1
2
3

MAT35B - ALGÈBRE L3A
Premier Semestre — 2021-2022

Dernier Dévoir Surveillé

Toute réponse non justifiée ne sera pas validée.

Le barème est donné à titre indicatif et non contractuel.

6pt **1.** On considère deux groupes H et K. On rappelle qu'un automorphisme de groupes $f : H \to H$ est **intérieur** s'il existe $x \in H$ tel que $f(h) = xhx^{-1}$ pour tout $h \in H$. On note $\mathsf{Int}(H)$ l'ensemble des automorphismes intérieurs de H, qui forme un sous-groupe de $\mathsf{Aut}_{\mathsf{Gr}}(H)$.

(*a*) Soit $\psi : K \to H$ un morphisme de groupes. On note dans cette question $\varphi : K \to \mathsf{Int}(H)$ le morphisme de groupes défini par :

$$\varphi(k)(h) = \psi(k)h\psi(k)^{-1}$$

pour tous $k \in K$ et $h \in H$. Montrer que l'application $f : H \rtimes_\varphi K \to H \times K$ donnée par $f(h,k) = (h\psi(k), k)$ pour tout $h \in H$ et $k \in K$ est un isomorphisme de groupes.

(*b*) On suppose dans cette question que le centre $\mathscr{Z}(H)$ de H est trivial, *i.e.* $\mathscr{Z}(H) = \{1_H\}$. On considère un morphisme de groupes $\varphi : K \to \mathsf{Int}(H)$.

(i) Montrer que l'application canonique

$$\begin{aligned} \mathsf{Ad} : H &\to \mathsf{Int(H)} \\ x &\mapsto (h \mapsto xhx^{-1}) \end{aligned}$$

est un isomorphisme de groupes.

(ii) En déduire l'existence d'un morphisme de groupes $\psi : K \to H$ tel que $\varphi = \mathsf{Ad} \circ \psi$. En conclure que les groupes $H \rtimes_\varphi K$ et $H \times K$ sont isomorphes.

(*c*) Soit $n \geq 3$ un entier différent de 6. On rappelle que l'on a alors l'égalité $\mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n) = \mathsf{Int}(\mathbb{S}_n)$. Montrer que tout produit semi-direct $\mathbb{S}_n \rtimes_\varphi K$ est isomorphe au groupe $\mathbb{S}_n \times K$.
Indication : si $\sigma \in \mathbb{S}_n$ commute avec les transpositions (1 2) et (1 3), que vaut $\sigma(1)$?

Solution.

(*a*) On voit bien que

$$\begin{aligned} f\big((h,k)\cdot_{H\rtimes_\varphi K}(h',k')\big) &= f\big(h\psi(k)h'\psi(k)^{-1},kk'\big)\\ &= \big(h\psi(k)h'\psi(k)^{-1}\psi(kk'),kk'\big)\\ &= \big(h\psi(k)h'\psi(k'),kk'\big) = \big(h\psi(k),k\big)\cdot\big(h'\psi(k'),k'\big)\\ &= f(h,k)\cdot f(h',k'), \end{aligned}$$

pour tous $h,h'\in H$ et $k,k'\in K$, ce qui nous dit que f est un morphisme de groupes. On considère l'application $g : H\times K\to H\rtimes_\varphi K$ donnée par $g(h,k) = (h\psi(k)^{-1},k)$ pour $h\in H$ et $k\in K$. C'est clair que $f\circ g = \mathsf{id}_{H\times K}$ et $g\circ f = \mathsf{id}_{H\rtimes_\varphi K}$. En conséquence, f est un isomorphisme de groupes.

(*b*) (i) On rappelle que le noyau du morphisme $\mathsf{Ad}_H : H\to\mathsf{Aut}_{\mathsf{Gr}}(H)$ est précisément $\mathscr{Z}(H)$ et son image est exactement $\mathsf{Int}(H)$. En conséquence, dans ce cas on a l'isomorphisme $\mathsf{Ad}_H : H\to\mathsf{Int}(H)$, vu que $\mathscr{Z}(H) = \{1_H\}$.

(ii) On définit $\phi : K\to H$ par $\phi = \mathsf{Ad}_H^{-1}\circ\varphi$. Alors, l'item précédent nous dit qu'il existe un isomorphisme de groupes entre $H\rtimes_\varphi K$ et $H\times K$.

(*c*) Il s'agit d'une conséquence directe de l'item précédent, vu que tout automorphisme de $\mathbb{S}_n$ est intérieur pour $n\geq 3$ différent de 6, d'après l'exercice **14** de la fiche 3, et $\mathscr{Z}(\mathbb{S}_n) = \{\mathsf{id}_{[\![1,n]\!]}\}$ pour $n\geq 3$. La dernière identité suit directement du fait que s'il existe $i,j\in[\![1,n]\!]$ différents tels que $\sigma\in\mathscr{Z}(\mathbb{S}_n)$ satisfait que $\sigma(i) = j$, on considère $k\in[\![1,n]\!]\setminus\{i,j\}$, vu que $n\geq 3$, et on note alors que $(\sigma(j)\ \sigma(k)) = \sigma(j\ k)\sigma^{-1} = (j\ k)$ impliquerait que $\sigma(j) = j$ ou $\sigma(k) = j$, ce qui est absurde car $\sigma(i) = j$.

4pt **2.** Étant donné un groupe G, on notera n_p la cardinalité de l'ensemble Syl_p de sous-groupes de Sylow de G associés au premier $p\in\mathbb{N}^*$.
Soit G un groupe groupe d'ordre 80.

(*a*) Montrer que $n_5\in\{1,16\}$.

(*b*) Montrer que, si $n_5 = 16$, alors

$$\left|\bigcup_{H\in\mathsf{Syl}_5} H\right| = 65 \quad\text{et}\quad n_2 = 1.$$

(*c*) Montrer que G n'est pas simple.

Solution.

(*a*) Comme $|G| = 2^4.5$, le théorème de Sylow nous dit que $n_5|16$ et $n_5\equiv 1\pmod 5$. La dernière condition équivaut à $n_5 = 1+5k$ avec $k\in\mathbb{N}$, ce qui, avec la première condition, nous dit que $n_5\in\{1,16\}$.

(*b*) On suppose $n_5 = 16$. Alors, il existe 16 sous-groupes de G d'ordre 5. On remarque que, si $H,H'\subseteq G$ sont deux sous-groupes d'ordre 5 tels que $H\neq H'$, alors $H\cap H' = \{1_G\}$, car $|H\cap H'|$ est un diviseur de $|H| = |H'| = 5$ différent de 5, d'après le

théorème de Lagrange. On conclut que

$$\left| \bigcup_{H \in \mathsf{Syl}_5} H \right| = 16.(5-1)+1 = 65.$$

Soit $K \subseteq G$ un sous-groupe de Sylow associé à $p = 2$. Alors,

$$K \cap \left(\bigcup_{H \in \mathsf{Syl}_5} H \right) = \bigcup_{H \in \mathsf{Syl}_5} (K \cap H) = \bigcup_{H \in \mathsf{Syl}_5} \{1_G\} = \{1_G\},$$

car $|K \cap H|$ divise $|K| = 16$ et $|H| = 5$. En conséquence,

$$\left| K \cup \left(\bigcup_{H \in \mathsf{Syl}_5} H \right) \right| = 65 + 16 - 1 = 80 = |G|,$$

ce qui implique que K est le seul sous-groupe de G d'ordre 16, vu que

$$K = \left(G \setminus \left(\bigcup_{H \in \mathsf{Syl}_5} H \right) \right) \cup \{1_G\}.$$

En conséquence, $n_2 = 1$.

(*c*) D'après les items précédents on a ou bien $n_5 = 1$ ou bien $n_2 = 1$. Cela nous dit que ou bien le sous-groupe de Sylow associé à $p = 5$ est distingué ou le sous-groupe de Sylow associé à $p = 2$ est distingué. En conséquence, G n'est pas distingué.

10pt

3. Comme d'habitude, dans cet exercice tous les anneaux seront supposés commutatifs et non nuls. Si A est un anneau, on notera $\mathsf{N}(A)$ l'ensemble des éléments non inversibles de A.

(*a*) Déterminer $\mathsf{N}(A)$ dans les cas suivants : $A = \mathbb{Z}$, $A = \mathbb{Z}/4\mathbb{Z}$ et $A = \mathbb{Z}/6\mathbb{Z}$.

(*b*) Démontrer que $\mathsf{N}(A)$ est un idéal d'un anneau A si et seulement si $\mathsf{N}(A)$ est stable par l'addition, *i.e.* $a + b \in \mathsf{N}(A)$ pour tous $a, b \in \mathsf{N}(A)$.

Un anneau A est dit **local** si l'ensemble de ses éléments non inversibles est un idéal.

(*c*) Un corps est-il un anneau local ? Parmi les anneaux $\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$ déterminer ceux qui sont locaux.

(*d*) Soit A un anneau local. Montrer que l'idéal $\mathsf{N}(A)$ est maximal, puis que c'est le seul idéal maximal de A.

(*e*) On se donne un entier $n \geq 2$. Montrer que l'anneau $\mathbb{Z}/n\mathbb{Z}$ est local si et seulement si n est une puissance d'un nombre premier.

Solution. Étant donné un anneau A, on notera $A^\times$ l'ensemble d'éléments inversibles de A. En particulier, $\mathsf{N}(A) = A \setminus A^\times$.

(*a*) On voit bien que $\mathbb{Z}^\times = \{\pm 1\}$, ce qui implique que $\mathsf{N}(\mathbb{Z}) = \mathbb{Z}\setminus\{\pm 1\}$. En effet, $n = 0$ n'est jamais inversible, et si $n \in \mathbb{Z}$ satisfait $|n| > 1$, alors $|nm| = |n||m| \geq |n| > 1$ pour tout $m \in \mathbb{Z}\setminus\{0\}$, ce qui implique que $nm = 1$ est impossible.

En outre, c'est immédiat à vérifier que $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\}$ et $(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\}$, ce qui implique que $\mathsf{N}(\mathbb{Z}/4\mathbb{Z}) = \{\bar{0}, \bar{4}\}$ et $\mathsf{N}(\mathbb{Z}/6\mathbb{Z}) = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$.

(*b*) On remarque d'abord que, étant donné $a, b \in A$, si $ab \in A^\times$, alors $a \in A^\times$ et $b \in A^\times$, car $b(ab)^{-1}$ est l'inverse de a et $a(ab)^{-1}$ est l'inverse de b. La contraposée nous dit alors que, si $a \in \mathsf{N}(A)$ et $b \in A$, alors $ab \in \mathsf{N}(A)$. En outre, on remarque que $a \in A^\times$ si et seulement si $-a \in A^\times$, car $-a^{-1}$ est l'inverse de $-a$, ce qui implique que $a \in \mathsf{N}(A)$ si et seulement si $-a \in \mathsf{N}(A)$. On conclut que $\mathsf{N}(A)$ est un idéal si et seulement $\mathsf{N}(A)$ est stable par l'addition.

(*c*) Si A est un corps, alors $A^\times = A\setminus\{0_A\}$, ce qui nous dit que $\mathsf{N}(A) = \{0_A\}$. Comme $\{0_A\}$ est un idéal de A, tout corps A est un anneau local.

D'après le calcul dans le premier item, $\mathsf{N}(\mathbb{Z}) = \{\pm 1\}$, ce qui n'est pas un idéal car $1 + 1 = 2 \notin \mathsf{N}(\mathbb{Z})$. En conséquence, $\mathbb{Z}$ n'est pas local. De façon analogue, le calcul dans le premier item nous dit que $\mathsf{N}(\mathbb{Z}/6\mathbb{Z}) = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$, ce qui n'est pas un idéal car $\bar{2} + \bar{3} = \bar{5} \notin \mathsf{N}(\mathbb{Z}/6\mathbb{Z})$. Par conséquent, $\mathbb{Z}/6\mathbb{Z}$ n'est pas local. Finalement, comme $\mathsf{N}(\mathbb{Z}/4\mathbb{Z}) = \{\bar{0}, \bar{2}\} = (\bar{2})$ est l'idéal engendré par $\bar{2}$, $\mathbb{Z}/4\mathbb{Z}$ est local.

(*d*) Comme $A\setminus\mathsf{N}(A) = A^\times \neq \emptyset$, car $1_A \in A^\times$, on voit que l'idéal $\mathsf{N}(A)$ est propre. Soit I un idéal de A tel que $\mathsf{N}(A) \subsetneq I$. Comme $A\setminus\mathsf{N}(A) = A^\times$, $I \cap A^\times \neq \emptyset$, ce qui nous dit que $I = A$. En effet, si $a \in I \cap A^\times$ et $b \in A$, alors $b = ba^{-1}.a \in I$. En conséquence, $\mathsf{N}(A)$ est un idéal maximal.

Soit $M \subsetneq A$ un idéal maximal. D'après ce que l'on a remarqué dans le paragraphe précédent $M \cap A^\times = \emptyset$, ce qui implique que $M \subseteq A\setminus A^\times = \mathsf{N}(A)$. La maximalité de M nous dit alors que $M = \mathsf{N}(A)$.

(*e*) On rappelle que

$$(\mathbb{Z}/n\mathbb{Z})^\times = \left\{\bar{m} \in \mathbb{Z}/n\mathbb{Z} : \mathsf{PGCD}(n, m) = 1\right\},$$

ce qui nous dit que

$$\mathsf{N}(\mathbb{Z}/n\mathbb{Z}) = \left\{\bar{m} \in \mathbb{Z}/n\mathbb{Z} : \mathsf{PGCD}(n, m) > 1\right\}. \tag{1}$$

En particulier,

$$\mathsf{N}(\mathbb{Z}/p^k\mathbb{Z}) = \left\{\bar{m} \in \mathbb{Z}/n\mathbb{Z} : p|m\right\} = (\bar{p}),$$

pour tout $p \in \mathbb{N}^*$ premier et $k \in \mathbb{N}^*$, ce qui nous dit que $\mathbb{Z}/p^k\mathbb{Z}$ est local dans ce cas. En outre, on affirme que, s'il existe deux premiers $p, q \in \mathbb{N}^*$ différents tels que $pq|n$, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas local. En effet, dans ce cas il existe $a, b \in \mathbb{Z}$ tels que $ap + bq = 1$, car p et q sont premiers entre eux, et $\overline{ap}$, $\overline{bq} \in \mathsf{N}(\mathbb{Z}/n\mathbb{Z})$ par (1), tandis que $\overline{ap} + \overline{bq} = \bar{1} \notin \mathsf{N}(\mathbb{Z}/n\mathbb{Z})$. Cela démontre le résultat.