École normale supérieure, année universitaire 2018-2019.
Cours *Algèbre 1*, corrigé de l'examen partiel du 7 novembre 2018.

**Exercice 1.**

(a) Pour tout sous-groupe distingué $\Gamma$ de $G$, notons $\Lambda_\Gamma$ l'ensemble des morphismes de $G$ dans $H$ de noyau $\Gamma$. On a alors $\mathrm{Hom}(G,H) = \coprod_{\Gamma \lhd G} \Lambda_\Gamma$. Par ailleurs si $\Gamma$ est un sous-groupe distingué de $G$, se donner un morphisme de $G$ vers $H$ de noyau $\Gamma$ revient à se donner un morphisme injectif de $G/\Gamma$ vers $H$. On a donc $M(G,H) = \sum_{\Gamma \lhd G} i(G/\Gamma, H)$.

(b) Si $G = \{e\}$ alors $M(G,H) = I(G,H) = 1$ pour tout groupe $H$ (il y a un seul morphisme de $G$ dans $H$, à savoir le morphisme trivial qui est évidemment injectif) et l'assertion requise est vraie avec $\mu_G = 1$ (ici $G$ est le seul sous-groupe distingué de $G$). On suppose le cardinal de $G$ strictement supérieur à 1 et l'assertion vraie pour les groupes de cardinal strictement inférieur à celui de $G$.
L'égalité $M(G,H) = \sum_{\Gamma \lhd G} I(G/\Gamma, H)$ peut se récrire

$$I(G,H) = M(G,H) - \sum_{\Gamma \lhd G, \Gamma \neq \{e\}} I(G/\Gamma, H).$$

Par hypothèse de récurrence, il existe pour tout sous-groupe distingué non trivial $\Gamma$ de $G$ une famille $(\mu_\Delta^\Gamma)_\Delta$ d'entiers relatifs (ne dépendant pas de $H$), indexée par l'ensemble des sous-groupes distingués de $G/\Gamma$, telle que $I(G/\Gamma, H) = \sum_{\Delta \lhd (G/\Gamma)} \mu_\Delta^\Gamma M((G/\Gamma)/\Delta, H)$. Modulo la bijection canonique entre l'ensemble des sous-groupes distingués de $G/\Gamma$ et l'ensemble des sous-groupes distingués de $G$ contenant $\Gamma$, on peut considérer que $\Delta$ parcourt l'ensemble des sous-groupes distingués de $G$ contenant $\Gamma$, et écrire

$$I(G/\Gamma, H) = \sum_{\Gamma \subset \Delta \lhd G} \mu_\Delta^\Gamma M(G/\Delta, H).$$

On a dès lors

$$\begin{aligned}
I(G,H) &= M(G,H) - \sum_{\Gamma \lhd G, \Gamma \neq \{e\}} I(G/\Gamma, H) \\
&= M(G,H) - \sum_{\Gamma \lhd G, \Gamma \neq \{e\}} \left( \sum_{\Gamma \subset \Delta \lhd G} \mu_\Delta^\Gamma M(G/\Delta, H) \right) \\
&= M(G,H) - \sum_{\Delta \lhd G} \left( \sum_{\{e\} \neq \Gamma \subset \Delta, \Gamma \lhd G} \mu_\Delta^\Gamma \right) M(G/\Delta, H) \\
&= M(G,H) - \sum_{\{e\} \neq \Delta \lhd G} \left( \sum_{\{e\} \neq \Gamma \subset \Delta, \Gamma \lhd G} \mu_\Delta^\Gamma \right) M(G/\Delta, H)
\end{aligned}$$

(la dernière égalité provient du fait que si $\Delta = \{e\}$ la somme $\sum_{\{e\} \neq \Gamma \subset \Delta} \cdots$ est vide). On obtient alors le résultat voulu en posant

$\mu_{\{e\}} = 1$ et $\mu_\Delta = -\sum_{\{e\}\neq\Gamma\subset\Delta,\Gamma\lhd G} \mu_\Delta^\Gamma$ pour tout sous-groupe distingué non trivial $\Delta$ de $G$.

(c)

(c1) Soit $G$ un groupe fini. Comme $X \times H$ est isomorphe à $X \times K$ on a $M(G, X \times H) = M(G, X \times K)$.

Se donner une application de $G$ dans $X \times H$ revient à se donner un couple $(\varphi, \psi)$ formé d'une application $\varphi$ de $G$ vers $X$ et d'une application $\psi$ de $G$ vers $H$ – au couple $(\varphi, \psi)$ correspond l'application $g \mapsto (\varphi(g), \psi(g))$. Et si on se donne un tel couple $(\varphi, \psi)$ alors $g \mapsto (\varphi(g), \psi(g))$ est un morphisme de groupes si et seulement si $\varphi$ et $\psi$ sont des morphismes de groupes – c'est une conséquence immédiate du fait que la loi de groupe de $X \times H$ est définie composante par composante. Par conséquent, se donner un morphisme de $G$ vers $X \times H$ revient à se donner un couple $(\varphi, \psi)$ formé d'un morphisme $\varphi$ de $G$ vers $X$ et d'un morphisme $\psi$ de $G$ vers $H$. Il s'ensuit que $M(G, X \times H) = M(G, X)M(G, H)$, et l'on a évidemment de même $M(G, X \times K) = M(G, X)M(G, K)$. Ceci entraîne, en vertu de l'égalité $M(G, X \times H) = M(G, X \times K)$ vue plus haut, que $M(G, X)M(G, H) = M(G, X)M(G, K)$, et finalement que $M(G, H) = M(G, K)$ (en effet $M(G, X)$ est non nul puisqu'il y a au moins un morphisme de $G$ vers $X$, à savoir le morphisme trivial).

(c2) Soit $G$ un groupe fini et soit $(\mu_\Gamma)$ la famille d'entiers relatifs de la question (b). On a

$$\begin{aligned} I(G, H) &= \sum_{\Gamma\lhd G} \mu_\Gamma M(G/\Gamma, H) \\ &= \sum_{\Gamma\lhd G} \mu_\Gamma M(G/\Gamma, K) \\ &= I(G, K) \end{aligned}$$

(la première et la troisième égalité viennent des propriétés de la famille $(\mu_\Gamma)$, et la seconde de ce qui a été vu en (c1)).

(c3) On a en particulier $I(H, H) = I(H, K)$. Or $i(H, H) \geqslant 1$ (il y a au moins un morphisme injectif de $H$ dans lui-même : l'identité !) ; par conséquent $i(H, K) \geqslant 1$ et il existe donc un morphisme injectif $u$ de $H$ dans $K$.

Or comme $X \times H$ est isomorphe à $X \times K$ ces deux groupes ont même cardinal. Autrement dit $|X| \cdot |H| = |X| \cdot |K|$ et on a donc $|H| = |K|$ car $|X| \neq 0$ (un groupe est toujours non vide). Il s'ensuit que le morphisme injectif $u$ est un isomorphisme.

(d) Considérons l'application de $G$ dans $G \times G$ qui envoie une suite $(g_i)_{i\in\mathbf{N}}$ sur le couple de suites $((g_{2i})_{i\in\mathbf{N}}, (g_{2i+1})_{i\in\mathbf{N}})$. C'est clairement un morphisme de groupes, et il est bijectif de réciproque

$$((h_i)_{i\in\mathbf{N}}, (k_i)_{i\in\mathbf{N}}) \mapsto (\ell_i)_{i\in\mathbf{N}}$$

où $\ell_i = h_{i/2}$ si $i$ est pair et $\ell_i = k_{(i-1)/2}$ si $i$ est impair.

**Exercice 2.** Écrivons $\sigma = C_{1,1} \dots C_{1,n_1} C_{2,1} \dots C_{2,n_2} \dots C_{r,1} \dots C_{r,n_r}$ où les $C_{i,j}$ sont des cycles à supports deux à deux disjoints, $C_{i,j}$ étant de longueur $\ell_i$ pour tout $(i,j)$.

(a) Soit $\tau \in S_n$. La permutation $\tau$ appartient au groupe $G$ si et seulement si $\tau\sigma\tau^{-1} = \sigma$, c'est-à-dire si et seulement si

$$(\tau C_{1,1}\tau^{-1})\dots(\tau C_{1,n_1}\tau^{-1})(\tau C_{2,1}\tau^{-1})\dots(\tau C_{2,n_2}\tau^{-1})\dots(\tau C_{r,1}\tau^{-1})(\tau C_{r,n_r}\tau^{-1}) = \sigma.$$

Compte-tenu de l'unicité de l'écriture comme produit de cycles à supports deux à deux disjoints et du fait que si $\Gamma$ est un cycle, $\tau\Gamma\tau^{-1}$ est un cycle de même longueur que $\Gamma$ et de support $\tau(\mathrm{Supp}(\Gamma))$, on voit que $\tau\sigma\tau^{-1} = \sigma$ si et seulement si il existe une famille $(\lambda_i)_{1 \leqslant i \leqslant r}$, où $\lambda_i \in S_{n_i}$ pour tout $i$, telle que $\tau C_{i,j}\tau^{-1}$ soit égale à $C_{i,\lambda_i(j)}$ pour tout $(i,j)$.
Se donner un élément de $G$ revient donc à choisir :
($\alpha$) pour tout $i$ compris entre 1 et $r$, une permutation $\lambda_i$ de $\{1,\dots,n_i\}$ (ce qui fait $\prod_i n_i!$ choix) ;
($\beta$) une permutation $\tau$ telle que $\tau C_{i,j}\tau^{-1} = C_{i,\lambda_i(j)}$ pour tout $(i,j)$.
Il reste donc, une famille $(\lambda_i)$ comme en ($\alpha$) étant donnée, à compter le nombre de permutations $\tau$ satisfaisant ($\beta$). Pour tout $(i,j)$, notons $E_{i,j}$ le support de $C_{i,j}$, et notons $F$ le complémentaire de $\coprod E_{i,j}$. Se donner une permutation $\tau$ satisfaisant ($\beta$) revient à se donner :
($\gamma$) une permutation $\xi$ de $F$ (il y a $(n - \sum_i \ell_i n_i)!$ choix) ;
($\delta$) pour tout $(i,j)$, une bijection $\tau_{i,j}$ entre $E_{i,j}$ et $E_{i,\lambda_i(j)}$ telle que $\tau_{i,j} C_{i,j} \tau_{i,j}^{-1} = C_{i,\lambda_i(j)}$ (en identifiant par abus un cycle avec la permutation qu'il induit sur son support).
Fixons $i$ et $j$. Écrivons $C_{i,j} = (a_1 \dots a_{\ell_i})$ et $C_{i,\lambda_i(j)} = (b_1 \dots b_{\ell_i})$. Une bijection $\zeta$ de $E_{i,j}$ sur $E_{i,\lambda_i(j)}$ vérifie l'égalité $\zeta C_{i,j} \zeta_{i,j}^{-1} = C_{i,\lambda_i(j)}$ si et seulement si $(\zeta(a_1)\dots,\zeta(a_{\ell_i})) = (b_1 \dots, b_{\ell_i})$. Or si $t$ est un entier compris entre 1 et $\ell_i$ tel que $\zeta(a_1) = b_t$ on a $(\zeta(a_1)\dots,\zeta(a_{\ell_i})) = (b_1 \dots, b_{\ell_i})$ si et seulement si $\zeta(a_k) = b_{[t+k]}$ pour tout $k$, où $[t+k]$ désigne l'unique entier compris entre 1 et $\ell_i$ égal à $t+k$ modulo $\ell_i$. Il y a donc exactement $\ell_i$ bijections $\zeta$ de $E_{i,j}$ sur $E_{i,\lambda_i(j)}$ telles que $\zeta C_{i,j} \zeta_{i,j}^{-1} = C_{i,\lambda_i(j)}$ : on peut choisir $\zeta(a_1)$ librement, et les autres valeurs sont imposées par l'égalité requise. On a en conséquence $\ell_i$ choix possibles pour $\tau_{i,j}$ à $(i,j)$ fixé ; l'indice $i$ parcourt $\{1,\dots,r\}$ et pour chaque $i$ l'indice $j$ parcourt $\{1,\dots,n_i\}$. On a donc $\prod_{1 \leqslant i \leqslant r} \ell_i^{n_i}$ choix pour la famille $(\tau_{ij})$. En récapitulant, on obtient l'égalité

$$|G| = \underbrace{\prod_{i=1}^{r} n_i!}_{\text{choix des } \lambda_i} \times \underbrace{(n - \sum_{i=1}^{r} n_i \ell_i)!}_{\text{choix de } \xi} \times \underbrace{\prod_{i=1}^{r} \ell_i^{n_i}}_{\text{choix des } \tau_{i,j}} .$$

Puisque $G$ s'interprète comme le stabilisateur de $\sigma$ sous l'action de $S_n$ sur lui-même par conjugaison, et puisque $C$ s'interprète comme l'orbite de $\sigma$ pour cette même action, il vient

$$|C| = \frac{n!}{(\prod_{i=1}^{r} n_i!) \cdot (n - \sum_{i=1}^{r} n_i \ell_i)! \cdot (\prod_{i=1}^{r} \ell_i^{n_i})}$$

(b) Supposons tout d'abord que $G \subset A_n$ et montrons que (i), (ii) et (iii) sont satisfaites. Fixons $i$. Le cycle $C_{i,1}$ commute avec $\sigma$ ; puisque $G \subset A_n$, la permutation $C_{i,1}$ est paire, ce qui veut dire que la longueur $\ell_i$ du cycle $C_i$ est impaire. Supposons qu'il existe un indice $i$ avec $n_i$ au moins égal à 2. Écrivons $C_{i1} = (a_1 \dots a_{\ell_i})$ et $C_{i2} = (b_1 \dots b_{\ell_i})$. Le produit $\tau = (a_1 b_1)(a_2 b_2) \dots (a_{\ell_i} b_{\ell_i})$ est une permutation impaire (car $\ell_i$ est impaire) ; par construction, la conjugaison par $\tau$ échange $C_{i1}$ et $C_{i2}$ et laisse invariant les autres cycles de la décomposition de $\sigma$. On a donc $\tau\sigma\tau^{-1} = \sigma$, ce qui veut dire que $\tau \in G$ et contredit l'hypothèse que $G \subset A_n$. Enfin supposons que $\sum n_i \ell_i < n - 1$. Dans ce cas $\sigma$ a au moins deux points fixes $a$ et $b$, et $(ab)$ est alors une permutation impaire commutant avec $\sigma$, ce qui contredit là encore l'inclusion $G \subset A_n$.

Réciproquement, supposons que (i), (ii) et (iii) sont satisfaites, et montrons que $G \subset A_n$ ; écrivons $C_i$ au lieu de $C_{i,1}$ pour tout $i$. Soit $\tau$ une permutation telle que $\tau\sigma\tau^{-1} = \sigma$. En reprenant le raisonnement de la première question et en utilisant le fait que les $C_i$ sont de longeurs deux à deux distinctes on voit que $\tau C_i \tau^{-1} = C_i$ pour tout $i$. Fixons $i$ ; si $C_i = (a_1 \dots a_{\ell_i})$ il existe $t_i$ compris entre 1 et $\ell_i$ tel que $\tau(a_k) = a_{[t_i+k]}$ pour tout $k$ (voir le traitement de la question (a), nous reprenons les notations que nous avons introduites à cette occasion) ; la restriction de $\tau$ au support de $C_i$ coïncide alors avec $C_i^{t_i}$. Par ailleurs le complémentaire de $\coprod \mathrm{Supp}(C_i)$ comprend au plus un point (en vertu de l'hypothèse (iii)), qui est le cas échéant nécessairement fixe par $\tau$. Il s'ensuit que $\tau$ est le produit des $C_i^{t_i}$, qui sont tous des permutations paires car chaque $C_i$ est de longueur impaire d'après l'hypothèse (i).

(c) Commençons par une remarque générale. Soit $\tau$ appartenant à $C$ et soit $H$ le commutant de $\tau$ dans $S_n$. L'orbite de $\tau$ sous l'action de $S_n$ par conjugaison est $C$, qui a donc pour cardinal $n!/|H|$ ; quant à l'orbite de $\tau$ sous l'action de $A_n$ par conjugaison, elle est contenue dans $C$ et son cardinal est $|A_n|/|H \cap A_n| = n!/(2|H \cap A_n|)$.

Supposons que (i), (ii) et (iii) soient satisfaites. Dans ce cas pour tout $\tau \in C$ de commutant $H$ dans $S_n$ on a $H \subset A_n$ (car $\tau$ a le même type de décomposition que $\sigma$, puisqu'il appartient à $C$). Par conséquent la classe de conjugaison de $\tau$ dans $A_n$ a pour cardinal $n!/(2|H|) = |C|/2$. Comme ceci vaut pour tout élément $\tau$ de $C$, on voit que celle-ci est réunion de deux classes de conjugaison de $A_n$, chacune de cardinal $|C|/2$.

Supposons que (i), (ii) et (iii) ne sont pas satisfaites. Dans ce cas $G$ n'est pas contenu dans $A_n$. La signature induit par conséquent un morphisme surjectif de $G$ vers $\{-1, 1\}$, de noyau $G \cap A_n$. Ce dernier est donc d'indice 2 dans $G$, si bien que

$$\frac{n!}{2|G \cap A_n|} = \frac{n!}{2\frac{|G|}{2}} = \frac{n!}{|G|} = |C|.$$

Ainsi la classe de conjugaison dans $A_n$ de $\sigma$ est de cardinal $|C|$, et est donc égale à $C$ toute entière, ce qui achève la démonstration.

**Exercice 3.**

(a) Soit $g \in G$, et soit $\iota_g$ l'automorphisme intérieur correspondant. Soit $\varphi$ un automorphisme de $G$. On a pour tout $h \in G$ les égalités

$$\begin{aligned}(\varphi \circ \iota_g \circ \varphi^{-1})(h) &= \varphi(\iota_g(\varphi^{-1}(h))) \\ &= \varphi(g\varphi^{-1}(h)g^{-1}) \\ &= \varphi(g)h\varphi(g)^{-1} \\ &= \iota_{\varphi(g)}(h).\end{aligned}$$

Par conséquent $\varphi \circ \iota_g \circ \varphi^{-1} = \iota_{\varphi(g)}$ ; le sous-groupe $\mathrm{Int}(G)$ de $\mathrm{Aut}(G)$ est donc stable par conjugaison dans $\mathrm{Aut}(G)$, c'est-à-dire distingué.

(b) Soit $s$ une section de $p$. On lui associe d'après le cours le morphisme de $Q$ dans $\mathrm{Aut}(G)$ défini par la formule

$$q \mapsto [g \mapsto u^{-1}(s(q)u(g)s(q)^{-1})].$$

Faisons deux commentaires :

- ◇ comme $u$ est injective elle induit un isomorphisme de $G$ sur $u(G)$ ; c'est sa réciproque que nous notons $u^{-1}$ ;
- ◇ comme $u(G) = \mathrm{Ker}(p)$ il est distingué dans $\Gamma$ ; pour tout $g \in G$ l'élément $s(q)u(g)s(q)^{-1}$ appartient donc bien à $u(G)$ et il est dès lors licite de lui appliquer $u^{-1}$.

(c) Soit $q$ un élément de $Q$. Choisissons un antécédent $\gamma$ arbitraire de $q$ dans $\Gamma$. Notons $a_\gamma$ l'automorphisme $g \mapsto u^{-1}(\gamma u(g)\gamma^{-1})$ de $G$ (cette formule a un sens pour les mêmes raisons que celles citées ci-dessus). Nous allons vérifier que sa classe $\pi(a_\gamma)$ dans $\mathrm{Out}(G)$ ne dépend que de $q$, et pas de $\gamma$. Soit donc $\delta$ un autre antécédent de $q$. Comme $p(\delta) = p(\gamma)$ on a $\delta\gamma^{-1} \in \mathrm{Ker}(p) = u(G)$ ; il existe donc $h \in G$ tel que $\delta = u(h)\gamma$. On a alors pour tout $g \in G$ les égalités

$$\begin{aligned}a_\delta(g) &= u^{-1}(\delta u(g)\delta^{-1}) \\ &= u^{-1}(u(h)\gamma u(g)\gamma^{-1}u(h^{-1})) \\ &= hu^{-1}(\gamma u(g)\gamma^{-1})h^{-1} \\ &= \iota_h(a_\gamma(g)).\end{aligned}$$

On a donc $a_\delta = \iota_h \circ a_\gamma$, si bien que $a_\delta$ et $a_\gamma$ ont même classe dans $\mathrm{Out}(G)$, comme annoncé.

On a donc construit pour tout élément $q$ de $Q$ un automorphisme extérieur $b_q$ de $G$ caractérisé par le fait que $b_q = \pi(a_\gamma)$ pour tout antécédent $\gamma$ de $q$ dans $\Gamma$. L'application $q \mapsto b_q$ est un morphisme de groupes de $Q$ dans $\mathrm{Out}(G)$. En effet, soient $q_1$ et $q_2$ deux éléments de $Q$ ; choisissons un antécédent $\gamma_1$ de $q_1$ et un antécédent $\gamma_2$ de $q_2$. Le produit $\gamma_1\gamma_2$ est alors un antécédent de $q_1q_2$. Pour tout élément $g$ de $G$ on a

$$\begin{aligned}a_{\gamma_1\gamma_2}(g) &= u^{-1}(\gamma_1\gamma_2 u(g)\gamma_2^{-1}\gamma_1^{-1}) \\ &= u^{-1}(\gamma_1 u(u^{-1}(\gamma_2 u(g)\gamma_2^{-1}))\gamma_1^{-1}) \\ &= u^{-1}(\gamma_1 u(a_{\gamma_2}(g))\gamma_1^{-1}) \\ &= a_{\gamma_1}(a_{\gamma_2}(g)).\end{aligned}$$

Par conséquent $a_{\gamma_1\gamma_2} = a_{\gamma_1} \circ a_{\gamma_2}$. En appliquant $\pi$ on obtient l'égalité $b_{q_1q_2} = b_{q_1} \circ b_{q_2}$ ce qu'il fallait démontrer (par abus, on note encore $\circ$ la loi interne de $\mathrm{Out}(G)$).

Si $p$ possède une section $s$ alors $s(q)$ est pour tout $q$ un antécédent de $q$ et on a donc $b_q = \pi(a_{s(q)}) = \pi(\varphi_s(q))$.

(d) Si $G$ est abélien alors $\mathrm{Int}(G) = \{\mathrm{Id}\}$ et $\mathrm{Out}(G)$ s'identifie donc à $\mathrm{Aut}(G)$. L' «action extérieure» $Q \to \mathrm{Out}(G)$ que nous avons construite est dans ce cas une vraie action $Q \to \mathrm{Aut}(G)$, même si $p$ n'a pas de section (et si $p$ a une section $s$ on retrouve l'action induite par $s$, qui ne dépend donc pas de $s$ – on a vu un exemple de ce phénomène lorsqu'on a étudié le groupe affine en cours).

Terminons cet extercie par une remarque : pour alléger les notations, on pouvait également dire dès le début «on identifie $G$ *via* $u$ à un sous-groupe de $\Gamma$». Dans ce cas, les formules obtenues sont nettement plus simple. Le morphisme $\varphi_s$ de $Q$ dans $\mathrm{Aut}(G)$ devient $g \mapsto s(q)gs(q)^{-1}$, et le morphisme $a_\gamma$ devient $g \mapsto \gamma g\gamma^{-1}$.

**Exercice 4.**

(a) Comme $i\colon a \mapsto (a, \overline{0})$ est un morphisme injectif de $\mathbf{Z}/m\mathbf{Z}$ dans $D$, il préserve l'ordre. L'ordre d'un élément $(a, 0)$ de $D$ est donc l'ordre de $a$ dans $\mathbf{Z}/m\mathbf{Z}$ (si $a = \overline{z}$, c'est donc $m/(\mathrm{PGCD}(m, z))$ ; puisque $m$ est impair, cet ordre est impair.

Déterminons maintenant l'ordre d'un élément de $D$ de la forme $(a, 1)$. On remarque que

$$(a, 1) \cdot (a, 1) = (a - a, 0) = (0, 0).$$

Ainsi $(a, 1)$ est de 2-torsion et comme il n'est pas égal au neutre $(0, 0)$ il est d'ordre 2.

(b) Soit $u$ un automorphisme de $D$. Posons $H = i(\mathbf{Z}/m\mathbf{Z}) = \mathbf{Z}/m\mathbf{Z} \times \{0\}$ ; comme $i$ est injectif il induit un isomorphisme de $\mathbf{Z}/m\mathbf{Z}$ sur $H$ dont on note $i^{-1}$ la réciproque Par la question (a), $H$ est l'ensemble des éléments d'ordre impair de $D$. Comme un automorphisme préserve l'ordre, $H$ est stable sous tout automorphisme $u$ de $D$ ; un tel automorphisme $u$ induit donc par restriction un automorphisme $r(u)$ de $H$, et $u \mapsto r(u)$ est un morphisme de $\mathrm{Aut}(D)$ dans $\mathrm{Aut}(H)$. L'application $u \mapsto i^{-1} \circ r(u) \circ i$ est alors un morphisme de $\mathrm{Aut}(D)$ dans $\mathrm{Aut}(\mathbf{Z}/m\mathbf{Z})$. Or on sait d'après le cours que $\alpha \mapsto (a \mapsto \alpha a)$ définit un isomorphisme de $(\mathbf{Z}/m\mathbf{Z})^\times$ sur $\mathrm{Aut}(\mathbf{Z}/m\mathbf{Z})$. Par conséquent il existe un morphisme $\mu$ de $\mathrm{Aut}(D)$ dans $(\mathbf{Z}/m\mathbf{Z})^\times$ tel que $(i^{-1} \circ r(u) \circ i)(a) = \mu(u)a$ pour tout $u$ et tout $a$, ce qui signifie exactement que $u(a, 0) = (\mu(u)a, 0)$.

Soit $\alpha \in (\mathbf{Z}/m\mathbf{Z})^\times$ et soit $s(\alpha)$ l'application de $D$ dans $D$ qui envoie $(a, b)$ sur $(\alpha a, b)$. On a pour tout couple $(a_1, b_1), (a_2, b_2)$ d'éléments de $D$

les égalités

$$\begin{aligned} s(\alpha)((a_1,b_1)\cdot(a_2,b_2)) &= s(\alpha)(a_1+(-1)^{b_1}a_2, b_1+b_2) \\ &= (\alpha a_1+(-1)^{b_1}\alpha a_2, b_1+b_2) \\ &= (\alpha a_1, b_1)\cdot(\alpha a_2, b_2) \\ &= s(\alpha)(a_1,b_1)\cdot s(\alpha)(a_2,b_2). \end{aligned}$$

Ainsi $s(\alpha)$ est un endomorphisme du groupe $D$. Il est immédiat que $s(\alpha_1\alpha_2) = s(\alpha_1)\circ s(\alpha_2)$, et que $s(1) = \mathrm{Id}$. On en déduit que $s(\alpha)$ est pour tout $\alpha$ un automorphisme de $D$ de réciproque $s(\alpha^{-1})$, puis que $s$ est un morphisme de groupes de $(\mathbf{Z}/m\mathbf{Z})^\times$ dans $\mathrm{Aut}(D)$. On a par construction $\lambda \circ s = \mathrm{Id}_{(\mathbf{Z}/m\mathbf{Z})^\times}$ ; ainsi $s$ est une section de $\lambda$. Son existence même entraîne la surjectivité de $\lambda$ (pour tout $\alpha$, l'automorphisme $s(\alpha)$ est un antécédent de $\alpha$ pour $\lambda$).

(c) Pour tout $u \in \mathrm{Aut}(D)$ l'élément $u(0,1)$ de $D$ est d'ordre 2, donc de la forme $(\lambda(u), 1)$, d'après (a). Nous allons montrer que l'application $\lambda$ induit un isomorphisme de $\mathrm{Ker}(\mu)$ sur $\mathbf{Z}/m\mathbf{Z}$. Vérifions pour commencer que $\lambda|_{\mathrm{Ker}((\mu)}$ est un morphisme. Soient donc $u$ et $v$ dans $\mathrm{Ker}(\mu)$. On a alors

$$\begin{aligned} (u\circ v)(0,1) &= u(\lambda(v),1) \\ &= u((\lambda(v),0)\cdot(0,1)) \\ &= u(\lambda(v),0)\cdot(\lambda(u),1) \\ &= (\lambda(v),0)\cdot(\lambda(u),1) \\ &= (\lambda(u)+\lambda(v),1) \end{aligned}$$

(l'avant-dernière égalité provient du fait que $u$ appartient à $\mathrm{Ker}(\mu)$, c'est-à-dire agit trivialement sur $H$). On a donc bien $\lambda(u\circ v) = \lambda(u)+\lambda(v)$.
Montrons que $\lambda|_{\mathrm{Ker}(\mu)}$ est injectif. Soit $u \in \mathrm{Ker}(\mu)$. On a alors pour tout $(a,b) \in D$ les égalités

$$\begin{aligned} u(a,b) &= u((a,0)\cdot(0,b) \\ &= (a,0)\cdot u(0,b) \end{aligned}$$

(la seconde provenant du fait que $u \in \mathrm{Ker}(\mu)$. On en déduit que $u(a,0) = (a,0$ pour tout $a$ et $u(a,1) = (a,0)\cdot(\lambda(u),1) = (a+\lambda(u),1)$. Ainsi $u$ est entièrement déterminé par $\lambda$, et $\lambda$ est en conséquence injectif.
Montrons que $\lambda$ est surjectif. Soit $u$ la conjugaison par $(1,0)$. Comme $(1,0)$ appartient à $H$ qui est abélien, l'automorphisme $u$ agit trivialement sur $H$ ; autrement dit, $u \in \mathrm{Ker}(\mu)$. On a par ailleurs les égalités

$$\begin{aligned} u(0,1) &= (1,0)\cdot(0,1)\cdot(-1,0) \\ &= (1,1)\cdot(-1,0) \\ &= (2,1). \end{aligned}$$

Par conséquent $\lambda(u) = 2 \in \mathbf{Z}/m\mathbf{Z}$. Mais comme $m$ est impair, 2 engendre $\mathbf{Z}/m\mathbf{Z}$. Par conséquent $\lambda|_{\mathrm{Ker}(\mu)}$ est surjectif.
Esquissons à titre indicatif une autre preuve de la surjectivité de $\lambda|_{\mathrm{Ker}(\mu)}$, qui demande moins de sens divinatoire. D'après les plus haut que s'il

existait $u$ dans $\mathrm{Ker}(\mu)$ tel que $\lambda(u) = 1$ on devrait avoir $u(a,0) = (a,0)$ et $u(a,1) = (a+1,1)$ pour tout $a$. L'idée est donc de vérifier que ces formules définissent bien un morphisme de groupes $u$ de $D$ dans $D$ , ce qui est un peu fastidieux mais sans difficulté. Il est ensuite immédiat que $u$ est bijectif, qu'il appartient à $\mathrm{Ker}(\mu)$ et que $\lambda(u) = 1$.

(d) Pour tout $x \in \mathbf{Z}/m\mathbf{Z}$, notons $u_x$ l'unique automorphisme appartenant à $\mathrm{Ker}(\mu)$ dont l'image par $\lambda$ vaut $x$. D'après les formules vues plus haut, on a $u_x(a,0) = (a,0)$ et $u_x(a,1) = (a+x,1)$ pour tout $a$.
On dispose d'une suite exacte

$$1 \longrightarrow \mathbf{Z}/m\mathbf{Z} \xrightarrow{x \mapsto u_x} \mathrm{Aut}(D) \xrightarrow{\lambda} (\mathbf{Z}/m\mathbf{Z})^\times \longrightarrow 1$$

et d'une section $s$ de $\lambda$. La formule

$$(x,\alpha) \mapsto u_x \circ s(\alpha) = (a,b) \mapsto \begin{cases} (\alpha a, 0) & \text{si } b = 0 \\ (\alpha a + x, 1) & \text{si } b = 1 \end{cases} .$$

induit alors un isomorphisme du produit semi-direct $\mathbf{Z}/m\mathbf{Z} \rtimes_\psi (\mathbf{Z}/m\mathbf{Z})^\times$ vers $\mathrm{Aut}(D)$, où $\psi$ est caractérisé par le fait que

$$s(\alpha) \circ u_x \circ s(\alpha^{-1}) = u_{\psi(\alpha)(x)}$$

pour tout $\alpha$ et tout $x$. En appliquant cette égalité de morphismes à $(0,1)$ il vient $(\alpha x, 1) = (\psi(\alpha)(x), 1)$ pour tout $\alpha$ et tout $x$. Ainsi $\psi$ envoie $\alpha$ sur la multiplication par $\alpha$ : c'est donc simplement l'isomorphisme canonique de $(\mathbf{Z}/m\mathbf{Z})^\times$ dans $\mathrm{Aut}(\mathbf{Z}/m\mathbf{Z})$.
Soit $(x,y)$ un élément de $D$ et soit $u$ la conjugaison par $(x,y)$. On a pour tout $(a,b) \in D$ les égalités

$$\begin{aligned} u(a,b) &= (x,y) \cdot (a,b) \cdot ((-1)^{y+1}x, y) \\ &= (x,y) \cdot (a + (-1)^{b+y+1}x, b+y) \\ &= ((-1)^y a + x(1 + (-1)^{b+1}), b). \end{aligned}$$

Ce dernier terme vaut $((-1)^y a, 0)$ si $b = 0$, et $((-1)^y a + 2x, 1)$ si $b = 1$. Par conséquent, $(x,y)$ est envoyé sur l'automorphisme de $D$ correspondant à l'élément $(2x, (-1)^y)$ de $\mathbf{Z}/m\mathbf{Z} \rtimes_\psi (\mathbf{Z}/m\mathbf{Z})^\times$.
Comme 2 est inversible modulo $m$ tout élément de $\mathbf{Z}/m\mathbf{Z}$ est de la forme $2x$ pour $x \in \mathbf{Z}/m\mathbf{Z}$. Le groupe des automorphismes intérieurs de $D$ s'identifie donc à $(\mathbf{Z}/m\mathbf{Z}) \rtimes_\psi \{-1, 1\} \subset \mathbf{Z}/m\mathbf{Z} \rtimes_\psi (\mathbf{Z}/m\mathbf{Z})^\times \simeq \mathrm{Aut}(D)$.