r).$$

Comme A est un sous-groupe de $\mathbb{Z}^2$ et que $(0, n) \in A$, on a donc que $(0, r) \in A$. On ne peut pas avoir $1 \leqslant r < n$ car cela contredirait la minimalité de n, et donc $r = 0$, d'où $x \equiv y \pmod{n}$, et donc $(x, y) \in A_n$.

Exercice 3 : un anneau intègre qui n'est pas factoriel (4 pts). *On définit*

$$\mathbb{Z}[i\sqrt{3}] = \{a + bi\sqrt{3}\ ,\ a, b \in \mathbb{Z}\}\ .$$

Pour gagner du temps, on admettra que $\mathbb{Z}[i\sqrt{3}]$ est un sous-anneau de $\mathbb{C}$. (Vous pouvez aussi le vérifier rapidement au brouillon.)

1) *Pour un élément $z = a + bi\sqrt{3} \in \mathbb{Z}[i\sqrt{3}]$ on définit sa norme*

$$N(z) = z\overline{z} = |z|^2 = a^2 + 3b^2\ .$$

a) *Montrer que pour tous $z, z' \in \mathbb{Z}[i\sqrt{3}]$ on a $N(zz') = N(z)N(z')$.*

Cette égalité est une conséquence immédiate de l'égalité, valide pour tous $z, z' \in \mathbb{C}$: $|zz'| = |z| \cdot |z'|$.

b) *Montrer qu'un $z \in \mathbb{Z}[i\sqrt{3}]$ est inversible si et seulement si $N(z) = 1$. Décrire le groupe $\mathbb{Z}[i\sqrt{3}]^\times$.*

On montre l'équivalence demandée :

- ▷ Soit $z \in \mathbb{Z}[i\sqrt{3}]$ tel que z est inversible, alors il existe $z' \in \mathbb{Z}[i\sqrt{3}]$ tel que $zz' = 1$. En prenant les normes et en utilisant la question précédente, on obtient $N(z)N(z') = 1$. Comme $N(z)$ et $N(z')$ sont des entiers naturels, on en conclut que $N(z) = N(z') = 1$.
- ▷ Soit $z \in \mathbb{Z}[i\sqrt{3}]$, et supposons que $N(z) = 1$. On a donc $z\overline{z} = 1$. On remarque que $\overline{z} \in \mathbb{Z}[i\sqrt{3}]$ car pour $z = a + bi\sqrt{3}$ on a $\overline{z} = a - bi\sqrt{3}$. Donc z est inversible dans $\mathbb{Z}[i\sqrt{3}]$, d'inverse $\overline{z}$.

On peut donc maintenant comprendre l'ensemble des inversibles de $\mathbb{Z}[i\sqrt{3}]$: pour $z = a + bi\sqrt{3} \in \mathbb{Z}[i\sqrt{3}]$ on a :

$$N(z) = 1 \quad \Longleftrightarrow \quad a^2 + 3b^2 = 1.$$

Clairement, vu que $a, b \in \mathbb{Z}$, cette égalité implique $b = 0$ puisque sinon on aurait $a^2 + 3b^2 \geqslant 3 \cdot 1^2 = 3$. Les seules solutions sont donc $(a, b) = (1, 0)$ et $(a, b) = (-1, 0)$, qui correspondent à $z = 1$ et $z = -1$. Donc le groupe des inversibles de $\mathbb{Z}[i\sqrt{3}]$ est

$$\mathbb{Z}[i\sqrt{3}]^\times = \{1, -1\}.$$

2) *Dresser les listes des éléments de norme 2 et de norme 4 dans $\mathbb{Z}[i\sqrt{3}]$.*

▷ Un élément $z = a + bi\sqrt{3} \in \mathbb{Z}[i\sqrt{3}]$ de norme 2 doit satisfaire $a^2 + 3b^2 = 2$. Cette égalité implique $b = 0$ car sinon on aurait $a^2 + 3b^2 \geqslant 3 \cdot 1^2 = 3$; on a donc $a^2 = 2$, qui est impossible. Conclusion : il n'y a aucun élément de norme 2 dans $\mathbb{Z}[i\sqrt{3}]$.

▷ Un élément $z = a + bi\sqrt{3} \in \mathbb{Z}[i\sqrt{3}]$ de norme 4 doit satisfaire $a^2 + 3b^2 = 4$. On a la possibilité $b = 0$ et $a = \pm 2$, qui correspondent à $z = 2$ et $z = -2$, et $b = \pm 1$ et $a = \pm 1$, qui correspondent à $z = 1 + i\sqrt{3}$, $z = -1 - i\sqrt{3}$, $z = 1 - i\sqrt{3}$, $z = -1 + i\sqrt{3}$. Ce sont les seules car si $|b| \geqslant 2$ alors $a^2 + 3b^2 \geqslant 3 \cdot 2^2 = 12$. Conclusion : les éléments de norme 4 dans $\mathbb{Z}[i\sqrt{3}]$ sont

$$2, -2, 1 + i\sqrt{3}, -1 - i\sqrt{3}, 1 - i\sqrt{3}, -1 + i\sqrt{3}.$$

3) *Montrer que tous les éléments de norme 4 sont irréductibles dans $\mathbb{Z}[i\sqrt{3}]$.*

[Cette question ne nécessite pas de savoir quels sont les éléments de norme 4 ; il suffit de savoir qu'il n'existe aucun élément de norme 2 et que les éléments de norme 1 sont inversibles...]
Soit $z \in \mathbb{Z}[i\sqrt{3}]$ un élément de norme 4. Clairement, z n'est ni 0 ni inversible, par la question 1)b). Soient $z_1, z_2 \in \mathbb{Z}[i\sqrt{3}]$ tels que $z = z_1 z_2$. En prenant la norme on obtient alors

$$N(z_1)N(z_2) = 4.$$

Comme $N(z_1), N(z_2)$ sont des entiers naturels, ils valent soit $1, 4$, soit $4, 1$, soit $2, 2$. Mais par la question précédente il n'existe aucun élément de norme 2 dans $\mathbb{Z}[i\sqrt{3}]$, et donc on a soit $N(z_1) = 1$ soit $N(z_2) = 1$. Par la question 1)b), on en conclut que z_1 ou z_2 est inversible. On a donc prouvé que z est irréductible.

4) *En déduire que $\mathbb{Z}[i\sqrt{3}]$ n'est pas un anneau factoriel. (Indication : multiplier entre eux les éléments de norme 4.)*

On a l'égalité :

$$(1 + i\sqrt{3})(1 - i\sqrt{3}) = 4 = 2 \cdot 2.$$

Par la question précédente, cela donne deux décompositions de 4 en produit d'éléments irréductibles dans $\mathbb{Z}[i\sqrt{3}]$. Ces deux décompositions sont *vraiment différentes* même à ordre et association près, car $1 + i\sqrt{3}$ et 2 ne sont pas associés. (En effet, par la question 1)b), deux éléments $z, z' \in \mathbb{Z}[i\sqrt{3}]$ sont associés si et seulement si $z = \pm z'$.) On en conclut que $\mathbb{Z}[i\sqrt{3}]$ n'est pas un anneau factoriel : c'est l'unicité de la décomposition en produit d'éléments irréductibles qui n'est pas vérifiée.

5) *(Question bonus) On a vu en TD que $\mathbb{Z}[i]$ est un anneau euclidien (et donc principal, donc factoriel). Si l'on essaye de copier la preuve de ce fait dans le cas de $\mathbb{Z}[i\sqrt{3}]$, qu'est-ce qui ne fonctionne pas ?*

Dans le cas de $\mathbb{Z}[i]$, le fait qui faisait tout fonctionner était que tout $z \in \mathbb{C}$ est à distance strictement inférieure à 1 d'un élément de $\mathbb{Z}[i]$. En effet, le pire cas est la distance $\frac{\sqrt{2}}{2} < 1$, qui correspond à un point au milieu d'un carré de côté 1.
Dans le cas de $\mathbb{Z}[i\sqrt{3}]$, le carré de côté 1 est remplacé par un rectangle de côtés 1 et $\sqrt{3}$, et un point au milieu d'un tel rectangle est à distance *exactement* 1 des 4 sommets du rectangle... L'argument qu'on a utilisé pour $\mathbb{Z}[i]$ ne s'applique donc pas ici.