1
2
3

MAT35B - ALGÈBRE L3A
Premier Semestre — 2022-2023

Troisième Devoir Surveillé

Toute réponse non justifiée ne sera pas validée.

Le barème est donné à titre indicatif et non contractuel.

3pt **1.** Quels sont tous les groupes de cardinal 15 à isomorphisme près ?

Solution. On va démontrer qu'il existe un seul groupe de cardinal 15 à isomorphisme près : $\mathbb{Z}/15.\mathbb{Z}$.

Pour $p \in \mathbb{N}^*$ on notera N_p le cardinal de l'ensemble $\{H \leq G : H \text{ est un } p\text{-sous-groupe de Sylow de } G\}$. Le théorème de Sylow nous dit que $N_p = 1 \pmod p$ et que $N_p | m$ pour $|G| = p^r m$ avec m et p premier entre eux. Dans notre cas $N_3 = 1 \pmod 3$ et $N_3|5$, et $N_5 = 1 \pmod 5$ et $N_5|3$. En ce qui concerne N_3, la deuxième condition nous dit que $N_3 \in \{1,5\}$, et la première condition implique alors que $N_3 = 1$. En ce qui concerne N_5, la dernière condition nous dit que $N_3 \in \{1,3\}$, et la condition restante implique alors que $N_5 = 1$. On remarque que $N_p = 1$ si et seulement s'il existe un seul p-sous-groupe de Sylow H_p, ce qui implique en plus que ce seul p-sous-groupe de Sylow est distingué. Comme $N_3 = N_5 = 1$, et les sous groupes de Sylow H_3 et H_5 sont distingués. On remarque en plus que $H_3 \cap H_5 = \{1_G\}$, vu que, par le théorème de Lagrange, $|H_3 \cap H_5|$ est un diviseur de $|H_3| = 3$ et de $|H_5| = 5$. L'application $m : H_3 \times H_5 \to G$ qui associe xy à $(x,y) \in H_3 \times H_5$ est alors injective, et comme $|G| = |H_3 \times H_5|$ est fini, on voit que m est une application bijective. On rappelle que, comme H_3 et H_5 sont distingués et m est une application bijective, H_3 et H_5 commutent dans G, vu que

$$m\big(\underbrace{(yxy^{-1})}_{\in H_3}, y\big) = (yxy^{-1})y = yx = x(x^{-1}yx) = m\big(x, \underbrace{(x^{-1}yx)}_{\in H_5}\big)$$

nous dit que $x = yxy^{-1}$, *i.e.* $xy = yx$, pour tous $x \in H_3$ et $y \in H_5$, ce qui implique que m est un isomorphisme de groupes. En conséquence, $G = H_3 \times H_5$. Or, comme $|H_p| = p$ pour $p \in \{3,5\}$ et p est premier, H_p est un groupe cyclique, ce qui nous dit qu'il existe un isomorphisme de groupes $\mathbb{Z}/p.\mathbb{Z} \to H_p$ pour $p \in \{3,5\}$. Cela induit un isomorphisme de groupes $\mathbb{Z}/15.\mathbb{Z} \simeq \mathbb{Z}/3.\mathbb{Z} \times \mathbb{Z}/5.\mathbb{Z} \to G$. En conséquence, il existe un seul groupe de cardinal 15 à isomorphisme près : $\mathbb{Z}/15.\mathbb{Z}$.

5pt **2.** (*a*) Soit G un groupe de cardinal 20. Montrer que G contient un sous-groupe distingué H de cardinal 5 et un sous-groupe K de cardinal 4 tels que $G = H \rtimes K$.

(*b*) Montrer qu'il existe des groupes G_1 et G_2 de cardinal 20 qui ne contiennent pas d'élément d'ordre 4 tels que G_1 est commutatif et G_2 ne l'est pas.

Solution.

(*a*) Pour $p \in \mathbb{N}^*$ on notera N_p le cardinal de l'ensemble $\{H \leq G : H \text{ est un } p\text{-sous-groupe de Sylow de } G\}$. Le théorème de Sylow nous dit que $N_p = 1 \pmod p$ et que $N_p | m$ pour $|G| = p^r m$ avec m et p premier entre eux. Dans notre cas $N_2 = 1 \pmod 2$ et $N_2|5$, et $N_5 = 1 \pmod 5$ et $N_5|4$. En ce qui concerne N_2, la deuxième condition nous dit que $N_3 \in \{1,5\}$, tandis que la première condition devient superflue. En ce qui concerne N_5, la dernière condition nous dit que $N_3 \in \{1,2,4\}$, et la condition restante implique alors que $N_5 = 1$. On remarque que $N_p = 1$ si et seulement s'il existe un seul p-sous-groupe de Sylow H_p, ce qui implique en plus que ce seul p-sous-groupe de Sylow est distingué. Soit $H = H_5$ le seul 5-sous-groupe de Sylow de G et soit K un 2-sous-groupe de Sylow de G. On remarque en plus que $H \cap K = \{1_G\}$, vu que, par le théorème de Lagrange, $|H \cap K|$ est un diviseur de $|H| = 5$ et de $|K| = 4$. L'application $m : H \times K \to G$ qui associe xy à $(x,y) \in H \times K$ est alors injective, et comme $|G| = |H \times K|$ est fini, on voit que m est une application bijective. En conséquence, G est le produit semi-direct $H \rtimes K$, comme on voulait démontrer.

(*b*) On voit bien que $G_1 = \mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/10.\mathbb{Z}$ est un groupe abélien de cardinal 20 qui ne contiennent pas d'élément d'ordre 4. En effet, l'ordre de l'élément $(a,b) \in \mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/10.\mathbb{Z}$ est le PPCM des ordres de $a \in \mathbb{Z}/2.\mathbb{Z}$ et de $b \in \mathbb{Z}/10.\mathbb{Z}$, vu que $(a,\bar{0}) \in \mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/10.\mathbb{Z}$ et $(\bar{0},b) \in \mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/10.\mathbb{Z}$ commutent dans G_1. Comme l'ordre de a est un diviseur de 2 et l'ordre de b est un diviseur de 10, le PPCM des ordres de a et de b est un diviseur de 10, et *a fortiori* différent de 4. En outre, c'est clair que $G_2 = \mathsf{D}_{10}$, *i.e.* le groupe diédral d'ordre 20, est un groupe non abélien de cardinal 20 qui ne contiennent pas d'élément d'ordre 4. En effet, $\mathsf{D}_{10} = \{\tau^i\sigma^j : i \in \{0,1\}, j \in [\![0,9]\!]\}$ où $\tau^2 = \sigma^{10} = 1_{\mathsf{D}_{10}}$ et $\tau\sigma\tau = \sigma^{-1}$, ce qui nous dit que $(\tau\sigma^j)^2 = 1_{\mathsf{D}_{10}}$ pour tout $j \in [\![0,9]\!]$. Cela implique que l'ordre de tout élément de la forme σ^j pour $j \in [\![0,9]\!]$ est un diviseur de 10, et *a fortiori* différent de 4, et que l'ordre de tout élément de la forme $\tau\sigma^j$ pour $j \in [\![0,9]\!]$ est 2.

12pt

3. Soit $\mathsf{ev}_i : \mathbb{Z}[X] \to \mathbb{C}$ le morphisme d'évaluation en i qui à un polynôme $P \in \mathbb{Z}[X]$ associe $P(i)$. On note $\mathbb{Z}[i]$ son image.

(*a*) Montrer que $\mathbb{Z}[i] = \{a + ib : a,b \in \mathbb{Z}\}$.

(*b*) Soit $I = (3+2i) \subseteq \mathbb{Z}[i]$ l'idéal de $\mathbb{Z}[i]$ engendré par $3+2i$ et $\theta : \mathbb{Z} \to \mathbb{Z}[i]/I$ la restriction à $\mathbb{Z}$ de la projection canonique de $\mathbb{Z}[i]$ sur $\mathbb{Z}[i]/I$. Montrer que le noyau de θ est un idéal de la forme $p\mathbb{Z}$ où $p \in \mathbb{Z}$ est un entier premier que l'on déterminera.

(*c*) Quelle est la caractéristique de l'anneau $\mathbb{Z}[i]/I$?

(*d*) Montrer que I contient un complexe $a + i$ où $a \in \mathbb{Z}$ est un entier que l'on explicitera.

(*e*) Utiliser l'item précédent pour montrer que θ est surjectif.

(*f*) L'idéal I est-il premier ? Maximal ?

(*g*) Déterminer l'idéal $K = \mathsf{Ker}(\mathsf{ev}_i)$ de $\mathbb{Z}[X]$. L'idéal K de $\mathbb{Z}[X]$ est-il premier ? Maximal ?

(*h*) Déterminer l'idéal $J = \mathsf{ev}_i^{-1}(I)$ de $\mathbb{Z}[X]$. L'idéal J de $\mathbb{Z}[X]$ est-il premier ? Maximal ?

Solution.

(*a*) Soit $P = a + bX$, avec $a, b \in \mathbb{Z}$. Alors, $\mathsf{ev}_i(P) = P(i) = a + bi$, ce qui nous dit que $\{a + ib : a, b \in \mathbb{Z}\} \subseteq \mathbb{Z}[i]$. En outre, soit $P(i) \in \mathbb{Z}[i]$ avec $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X]$. On voit bien que

$$\begin{aligned}\mathsf{ev}_i(P) = P(i) &= \sum_{k=0}^{d} a_k i^k \\ &= \underbrace{\Big(\sum_{k=0}^{\lfloor d/2 \rfloor} a_{2k}(-1)^k\Big)}_{\in\mathbb{Z}} + \underbrace{\Big(\sum_{k=0}^{\lfloor (d-1)/2 \rfloor} a_{2k+1}(-1)^k\Big)}_{\in\mathbb{Z}} i \in \{a + ib : a, b \in \mathbb{Z}\},\end{aligned}$$

où $\lfloor x \rfloor = \max\{n \in \mathbb{Z} : n \leq x\}$ pour tout $x \in \mathbb{R}$. En conséquence, $\mathbb{Z}[i] \subseteq \{a + ib : a, b \in \mathbb{Z}\}$, ce qui implique que $\{a + ib : a, b \in \mathbb{Z}\} = \mathbb{Z}[i]$.

(*b*) On affirme que $\mathsf{Ker}(\theta) = 13.\mathbb{Z}$. Pour cela, on note d'abord que par définition de θ, $\mathsf{Ker}(\theta) = I \cap \mathbb{Z}$. Or, un élément général de I est de la forme $z = (a+bi)(3+2i) = (3a-2b)+(2a+3b)i$, avec $a, b \in \mathbb{Z}$. Alors $z = (3a-2b)+(2a+3b)i \in I \cap \mathbb{Z}$ si et seulement si $2a+3b = 0$. Cela implique que $3|a$, *i.e.* $a = 3m$ avec $m \in \mathbb{Z}$, et en conséquence $3b = -6m$, *i.e.* $b = -2m$. C'est clair que $a = 3m$ et $b = -2m$ avec $m \in \mathbb{Z}$ est une solution de $2a + 3b = 0$, ce qui nous dit que toute solution entière de $2a + 3b = 0$ est de la forme $a = 3m$ et $b = -2m$ avec $m \in \mathbb{Z}$. Par conséquent, $z = (3a-2b)+(2a+3b)i \in I \cap \mathbb{Z}$ si et seulement si $z = (3a-2b)+(2a+3b)i = 9m + 4m = 13.m$ avec $m \in \mathbb{Z}$, *i.e.* $I \cap \mathbb{Z} = 13.\mathbb{Z}$. En conséquence, $\mathsf{Ker}(\theta) = 13.\mathbb{Z}$.

(*c*) Comme θ est le seul morphisme d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}[i]/I$ et son noyau est engendré par 13, la caractéristique de $\mathbb{Z}[i]/I$ est 13.

(*d*) On voit bien que $-5 + i = (-1 + i)(3 + 2i) \in I$.

(*e*) C'est clair que $a+bi = (a+5b)+b(-5+i)$ pour tous $a, b \in \mathbb{Z}$, ce qui implique que $\overline{a + bi} = \theta(a + 5b)$, vu que $b(-5 + i) \in I$. En conséquence, θ est une application surjective.

(*f*) En employant l'isomorphisme d'anneaux $\bar{\theta} : \mathbb{Z}/13.\mathbb{Z} \to \mathbb{Z}[i]/I$ induit par θ et le fait que 13 est premier on conclut que $\mathbb{Z}[i]/I$ est un corps. En conséquence, l'idéal I es maximal et, en particulier, il est premier.

(*g*) On voit bien que $X^2+1 \in K$, vu que $\mathsf{ev}_i(X^2+1) = 0$, ce qui implique que $(X^2+1) \subseteq K$. On affirme que $(X^2 + 1) = K$. On note d'abord que, étant donné $T = aX + b \in \mathbb{Z}[X]$ avec $a \neq 0$, alors $T(i) \neq 0$, *i.e.* $T \notin K$. En effet, $T(i) = ai+b = 0$ impliquerait $i = -b/a \in \mathbb{Q}$, ce qui est absurde, car $i \in \mathbb{C} \setminus \mathbb{R}$, donc *a fortiori* $i \in \mathbb{C} \setminus \mathbb{Q}$. Soit $P \in K$, *i.e.* $P \in \mathbb{Z}[X]$ et $P(i) = 0$. Comme $X^2 + 1$ est un polynôme unitaire, il existe $Q, R \in \mathbb{Z}[X]$ tels que $P = Q(X^2 + 1) + R$ et $\deg(R) < \deg(X^2 + 1) = 2$. En conséquence, $R = P - Q(X^2 + 1) \in K$, vu que $(X^2 + 1) \in K$, ce qui implique que $R = 0$, *i.e.* $P \in (X^2 + 1)$. Par conséquent, $K \subseteq (X^2 + 1)$ et alors $(X^2 + 1) = K$.

Par ailleurs, comme $\mathsf{ev}_i : \mathbb{Z}[X] \to \mathbb{C}$ est un morphisme d'anneaux avec image $\mathbb{Z}[i]$, il induit un isomorphisme d'anneaux $\bar{\mathsf{ev}}_i : \mathbb{Z}[X]/K \to \mathbb{Z}[i]$. Comme $\mathbb{Z}[i] \subseteq \mathbb{C}$ est un sous-anneau d'un anneau intègre, il est intègre, ce qui implique que K est

un idéal premier. On affirme que $\mathbb{Z}[i]$ n'est pas un corps. De façon élémentaire on peut dire par exemple que $1+i \in \mathbb{Z}[i]$ n'est pas inversible, car son inverse (unique) dans $\mathbb{Q}[i] \supseteq \mathbb{Z}[i]$ est $1/2-i/2$, qui n'appartient pas à $\mathbb{Z}[i]$. On peut aussi donner un argument plus géneral. Pour $z = a + bi \in \mathbb{Z}[i]$, on pose $N(z) = a^2 + b^2 = 1$. Noter que $N(z) \in \mathbb{N}$ pour tout $z \in \mathbb{Z}[i]$, et $N(z_1.z_2) = N(z_1).N(z_2)$ pour tous $z_1, z_2 \in \mathbb{Z}[i]$. Or, on remarque d'abord que $z = a + bi \in \mathbb{Z}[i]$ est inversible si et seulement si $N(z) = a^2+b^2 = 1$. En effet, s'il existe $w \in \mathbb{Z}[i]$ tel que $z.w = 1$, alors $1 = N(1) = N(z).N(w)$, ce qui implique $N(z) = N(w) = 1$, vu que $N(z), N(w) \in \mathbb{N}$. Réciproquement, si $N(z) = 1$, alors $\bar{z} = a-bi \in \mathbb{Z}[i]$ est l'inverse de z. On note finalement que $1 + i \in \mathbb{Z}[i]$ n'est pas inversible, car $N(1 + i) = 2 \neq 1$. Comme $\mathbb{Z}[i]$ n'est pas un corps, K n'est pas maximal.

(*h*) On affirme que $J = (X^2 + 1, 2X + 3)$. Pour le démontrer on peut procéder directement, car $P \in J$ équivaut à $\mathsf{ev}_i(P) \in I$, *i.e.* il existe $Q \in \mathbb{Z}[X]$ tel que $\mathsf{ev}_i(P) = \mathsf{ev}_i(3 + 2X)\,\mathsf{ev}_i(Q) = \mathsf{ev}_i((3 + 2X)Q)$. Cette dernière condition équivaut à l'existence de $Q \in \mathbb{Z}[X]$ tel que $P - (3 + 2X)Q \in \mathsf{Ker}(\mathsf{ev}_i)$, *i.e.* il existe $Q, R \in \mathbb{Z}[X]$ tels que $P = (3+2X)Q+(X^2+1)R$. Une autre façon de le démontrer utilise que, étant donné un morphisme d'anneaux surjectif $\varphi : A \to B$ l'application

$$\left\{\mathscr{I} \text{ idéal de } A \text{ contenant } \mathsf{Ker}(\varphi)\right\} \longrightarrow \left\{\mathscr{J} \text{ idéal de } B\right\}$$

qui associe $\varphi(\mathscr{I})$ à $\mathscr{I}$ est une bijection, dont la réciproque associe $\varphi^{-1}(\mathscr{J})$ à $\mathscr{J}$. Soit $J' = (X^2 + 1, 2X + 3)$. Alors, on voit bien que $(X^2 + 1) = K \subseteq J'$ et $(X^2 + 1) = K \subseteq J$. Comme $\mathsf{ev}_i(J') = (2i + 3) = I = \mathsf{ev}_i(\mathsf{ev}_i^{-1}(I)) = \mathsf{ev}_i(J)$, vu que $\mathsf{ev}_i : \mathbb{Z}[X] \to \mathbb{Z}[i]$ est surjectif et $I \subseteq \mathbb{Z}[i]$, on conclut que $J = J' = (X^2+1, 2X+3)$, comme on voulait démontrer.

Finalement, on note que ev_i induit un isomorphisme d'anneaux $\widehat{\mathsf{ev}}_i : \mathbb{Z}[X]/J \to \mathbb{Z}[i]/I$. Comme $\mathbb{Z}[i]/I \simeq \mathbb{Z}/13.\mathbb{Z}$ est un corps, l'idéal J est maximal et, en particulier, il est premier.