Devoir Surveillé n° 7 (4h)

Correction du problème 1 – Sur le nombre d'automorphismes d'un groupe fini
(d'après un article de Paul Lescot, en réponse à une question de Nicolas Tosel, RMS 2015)

Le but de ce problème est de montrer l'existence d'une fonction f de $\mathbb{N}$ dans $\mathbb{N}$ telle que pour tout groupe fini G, $|G| \leqslant f(|\mathrm{Aut}(G)|)$, où $\mathrm{Aut}(G)$ est le groupe des automorphismes de G, c'est-à-dire les morphismes bijectifs de G dans G.

Lorsqu'il n'y a pas d'ambiguïté, on notera e au lieu de e_G.

Partie I – Facteurs directs

1. (a) Soit $p : H \times K \to G$ définie par $p(h,k) = hk$.
   - p est un morphisme. En effet, pour tous (h,k) et (h',k') dans $H \times K$,
   $$p((h,k)(h',k')) = p(hh',kk') = hh'kk' = hkh'k',$$
   puisque G est abélien. Ainsi, $p((h,k)(h',k')) = p(h,k)p(h',k')$
   - p est surjective du fait que $HK = G$
   - Soit $(h,k) \in \mathrm{Ker}(p)$. On a alors $hk = e_G$, donc $h = k^{-1} \in H \cap K = \{e_G\}$. On en déduit que $(h,k) = e_{H\times K}$. Ainsi, le noyau de p est trivial, donc p est injective.

   On en déduit que p est un isomorphisme, donc que $\boxed{H \text{ est un facteur direct de } G}$ (et K aussi).

   (b) Soit G un groupe abélien et H un sous-groupe de G. On suppose qu'il existe un morphisme $p : G \to H$ tel que $p_{|H} = \mathrm{id}_H$.
   - Soit $g \in H \cap \mathrm{Ker}(p)$. On a alors $p(g) = \mathrm{id}(g) = g$, car $g \in G$, et $p(g) = e$ car $g \in \mathrm{Ker}(p)$. Ainsi, $g = e$. On en déduit que $H \cap \mathrm{Ker}(p) = \{e\}$
   - Soit $g \in G$. Alors $g = gp(g)^{-1}p(g)$. Or,
   $$p(gp(g)^{-1}) = p(g)p(p(g)^{-1}),$$
   mais puisuqe $p(g)$ et donc aussi $p(g)^{-1}$ sont dans H, $p(p(g)^{-1}) = p(g)^{-1}$, d'où $p(gp(g)^{-1}) = e$. Par conséquent, g est le produit d'un élément de $\mathrm{Ker}(p)$ et d'un élément de $\mathrm{Im}(p) = H$. On a bien $G = H\,\mathrm{Ker}(p)$.

   Ainsi, $\boxed{H \text{ est un facteur direct de } G}$

2. Soit G un groupe quelconque et H et K deux sous-groupes distingués de G tels que $H \cap K = \{e_G\}$ et $HK = G$.

   (a) Soit $h \in H$ et $k \in K$. Puisque H est distingué, il existe $h' \in H$ tel que $khk^{-1} = h'$. Il existe alors $k' \in K$ tel que $k' = h^{-1}kh = h^{-1}h'k$, car K est distingué. On en déduit que $h^{-1}h' = k'k^{-1} \in H \cap K$, donc $h^{-1}h' = e$ et $k'k^{-1} = e$, d'où $h = h'$ et $k = k'$. On en déduit que $\boxed{hk = kh}$.

   (b) La preuve de la question 1(a) s'adapte bien. On utilise la commutation des éléments de H et de K prouvée dabns la question précédente. pour justifier que p est un morphisme ; les autres points ne nécessitent pas d'hypothèse de commutation. Ainsi, $\boxed{H \text{ est un facteur direct de } G}$.

Partie II – Le cas abélien

Dans cette partie, on prouve le résultat annoncé dans le cas où G est un groupe abélien, en commençant par le cas d'un p-groupe.

1. Soit p un nombre premier, et G un p-groupe abélien, d'ordre p^n, $n \in \mathbb{N}^*$. Soit ω l'exposant de G.

(a) Tout élément de G a un ordre divisant $|G|$, d'après le théorème de Lagrange. Ainsi, le ppcm de ces ordres divise aussi $|G|$. Comme G est un p-groupe, les diviseurs de $|G|$ sont des puissances de p. Ainsi, il existe $r \in \mathbb{N}$ tel que $\boxed{\omega = p^r}$.

(b) Soit x et y deux éléments d'ordre ω (on peut trouver de tels éléments en vertu du théorème rappelé sur l'exposant d'un groupe abélien). Les éléments x et y sont donc d'ordre maximal dans G. D'après le troisième point rappelé du théorème de structure des groupes abéliens finis, $< x >$ et $< y >$ sont des facteurs directs de G. On peut donc trouver deux sous-groupes H_1 et H_2 de G tels que $\boxed{G \cong < x > \times H_1}$ et $\boxed{G \cong < y > \times H_2}$. Les groupes H_1 et H_2 sont abéliens, et leur décomposition en produit de p-groupes cycliques est unique, d'après le théorème de structure. De plus, comme x et y sont de même ordre, $< x > \cong < y >$. Ainsi, si la décomposition de H_1 n'est pas la même que celle de H_2, cela contredit l'unicité de la décomposition en p-groupes cycliques de G. On en déduit que $\boxed{H_1 \cong H_2}$.

(c) On se donne un isomorphisme $\psi : H_1 \to H_2$, et on définit $\beta : (x^m, h_1) \mapsto (y^m, \psi(h_1))$ de $< x > \times H_1$ dans $< y > \times H_2$

- L'application β est bien définie. En effet, puisque x et y ont même ordre, $x^m = x^{m'}$ équivaut à $y^m = y^{m'}$.
- Il s'agit d'un morphisme. En effet, pour tout $(a, h_1) \in < x > \times H_1$ et $(a', h_1') \in < x > \times H_1$, en écrivant $a = x^m$ et $a' = x^{m'}$, il vient :

$$\beta((a, h_1)(a', h_1')) = \beta(x^{m+m'}, h_1 h_1') = y^{m+m'}\psi(h_1 h_1') = y^m \psi(h_1) y^{m'} \psi(h_1') = \beta(a, h_1)\beta(a', h_1').$$

- On peut définir de même l'application $\gamma :< y > \times H_2 \to < x > \times H_1$ par $\gamma((y^m, h_2)) = x^m \psi^{-1}(h_2)$. L'application γ est clairement la réciproque de β, d'où la bijectivité de β.

On en déduit que $\boxed{\beta \text{ est un isomorphisme}}$.

(d) Puisque $< x >$ et $< y >$ sont des facteurs directs de G, les produits $< x > \times H_1$ et $< y > \times H_2$ peuvent être vus comme des produits directs internes. Ainsi, $p_1 : (x^m, h_1) \mapsto x^m h_1$ et $p_2 : (y^m, h_2) \mapsto y^m h_2$ sont des isomorphismes entre $< x > \times H_1$ et G et entre $< y > \times H_2$ et G. On vérifie alors facilement que $\alpha = p_2 \circ \beta \circ p_1^{-1}$ est un isomorphisme (comme composée d'isomorphisme), donc un automorphisme de G, vérifiant $\boxed{\alpha(x) = y}$.

(e) Soit $f : x \mapsto x^{p^{r-1}}$ de G dans G. Soit x et y dans G. On a alors

$$f(xy) = (xy)^{p^{r-1}} = x^{p^{r-1}} y^{p^{r-1}} = f(x)f(y),$$

puisque G est abélien. Soit $\mathcal{O}$ l'ensemble des éléments d'ordre ω de G.

- Si $x \in \mathcal{O}$, x est d'ordre p^r, donc $x^{p^{r-1}} \neq e$. Ainsi, $x \notin \mathrm{Ker}(f)$.
- Si $x \in G \setminus \mathcal{O}$, alors $\mathrm{ord}(x)$ est un diviseur strict de p^r, donc un diviseur de p^{r-1}. On en déduit que $x^{p^{r-1}} = e$. Ainsi, $x \in \mathrm{Ker}(f)$.

On en déduit que $G \setminus \mathcal{O} = \mathrm{Ker}(f)$. Ainsi, $\boxed{G \setminus \mathcal{O} \text{ est un sous-groupe de } G}$.

(f) Il existe au moins un élément d'ordre ω, d'après le théorème sur l'exposant des groupes abéliens. Ainsi, l'ordre de $G \setminus \mathcal{O}$ est strictement plus petit que $|G|$ et divise $|G| = p^n$. On en déduit que $|G \setminus \mathcal{O}| \leqslant p^{n-1}$, puis que

$$\boxed{|\mathcal{O}| \geqslant p^n - p^{n-1} = p^{n-1}(p-1)}.$$

(g) Soit x un élément fixé de $\mathcal{O}$. Pour tout y de $\mathcal{O}$, il existe un automorphisme α de G tel que $\alpha(x) = y$, d'après 1(c). Ainsi, $\boxed{|\mathrm{Aut}(G)| \geqslant \mathcal{O} \geqslant p^{n-1}(p-1) = \varphi(p^n)}$.

2. Soit maintenant G un groupe abélien d'ordre $p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$.

(a) Le produit de p-groupes abéliens est un p-groupe abélien. Ainsi, en regroupant dans la décomposition de G en produit de p groupes cycliques les facteurs suivant la valeur de p, on trouve une décomposition de G en produit de q_i-groupes, les q_i étant des entiers premiers 2 à 2 distincts En d'autres termes, G est isomorphe à un produit $G_1 \times G_2 \times \cdots \times G_s$, où $|G_s| = q_i^{m_1}$. Mais alors

$$|G| = q_1^{m_1} \cdots q_s^{m_s}.$$

Par unicité de la décomposition en facteurs premiers de G, on en déduit que $r = s$, et que quitte à opérer une permutation des indices, pour tout $i \in [\![1, r]\!]$, $q_i = p_i$ et $m_i = n_i$.

On a bien prouvé l'existence de groupes abéliens $\boxed{G_i \text{ d'ordre } p_i^{\alpha_i}}$ tels que $\boxed{G \text{ soit isomorphe à } G_1 \times \cdots \times G_r}$.

(b) Quitte à composer par des isomorphismes, on peut supposer que $G = G_1 \times \cdots \times G_r$. On définit alors

$$\Phi : \mathrm{Aut}(G_1) \times \cdots \times \mathrm{Aut}(G_r) \longrightarrow \mathrm{Aut}(G)$$

de la façon suivant : l'automorphisme $f = \Phi(\varphi_1, \cdot, \varphi_r)$ est défini sur $g = (g_1, \ldots, g_r)$ par

$$f(g_1, \ldots, g_r) = (\varphi_1(g_1), \ldots, \varphi_r(g_r)).$$

- f est bien un automorphisme, le respect de $\times$ provenant du respect de $\times$ par chaque φ_i, et une réciproque étant donnée par $\Phi(\varphi_1^{-1}, \ldots, \varphi_r^{-1})$.
- Une vérification immédiate montre que Φ est un morphisme de groupe
- Si $\Phi(\varphi_1, \ldots, \varphi_r) = \mathrm{id}_G$, alors pour tout $(g_1, \ldots, g_r) \in G$, $(\varphi_1(g_1), \ldots, \varphi_r(g_r)) = (g_1, \ldots, g_r)$, donc $\varphi_1 = \mathrm{id}_{G_1}, \ldots, \varphi_r = \mathrm{id}_{G_r}$. Ainsi, le noyau de Φ est réduit à l'élément neutre, donc Φ est injective.

Puisque Φ est un morphisme injectif, son image est un $\boxed{\text{sous-groupe de } \mathrm{Aut}(G)}$ isomorphe au produit $\boxed{\mathrm{Aut}(G_1) \times \cdots \times \mathrm{Aut}(G_n)}$

(c) Ainsi,

$$|\mathrm{Aut}(G)| \geqslant |\mathrm{Aut}(G_1) \times \cdots \times \mathrm{Aut}(G_r)| = \prod_{i=1}^{r} |\mathrm{Aut}(G_i)| \geqslant \prod_{i=1}^{r} p_i^{n_1 - 1}(1 - p_i) = \prod_{i=1}^{r} \varphi(p_i^{n_i}).$$

La multiplicativité de φ rappelée dans l'énoncé nous permet alors de conclure que $\boxed{|\mathrm{Aut}(G)| \geqslant \varphi(|G|)}$.

3. (a) Soit $k \in \mathbb{N}$, $k \geqslant 2$, et $n \in \varphi^{-1}(\llbracket 2, k \rrbracket)$. Écrivons $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Alors,

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1).$$

Notamment, pour tout $i \in \llbracket 1, r \rrbracket$:

- $k \geqslant \varphi(n) \geqslant p_i - 1$, donc $\boxed{p_i \leqslant k + 1}$
- $k \geqslant \varphi(n) \geqslant p_i^{\alpha_i - 1} \geqslant 2^{\alpha_i - 1}$, donc $\boxed{\alpha_i \leqslant \log_2(k) + 1}$.

(b) Ainsi, pour tout $n \in \varphi^{-1}(\{k\}) \subset \varphi^{-1}(\llbracket 2, k \rrbracket)$, $n \leqslant \prod_{p \in \mathcal{P}, p \leqslant k+1} p^{\alpha}$, où $\alpha = \lfloor \log_2(k) + 1 \rfloor$.

On en déduit que $\boxed{\varphi^{-1}(\{k\}) \text{ est borné}}$.

(c) On définit $h(1) = 1$ (le groupe trivial n'a qu'un automorphisme) et pour tout $k \geqslant 2$, $h(k) = \max \varphi^{-1}([\llbracket 2, k \rrbracket)$. Cette fonction h est clairement croissante. De plus, pour tout groupe abélien fini G d'ordre n, si $|G| > h(|\mathrm{Aut}(G)|)$, alors $\varphi(|G|) > |\mathrm{Aut}(G)|$, par définition de h, ce qui contredit 2c. On en déduit que

$$\boxed{|G| \leqslant h(|\mathrm{Aut}(G)|)}.$$

Partie III – Groupe des homomorphismes de groupes abéliens

1. Soit φ et ψ des éléments de $\mathrm{Hom}(A, B)$. Alors, pour tout $(a, a') \in A^2$,

$$\varphi \times \psi(aa') = \varphi(aa')\psi(aa') = \varphi(a)\varphi(a')\psi(a)\psi(a') = \varphi(a)\psi(a)\varphi(a')\psi(a') = (\psi \times \psi(a))(\varphi \times \psi(a')).$$

Ainsi, $\boxed{\psi \times \psi \in \mathrm{Hom}(A, B).}$ On remraquera qu'on a utilisé la commutativité de $\times$ dans le groupe abélien B.

2. La loi $\times$ ainsi définie est clairement associative, du fait de l'associativité de celle de B. Elle est commutative, du fait de la commutativité de celle de B. Le morphisme $a \mapsto \mathrm{e}_B$ est un élément neutre.

Étant donné $\varphi \in \mathrm{Hom}(A, B)$, l'application ψ définie par $\psi(a) = \varphi(a)^{-1}$ est encore dans $\mathrm{Hom}(A, B)$. En effet, B étant abélien,

$$\psi(ab) = \varphi(ab)^{-1} = (\varphi(a)\varphi(b))^{-1} = \varphi(b)^{-1}\varphi(a)^{-1} = \psi(a)\psi(b).$$

On vérifie facilement que ψ est l'inverse de φ.

Ainsi, $\boxed{(\mathrm{Hom}(A, B), \times) \text{ est un groupe abélien}}$.

3. (a) Soit $f : A \to A'$ est un isomorphisme de groupes, et $\Phi : g \mapsto g \circ f$ de $\mathrm{Hom}(A', B)$ dans $\mathrm{Hom}(A, B)$.

- Soit g_1 et g_2 dans $\mathrm{Hom}(A', B)$. Alors, pour tout $a \in A$

$$\Phi(g_1 \times g_2)(a) = (g_1 \times g_2)(f(a)) = g_1(f(a))g_2(f(a)) = \Phi(g_1)(a)\Phi(g_2)(a).$$

  On a donc $\Phi(g_1 \times g_2) = \Phi(g_1) \times \Phi(g_2)$, donc Φ est un morphisme de groupe.
- L'application $h \mapsto h \circ f^{-1}$ de $\mathrm{Hom}(A', B)$ dans $\mathrm{Hom}(A, B)$ est clairement réciproque de Φ, donc Φ est bijective.

Ainsi, $\boxed{\Phi \text{ est un isomorphisme}}$.

(b) De même, étant donné $f : B \to B'$ un isomorphisme de B sur B', on considère $\Psi : \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, B')$ par $g \mapsto f \circ g$.
- Pour tout $a \in A$,

$$\Psi(g_1 \times g_2(a)) = f(g_1 \times g_2(a)) = f(g_1(a))f(g_2(a)) = \Psi(g_1)(a)\Psi(g_2)(a).$$

  Ainsi, $\Psi(g_1 \times g_2) = \Psi(g_1) \times \Psi(g_2)$, donc Ψ est un morphisme de groupes.
  Comme plus haut, on trouve une réciproque en considérant $g \mapsto f^{-1} \circ g$, ainsi, $\boxed{\Psi \text{ est un isomorphisme}}$.

4. Soit A, B et C trois groupes abéliens.

(a) Soit $\psi \in \mathrm{Hom}(A \times B, C)$, et $\psi_A : x \mapsto \psi(x, e_B)$. Soit a_1 et a_2 des éléments de A. Alors,

$$\psi_A(a_1a_2) = \psi(a_1a_2, e) = \psi((a_1, e)(a_2, e)) = \psi(a_1, e)\psi(a_2, e) = \psi_A(a_1)\psi_A(a_2).$$

(b) Soit $\Phi : \psi \mapsto (\psi_A, \psi_B)$. On remarque d'abord que si ψ_1 et ψ_2 sont dans $\mathrm{Hom}(A \times B, C)$, alors

$$(\psi_1)_A \times (\psi_2)_A(a) = \psi_1(a, e) \times \psi_2(a, e) = (\psi_1 \times \psi_2)_A(a).$$

Ainsi, on obtient de façon immédiate $\Phi(\psi_1 \times \psi_2) = \Phi(\psi_1) \times \Phi(\psi_2)$. par conséquent, Φ est un morphisme.
Par ailleurs, on vérifie sans peine que l'application $(\varphi, \psi) \mapsto \theta$ où $\varphi \in \mathrm{Hom}(A, C)$, $\psi \in \mathrm{Hom}(B, C)$ et θ définie par

$$\theta((a, b)) = (\varphi(a), \psi(b))$$

est une réciproque de Φ. Ainsi, Φ est un isomorphisme.

5. On définit l'isomorphisme par $\Psi : \varphi \mapsto (p_A \circ \varphi, p_B \circ \varphi)$, où p_A et p_B sont les projections de $A \times B$ sur A et B respectivement. Ces projections sont clairement des morphismes, d'où la bonne définition de Ψ. On montre comme dans la question précédente que c'est un isomorphisme. Cela ne présente aucune difficulté.

6. Soient m et n deux entiers naturels. On prendra garde dans cette question au fait que $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$ sont considérés additivement.

(a) On a $n\psi(1) = \psi(n) = 0$, donc $\boxed{\mathrm{ord}(\psi(n))|n}$.

(b) Puisque $\psi(1)$ est dans $\mathbb{Z}/m\mathbb{Z}$ d'ordre m, son ordre divise aussi m par le théorème de Lagrange. Ainsi, $\mathrm{ord}(x)$ est un diviseur de $n \wedge m$. Par conséquent, si x est un représentant dans $\mathbb{Z}$ de $\varphi(1)$, $m|(n \wedge m)x$, donc $\frac{m}{m \wedge n}|x$, donc $x \in \frac{m}{n \wedge m}\mathbb{Z}$. On en déduit que $\boxed{\psi(1) \in \left(\frac{m}{n \wedge m}\mathbb{Z}\right)/m\mathbb{Z}}$

(c) Soit $\Phi : \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \to \left(\frac{m}{n \wedge m}\mathbb{Z}\right)/m\mathbb{Z}$ définie par $\Phi(\varphi) = \varphi(1)$.
- Il s'agit clairement d'un morphisme (attention, ici, toutes les lois sont additives).
- Φ est injective. En effet, si $\Phi(\varphi_1) = \Phi(\varphi_2)$, $\varphi_1(1) = \varphi_2(1)$, puis, pour tout $k \in \mathbb{Z}/n\mathbb{Z}$, $\varphi_1(k) = k\varphi_1(1) = k\varphi_2(1) = \varphi_2(k)$.
- Φ est surjective. En effet, soit $a \in \left(\frac{m}{n \wedge m}\mathbb{Z}\right)/m\mathbb{Z}$, et b un représentant dans $\frac{m}{n \wedge m}\mathbb{Z}$ de a. L'application $x \mapsto bx$ de $\mathbb{Z}$ dans $\mathbb{Z}$ définit, par passage au quotient, une application de $\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$. De plus, si $x \equiv 0\ [n]$, $nx \in \frac{mn}{n \wedge m}\mathbb{Z} = (n \vee m)\mathbb{Z} \subset m\mathbb{Z}$. Ainsi, nx est nul modulo m. L'application $x \mapsto \overline{bx}$ passe donc au quotient et définit une application $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Par sa définition même, cette application est un morphisme, et $\Phi(\varphi) = a$.

On en déduit que Φ est un isomorphisme, et $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ est isomorphe à $\left(\frac{m}{n \wedge m}\mathbb{Z}\right)/m\mathbb{Z}$. De plus, comme $\frac{d\mathbb{Z}}{da\mathbb{Z}}$ est isomorphe à $\mathbb{Z}/a\mathbb{Z}$, on conclut que $\boxed{\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \text{ est isomorphe à } \mathbb{Z}/(n \wedge m)\mathbb{Z}}$.

7. La question précédente donne un résultat symétrique en n et m. On en déduit que $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ est isomorphe à $\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n)$. On utilise alors le théorème de structure et les questions 4 et 5 itérées) pour conclure : Soit A et B deux groupes abéliens, qu'on décompose en produit de groupes cycliques :

$$A = \prod_{i=1}^{r} A_i, \qquad B = \prod_{j=1}^{s} B_j,$$

les A_i et B_i étant cycliques. Les questions 4, 5 et 6c montrent alors que

$$\mathrm{Hom}(A,B) \cong \prod_{i=1}^{r}\prod_{j=1}^{s} \mathrm{Hom}(A_i,B_j) \cong \prod_{i=1}^{r}\prod_{j=1}^{s} \mathrm{Hom}(B_j,A_i) \cong \mathrm{Hom}(B,A).$$

Ainsi, $\boxed{\mathrm{Hom}(A,B) \text{ et } \mathrm{Hom}(B,A) \text{ sont isomorphes}}$.

8. Soit G un groupe abélien fini, et $G = G_1 \times \cdots \times G_r$ une décomposition de G en produit de groupes cycliques, en vertu du théorème de structure des groupes abéliens.

   (a) Puisque G_i est cyclique, disons isomorphe à un $\mathbb{Z}/n\mathbb{Z}$,

   $$\mathrm{Hom}(G_i,G_i) \cong \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/(n\wedge n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \cong \boxed{G_i}.$$

   (b) Si un groupe A est isomorphe par Φ à $B\times C$, alors l'image réciproque par Φ du sous-groupe $B\times\{e\}$ de $B\times C$ est un sous groupe de A isomorphe à B. Or,

   $$\mathrm{Hom}(G,G) \cong \prod_{1\leqslant i,j\leqslant r} \mathrm{Hom}(G_i,G_j) \cong \prod_{i=1}^{r} \mathrm{Hom}(G_i,G_i) \times \prod_{1\leqslant i\neq j\leqslant r} \mathrm{Hom}(G_i,G_j).$$

   Ainsi $\mathrm{Hom}(G,G)$ contient un sous-groupe isomorphe à $\boxed{\prod_{i=1}^{r} \mathrm{Hom}(G_i,G_i) = \mathrm{Hom}(G_1,G_1)\times\cdots\times\mathrm{Hom}(G_r,G_r)}$.

   (c) D'après 8a, $\mathrm{Hom}(G,G)$ contient donc un sous-groupe isomorphe à $G_1\times\cdots\times G_r \cong G$. D'après le théorème de Lagrange, il en découle que $\boxed{|G| \text{ divise } |\mathrm{Hom}(G,G)|}$.

9. Soit A et B deux groupes abéliens finis, C un sous-groupe de A et D un sous-groupe de B. On suppose que $C \cong B/D$.

   (a) Soit $\psi : B/D \to C$ un isomorphisme. Soit $f \in \mathrm{Hom}(B/D,C)$. On définit $\Phi(f) = i\circ f\circ\pi$, où π est la projection canonique de B sur B/D et i est le morphisme d'inclusion de C dans A. En tant que compsé de morphismes, $\Phi(f)$ est bien un élément de $\mathrm{Hom}(B,A)$. La définition du produit et le respect du produit par i montrent que Φ est lui-même un morphisme. Par ailleurs, si f n'est pas le morphisme trivial, il existe $\bar{b}$ dans B/D tel que $f(\bar{b}) \neq e$. Alors $\Phi(f)(b) = f(\bar{b}) \neq 1$. Par conséquent, le noyau de Φ est réduit au morphisme trivial.
   Ainsi, $\boxed{\Phi : \mathrm{Hom}\,(B/D,C) \to \mathrm{Hom}(B,A) \text{ est un morphisme injectif}}$.

   (b) L'image par Φ de $\mathrm{Hom}\,(B/D,C)$ est un sous-groupe de $\mathrm{Hom}(B,A)$ isomorphe à $\mathrm{Hom}\,(B/D,C)$ lui-même isomorphe à $\mathrm{Hom}\,(C,C)$. Or, $\mathrm{Hom}(B,A)$ est isomorphe à $\mathrm{Hom}(A,B)$. Ce dernier contient donc un sous groupe isomorphe à $\mathrm{Hom}(C,C)$. Le théorème de Lagrange permet de conclure que $|\mathrm{Hom}(C,C)|$ divise $|\mathrm{Hom}(A,B)|$. On utilise alors la question 8c pour conclure que $\boxed{|C| \text{ divise } |\mathrm{Hom}(A,B)|}$.

Partie IV – Autour du groupe dérivé

1. Soit $[a,b]$ un commutateur et $z \in G$:

   $$[a,b]z = a^{-1}b^{-1}abz = zz^{-1}a^{-1}zz^{-1}b^{-1}zz^{-1}azz^{-1}bz = z(z^{-1}az)^{-1}(z^{-1}bz)^{-1}(z^{-1}az)(z^{-1}bz) = [a,b]z = \boxed{z[a^z,b^z]}.$$

2. On remarque que l'inverse d'un commutateur est encore un commutateur. Ainsi, le groupe engendré par les commutateurs est l'ensemble de tous les produits qu'on peut former avec des commutateurs. Soit $x \in G'$. Il existe donc $c_1,\ldots,c_n$ des commutateurs tels que

   $$x = c_1\ldots c_n.$$

   Alors, d'après la question précédente, pour $z \in G$:

   $$x^z = (c_1\ldots c_n)^z = c_1^z\ldots c_n^z = c_1'\ldots c_i',$$

   où, pour tout $c_i = [a_i,b_i]$, $c_i' = [a_i^z,b_i^z]$. Ainsi $x^z \in G'$, donc $\boxed{G' \text{ est distingué dans } G}$.
   Soit $\bar{g}$ et $\bar{h}$ deux éléments de G/G'. Puisque $g^{-1}h^{-1}gh \in G'$, $\overline{g^{-1}h^{-1}gh} = e$, donc $\bar{g}\bar{h} = \bar{h}\bar{g}$. Ainsi, $\boxed{G/G' \text{ est abélien}}$.

3. (a) Soit a, b, c, d des éléments de G tels que $\bar{a} = \bar{c}$ et $\bar{b} = \bar{d}$ dans le quotient $G/Z(G)$. On a alors $c = aZ(G)$ et $d = bZ(G)$, donc il existe z_1 et z_2 tels que $c = az_1$ et $d = bz_2$. On a alors

$$[c, d] = z_1^{-1}a^{-1}z_2^{-1}b^{-1}az_1bz_2 = z_1^{-1}z_2^{-1}z_2a^{-1}b^{-1}ab = [a, b],$$

puisque z_1 et z_2 (et donc leurs inverses) sont dans le centre de G, donc commutent avec tout élément de G.

(b) Les couples $[a, b]$ et $[c, d]$ définissent des commutateurs distincts si et seulement si les couples $(\bar{a}, \bar{b})$ et $(\bar{c}, \bar{d})$ sont distincts dans $(G/Z(G))^2$. Ainsi, il y a au plus autant de commutateurs distincts que de couples dans $(G/Z(G))^2$. Il y a donc au plus $\boxed{m^2 \text{ commutateurs distincts}}$.

4. Soit $x \in G'$. Ainsi, x peut s'écrire comme un produit fini de commutateur (en vertu de la remarque faite précédemment, les inverses de commutateurs étant aussi des commutateurs). On considère désormais un produit en un nombre *minimal* n de commutateurs :

$$x = c_1 \cdots c_n.$$

On veut montrer que $n \leqslant m^3$. Pour cela, on raisonne par l'absurde, en supposant que $n \geqslant m^3 + 1$. Le but des questions suivantes est de trouver une contradiction sur la minimalité de n, autrement dit, de réussir à écrire x comme produit d'un nombre plus petit de commutateur.

(a) Puisqu'un il a au plus m^2 commutateurs distincts, si tous les commutateurs apparaissaient au plus m fois dans le produit $c_1 \cdots c_n$, le nombre de termes de ce produit serait au plus égal à $m^2 \times m$, ce qui contredit $n \geqslant m^3 + 1$.
Ainsi, $\boxed{\text{il existe un commutateur } c \text{ apparaissant au moins } m+1 \text{ parmi les } c_i}$.

(b) D'après la question 1, en prenant $z = c$, on peut permuter le premier des facteurs c avec chacun des commutateurs qui le précède. Le commutateur qu'on permute avec c est modifié en un autre commutateur, mais c est préservé. On peut ainsi ramener ce facteur c tout au début du produit. On fait ensuite la même chose avec le second facteur c, en le ramenant en deuxième position, etc. De la sorte, on ramène les $m+1$ premiers facteurs c (il peut y en avoir d'autres) en tête de produit. Cela change la valeur des autres commutateurs, mais par leur nombre. Ainsi, il existe des commutateurs $c'_1, \ldots, c'_{n-m-1}$ tels que

$$\boxed{x = c^{m+1}c'_1 \cdots c'_{n-m-1}}.$$

(c) Soit u et v tels que $c = [u, v]$. On a alors

$$\begin{aligned}(u^{-1}cu)^{m-1}[u^2, v] &= u^{-1}c^{m-1}uu^{-2}v^{-1}u^2v = u^{-1}c^{m-1}u^{-1}v^{-1}u^2v \\ &= u^{-1}c^mc^{-1}u^{-1}v^{-1}u^2v = u^{-1}c^mv^{-1}u^{-1}vuu^{-1}v^{-1}u^2v \\ &= u^{-1}c^mv^{-1}uv\end{aligned}$$

Or, $G/Z(G)$ est d'ordre m, donc, d'après le théorème de Lagrange, $\bar{c}$ est d'ordre m, soit $\overline{c^m} = \bar{e}$, ce qui équivaut à $c^m \in Z(G)$. Par conséquent, $u^{-1}c^m = c^mu^{-1}$, donc :

$$(u^{-1}cu)^{m-1}[u^2, v] = c^mu^{-1}v^{-1}uv = c^{m+1}.$$

(d) Or, $u^{-1}cu = c^u$ est un commutateur. Ainsi, c^{m+1} s'écrit comme produit de m commutateurs, puis, en remplaçant dans 4b, le terme c^{m+1} par ce produit, on exprime x comme produit de $n-1$ commutateurs.
Cela contredit la minimalité de n, donc l'hypothèse initiale $n \geqslant n^3 + 1$ est erronée. On en déduit que $\boxed{n \leqslant m^3}$.

5. Tout x de G' s'écrit donc comme produit d'au plus n commutateurs, et même d'exactement m^3 commutateurs (puisqu'on peut compléter en multipliant autant de fois que nécessaire par $[e, e] = e$). Ainsi, il y a au plus autant d'éléments dans G' que de choix possibles de n commutateurs. Comme il y a au plus m^2 commutateurs distincts, cela fait au plus $(m^2)^{m^3}$ choix possibles. Ainsi, $\boxed{|G'| \leqslant m^{2m^3}}$.

Partie V – Étude d'un endomorphisme de G

1. Soit p un nombre premier et $G = \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_\ell}\mathbb{Z}$. Soit $y \in G$ un élément d'ordre p^{k+1} ($k \in \mathbb{N}$), tel qu'il n'existe pas d'élément $x \in G$ et d'entier $k' > k$ vérifiant $y^{p^k} = x^{p^{k'}}$. On note $y = (y_1, \ldots, y_\ell)$ la décomposition de y dans la somme directe décrivant G.

   (a) Puisque y est d'ordre p^{k+1}, $p^{k+1}y = 0$, c'est-à-dire

   $$(p^{k+1}y_1, \ldots, p^{k+1}y_k) = (0, \ldots, 0)$$

   (notez ici le passage en notation additive !). On en déduit que pour tout $i \in [\![1, \ell]\!]$, $p^{k+1}y_i = 0$ dans $\mathbb{Z}/p^{n_i}\mathbb{Z}$, donc que $\mathrm{ord}(y_i) | p^{k+1}$. Par conséquent, il existe $\boxed{s_i \leqslant k+1 \text{ tel que } y_i \text{ est d'ordre } p^{s_i}}$.

   (b) Soit $I = \{i \in [\![1, k]\!] \text{ tel que } s_i = k+1\}$. Supposons que pour tout $i \in I$, $< y_i > \neq \mathbb{Z}/p^{n_i}\mathbb{Z}$. Soient $\tilde{y_i}$ des représentants dans $\mathbb{Z}$ des y_i. Puisque y_i n'engendre pas $\mathbb{Z}/p^{n_i}\mathbb{Z}$, $\tilde{y_i}$ n'est pas premier avec p^{n_i} (en effet, sinon, d'après le théorème de Bézout, il serait inversible, donc il existerait z tel que $y_i z = 1$; en notant n un représentant de z dans $\mathbb{Z}$, $ny_i = 1$; comme 1 engendre $\mathbb{Z}/p^{n_i}\mathbb{Z}$, on en déduit alors que y_i aussi).

   Ainsi, p divise $\tilde{y_i}$. Considérons alors $x = (x_1, \ldots, x_\ell)$ où x_i est nul pour tout $i \notin I$, et $x_i = \overline{\left(\frac{y_i}{p}\right)}$ si $i \in I$. On a alors
   - pour tout $i \in I$, $p^{k+1}x_i = p^k y_i$
   - pour tout $i \notin I$, $p^{k+1}x_i = 0 = p^k y_i$ (car dans ce cas, y_i est d'ordre strictement inférieur à p^{k+1} et divisant p^{n_i}, donc d'ordre au plus p^k).

   On a donc trouvé x tel que $p^{k+1}x = p^k y$. Cela contredit les hypothèses. Par conséquent, il existe $i \in I$ tel que $\boxed{< y_i >= \mathbb{Z}/p^{n_i}\mathbb{Z}}$ (et donc $k+1 = n_i$).

   (c) L'entier $\tilde{y_i}$ est alors inversible (multiplicativement) modulo n_i (puisque la classe de 1 est dans le groupe qu'il engendre). Soit a son inverse modulo n_i. Considérons alors $p : G \longrightarrow < y >$ défini par $p(x_1, \ldots, x_\ell) = ax_i v$. Il s'agit de façon évidente d'un morphisme de groupes, et pour tout $z \in < y >$, $z = my$, on a

   $$p(z) = az_i v = amy_i v = mv,$$

   puisque par définition de a, $ay_i = 1$. On en déduit que $p_{|<v>} = \mathrm{id}_{<v>}$. La question I-1b permet de conclure que $\boxed{< v > \text{ est un facteur direct de } G}$.

2. Soit G un groupe multiplicatif fini quelconque, et $\varphi \in \mathrm{Hom}(G, Z(G))$. On définit $\alpha : G \to G$ par $\alpha(g) = g\varphi(g)$.

   (a) Soit $c = [u, v]$ un commutateur. On a alors

   $$\varphi(c) = \varphi(u^{-1}v^{-1}uv) = \varphi(u)^{-1}\varphi(v)^{-1}\varphi(u)\varphi(v) = \varphi(u)^{-1}\varphi(u)\varphi(v^{-1})\varphi(v) = e_G,$$

   du fait que $\varphi(u) \in Z(G)$. On en déduit que tout produit de commutateurs est aussi envoyé sur e_G par φ, donc, $\boxed{\text{pour tout } g \in G',\ \varphi(g) = e_G}$.

   (b) Soit g et h des éléments de G. On a alors :

   $$\alpha(g)\alpha(h) = g\varphi(g)h\varphi(h) = gh\varphi(g)\varphi(h) = gh\varphi(gh) = \alpha(gh),$$

   toujours du fait que $\varphi(g) \in Z(G)$. Ainsi, $\boxed{\alpha \in \mathrm{Hom}(G, G).}$

3. Avec les notations de la question précédente, on montre dans cette question que si α n'est pas injective, alors G possède un facteur direct abélien non trivial. On suppose donc α non injective, et on considère un élément x d'ordre premier p dans $\mathrm{Ker}(\alpha)$. On note qu'on peut trouver un tel élément, quitte à prendre une puissance $\frac{n}{p}$-ième d'un élément non trivial, d'ordre n divisible par p. On note $k \in \mathbb{N}$ l'entier maximal tel que la classe $\bar{x}$ de x dans G/G' est une puissance p^k-ième, et on se donne $a \in G$ tel que $\bar{x} = \bar{a}^{p^k}$. Ainsi, il n'existe pas de b dans G et $\ell > k$ tel que $\bar{x} = \bar{b}^{p^\ell}$. On note enfin $y = \varphi(a)$.

   (a) Puisque $x \in \mathrm{Ker}(\alpha)$, $x\varphi(x) = e$, donc

   $$\bar{x}\varphi(\bar{a}^{p^k}) = e, \qquad \text{puis:} \qquad \bar{y}^{p^k} = \bar{x}^{-1} \qquad \text{puis:} \qquad \bar{y}^{p^{k+1}} = x^{-p} = e,$$

   puisque x est d'ordre p. Ainsi, $\mathrm{ord}(\bar{y})$ divise p^{k+1}.
   On peut remarquer par ailleurs que $x \notin G'$, sinon $\varphi(x) = e_G$, puis $\alpha(x) = x$. Comme x est supposé d'ordre p, il est différent de e, ce qui contredit le fait que $x \in \mathrm{Ker}(\alpha)$. Ainsi, puisque $x \notin G'$, $\bar{x} \neq \bar{e}$, et $\bar{x}^{-1} \neq \bar{e}$. On en déduit que $\mathrm{ord}\bar{y}$ ne divise pas p^k

Des deux points précédents, il découle que $\boxed{\text{ord}(\bar{y}) = p^{k+1}}$.

Puisque $\bar{a}^{p^k} = \bar{x}$, il existe $z \in G'$ tel que $a^{p^k} = xz$. On a alors

$$y^{p^k} = \varphi(a)^{p^k} = \varphi(a^{p^k}) = \varphi(xz) = \varphi(x)\varphi(z).$$

Mais comme $z \in G'$, $\varphi(z) = e$, donc

$$y^{p^k} = \varphi(x) = x^{-1} \neq e \qquad \text{puis:} \qquad y^{p^{k_1}} = x^{-p} = e.$$

Ainsi, $\boxed{\text{ord}(y) = p^{k+1}}$.

(b) Puisque G/G' est un groupe abélien, on peut lui appliquer le théorème de structure et séparer d'un côté les p-groupes cycliques, de l'autre côté tous les autres, d'ordre premier avec p. Ainsi, G/G' est isomorphe au premoduit direct (externe) d'un p-groupe et d'un groupe d'ordre premier avec p. Comme on l'a déjà justifié plus haut, il existe dans G des sous-groupes isomorphes aux deux facteurs de ce produit cartésien tels que G soit le $\boxed{\text{produit direct interne}}$ de ces deux groupes, l'un d'eux étant un $\boxed{p\text{-groupe}}$, l'autre étant $\boxed{\text{d'ordre premier avec } p}$.

(c) Puisque $\bar{y} \in G/G'$, et puisque $G/G' = AB$, on peut écrire $\bar{y} = ab$, pour $a \in A$ et $b \in B$. Puisque $\bar{y}$ est d'ordre p^{k+1}, $a^{p^{k+1}} = b^{-p^{k+1}} \in A \cap B$. Mais d'après I-2, $A \cap B = \{e\}$, donc $a^{p^{k+1}} = b^{-p^{k+1}} = e$. En particulier, l'ordre de b divise p^{k+1}. Mais il divise aussi $|B|$ qui est premier avec p. Ainsi, $\text{ord}(b) = 1$, et $b = e$. On en déduit que $\boxed{\bar{y} = a \in A}$.

L'élément $\bar{y}$ de A vérifie les hypothèses de la question 1 (A étant isomorphe à un groupe G tel que dans cette question). En effet, $\bar{y}^{-p^k} = \bar{x}$ ne peut, par définition de k, pas s'écrire comme puissance d'ordre plus élevé que k, donc $\bar{y}^{p^k}$ non plus. Ainsi, d'après la question 1, $\boxed{< y > \text{ est un facteur direct de } A}$.

On note C un sous-groupe de A tel que A soit le produit direct interne de $< \bar{y} >$ et de C.

(d) Soit $\pi : G \mapsto G/G'$ la projection canonique définie par $\pi(g) = \bar{g}$.

- Soit $g \in G$ et $c \in \pi^{-1}(C)$. On a alors :

$$\pi(gcg^{-1}) = \pi(g)\pi(c)\pi(g^{-1}) = \pi(g)\pi(g^{-1})\pi(c) = \pi(c).$$

En effet, π est à valeurs dans G/G' qui est abélien. Ainsi, puisque par définition de c, $\pi(c) \in C$, on a $\pi(gcg^{-1}) \in C$, donc $gcg^{-1} \in \pi^{-1}(C)$. Ainsi, $\boxed{\pi^{-1}(C) \text{ est distingué dans } G.}$

- Le même raisonnement montre que $\boxed{\pi^{-1}(B) \text{ est distingué dans } G}$.
- Puisque φ est à valeurs dans $\mathbb{Z}$ et $y = \varphi(a)$, $y \in Z(G)$, donc tout $y^k \in Z(G)$. On en déduit que pour tout élément de $< y >$, qu'on peut écrire y^k, et pour tout $g \in G$,

$$gy^k g^{-1} = gg^{-1}y^k = y^k \in < y > .$$

Ainsi, $\boxed{< y > \text{ est un sous-groupe distingué de } G}$.

(e) Soit $g \in G$. Ainsi, $\pi(G)$ est dans G/G', qui est le produit direct de $< \bar{y} >$, C et B. On peut donc trouver $m \in \mathbb{Z}$, $c \in C$ et $b \in B$ tels que

$$\pi(g) = \bar{y}^m cb = \pi(y^m)cb.$$

Soit r un antécédant par π (qui est surjective) de $b^{-1} \in B$. On a alors $r \in \pi^{-1}(B)$, et

$$c = \pi(y^{-m})\pi(g)\pi(r^1) = \pi(y^{-m}gr).$$

Puisque $c \in C$, on a bien $\boxed{\pi(y^{-m}gr) \in C}$.

(f) On a alors, pour tout $g \in G$, $g = y^m(y^{-m}gr)r^{-1}$. Or, $y^{-m}gr \in \pi^{-1}(C)$ d'après la question précédente, et $r^{-1} \in \pi^{-1}(B)$. Donc $(y^{-m}gr)r^{-1} \in \pi^{-1}(C)\pi^{-1}(B) = H$, puis $g \in < y > H$.

Ainsi, $G \subset < y > H$, et l'inclusion réciproque étant évidente, $\boxed{G = < y > H}$.

(g) Soit $z \in < y > \cap H$. Il existe m tel que $z = y^m$, et $z \in H$. On a alors $\pi(z) = \bar{y}^m$ et $\pi(z) \in CB$. Or, d'après la question I-2 (ou ici I-1(a) car on est dans le cas abélien), $< \bar{y} > \cap CB = \{\bar{e}\}$, donc $\bar{y}^m = \bar{e}$. Ainsi, $\text{ord}(y) = p^{k+1} | m$. Mais $\text{ord}(y) = \text{ord}(\bar{y})$ d'après 3a, donc $y^m = e$, puis $z = e$. Ainsi, $< y > \cap H = \{\text{e}\}$.

D'après la question précédente, $< y > H = G$.

- Enfin, $< y >$ est distingué dans G, et H aussi en tant que produit de deux groupes distingués (en effet, si $h = bc \in H$ et $g \in G$, $gcg^{-1} \in C$ et $gbg^{-1} \in B$, donc $ghg^{-1} = gcg^{-1}gbg^{-1} \in CB = H$).

Ainsi, d'après la question I-2 (mais pas I-1(a) car on n'est plus dans le cas abélien), $\boxed{< y > \text{ est un facteur direct de } G.}$

On en déduit que si $x \mapsto x\varphi(x)$ n'est pas injective, alors G admet un facteur direct abélien non trivial $< y >$.

Partie VI – Un sous-groupe de $\mathrm{Aut}(G)$

On suppose que G est un groupe fini n'ayant aucun facteur direct abélien non trivial

1. Soit $\theta \in \mathrm{Aut}(G)$.
   (a) Soit $z \in Z(G)$, et $g \in G$. Comme θ est surjective, il existe $h \in G$ tel que $g = \theta(h)$. On a alors
   $$g\theta(z) = \theta(h)\theta(z) = \theta(hz) = \theta(zh),$$
   car $z \in Z(G)$. Ainsi,
   $$g\theta(z) = \theta(z)\theta(h) = \theta(z)g.$$
   On en déduit que $\boxed{\theta(z) \in Z(G)}$.
   (b) On peut commencer par composer à l'arriver par la projection $Z \to Z/Z(G)$. On définit alors $bar\theta : G \to G/Z(G)$. D'après la question précédente, pour tout $z \in Z(G)$, $\bar{\theta}(z) = \bar{e}$, donc $\bar{\theta}$ passe au quotient et définit un morphisme $\boxed{\tilde{\theta} = G/Z(G) \to G/Z(G)}$. Par définition, ce morphisme vérifie :
   $$\boxed{\tilde{\theta}(\bar{g}) = \overline{\theta}(g))}.$$
   La surjectivité est préservée dans cette construction. De plus G est fini, donc aussi $G/Z(G)$, donc la surjectivité implique la bijectivité. Ainsi $\boxed{\tilde{\theta} \text{ est un automorphisme de } \mathrm{Aut}(G/Z(G))}$.
2. L'application $\Phi : \theta \mapsto \tilde{\theta}$ est un morphisme de groupe. En effet :
   $$\tilde{\theta_2} \circ \tilde{\theta_1}(\bar{g}) = \tilde{\theta_2}(\overline{\theta_1(g)}) = \overline{\theta_1 \circ \theta_2(g)} = \widetilde{\theta_1 \circ \theta_2}(\bar{g}).$$
   Ainsi, $\boxed{A_c = \mathrm{Ker}(\Phi) \text{ est un sous-groupe de } \mathrm{Aut}(G)}$.
3. Soit α un élément de A_c.
   (a) Puisque $\alpha \in A_c$, pour tout $x \in G$, en désignant par $\bar{x}$ sa classe modulo $Z(G)$, on a $\overline{\alpha(x)} = \bar{x}$. Ainsi, $\alpha(x) \in xZ(G)$. Il existe donc $\boxed{\theta_\alpha(x) \in Z(G)}$ tel que $\boxed{\alpha(x) = x\theta_\alpha(x)}$. Cet élément est unique par régularité dans G.
   (b) Soit g et h dans G. On a alors
   $$\alpha(gh) = \alpha(g)\alpha(h) = g\theta_\alpha(g)h\theta_\alpha(h) = gh\theta_\alpha(g)\theta_\alpha(h),$$
   car $\theta_\alpha(g) \in Z(G)$. La définition et l'unicité de $\theta_\alpha(gh)$ amène alors
   $$\boxed{\theta_\alpha(gh) = \theta_\alpha(g)\theta_\alpha(h)}.$$
   Ainsi, $\boxed{\theta_\alpha \in \mathrm{Hom}(G, Z(G))}$.
4. - Soit α et β dans A_c. Supposons $\theta_\alpha = \theta_\beta$. Alors pour tout $g \in G$, $g\theta_\alpha(g) = g\theta_\beta(g)$, c'est-à-dire $\alpha(g) = \beta(g)$. Ainsi, $\alpha = \beta$. On en déduit que $\boxed{\Phi \text{ est injective}}$.
   - Étant donné $\theta \in \mathrm{Hom}(G, Z(G))$, l'application $\alpha : g \mapsto g\theta(g)$ est un morphisme (V-2b) injectif, sinon la question V-3f entre en contradiction avec le fait que G ne possède pas de facteur abélien non trivial. Comme G est fini, on en déduit que α est un automophisme. Il vérifie par construction $\Phi(\alpha) = \theta$. Ainsi, Φ est surjective.

   On en déduit que $\boxed{\Phi \text{ est bijective}}$.
5. Ainsi, le sous-groupe A_c de $\mathrm{Aut}(G)$ est d'ordre $|\mathrm{Hom}(G, Z(G))|$.
   Or tout $\theta \in \mathrm{Hom}(G, Z(G))$ est trivial sur G' (V-2a). On en déduit que θ passe au quotient et définit $\tilde{\theta}$ dans $\mathrm{Hom}(G/G', Z(G))$. Réciproquement un morphisme $\tilde{\theta}$ de $\mathrm{Hom}(G/G', Z(G))$ définit un morphisme $\theta = \tilde{\theta} \circ \pi$. de $\mathrm{Hom}(G, Z(G))$. Ces deux constructions sont clairement réciproques l'une de l'autre. Ainsi, $\theta \mapsto \tilde{\theta}$ est une bijection de $\mathrm{Hom}(G, Z(G))$ sur $\mathrm{Hom}(G/G', Z(G))$.
   Ces deux ensembles ont donc même cardinal. On en déduit que A_c est d'ordre $\boxed{\mathrm{Hom}(G/G', Z(G))}$

Partie VII – Le résultat final

Soit G un groupe fini, et $N = |\mathrm{Aut}(G)|$. Soit E un facteur direct abélien de G d'ordre maximal. Il existe donc un sous-groupe H de G tel que $G \simeq E \times H$.

1. Puisque E est un groupe abélien fini, la question II-3c amène $|E| \leqslant h(|\mathrm{Aut}(E)|)$. La définition de h donnée en II-3c montre que h est croissante. De plus l'application $\alpha \mapsto \alpha \times \mathrm{id}_H$ est un morphisme injectif de $\mathrm{Aut}(E)$ dans $\mathrm{Aut}(H)$. On en déduit que $|\mathrm{Aut}(E)| \leqslant |Aut(G)|$. Ainsi, $\boxed{|E| \leqslant h(|\mathrm{Aut}(N)|) = h(N)}$

2. Le groupe H n'admet pas de facteur direct abélien K non trivial, sinon $A \times K$ serait un facteur direct abélien de G contredisant la maximalité de A. Ainsi, d'après la partie VI, $\mathrm{Aut}(G)$ possède un sous-groupe d'ordre $|\mathrm{Hom}\,(H/H', Z(H))\,|$. Le théorème de Lagrange permet de conclure que $\boxed{|\mathrm{Hom}\,(H/H', Z(H))| \text{ divise } \mathrm{Aut}(H)}$.

3. - Puisque $Z(H)$ est abélien, $Z(H) \cap H'$ est distingué dans $Z(H)$, d'où la bonne définition du groupe $Z(H)/Z(H) \cap H'$.
   - Soit $h \in H'$ et $g \in Z(H)H'$. Il existe $z \in Z(H)$ et $h' \in H'$ tels que $g = zh'$. On a alors, puisque z est dans le centre :
   $$ghg^{-1} = zh'hh'^{-1}z^{-1} = h'h(h')^{-1}zz^{-1} = h'h(h')^{-1} \in H'$$
   Ainsi, H' est distingué dans $Z(H)H'$.
   - Soit $i : Z(H) \to Z(H)H'$ l'inclusion. On peut composer par la projection $\pi : Z(H)H' \to Z(H')/H'$. Cela définit $\pi \circ i : Z(H) \mapsto Z(H)H'/H'$. Par ailleurs, pour tout $z \in Z(H) \cap H'$, $\pi \circ i(z) = \pi(z) = 0$, puisque $z \in H'$. Ainsi, $\pi \circ i$ passe au quotient et définit un morphisme $\varphi : Z(H)/Z(H) \cap H' \to Z(H)H'/H'$.
   - Soit gH' une classe dans $Z(H)H'/H'$, $g \in Z(H)H'$. Il existe donc $z \in Z(H)$ et $h \in H'$ tels que $g = zh$. Ainsi, $gH' = zH' = \pi \circ i(z) = \varphi(\bar{z})$ ($\bar{z}$ étant la classe de z modulo $Z(H) \cap H'$). Ainsi, φ est surjective.
   - Soit $\bar{z} \in \mathrm{Ker}(\varphi)$. On a donc $\pi \circ i(z) = 0$, donc $i(z) = z \in H'$. Ainsi, $z \in Z(H) \cap H'$, donc $\bar{z} = 0$. Le noyau de φ est donc trivial. On en déduit que φ est injective.

   Ainsi, φ est un $\boxed{\text{isomorphisme entre } Z(H)/Z(H) \cap H' \text{ et } Z(H)H'/H'}$.

4. On utilise la question III-9b avec les groupes (abéliens) $A = H/H'$, $B = Z(H)$, $C = Z(H)H'/H' \subset H/H'$ et $D = Z(H) \cap H'$. La question précédente montre que $C \cong B/D$, et la question III-9b amène que $|C|$ divise $|\mathrm{Hom}\,(H/H', Z(H))|$, donc $\boxed{|Z(H)/(Z(H) \cap H')| \text{ divise } |\mathrm{Hom}\,(H/H', Z(H))|}$.
   En combinant avec la question 2, $|Z(H)/(Z(H) \cap H')|$ divise $|Aut(G)| = N$, donc en particulier est inférieur à N. On en déduit que $\boxed{|Z(H)| \leqslant N|Z(H) \cap H'| \leqslant N|H'|.}$

5. Soit, pour $z \in H$, l'application $\varphi_z : g \mapsto zgz^{-1}$.
   (a) L'application φ va bien de H dans H. Soit h, h' dans H. On a $\varphi_z(hh') = zhh'z^{-1} = zhz^{-1}zh'z^{-1} = \varphi_z(h)\varphi_z(h')$. Ainsi, φ_z est un morphisme. Il admet une réciproque $\varphi_{z^{-1}}$. Ainsi, $\boxed{\varphi_z \text{ est un automorphisme de } H}$.
   (b) Soit z et z' deux éléments de H. On suppose que pour tout $h \in H$, $zhz^{-1} = z'h(z')^{-1}$, donc $(z'^{-1}z)h = h(z'^{-1}z)$. Ainsi, $z'^{-1}z \in Z(G)$, donc $z \in z'Z(H)$. Par conséquent, $\boxed{z \text{ et } z' \text{ sont dans la même classe modulo } Z(H).}$
   Réciproquement, si z et z' sont dans la même classe modulo $Z(H)$, $z'^{-1}z \in Z(H)$, donc pour tout $h \in H$, $(z'^{-1}z)h = h(z'^{-1}z)$, ce qui implique $\varphi_z(h) = \varphi_{z'}(h)$, donc $\boxed{\varphi_z = \varphi_{z'}}$.
   (c) Il y a donc autant d'automorphismes intérieurs distincts que de classes de conjugaison modulo $Z(H)$. Comme les automorphismes intérieurs sont des automorphismes, on en déduit que $\boxed{|H/Z(H)| \leqslant N}$.

6. Comme on l'a déjà justifié, H étant un facteur direct de G, on dispose d'une injection $\mathrm{Aut}(H) \to \mathrm{Aut}(G)$. Ainsi, $|\mathrm{Aut}(H)| \leqslant N$. D'après la question IV-5, on a donc $|G'| \leqslant N^{2N^3}$. Ainsi, d'après les questions 4 et 5c,
   $$|H| \leqslant N|Z(G)| \leqslant N^2|G'| \leqslant N^{2N^3+2}.$$
   On a donc
   $$|G| \leqslant |E| \times |H| \leqslant \boxed{N^{2N^3+2}h(N)} = f(N).$$

7. On observe que $\lim_{N \to +\infty} f(N) = +\infty$. Soit alors $A \in \mathbb{N}$ et N_0. Soit $n_0 = f(A)$, et G un groupe tel que $|G| > n_0$. On a alors $f(A) < |G| \leqslant f(|\mathrm{Aut}(G)|)$, donc, f étant trivialement strictement croissante (puisque h est croissante), $|Aut(G)| > A$. En particulier, pour tout $n > n_0$, $m_n > A$. On en déduit que $\boxed{\lim\limits_{n \to +\infty} m_n = +\infty}$.