Produits semi-directs, groupe linéaire : correction

Exercice 1.

1. Soit
$$\begin{aligned} \varphi : \mathrm{H} &\to \operatorname{Aut}\mathrm{N} \\ h &\mapsto \begin{pmatrix} \mathrm{N} \to \mathrm{N} \\ n \mapsto hnh^{-1} \end{pmatrix}. \end{aligned}$$
Cette application est bien définie car, N étant distingué, tout automorphisme intérieur de G se restreint en un automorphisme de N.
En outre, pour tous $h_1, h_2 \in \mathrm{H}$, $n \in \mathrm{N}$, on a
$$\begin{aligned} \big(\varphi(h_1) \circ \varphi(h_2)\big)(n) &= \varphi(h_1)\big(\varphi(h_2)(n)\big) \\ &= \varphi(h_1)\left(h_2 n h_2^{-1}\right) \\ &= h_1 h_2 n h_2^{-1} h_1^{-1} \\ &= \varphi(h_1 h_2)(n) \end{aligned}$$
donc φ est un morphisme de groupes. Nous allons montrer que $\mathrm{G} \simeq \mathrm{N} \rtimes_\varphi \mathrm{H}$.
Soit donc
$$\begin{aligned} \psi : \mathrm{N} \rtimes_\varphi \mathrm{H} &\to \mathrm{G} \\ (n,h) &\mapsto nh. \end{aligned}$$
On voit que c'est un morphisme de groupes :
$$\begin{aligned} \psi(1_{\mathrm{N}\rtimes_\varphi \mathrm{H}}) = \psi(1_\mathrm{N}, 1_\mathrm{H}) &= 1_\mathrm{G}. \\ \psi(n_1,h_1)\psi(n_2,h_2) &= n_1 h_1 n_2 h_2 \\ &= n_1 h_1 n_2 h_1^{-1} h_1 h_2 \\ &= n_1 \varphi(h_1)(n_2) \cdot h_1 h_2 \\ &= \psi(n_1 \varphi(h_1)(n_2), h_1 h_2) \\ &= \psi((n_1,h_1)\cdot(n_2,h_2)). \end{aligned}$$
En outre, le morphisme ψ est injectif : si $\psi(n,h) = 1_\mathrm{G}$, on a $n = h^{-1}$. Cela entraîne que $n \in \mathrm{N} \cap \mathrm{H}$ et donc que $n = 1$, et $(n,h) = (1_\mathrm{N}, 1_\mathrm{H})$.
Enfin, comme
$$\forall n \in \mathrm{N}, \psi(n, 1_\mathrm{H}) = n \qquad \text{et} \qquad \forall h \in \mathrm{H}, \psi(1_\mathrm{N}, h) = h,$$
l'image de ψ contient à la fois N et H, et donc $\mathrm{G} = \langle \mathrm{N} \cup \mathrm{H} \rangle$.
Remarquons d'ailleurs que ce critère est en fait une condition nécessaire et suffisante : si G est le groupe $\mathrm{N} \rtimes_\varphi \mathrm{H}$, les sous-groupes $\mathrm{N}' = \{(n, 1_\mathrm{H}) \mid n \in \mathrm{N}\}$ et $\mathrm{H}' = \{(1_\mathrm{N}, h) \mid h \in \mathrm{H}\}$ sont isomorphes à N et H, respectivement, et vérifient les hypothèses de la question 1. Dans la pratique, d'ailleurs, on identifie ces sous-groupes aux groupes « abstraits » N et H.

2. Si H est lui aussi distingué dans G, on a
$$\forall n \in \mathrm{N}, \forall h \in \mathrm{H}, nh = hn.$$

En effet, le commutateur

$$[n,h] = nhn^{-1}h^{-1} = \underbrace{nhn^{-1}}_{\in \mathrm{H}} h^{-1} = n\underbrace{hn^{-1}h^{-1}}_{\in \mathrm{N}}$$

appartient alors à la fois à H et à N, et donc est égal à 1. Ainsi, le morphisme φ défini à la première question est le morphisme trivial

$$\varphi_0 : \mathrm{H} \to \{\mathrm{id}_\mathrm{N}\} \subseteq \mathrm{Aut}\,\mathrm{N}$$

ce qui implique

$$\mathrm{G} \simeq \mathrm{N} \rtimes_{\varphi_0} \mathrm{H} = \mathrm{N} \times \mathrm{H}.$$

3. Si $\mathrm{G} = \mathfrak{S}(n)$, $\mathrm{N} = \mathfrak{A}(n)$ et $\mathrm{H} = \langle(12)\rangle = \{\mathrm{id}, (12)\}$ vérifient les hypothèses de la question précédente : la seule chose à vérifier est que $\mathrm{HN} = \mathfrak{S}(n)$, ce que l'on peut faire d'au moins deux façons différentes :
   – en remarquant que, comme $[\mathfrak{S}(n) : \mathfrak{A}(n)] = 2$, tout sous-groupe contenant strictement $\mathfrak{A}(n)$ est $\mathfrak{S}(n)$ tout entier ;
   – en remarquant que si $\sigma \notin \mathfrak{A}(n)$, on a $(12)\sigma \in \mathfrak{A}(n)$, donc $\mathfrak{S}(n) = \mathfrak{A}(n) \sqcup (12)\mathfrak{A}(n) \subseteq \langle(12), \mathfrak{A}(n)\rangle$.
   Cela entraîne que $\mathfrak{S}(n)$ est isomorphe à un produit semi-direct $\mathfrak{A}(n) \rtimes \mathbf{Z}/2\mathbf{Z}$.
   En revanche, $\mathfrak{S}(n)$ n'est pas isomorphe au produit direct $\mathfrak{A}(n) \times \mathbf{Z}/2\mathbf{Z}$: cela impliquerait par exemple l'existence d'un élément d'ordre 2 (le générateur du deuxième facteur) dans le centre de $\mathfrak{S}(n)$, dont on sait pourtant qu'il est trivial.
4. Pour les groupes d'isométries d'un solide "régulier", la méthode est la suivante :
   – On commence par montrer que l'ensemble des sommets est préservé. On peut pour cela remarquer que l'ensemble des sommets est l'ensemble des points extrémaux du solide, et que les isométries sont des affinités, donc elles préservent le barycentre. On en déduit en outre que toute isométrie du solide fixe le centre O du solide (puisqu'il est par définition l'isobarycentre de ses sommets).
   – On utilise enfin qu'une affinité est entièrement déterminée par l'image d'un repère pour majore le cardinal du groupe des isométries. Considérons le repère formé par deux sommets consécutifs et le centre du solide. Sous l'action d'une isométrie, le centre est fixé, le premier sommet est envoyé sur l'un des n autres, et son voisin sur un voisin de son image. Il y a donc au plus $2n$ possibilités. On en déduit pour le groupe d'isométrie D_{2n} d'un n-gone régulier : $|\mathrm{D}_{2n}| \leq 2n$.
   – D'autre part, on connait $2n$ isométries d'un n-gone régulier : n de centre O et d'angle $2\pi/n$, plus n symétries d'axes passant par les paires de sommets opposées (si n pair) ou bien un sommet et le milieu du côté opposé (si n impair). On en déduit grâce à la majoration précédente que ce sont les seules isométries du solide.
   Remarque : La même méthode appliquée au tétraèdre donne $4*3*2 = 24$ isométries au plus. Pour le cube on trouve $8*3*2 = 48$ isométries au plus, $6*4*2 = 48$ pour l'octaèdre, $20*3*2 = 120$ pour le dodécaèdre et $12*5*2 = 120$ pour l'icosaèdre. Pouvez-vous, dans chaque cas, énumérer les isométries "évidentes" du solide, et déterminer le groupe de ses isométries ?
   – Revenons à nos polygones. Les rotations forment un sous-groupe cyclique d'ordre n, c'est-à-dire d'indice 2, donc distingué (on peut aussi voir que le conjugué d'une rotation de centre O et d'angle θ par une isométrie du solide est une rotation de centre O et d'angle θ ou $-\theta$). Il est d'intersection triviale avec $< \mathrm{I}d, s >$ où s est n'importe qu'elle symétrie, et ils génèrent ensemble tout le groupe (leur union contient plus de la motié des éléments, le sous-groupe engendré est donc d'indice strictement inférieur à 2) (on peut aussi voir que si s est d'axe Δ, le conjugué de s par r est la symétrie d'axe $r(\Delta)$ et qu'on obtient ainsi toutes les symétries). On en déduit que G est un produit semi-direct de $\mathbf{Z}/n\mathbf{Z}$ par $\mathbf{Z}/2\mathbf{Z}$. Puisque G n'est pas abélien, le produit n'est pas direct.

5. Il y a beaucoup de façons de justifier cela :
   - on peut remarquer que si $\mathbf{Z}/4\mathbf{Z}$ était un produit semi-direct non trivial (et donc de $\mathbf{Z}/2\mathbf{Z}$ par $\mathbf{Z}/2\mathbf{Z}$, puisqu'il n'y a, à isomorphisme près, qu'un groupe d'ordre 2), il serait isomorphe au produit direct $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$
     - parce qu'il n'y a pas de morphisme non trivial $\varphi : \mathbf{Z}/2\mathbf{Z} \to \mathrm{Aut}\,\mathbf{Z}/2\mathbf{Z}$ (le groupe de droite est trivial) ;
     - parce que $\mathbf{Z}/4\mathbf{Z}$ est abélien (et on peut alors appliquer la question 2.),

     ce qui n'est pas le cas ($\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ n'a pas d'élément d'ordre 4).
   - on peut également remarquer que, $\mathbf{Z}/4\mathbf{Z}$ ne contenant qu'un seul sous-groupe d'ordre 2, il serait impossible de trouver deux sous-groupes jouant les rôles du N et du H de la question 1.

Exercice 2.

1. D'après le théorème de Sylow, le nombre n_q de q-sous-groupes de Sylow de G divise p et est congru à 1 modulo q. Comme $p < q$, cela entraîne qu'il n'y a qu'un seul q-sous-groupe de Sylow N, qui est donc distingué.

   Soit maintenant H un p-sous-groupe de Sylow. Les sous-groupes H et N vérifient les hypothèses de la première question de l'exercice 1 :
   - un élément de $\mathrm{N} \cap \mathrm{H}$ aurait, d'après le théorème de Lagrange, un ordre divisant à la fois p et q. On a donc bien $\mathrm{N} \cap \mathrm{H} = \{1_\mathrm{G}\}$.
   - le sous-groupe NH engendré par H et N contient des éléments d'ordre p et d'ordre q donc, d'après le théorème de Lagrange, son ordre est un multiple de pq, ce qui entraîne $\mathrm{G} = \mathrm{NH}$.

   On a donc $\mathrm{G} \simeq \mathrm{N} \rtimes_\varphi \mathrm{H}$, pour un certain morphisme $\varphi : \mathbf{Z}/p\mathbf{Z} \to \mathrm{Aut}(\mathbf{Z}/q\mathbf{Z})$. Notons que ce dernier groupe s'identifie naturellement à $(\mathbf{Z}/q\mathbf{Z})^\times$ et est donc un groupe cyclique d'ordre $q-1$. On distingue alors deux cas :
   - si p ne divise pas $q-1$, le seul morphisme possible est le morphisme trivial

     $$\varphi_0 : \mathbf{Z}/p\mathbf{Z} \to \{\mathrm{id}\} \subseteq \mathrm{Aut}\,\mathbf{Z}/q\mathbf{Z},$$

     et

     $$\mathrm{G} \simeq \mathbf{Z}/p\mathbf{Z} \rtimes_{\varphi_0} \mathbf{Z}/q\mathbf{Z} \simeq \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z} \simeq \mathbf{Z}/pq\mathbf{Z}.$$

   - si p divise $q-1$, on peut choisir un morphisme injectif

     $$\varphi_1 : \mathbf{Z}/p\mathbf{Z} \to \mathrm{Aut}\,\mathbf{Z}/q\mathbf{Z}.$$

     Les morphismes de $\mathbf{Z}/p\mathbf{Z}$ vers $\mathrm{Aut}\,\mathbf{Z}/q\mathbf{Z}$ sont alors de deux types : il y a le morphisme trivial φ_0 et les morphismes injectifs, dont l'image est le seul sous-groupe d'ordre p de $\mathrm{Aut}\,\mathbf{Z}/q\mathbf{Z}$ (rappelons qu'un groupe cyclique d'ordre n possède un unique sous-groupe d'ordre d, pour tout diviseur d de n). Ces derniers sont donc de la forme

     $$\varphi_1 \circ \psi : \mathbf{Z}/p\mathbf{Z} \xrightarrow{\psi} \mathbf{Z}/p\mathbf{Z} \xrightarrow{\varphi_1} \mathrm{Aut}\,\mathbf{Z}/q\mathbf{Z},$$

     pour un certain automorphisme $\psi \in \mathrm{Aut}\,\mathbf{Z}/p\mathbf{Z}$. Il reste à voir que cette composition par un automorphisme ne change pas, à isomorphisme près, le produit semi direct : soit donc $\psi \in \mathrm{Aut}\,\mathbf{Z}/p\mathbf{Z}$ et

     $$\begin{array}{rcl} \chi : \mathbf{Z}/q\mathbf{Z} \rtimes_{\varphi_1} \mathbf{Z}/p\mathbf{Z} & \to & \mathbf{Z}/q\mathbf{Z} \rtimes_{\varphi_1 \circ \psi} \mathbf{Z}/p\mathbf{Z} \\ (n,h) & \mapsto & (n, \psi^{-1}(h)). \end{array}$$

     Pour plus de sécurité et malgré la lourdeur de notation que cela entraîne, notons $*_{\varphi_1}$ et $*_{\varphi_1 \circ \psi}$ les lois des deux groupes en présence.

L'application χ est clairement bijective et vérifie tout aussi clairement

$$\chi\left(1_{\mathbf{Z}/q\mathbf{Z}\rtimes_{\varphi_1}\mathbf{Z}/p\mathbf{Z}}\right)=\chi([1]_q,[1]_p)=([1]_q,\psi^{-1}([1]_p))=([1]_q,[1]_p)=1_{\mathbf{Z}/q\mathbf{Z}\rtimes_{\varphi_1\circ\psi}\mathbf{Z}/p\mathbf{Z}}.$$

La seule chose à vérifier est que χ respecte les lois de groupes :

$$\begin{aligned}\chi(n_1,h_1)*_{\varphi_1\circ\psi}\chi(n_2,h_2)&=\left(n_1,\psi^{-1}(h_1)\right)*_{\varphi_1\circ\psi}\left(n_2,\psi^{-1}(h_2)\right)\\&=\left(n_1\left(\varphi_1\circ\psi\right)(\psi^{-1}(h_1))(n_2),\psi^{-1}(h_1)\psi^{-1}(h_2)\right)\\&=\left(n_1\varphi_1(h_1)(n_2),\psi^{-1}(h_1h_2)\right)\\&=\chi(n_1\varphi_1(h_1)(n_2),h_1h_2)\\&=\chi\left((n_1,h_1)*_{\varphi_1}(n_2,h_2)\right).\end{aligned}$$

L'application χ est donc bien un isomorphisme de groupes. En résumé, on a démontré que si $\psi\in\operatorname{Aut}\mathrm{H}$, les produits semi-directs $\mathrm{N}\rtimes_\varphi\mathrm{H}$ et $\mathrm{N}\rtimes_{\varphi\circ\psi}\mathrm{H}$ sont isomorphes.
Dans le cas qui nous préoccupe, on a donc (au plus) deux produits semi-directs à isomorphisme près, le produit direct $\mathbf{Z}/q\mathbf{Z}\rtimes_{\varphi_0}\mathbf{Z}/p\mathbf{Z}\simeq\mathbf{Z}/q\mathbf{Z}\times\mathbf{Z}/p\mathbf{Z}\simeq\mathbf{Z}/pq\mathbf{Z}$ et le produit semi-direct $\mathbf{Z}/q\mathbf{Z}\rtimes_{\varphi_1}\mathbf{Z}/p\mathbf{Z}$. Ce sont bien deux sous-groupes non isomorphes : si $\mathbf{Z}/q\mathbf{Z}\rtimes_{\varphi_1}\mathbf{Z}/p\mathbf{Z}$ était isomorphe au produit direct, il serait abélien et le morphisme φ_1 défini par l'action par conjugaison du deuxième facteur sur le premier serait trivial, ce qui n'est pas le cas.

La classification des groupes d'ordre pq est donc la suivante : le groupe cyclique d'ordre pq est le seul groupe d'ordre pq avec $p<q$, sauf si p divise $q-1$, auquel cas il y a un unique groupe non cyclique (et même non abélien) $\mathbf{Z}/q\mathbf{Z}\rtimes\mathbf{Z}/p\mathbf{Z}$. Notons que si $p=2$ et q est impair, ce groupe est simplement le groupe diédral D_{2q}.

2. Dans cette question, on note $\mathrm{C}_n=\mathbf{Z}/n\mathbf{Z}$ le groupe cyclique d'ordre n.
En plus des groupes d'ordre 12 connus (deux abéliens : C_{12} et $\mathrm{C}_6\times\mathrm{C}_2$ et deux non abéliens : le groupe diédral D_{12} et le groupe alterné $\mathfrak{A}(4)$), il y a un produit semi-direct $\mathrm{T}=\mathrm{C}_3\rtimes\mathrm{C}_4$ donné par l'unique morphisme $\mathrm{C}_4\to\operatorname{Aut}\mathrm{C}_3$ non trivial, à savoir

$$\begin{aligned}\mathrm{C}_4&\to\quad\operatorname{Aut}\mathrm{C}_3=\{\mathrm{id},-\mathrm{id}\}\\[4]_4&\mapsto\begin{cases}\mathrm{id}&\text{si } n\equiv0\,(\mathrm{mod}\,2)\\-\mathrm{id}&\text{si } n\equiv1\,(\mathrm{mod}\,2).\end{cases}\end{aligned}$$

Ce sont bien cinq groupes différents, même à isomorphisme près : il est facile de distinguer les abéliens, et les autres se distinguent par exemple par le nombre d'involutions qu'ils contiennent :
– le groupe diédral D_{12} a huit involutions : l'identité, la symétrie centrale et les six réflexions (trois par rapport aux diagonales de l'hexagone, trois par rapport aux médiatrices) ;
– le groupe alterné $\mathfrak{A}(4)$ a quatre involutions : l'identité et les trois bitranspositions (12)(34), (13)(24) et (14)(23) ;
– le produit semi-direct T a deux involutions :

$$([n]_3,[m]_4)^2=\begin{cases}([n]_3+[n_3],[m]_4+[m]_4)&\text{si } m\equiv0\,(\mathrm{mod}\,2)\\([n]_3-[n_3],[m]_4+[m]_4)&\text{si } m\equiv1\,(\mathrm{mod}\,2),\end{cases}$$

donc

$$([n]_3,[m]_4)^2=([0]_3,[0]_4)\Leftrightarrow([n]_3,[m]_4)\in\{([0]_3,[0]_4),([0]_3,[2]_4)\}.$$

Nous allons donc montrer que réciproquement, tout groupe d'ordre 12 est isomorphe à C_{12}, $\mathrm{C}_6\times\mathrm{C}_2$, $\mathfrak{A}(4)$, D_{12} ou T.
Soit G un groupe d'ordre 12.

Commençons par observer que le théorème de Sylow nous garantit l'existence d'un sous-groupe d'ordre 3 (qui sera donc isomorphe à C_3) et d'un sous-groupe d'ordre 4 (qui sera donc isomorphe à C_4 ou à $C_2 \times C_2$). Le groupe engendré par ces deux sous-groupes est G tout entier (le cardinal d'un sous-groupe divisant le cardinal du groupe, le cardinal du sous-groupe engendré est un multiple de 12) et ces deux sous-groupes s'intersectent trivialement. Ainsi, on peut chercher à appliquer les questions de l'exercice précédent : si les deux sous-groupes de Sylow sont distingués, G est isomorphe à un produit direct (exercice 1, question 2) et si un seul est distingué, G est isomorphe à un produit semi-direct (exercice 1, question 1).
En outre, tous les p-sous-groupes de Sylow étant conjugués, se demander si un groupe de Sylow est distingué revient à se demander s'il est le seul. Si on note n_p le nombre de p-sous-groupes de Sylow, les propriétés générales données par le théorème de Sylow ($n_p \equiv 1 \pmod p$ et n_p divise $|G|$) nous laissent *a priori* quatre possibilités :

$$(1)\,(n_2,n_3)=(1,1)\,;\quad (2)\,(n_2,n_3)=(3,1)\,;\quad (3)\,(n_2,n_3)=(1,4)\,;\quad (4)\,(n_2,n_3)=(3,4).$$

Comme on l'a dit, la première possibilité entraîne que G est le produit direct de ses sous-groupes de Sylow. Il est donc isomorphe à $C_2 \times C_2 \times C_3 \simeq C_2 \times C_6$ ou à $C_4 \times C_3 \simeq C_{12}$.
La dernière possibilité est exclue par un argument de « manque de place » classique : puisque les 3-sous-groupes de Sylow sont cycliques d'ordre 3, ils n'ont pas de sous-groupe non trivial. En particulier, ils s'intersectent deux à deux trivialement. Ainsi, si $n_3 = 4$, il y a $4 \times (3-1) = 8$ éléments non triviaux dans les 3-sous-groupes de Sylow, c'est-à-dire 8 éléments d'ordre 3. Aucun de ces éléments ne peut appartenir à un 2-sous-groupe de Sylow, donc il ne reste plus de place que pour un unique 2-sous-groupe de Sylow ($12-8=4$). On a montré $n_3 = 4 \Rightarrow n_2 = 1$, c'est-à-dire qu'on a exclu la dernière possibilité.
La troisième possibilité entraîne que G est isomorphe au groupe alterné $\mathfrak{A}(4)$:
L'action de G par conjugaison permute les quatre 3-sous-groupes de Sylow et fournit donc un morphisme

$$G \to \mathfrak{S}(4),$$

dont l'image est un sous-groupe transitif de $\mathfrak{S}(4)$ (c'est-à-dire un sous-groupe agissant transitivement sur les quatre objets ; cela n'est qu'une traduction du fait que les sous-groupes de Sylow sont tous conjugués). En particulier, d'après la formule des classes, l'image de ce morphisme a un cardinal multiple de 4. Ce cardinal ne peut pas être exactement 4 (cela impliquerait que le morphisme ait un noyau de cardinal 3, mais c'est impossible car on sait qu'aucun 3-sous-groupe de Sylow n'est distingué) donc il est égal à 12. Autrement dit, le morphisme $G \to \mathfrak{S}(4)$ est injectif. Comme $\mathfrak{A}(4)$ est le seul sous-groupe d'indice 2 de $\mathfrak{S}(4)$, on a $G \simeq \mathfrak{A}(4)$.
Il ne nous reste donc qu'à traiter la deuxième possibilité. On a donc un 3-sous-groupe de Sylow distingué $N \subseteq G$ et un 2-sous-groupe de Sylow (non distingué) H tels que $N \cap H = \{1\}$ et que $NH = G$, ce qui entraîne G est isomorphe à un produit semi-direct $N \rtimes_\varphi H$, avec $N \simeq C_3$ et H d'ordre 4. Il va falloir distinguer les différents morphismes $\varphi : H \to \operatorname{Aut} N$ pouvant intervenir. Remarquons que, N étant cyclique d'ordre 3, le groupe des automorphismes de N est un groupe d'ordre 2.

- H *est isomorphe à* C_4. Il y a deux morphismes de C_4 dans $\operatorname{Aut} C_3$, le morphisme trivial et un morphisme non trivial. Le premier mène à un produit direct (ce qui est exclu, car G serait alors abélien et H serait distingué) et le second mène au groupe T que nous avons construit.
- H *est isomorphe à* $C_2 \times C_2$. Il y a quatre morphismes possibles de $C_2 \times C_2$ dans $C_2 \simeq \operatorname{Aut} N$ (remarquez qu'un morphisme de groupes $C_2^n \to C_2^m$ est la même chose qu'une application $\mathbf{F}_2$-linéaire $\mathbf{F}_2^n \to \mathbf{F}_2^m$). L'un des quatre est le morphisme trivial (qui est exclu, comme plus haut), et les trois autres sont de la forme $p \circ \psi$, où p est la projection $C_2 \times C_2 \to C_2$ sur le premier facteur et φ est un automorphisme de groupes de $C_2 \times C_2$.

Comme on l'a vu à la première question de cet exercice, composer le morphisme $\varphi : H \to \mathrm{Aut}\, N$ (à droite) par un automorphisme de H ne change pas le produit semi-direct, à isomorphisme près. Le groupe G est donc isomorphe à $C_3 \rtimes_p (C_2 \times C_2)$.

On a donc bien montré que tout groupe G d'ordre 12 est isomorphe à $C_2 \times C_6$, C_{12}, $\mathfrak{A}(4)$, T ou $C_3 \rtimes_p (C_2 \times C_2)$. En appliquant ce théorème au groupe diédral (et en se rappelant que l'on avait vu que celui-ci n'était isomorphe à aucun des quatre autres), on obtient $D_{12} \simeq C_3 \rtimes_p (C_2 \times C_2)$, ce qui complète la classification. [1]

Remarques.
- Le groupe $\mathfrak{S}(3) \times C_2$ est d'ordre 12. Où est-il ?
- Vous devriez maintenant être en mesure de classer tous les groupes d'ordre ≤ 15. Vérifiez-le. (En revanche, il y a, à isomorphisme près, 14 groupes d'ordre 16...)

3. Remarquons que la condition « tous les groupes d'ordre n sont isomorphes » est évidemment équivalente à la condition « tous les groupes d'ordre n sont cycliques. »

   Commençons par démontrer la condition nécessaire : si n n'est pas de la forme prescrite par l'énoncé, c'est que l'une des deux possiblités suivantes advient :
   - n est divisible par le carré p^2 d'un nombre premier, disons $n = p^2 m$. Dans ce cas, le groupe abélien $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ d'ordre n n'est pas cyclique, d'après le théorème de classification des groupes abéliens finis (ou parce qu'il a trop d'éléments d'ordre p) ;
   - n est divisible par le produit pq de deux nombres premiers $p < q$ tels que p divise $q-1$, disons $n = pqm$. Dans ce cas, la question précédente montre l'existence d'un produit semi-direct non abélien $\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$, et le groupe $(\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}) \times \mathbf{Z}/m\mathbf{Z}$ d'ordre n n'est pas cylique.

   La condition suffisante est considérablement plus difficile que ce que je pensais, j'en suis désolé... Le plan est pourtant simple : on va considérer un exemple imaginaire de groupe G non cyclique minimal dont l'ordre vérifie l'hypothèse. On va alors utiliser un résultat intermédiaire affirmant qu'un tel groupe ne peut pas être simple, ce qui nous donnera un sous-groupe distingué non trivial $N \subseteq G$. Par minimalité du contre-exemple, le sous-groupe N et le quotient G/N, dont les ordres vérifient encore l'hypothèse, seront cyliques. On concluera alors en utilisant le résultat classique selon lequel le quotient d'un groupe par un sous-groupe central n'est cyclique que si le groupe est abélien.

   Lemme. Soit G un groupe non cyclique dont tous les sous-groupes stricts sont cycliques. Alors G ne peut pas être simple.

   Preuve. Supposons au contraire que G soit simple, non cyclique et que tous ses sous-groupes stricts soient cycliques.

   Remarquons déjà que deux sous-groupes maximaux différents de G s'intersectent trivialement : si H et K sont deux tels sous-groupes, le normalisateur de leur intersection $N(H \cap K)$ les contient tous les deux, ce qui entraîne par maximalité que $N(H \cap K) = G$, et donc que $H \cap K$ soit distingué dans G. Par simplicité, on a bien $H \cap K = \{1_G\}$.

   Soit maintenant $H \subseteq G$ un sous-groupe maximal. D'après la question 2 de l'exercice 4, ses conjugués ne recouvrent pas G. Il existe donc un élément n'appartenant pas à un des conjugués de H et donc un sous-groupe maximal K contenant cet élément. Par définition, ni K ni aucun de ses conjugués n'est conjugué à H : si on note $\mathscr{C}(H)$ (resp. $\mathscr{C}(K)$) l'ensemble des éléments de G différents de l'identité appartenant à un conjugué de H (resp. K), on a donc $\mathscr{C}(H) \cap \mathscr{C}(K) = \varnothing$.

1. J'admets, cet argument est un peu mesquin. Comprendre véritablement l'isomorphisme $D_{12} \simeq C_3 \rtimes_p (C_2 \times C_2)$ est un bon exercice.

Dénombrons maintenant ces ensembles : en général, un sous-groupe $S \subseteq G$ a $[G : N(S)]$ conjugués distincts ($N(S)$ est précisément le stabilisateur de S dans l'action de G par conjugaison sur ses sous-groupes). Dans notre cas, $N(H)$ est un sous-groupe contenant H : puisqu'il ne peut pas être G tout entier (cela entraînerait que H soit distingué dans G) et que H est maximal, on a $N(H) = H$.

Ainsi, H a $[G : H]$ conjugués, et ceux-ci s'intersectent trivialement. On a donc

$$|\mathscr{C}(H)| = [G : H] \cdot (|H| - 1) = |G| - |H|.$$

De la même façon, évidemment, $|\mathscr{C}(K)| = |G| - |K|$.

Mais on arrive à une contradiction : $\mathscr{C}(H)$ et $\mathscr{C}(G)$ sont des ensembles disjoints de cardinal $\geq |G|/2$ inclus dans $G \setminus \{1_G\}$, de cardinal $|G| - 1$. L'hypothèse de départ était donc absurde, ce qui entraîne que G ne peut pas être simple.

À ce stade, on peut attaquer la preuve du théorème : soit G un contre-exemple minimal à la propriété que l'on cherche à démontrer. En particulier, d'après le lemme qui précède, G a un sous-groupe distingué non trivial. Puisque G est un contre-exemple minimal, N et G/N, dont les ordres vérifient l'hypothèse de la propriété que l'on cherche à démontrer, sont tous deux cycliques. Le but est de montrer que N est inclus dans le centre de G et d'appliquer le résultat classique suivant.

Lemme. Soit $N \subseteq Z(G)$ un sous-groupe central. Si G/N est cyclique, alors G est abélien.

Preuve. Soit $x \in G$ un élément dont la classe $[x]_N \in G/N$ engendre le groupe quotient. Si $n = |G/N|$, on a donc

$$G/N = \left\{[1]_N, [x]_N, \ldots, [x^{n-1}]_N\right\},$$

ce qui entraîne $G = N \sqcup xN \sqcup \cdots \sqcup x^{n-1}N$. La centralité de N entraîne alors immédiatement que N est abélien :

$$\left(x^{k_1} n_1\right) \cdot \left(x^{k_2} n_2\right) = x^{k_1+k_2} n_1 n_2 = \left(x^{k_2} n_2\right) \cdot \left(x^{k_1} n_1\right).$$

Il nous reste donc à voir pourquoi N est inclus dans le centre de G, autrement dit pourquoi le centralisateur $C(N) = \{x \in G \mid \forall n \in N, xn = nx\}$ de N est égal à G tout entier.

Pour cela, remarquons que, comme N est distingué, G agit sur N par conjugaison (et la restriction à N de ces conjugaisons donne des automorphismes de N). Le noyau de cette action est précisément le centralisateur de N. D'après le théorème de factorisation, cela entraîne que le quotient G/C(N) s'identifie à un sous-groupe de Aut N. Mais G/C(N) a pour ordre un diviseur de $|G| = p_1 \cdots p_r$, alors que Aut N a pour ordre $\varphi(n)$, qui est le produit d'un certain nombre de $(p_j - 1)$. D'après l'hypothèse, |G/C(N)| et |Aut N| sont donc premiers entre eux ; ainsi, la seule possiblité pour qu'un morphisme injectif $G/C(N) \to \mathrm{Aut}\, N$ existe est que G/C(N) soit trivial et donc que $C(N) = G$.

Cela conclut (enfin !) la preuve : N est central, donc, d'après le résultat précédent, G est abélien. Comme son cardinal est le produit de nombres premiers distincts, il est alors automatiquement cyclique, ce qui clôt la preuve.

Remarque. Quoiqu'élémentaire, cette preuve reste assez compliquée. Il n'existe à ma connaissance aucune preuve véritablement facile du résultat (ce qui fait qu'il eût mieux valu ne pas le mettre dans la feuille de TD, *mea maxima culpa.*) On peut en revanche signaler qu'il en existe des preuves plus directes reposant sur des résultats importants, mais plus difficiles, de la théorie des groupes finis.

Le *théorème du p-complément de Burnside* affirme que si G a un sous-groupe de Sylow S inclus dans le centre de son normalisateur, alors celui-ci possède automatiquement un *complément distingué* N, c'est-à-dire qu'il existe un sous-groupe distingué $N \subseteq G$ tel que $G = SN$ et $S \cap N = \{1_G\}$ (en particulier, G est un produit semi-direct de N par S). On montre que c'est notamment le cas d'un p-sous groupe de Sylow de G si celui-ci est cyclique et que p est le plus petit facteur premier de $|G|$.

Ce résultat permet alors de donner une preuve par récurrence immédiate du résultat. (Cf. au choix les exercices de la section 8.F. du *Cours d'algèbre* de Daniel Perrin, la section "Transfer and Burnside's theorem" du chapitre 7 de *An Introduction to the Theory of Groups* de Joseph Rotman, les théorèmes 5.62 et 5.63 de *Gruppi* d'Antonio Machì...)

4. On sait que si $n = p_1^{v_{p_1}} \cdots p_r^{v_{p_r}}$ est la décomposition de n en facteurs premiers, alors

$$\varphi(n) = (p_1 - 1)p_1^{v_{p_1}-1} \cdots (p_r - 1)p_r^{v_{p_r}-1}.$$

On voit donc que si n et $\varphi(n)$ sont premiers entre eux, les v_{p_i} doivent être tous égaux à 1 (c'est-à-dire que n doit être sans facteur carré) et que l'on a alors simplement

$$\text{pgcd}(n, \varphi(n)) = 1 \Leftrightarrow \forall j \in \{1, \ldots, r\}, p_j \text{ ne divise pas } (p_1 - 1) \cdots (p_r - 1),$$

ce qui est clairement équivalent à la condition de l'énoncé.

Exercice 3. Supposons $n \geq 2$. On va démontrer que

$$\text{ZGL}_n(A) = \left\{ \lambda I_n \,\middle|\, \lambda \in A^\times \cap Z(A) \right\}.$$

Une inclusion est claire : si $\lambda \in A^\times$, il en va de même de $\lambda^n = \text{dét}(\lambda I_n)$, donc $\lambda I_n \in \text{GL}_n(A)$, et cette matrice commute clairement avec tout le monde.
Réciproquement, soit $M = \sum_{i,j} m_{i,j} e_{i,j}$ une matrice dans le centre de $\text{GL}_n(A)$. En particulier, M doit commuter avec les matrices de transvection $I_n + \mu e_{i_0,j_0}$, pour $i_0 \neq j_0$ et $\mu \in A$ (ces matrices sont inversibles, d'inverse $I_n - \mu e_{i_0,j_0}$). Comme

$$M\left(I_n + \mu e_{i_0,j_0}\right) = M + \sum_{i,j} m_{i,j} e_{i,j} \mu e_{i_0,j_0} = M + \sum_i m_{i,i_0} \mu e_{i,j_0}$$
$$\left(I_n + \mu e_{i_0,j_0}\right) M = M + \sum_{i,j} \mu e_{i_0,j_0} m_{i,j} e_{i,j} = M + \sum_j \mu m_{j_0,j} e_{i_0,j},$$

l'égalité $M\left(I_n + e_{i_0,j_0}\right) = \left(I_n + e_{i_0,j_0}\right) M$ implique donc

$$\begin{cases} \forall i \neq i_0, m_{i,i_0}\mu = 0 \\ \forall j \neq j_0, \mu m_{j_0,j} = 0 \end{cases} \qquad \text{et} \qquad m_{i_0,i_0}\mu = \mu m_{j_0,j_0}.$$

Ces égalités étant valables pour tous les indices (i_0, j_0) et tout $\mu \in A$, elles entraînent que M est une matrice scalaire : il existe $\lambda \in A$ tel que $M = \lambda I_n$ (il suffit de prendre $\mu = 1$) et que le coefficient $\lambda \in A$ commute avec tous les éléments de A.
Comme M est inversible, λ^n est inversible. Comme en outre λ est central, cela implique que λ est inversible : si μ est l'inverse de λ^n, on a $\lambda^n \mu = \mu \lambda^n = 1$, et $\mu \lambda^{n-1} = \lambda^{n-1} \mu$ est l'inverse de λ.
On a donc bien $M \in \left\{ \lambda I_n \,\middle|\, \lambda \in A^\times \cap Z(A) \right\}$.

Remarque : Si $n = 1$, $\text{GL}_n(A) = A^\times$. En général, le centre $Z(A^\times)$ de ce groupe est strictement plus grand que $\left\{ \lambda I_n \,\middle|\, \lambda \in A^\times \cap Z(A) \right\}$: un élément inversible peut très bien commuter avec tous les éléments inversibles sans pour autant commuter avec tous les éléments de l'anneau.

Par exemple soit K un corps et $\sigma : K \to K$ un automorphisme. On définit alors l'anneau $K[X;\sigma]$ des polynômes tordus comme l'anneau des éléments de la forme $\sum_{i=0}^{n} a_i X^i$, pour un $(n+1)$-uplet $(a_i)_{i=0}^n \in K^{n+1}$, et où la multiplication est définie par la formule

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot \left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i \sigma^i(b_j)\right) X^k.$$

Par exemple, si $\sigma : \mathbf{C} \to \mathbf{C}$ est la conjugaison, $\mathbf{C}[X;\sigma]$ ressemble à l'anneau $\mathbf{C}[X]$ des polynômes, à ceci près que les coefficients et la variable X ne commutent plus, mais qu'on a en revanche la relation

$$\forall a \in \mathbf{C}, X a = \overline{a} X.$$

On vérifie alors facilement que cela définit bien un anneau tel que
– le centre de $\mathbf{C}[X;\sigma]$ est le sous-anneau $\left\{\sum_{i=0}^{n} a_i X^i \,\middle|\, (a_i)_{i=0}^n \in \mathbf{R}^{n+1}\right\}$, isomorphe à $\mathbf{R}[X]$.
– les éléments inversibles de $\mathbf{C}[X;\sigma]$ sont les constantes non nulles.
En particulier,

$$(\mathbf{C}[X;\sigma])^\times \cap Z(\mathbf{C}[X;\sigma]) = \mathbf{C}^\times \cap \mathbf{R}[X] = \mathbf{R}^\times \subsetneq Z\left(\mathbf{C}[X;\sigma]^\times\right) = Z(\mathbf{C}^\times) = \mathbf{C}^\times.$$

On pourra apprendre beaucoup de choses sur les anneaux non commutatifs dans l'excellent livre *A First Course in Noncommutative Rings* de Tsit Yuen Lam, où notre anneau de polynômes tordus est l'exemple (1.7).

Exercice 4.

1. Une matrice inversible est dans B si et seulement si elle est triangulaire, et dans un conjugué de B si et seulement si elle est trigonalisable. La question revient donc à montrer que toute matrice 2×2 à coefficients dans K est trigonalisable.

   On sait bien qu'une matrice à coefficients dans K est trigonalisable sur K si et seulement si son polynôme caractéristique est scindé sur K. Puisque K est supposé quadratiquement clos, c'est le cas de tout polynôme de degré 2, et en particulier de tout polynôme caractéristique de matrice 2×2.

2. C'est un théorème de Jordan.

   Le point-clef est que si $g \in G$ et $h \in H$, on a évidemment $(gh)H(gh)^{-1} = gHg^{-1}$. En particulier, le conjugué gHg^{-1} ne dépend que de la classe de g dans l'ensemble des classes à gauche G/H. On choisit alors un système de représentants T des classes à gauche. Par définition, le cardinal de T est le cardinal de G/H, c'est-à-dire l'indice $[G:H] = |G|/|H|$ de H.

   En utilisant que l'élément neutre appartient à tous les conjugués de H, on compte alors

$$\left|\bigcup_{g\in G} gHg^{-1}\right| = \left|\bigcup_{g\in T} gHg^{-1}\right| = \left|\bigcup_{g\in T} \left(gHg^{-1} \setminus \{1\}\right)\right| + 1$$
$$= [G:H](|H|-1)+1 = G - ([G:H]-1),$$

   ce qui est bien strictement inférieur à G.

On trouvera des corollaires de cette formule et d'intéressants développements au chapitre 6 du cours *Groupes finis* de Jean-Pierre Serre. [2]

Exercice 5.

2. http://www.college-de-france.fr/media/historique/UPL61389_groupes_finis.pdf

1. Soit $M \in GL_2(\mathbf{Z})$ d'ordre fini. En particulier, M est annulée par le polynôme $X^n - 1$, qui est scindé et à racines simples dans $\mathbf{C}$. On peut donc diagonaliser M dans $\mathbf{C}$: $M \underset{\mathbf{C}}{\sim} \mathrm{diag}(\zeta_1, \zeta_2)$. Les valeurs propres ζ_1 et ζ_2 sont donc à la fois des racines de l'unité (car $M^n = I_2$) et des entiers algébriques de degré ≤ 2 (car elles annulent le polynôme caractéristique de M). On peut alors démontrer que ces racines sont des racines quatrièmes ou sixièmes de l'unité (il y a au moins deux méthodes : on peut utiliser que $\varphi(n) \in \{1,2\} \Leftrightarrow n \in \{1,2,3,4,6\}$; ou utiliser le fait que, comme les ζ sont des entiers algébriques, $2\,\mathrm{Ré}\,\zeta \in \mathbf{Z}$). En particulier, $\zeta_1^{12} = \zeta_2^{12} = 1$, ce qui implique $M^{12} = I_2$.
2. Soit $A \in SL_2(\mathbf{F}_p)$. On va distinguer trois cas :
   - A est diagonalisable sur $\mathbf{F}_p$: on a donc $A \underset{\mathbf{F}_p}{\sim} \mathrm{diag}(\zeta_1, \zeta_2)$, avec $\zeta_i \in \mathbf{F}_p^\times$. Comme ce groupe est d'ordre $p-1$, on a $\zeta_1^{p-1} = \zeta_2^{p-1} = 1$, et donc $A^{p-1} = I_2$.
   - A n'est pas diagonalisable, même sur une clôture algébrique : cela entraîne que son polynôme caractéristique n'est pas à racines simples. Comme $\det A = 1$, il n'y a que deux cas possibles : $\chi_A = X^2 \pm 1$. Dans tous les cas, le polynôme caractéristique est scindé sur $\mathbf{F}_p$, et l'on peut trigonaliser A :
   $$A \underset{\mathbf{F}_p}{\sim} \begin{pmatrix} 1 & \tau \\ 0 & 1 \end{pmatrix} \qquad \text{ou} \qquad A \underset{\mathbf{F}_p}{\sim} \begin{pmatrix} -1 & \tau \\ 0 & -1 \end{pmatrix},$$
   pour un certain $\tau \in \mathbf{F}_p$.
   Comme $\begin{pmatrix} 1 & \tau \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & k\tau \\ 0 & 1 \end{pmatrix}$, l'ordre de A dans le premier cas est inférieur ou égal à p. Si A est du deuxième type, A^2 est du premier, et $A^{2p} = I_2$.
   - A est diagonalisable sur $\overline{\mathbf{F}_p}$, mais pas sur $\mathbf{F}_p$. Cela entraîne que ses valeurs propres ne sont pas dans $\mathbf{F}_p$ et donc que le polynôme caractéristique χ_A est irréductible sur $\mathbf{F}_p$. Comme $\mathbf{F}_p$ n'a qu'une seule extension quadratique, le corps de rupture du polynôme caractéristique est donc $\mathbf{F}_{p^2}$. Comme $\mathbf{F}_p$ est un corps parfait, l'extension $\mathbf{F}_{p^2}/\mathbf{F}_p$ est séparable et le polynôme caractéristique de A est scindé à racines simples sur $\mathbf{F}_{p^2}$ et on a
   $$A \underset{\mathbf{F}_{p^2}}{\sim} \mathrm{diag}(\zeta_1, \zeta_2).$$
   On peut maintenant utiliser deux relations entre ces valeurs propres :
   - Comme $A \in SL_2(\mathbf{F}_p)$, on a $\zeta_1\zeta_2 = 1$.
   - Comme le polynôme caractéristique de A est le polynôme minimal de ζ_1 et de ζ_2, on a $\zeta_2 = \sigma(\zeta_1)$, où $\sigma : \mathbf{F}_{p^2} \to \mathbf{F}_{p^2}$ est l'unique automorphisme non trivial de $\mathbf{F}_{p^2}$, à savoir l'automorphisme de Frobenius $x \mapsto x^p$ (qui est bien une involution). On a donc $\zeta_2 = \zeta_1^p$.

   En résumé, $\zeta_1^{p+1} = 1$, et il en va de même de ζ_2. On a donc $A^{p+1} = I_2$.

   Dans tous les cas, l'ordre de A est bien inférieur ou égal à $2p$.

Exercice 6.

1. On fait agir $GL_n(A)$ sur A^n par multiplication. On note $\sim$ la relation d'équivalence ainsi obtenue : $v \sim w$ si et seulement si $\exists M \in GL_n(A) : Mv = w$. Cela posé, il s'agit donc de montrer que tout vecteur est équivalent à un vecteur dont toutes les coordonnées sauf la première sont nulles.

   On procède par récurrence :
   - Si $n = 2$, c'est une conséquence du théorème de Bézout : on peut écrire $a_1 = d\,a_1'$ et $a_2 = d\,a_2'$, avec $d = \mathrm{pgcd}(a_1, a_2)$ et a_1' et a_2' premiers entre eux. Le théorème de Bézout permet alors de trouver u et v tels que $a_1'v - a_2'u = 1$. On a alors
   $$\begin{pmatrix} a_1' & u \\ a_2' & v \end{pmatrix} \in GL_2(A) \qquad \text{et} \qquad \begin{pmatrix} a_1' & u \\ a_2' & v \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a_1' \\ a_2' \end{pmatrix}.$$

En particulier,

$$\begin{pmatrix} a_1' & u \\ a_2' & v \end{pmatrix} \cdot \begin{pmatrix} d \\ 0 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \sim \begin{pmatrix} d \\ 0 \end{pmatrix}.$$

– Supposons maintenant le résultat démontré au rang n. Faisons deux remarques : d'abord, si $\mathrm{M} \in \mathrm{GL}_n(\mathrm{A})$, la matrice diagonale par blocs $\mathrm{diag}(\mathrm{M}, 1) \in \mathrm{M}_{n+1}(\mathrm{A})$ est encore inversible. En outre, toutes les matrices de permutation sont inversibles. On peut alors démontrer le résultat en appliquant deux fois l'hypothèse de récurrence :

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \\ a_{n+1} \end{pmatrix} \sim \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \\ a_{n+1} \end{pmatrix} \sim \begin{pmatrix} d \\ a_{n+1} \\ \vdots \\ 0 \\ 0 \end{pmatrix} \sim \begin{pmatrix} d' \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}.$$

2. Montrons que si un anneau est de Hermite, tout idéal engendré par deux éléments est principal : soit $a, b \in \mathrm{A}$ et $\mathrm{P} \in \mathrm{GL}_2(\mathrm{A})$, $d \in \mathrm{A}$ tel que $\begin{pmatrix} a \\ b \end{pmatrix} = \mathrm{P} \begin{pmatrix} d \\ 0 \end{pmatrix}$. On a alors

$$\begin{aligned}
(a, b) &= \left\{ au + bv \,\middle|\, (u, v) \in \mathrm{A}^2 \right\} \\
&= \left\{ \begin{pmatrix} u & v \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} \,\middle|\, (u, v) \in \mathrm{A}^2 \right\} \\
&= \left\{ \begin{pmatrix} u & v \end{pmatrix} \mathrm{P} \begin{pmatrix} d \\ 0 \end{pmatrix} \,\middle|\, (u, v) \in \mathrm{A}^2 \right\} \\
&= \left\{ \begin{pmatrix} u' & v' \end{pmatrix} \cdot \begin{pmatrix} d \\ 0 \end{pmatrix} \,\middle|\, (u', v') \in \mathrm{A}^2 \right\} \\
&= \left\{ du' \,\middle|\, (u', v') \in \mathrm{A}^2 \right\} \\
&= (d),
\end{aligned}$$

la quatrième égalité étant due au fait que la multiplication à droite par P est une application linéaire bijective.

Remarque. Pour des raisons évidentes, un anneau intègre est dit *de Bézout* si tout idéal engendré par deux éléments est principal. On montre alors facilement que tout idéal de type fini est principal (ce qui entraîne qu'un anneau à la fois de Bézout et noethérien est principal). Comme on peut le constater, la première question n'a en fait utilisé que le fait que A était de Bézout donc les deux premières questions montrent qu'un anneau intègre est de Hermite si et seulement s'il est de Bézout.

Par exemple, l'anneau $\mathbf{C}[\mathrm{X}, \mathrm{Y}]$ n'a pas cette propriété (l'idéal engendré par X et Y n'est pas principal), donc il n'est pas de Hermite.

3. Si $a_1, \ldots, a_n$ sont des entiers premiers entre eux, la première question entraîne l'existence d'un entier d tel que

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \sim \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad \text{donc on peut trouver } \mathrm{P} \in \mathrm{GL}_n(\mathbf{Z}) \text{ tel que} \qquad \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \mathrm{P} \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

La preuve de la deuxième question (généralisée au cas des matrices $n \times n$, ce qui ne pose aucune difficulté) montre alors l'égalité des idéaux $(a_1, \dots, a_n) = (d)$. En particulier, d est, au signe près, le pgcd des a_i.

Quitte à multiplier P par $\mathrm{diag}(\pm 1, 1, \dots, 1)$, on peut supposer $d = \mathrm{pgcd}(a_i)$; quitte à la multiplier par $\mathrm{diag}(1, 1, \dots, \pm 1)$ (ce qui ne change pas la valeur de d), on peut en outre supposer $\det \mathrm{P} = 1$.

En particulier, la matrice $\mathrm{P}\,\mathrm{diag}(d, 1, \dots, 1)$ est une matrice de déterminant $d = \mathrm{pgcd}(a_i)$ et de première colonne

$$\mathrm{P}\,\mathrm{diag}(d, 1, \dots, 1) \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \mathrm{P} \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix},$$

ce qui démontre le théorème de Hermite.

Exercice 7.

1. On a vu en cours que si K est un corps, $\mathrm{E}_n(\mathrm{K}) = \mathrm{SL}_n(\mathrm{K})$.
2. Si $\mathrm{A} \notin \mathrm{M}_2(\mathrm{K})$, on peut écrire $\mathrm{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \mathrm{FD}(a) + a' & \mathrm{FD}(b) + b' \\ \mathrm{FD}(c) + c' & \mathrm{FD}(d) + d' \end{pmatrix}$, où a' est de degré strictement inférieur à $\mathrm{FD}(a)$ (et *idem* pour b, c et d) et où au moins l'un des coefficients de FD(A) n'est pas dans K.

   Comme l'inégalité $\deg \det \mathrm{A} = \deg(ad - bc) \leq \max(\deg ad, \deg bc)$ est stricte (ici, deg est le degré total), c'est que les termes dominants de ad et bc sont égaux. On a donc $\mathrm{FD}(ad) = \mathrm{FD}(bc)$ et $\det \mathrm{FD}(\mathrm{A}) = \mathrm{FD}(a)\mathrm{FD}(d) - \mathrm{FD}(b)\mathrm{FD}(c) = \mathrm{FD}(ad) - \mathrm{FD}(bc) = 0$.
3. Par définition, A s'écrit $\mathrm{A} = \mathrm{E}_1 \cdots \mathrm{E}_m$, où chaque E_i est de la forme $\begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}$ ou $\begin{pmatrix} 1 & 0 \\ f & 1 \end{pmatrix}$. On va démontrer le résultat par récurrence sur m. Le cas $m = 1$ est évident : $\mathrm{A} = \mathrm{E}_1$ a un coefficient nul.

   Supposons donc le résultat démontré pour $m - 1$ et posons

   $$\mathrm{A}' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \mathrm{E}_1 \cdots \mathrm{E}_{m-1} \in \mathrm{E}_2(\mathrm{R}).$$

   D'après l'hypothèse de récurrence, trois choses peuvent arriver :

   i. L'un des coefficients de A′ est nul, disons $c = 0$ (les autres cas sont similaires). On a alors $\mathrm{A}' = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ et $\det \mathrm{A}' = 1$ implique $ad = 1$ et $a, d \in \mathrm{R}^* = \mathrm{A}^*$.

   Si $\mathrm{E}_m = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}$, $\mathrm{A} = \mathrm{A}'\mathrm{E}_m$ garde un coefficient nul en bas à gauche. Il reste donc surtout à traiter le cas $\mathrm{E}_m = \begin{pmatrix} 1 & 0 \\ f & 1 \end{pmatrix}$. Dans ce cas, $\mathrm{A} = \begin{pmatrix} a + bf & b \\ df & d \end{pmatrix}$.

   Déjà, si $b = 0$ ou $f = 0$, la matrice A a un coefficient nul et le résultat est démontré. On peut donc supposer b et f non nuls. Si bf était un élement non nul de K, il en serait de même de b, de f et donc de df ; la matrice A serait donc à coefficients dans K, ce qui est exclu par hypothèse. On a donc $bf \notin \mathrm{K}$, ce qui permet de déterminer la forme dominante de A : $\mathrm{FD}(\mathrm{A}) = \begin{pmatrix} \mathrm{FD}(b)\mathrm{FD}(f) & \mathrm{FD}(b) \\ d\,\mathrm{FD}(f) & d \end{pmatrix}$. La première ligne de cette matrice valant $\mathrm{FD}(b)/d$ fois la seconde, le résultat est démontré.

ii. $A' \in M_2(K)$ n'a aucun coefficient nul : $a, b, c, d \in K^*$.
Supposons en outre $E_m = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}$ (l'autre cas est similaire). On a alors $A = \begin{pmatrix} a & af+c \\ c & cf+d \end{pmatrix}$.
Comme A est supposée ne pas appartenir à $M_2(K)$, on a $f \notin K$ et $FD(A) = \begin{pmatrix} a & af \\ c & cf \end{pmatrix}$. La première ligne de FD(A) est donc a/c fois la seconde et le résultat est démontré.

iii. L'une des lignes de FD(A′) est multiple de l'autre, disons

$$(FD(a), FD(b)) = h(FD(c), FD(d)) \text{ (l'autre cas est similaire).}$$

Supposons en outre $E_m = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}$, donc $A = \begin{pmatrix} a & af+b \\ c & cf+d \end{pmatrix}$. D'après la question précédente, $\det FD(A) = 0$. On a donc

$$FD(c)FD(af+b) = FD(a)FD(cf+d) = hFD(c)FD(cf+d),$$

ce qui implique $FD(af+b) = hFD(cf+b)$. On a alors la relation de proportionnalité voulue $(FD(a), FD(af+b)) = h(FD(c), FD(cf+d))$. Le cas $E_m = \begin{pmatrix} 1 & 0 \\ f & 1 \end{pmatrix}$ est similaire.

4. La matrice de Cohn a pour forme dominante $FD(C) = \begin{pmatrix} xy & x^2 \\ -y^2 & -xy \end{pmatrix}$. Aucun des deux vecteurs (xy, x^2) et $(-y^2, -xy)$ n'est multiple de l'autre. La question précédente implique $C \notin E_2(R)$, même si $\det C = (1+xy)(1-xy)+x^2y^2 = 1$.