**Devoir Surveillé n° 7 (4h)**

*La présentation, la lisibilité, l'orthographe, la qualité de la rédaction, la clarté, la précision et la concision des raisonnements entreront pour une part importante dans l'appréciation des copies.*

*Les candidats sont invités à encadrer dans la mesure du possible les résultats de leurs calculs.*

*L'usage de tout document et de tout matériel électronique est interdit. Notamment, les téléphones portables doivent être* éteints *et* rangés.

**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 $G$.*

**Définitions et terminologie**

- *On dira qu'un groupe $G$ est multiplicatif si l'opération considérée est le produit $\times$ ; on s'autorisera dans ce cas l'omission du signe opératoire en écrivant $ab$ au lieu de $a \times b$. On dira que le groupe est additif si l'opération considéré est l'addition $+$.*
- *Le neutre d'un groupe $G$ sera noté $e_G$.*
- *Deux groupes $G$ et $H$ sont dit isomorphes s'il existe un isomorphisme $\varphi : G \to H$. On notera dans ce cas $G \cong H$*
- *L'ensemble des automorphismes $\mathrm{Aut}(G)$ est muni de sa structure de groupe habituelle, la loi étant la composition des automorphismes.*
- *Soit $x \in G$. On note $\mathrm{ord}(x)$ l'ordre de l'élément $x$.*
- *Soit $G$ un groupe multiplicatif et $H$ et $K$ deux sous-groupes de $G$. Alors $HK$ désigne l'ensemble $\{hk, h \in H, k \in K\}$. Ce n'est pas nécessairement un groupe.*
- *Étant donné deux groupes multiplicatifs $H$ et $K$, le produit cartésien $H \times K$ peut-être muni du produit défini par $(h,k) \times (h',k') = (hh', kk')$. $H \times K$ est alors un groupe, appelé produit direct (externe) de $H$ et $K$.*
- *On dit qu'un sous-groupe $H$ de $G$ est un facteur direct de $G$ s'il existe un sous-groupe $K$ tel que $(h,k) \mapsto hk$ définisse un isomorphisme de $H \times K$ dans $G$. Remarquez que cela implique que $G = HK$. On dira dans ce cas que $G$ est le produit direct interne de $H$ et $K$.*
- *Soit $p$ un nombre premier. On dit qu'un groupe $G$ est un $p$-groupe si son ordre est égal à une puissance de $p$.*
- *Soit $G$ un groupe abélien. L'exposant de $G$ est le ppcm des ordres des éléments du groupe $G$.*
- *Le centre $Z(G)$ d'un groupe $G$ est l'ensemble des éléments de $G$ commutant avec tout autre.*
- *Un sous-groupe $H$ de $G$ est dit distingué s'il est stable par conjugaison, donc si pour tout $h \in H$ et $g \in G$, $ghg^{-1} \in H$.*
- *Soit $n \in \mathbb{N}$, $n \geqslant 2$. On note $\varphi(n)$ le nombre d'entiers de $[\![1, n]\!]$ qui sont premiers avec $n$ (indicatrice d'Euler).*

**Résultats admis**

*On pourra utiliser sans les redémontrer les résultats suivants (vus en exercice ou en DM) :*

- *Exposant d'un groupe abélien : $G$ étant un groupe abélien, et $\omega$ son exposant, il existe dans $G$ un élément d'ordre $\omega$.*
- *Classification des groupes abéliens finis :*
  - *tout groupe abélien fini est isomorphe à un groupe $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$.*

- *Si on impose de plus que les $n_i$ soient de la forme $p_i^{\alpha_i}$, avec $p_i$ premier, cette décomposition est unique, à l'ordre près des facteurs.*
  *NB : la propriété d'unicité est exprimée de façon un peu différente que dans votre DM, mais s'y ramène facilement.*
- *Au cours de la démonstration de ce résultat est apparu le fait suivant, qu'on pourra utiliser aussi : si $x$ est un élément d'ordre maximal de $G$ (dont d'ordre égal à l'exposant de $G$), alors $< x >$ est un facteur direct de $G$.*

- *Si $H$ est un sous-groupe distingué de $G$, les classes à gauche et à droite modulo $H$ sont égales, et la loi de $G$ passe au quotient sur $G/H$ (ensemble des classes à gauche ou droite), définissant une structure de groupe sur $G/H$.*
- *En particulier $Z(G)$ est un sous-groupe distingué de $G$ ; on peut donc considérer le groupe quotient $G/Z(G)$.*
- *Premier théorème d'isomorphisme : Soit $f$ un morphisme de $G$ dans $H$. Alors $f$ passe au quotient et définit un morphisme injectif $\tilde{f} : G/\operatorname{Ker}(f) \to H$.*
- *Valeurs de l'indicatrice d'Euler : Si $p$ est un nombre premier et $a > 0$, $\varphi(p^a) = p^{a-1}(p-1)$. Si $n$ et $m$ sont premiers entre eux, $\varphi(nm) = \varphi(n)\varphi(m)$.*

## Partie I – Facteurs directs

1. (a) Soit $G$ un groupe abélien. Soit $H$ et $K$ deux sous-groupes de $G$ tels que $HK = G$ et $H \cap K = \{\mathrm{e}_G\}$, où $HK$ désigne l'ensemble des produits d'un élément de $H$ et d'un élément de $K$. Montrer que $H$ est un facteur direct de $G$.

   (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 $p_{|H} = \mathrm{id}_H$. En considérant $\operatorname{Ker}(p)$, montrer que $H$ est un facteur direct de $G$.
   Indication : on pourra constater que pour tout $g \in G$, $gp(g)^{-1} \in \operatorname{Ker}(p)$.

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) Montrer que pour tout $h \in H$ et $k \in K$, $hk = kh$.
   (b) Montrer que $H$ 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. On notera que cette partie utilise un certain nombre des résultats admis dans le préambule.*

1. Soit $p$ un nombre premier, et $G$ un $p$-groupe abélien, d'ordre $p^n$, $n \in \mathbb{N}^*$. Soit $\omega$ l'exposant de $G$.
   (a) Justifier qu'il existe $r \in \mathbb{N}$ tel que $\omega = p^r$.
   (b) Soit $x$ et $y$ deux éléments d'ordre $\omega$. Justifier qu'il existe deux groupes $H_1$ et $H_2$ tels que

$$G \cong < x > \times H_1 \qquad \text{et} \qquad G \cong < y > \times H_2, \qquad \text{et} \qquad H_1 \cong H_2.$$

   (c) On se donne un isomorphisme $\psi : H_1 \to H_2$. Justifier que $\beta : (x^m, h_1) \mapsto (y^m, \psi(h_1))$ est bien défini et est un isomophisme.
   (d) En déduire l'existence d'un automorphisme $\alpha$ de $G$ tel que $\alpha(x) = y$.
   (e) Soit $\mathcal{O}$ l'ensemble des éléments d'ordre $\omega$ de $G$. Justifier que $f : x \mapsto x^{p^{r-1}}$ est un endomorphisme de $G$, et en déduire que $G \setminus \mathcal{O}$ est un groupe.
   (f) En majorant l'ordre du groupe $G \setminus \mathcal{O}$, en déduire que

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

   (g) En déduire enfin que $|\operatorname{Aut}(G)| \geqslant p^{n-1}(p-1) = \varphi(p^n)$, où $\varphi$ est l'indicatrice d'Euler.

2. Soit maintenant $G$ un groupe abélien d'ordre $p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$, les $p_i$ étant des entiers premiers 2 à 2 distincts.

(a) Justifier l'existence de groupes abéliens $G_i$ d'ordre $p_i^{\alpha_i}$ tels que $G$ soit isomorphe à $G_1 \times \cdots \times G_r$.

(b) Justifier que $\mathrm{Aut}(G)$ contient un sous-groupe isomorphe à $\mathrm{Aut}(G_1) \times \cdots \times \mathrm{Aut}(G_r)$.

(c) En déduire que $|\mathrm{Aut}(G)| \geqslant \varphi(|G|)$, où $\varphi$ est l'indicatrice d'Euler.

3. (a) Soit $k \in \mathbb{N}$, $k \geqslant 2$, et $n \in \varphi^{-1}(\llbracket 2, k \rrbracket)$. Montrer que tous les entiers premiers $p$ intervenant dans la décomposition primaire de $n$ vérifient $p \leqslant k+1$, et que leur multiplicité dans la décomposition de $n$ est inférieure ou égale à $\log_2(k) + 1$.

(b) En déduire que pour tout $k \geqslant 2$, $\varphi^{-1}(\{k\})$ est borné.

(c) En déduire enfin l'existence d'une application croissante $h : \mathbb{N}^* \to \mathbb{N}^*$ telle que pour tout $G$ abélien, $|G| \leqslant h(|\mathrm{Aut}(G)|)$.

## Partie III – Groupe des homomorphismes de groupes abéliens

*Soit $A$ et $B$ deux groupes abéliens multiplicatifs. L'ensemble* $\mathrm{Hom}(A, B)$ *des homomorphismes de $A$ vers $B$ peut être muni de l'opération $\times$ définie, pour $\varphi$ et psi dans* $\mathrm{Hom}(A, B)$*, par :*

$$\varphi \times \psi : a \longmapsto \varphi(a)\psi(a),$$

*le produit $\varphi(a)\psi(a)$ étant dans $B$.*

1. Montrer que si $\varphi$ et $\psi$ sont des éléments de $\mathrm{Hom}(A, B)$, il en est de même de $\varphi \times \psi$.
2. Montrer que $(\mathrm{Hom}(A, B), \times)$ est un groupe abélien.
3. (a) Montrer que si $f : A \to A'$ est un isomorphisme de groupes, alors $\Phi : g \mapsto g \circ f$ est un isomorphisme de $\mathrm{Hom}(A', B)$ dans $\mathrm{Hom}(A, B)$.

   (b) Montrer de même que si $B$ et $B'$ sont isomorphes, alors $\mathrm{Hom}(A, B)$ et $\mathrm{Hom}(A, B')$ également.
4. Soit $A$, $B$ et $C$ trois groupes abéliens.

   (a) Soit $\psi \in \mathrm{Hom}(A \times B, C)$. Montrer que $\psi_A : x \mapsto \psi(x, e_B)$ est un élément de $\mathrm{Hom}(A, C)$.

   On montrerait de même (mais on ne demande pas de le faire) que $\psi_B : y \mapsto \psi(e_A, y)$ est un élément de $\mathrm{Hom}(B, C)$

   (b) En considérant $\Phi : \psi \mapsto (\psi_A, \psi_B)$, montrer que

$$\mathrm{Hom}(A \times B, C) \cong \mathrm{Hom}(A, C) \times \mathrm{Hom}(B, C)$$

5. Montrer de même que $\mathrm{Hom}(A, B \times C) \cong \mathrm{Hom}(A, B) \times \mathrm{Hom}(A, C)$.
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) Soit $\psi \in \mathrm{Hom}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right)$. Montrer que $\mathrm{ord}(\psi(1))|n$.

   (b) En déduire que $\psi(1) \in \left(\frac{m}{n \wedge m}\mathbb{Z}\right)/m\mathbb{Z}$.

   (c) Montrer que $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ est isomorphe à $\mathbb{Z}/(n \wedge m)\mathbb{Z}$.
7. Montrer que pour tous groupes abéliens $A$ et $B$, $\mathrm{Hom}(A, B)$ et $\mathrm{Hom}(B, A)$ 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) À l'aide des résultats précédents, montrer que pour tout $i \in \llbracket 1, r \rrbracket$, $\mathrm{Hom}(G_i, G_i) \cong G_i$.

   (b) Montrer que $\mathrm{Hom}(G, G)$ contient un sous-groupe $H$ isomorphe à $\mathrm{Hom}(G_1, G_1) \times \cdots \times \mathrm{Hom}(G_r, G_r)$.

   (c) En déduire que $|G|$ 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) Construire un morphisme injectif $\Phi : \mathrm{Hom}\left(B/D, C\right) \to \mathrm{Hom}(B, A)$.

   (b) En déduire que $|C|$ divise $|\mathrm{Hom}(A, B)|$.

## Partie IV – Autour du groupe dérivé

*Soit $G$ un groupe fini, et $x$ et $y$ deux éléments de $G$. On note $[x,y]$ le commutateur de $x$ et $y$, défini par :*

$$[x,y] = x^{-1}y^{-1}xy.$$

*On note $G'$ le sous-groupe de $G$ engendré par l'ensemble $\{[x,y], x \in G, y \in G\}$ de tous les commutateurs. Le groupe $G'$ est appelé groupe dérivé de $G$. On note $m$ l'ordre du groupe $G/Z(G)$.*

1. On note, pour $x, z \in G$, $x^z = z^{-1}xz$ le conjugué de $x$ par $z$. Montrer que si $a$, $b$ et $z$ sont des éléments de $G$, alors $[a,b]z = z[a^z, b^z]$.
2. Montrer que $G'$ est un sous-groupe distingué de $G$ et que $G/G'$ 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 $G/Z(G)$. Montrer que $[a,b] = [c,d]$.
   (b) En déduire qu'il y a au plus $m^2$ commutateurs distincts.
4. Soit $x \in G'$. Ainsi, $x$ peut s'écrire comme un produit fini de commutateur. On considère désormais un produit en un nombre *minimal* $n$ de commutateurs :

   $$x = c_1 \cdots c_n.$$

   On suppose que $n \geqslant m^3 + 1$.
   (a) Justifier qu'il existe un commutateur $c$ apparaissant au moins $m+1$ fois parmi les $c_i$
   (b) Montrer qu'il existe des commutateurs $c'_1, \ldots, c'_{n-m-1}$ tels que

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

   (c) Soit $u$ et $v$ tels que $c = [u,v]$. Montrer que $c^{m+1} = (u^{-1}cu)^{m-1}[u^2, v]$.
   (d) En déduire que $n \leqslant m^3$.
5. Montrer que $|G'| \leqslant m^{2m^3}$.

## 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) Justifier que pour tout $i \in [\![1, \ell]\!]$, l'élément $y_i$ de $\mathbb{Z}/p^{n_i}\mathbb{Z}$ est d'ordre $p^{s_i}$, $s_i \leqslant k+1$.
   (b) Soit $I = \{i \in [\![1,\ell]\!] \text{ tel que } s_i = k+1\}$. Montrer qu'il existe $i \in I$ tel que $n_i = k+1$ et $< y_i >= \mathbb{Z}/p^{n_i}\mathbb{Z}$.
   (c) À l'aide d'un résultat de la partie I, montrer que $< y >$ est un facteur direct de $G$.
2. Soit $G$ un groupe fini quelconque, noté multiplicativement. Soit $\varphi \in \mathrm{Hom}(G, Z(G))$. On définit $\alpha : G \to G$ par $\alpha(g) = g\varphi(g)$.
   (a) Montrer que pour tout $g \in G'$, $\varphi(g) = e_G$ ($G'$ désigne le groupe dérivé)
   (b) Montrer que $\alpha \in \mathrm{Hom}(G, G)$.
3. Avec les notations de la question précédente, on montre dans cette question que si $\alpha$ n'est pas injective, alors $G$ possède un facteur direct abélien non trivial. On suppose donc $\alpha$ non injective, et on considère un élément $x$ d'ordre premier $p$ dans $\mathrm{Ker}(\alpha)$. 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) Montrer que $y$ et $\bar{y}$ sont d'ordre $p^{k+1}$.
   (b) Justifier l'existence de deux sous-groupes $A$ et $B$ de $G/G'$ tels que $A$ soit un $p$-groupe et $B$ soit d'ordre premier avec $p$ et tels que $G/G'$ soit le produit direct interne de $A$ et $B$
   (c) Montrer que $\bar{y} \in A$ et que $< \bar{y} >$ 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 $\pi(g) = \bar{g}$. Montrer que $\pi^{-1}(C)$, $\pi^{-1}(B)$ et $< y >$ sont des sous-groupes distingués de $G$.

(e) Soit $g \in G$. Justifier qu'il existe $m \in \mathbb{Z}$ et $r \in \pi^{-1}(B)$ tel que $\pi(y^{-m}gr) \in C$.

(f) En déduire que $G =< y > H$, où $H = \pi^{-1}(C)\pi^{-1}(B)$.

(g) Montrer que $< y >$ est un facteur direct de $G$.

**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 (c'est-à-dire non égal à $\{e\}$). On montre dans ce cas l'existence d'un sous-groupe de* $\mathrm{Aut}(G)$ *d'ordre contrôlé.*

1. Soit $\theta \in \mathrm{Aut}(G)$.
   (a) Montrer que si $z \in Z(G)$, alors $\theta(z) \in Z(G)$.
   (b) En déduire que $\theta$ définit un automorphisme $\tilde{\theta}$ de $\mathrm{Aut}(G/Z(G))$, tel que pour tout $g \in G$, $\overline{\theta(g)} = \tilde{\theta}(\bar{g})$.
2. Soit $A_c$ le sous-ensemble de $\mathrm{Aut}(G)$ des automorphismes $\theta$ tels que $\tilde{\theta} = \mathrm{id}_{G/Z(G)}$. Montrer que $A_c$ est un sous-groupe de $\mathrm{Aut}(G)$.
3. Soit $\alpha$ un élément de $A_c$.
   (a) Justifier l'existence, pour tout $x \in G$, d'un unique élément $\theta_\alpha(x)$ de $Z(G)$ tel que $\alpha(x) = x\theta_\alpha(x)$.
   (b) Montrer que $\theta_\alpha \in \mathrm{Hom}(G, Z(G))$.
4. Soit $\Phi : A_c \longrightarrow \mathrm{Hom}(G, Z(G))$ l'application qui à $\alpha$ associe $\theta_\alpha$. Justifier que $\Phi$ est bijective.
5. Montrer que $\mathrm{Aut}(G)$ possède un sous-groupe d'ordre $|\mathrm{Hom}(G/G', Z(G))|$.

**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. Montrer que $|E| \leqslant h(N)$, où $h$ est la fonction définie en II-3c.
2. Montrer que $|\mathrm{Hom}\,(H/H', Z(H))|$ divise $\mathrm{Aut}(H)$.
3. Montrer que $Z(H)H'/H' \cong Z(H)/(Z(H) \cap H')$.
4. En déduire que l'ordre de $Z(H)/(Z(H) \cap H')$ divise $|\mathrm{Hom}\,(H/H', Z(H))|$, puis que $|Z(H)| \leqslant N|H'|$.
5. Soit, pour $z \in H$, l'application $\varphi_z : g \mapsto zgz^{-1}$.
   (a) Montrer que $\varphi$ est un automorphisme de $H$ (appelé automorphisme intérieur de $H$).
   (b) Soit $z$ et $z'$ deux éléments de $H$. Montrer que $\varphi_z = \varphi_{z'}$ si et seulement si $z$ et $z'$ sont dans la même classe modulo $Z(H)$.
   (c) En déduire que $|H/Z(H)| \leqslant N$.
6. Montrer que $|G| \leqslant h(N)N^{2N^3+2}$.
7. Soit, pour $n \in \mathbb{N}$, $m_n$ l'ordre minimum de $\mathrm{Aut}(G)$ lorsque $G$ parcourt l'ensemble des groupes d'ordre $n$. Montrer que $\lim\limits_{n\to+\infty} m_n = +\infty$.