Sur les automorphismes d'un groupe fini

par Paul LESCOT

? ?

RÉSUMÉ. *? ?*

MOTS-CLÉS : *groupe, morphisme de groupe, groupe abélien, groupe cyclique, centre, commutateur, facteur direct.*

1. Introduction

L'objet de cette note est d'établir le résultat suivant, conjecturé par Nicolas Tosel en 1997 :

Théorème 1. *Il existe une fonction $f : \mathbf{N}^* \to \mathbf{N}^*$ telle que, pour tout groupe fini G, l'on ait $|G| \leqslant f(|Aut(G)|)$.*

Etant donné le Théorème de Cayley selon lequel un groupe fini d'ordre n est isomorphe à un sous–groupe du groupe symétrique Σ_n de degré n, il apparaît que n'existe, pour chaque n, qu'une famille finie de types d'isomorphisme de groupes finis d'ordre n. Le Théorème peut donc être reformulé ainsi

Théorème 2. *Pour tout groupe fini H, la famille des groupes finis G tels que $Aut(G) \simeq H$ ne comprend qu'un nombre fini de classes d'isomorphisme.*

Lorsque l'on restreint G à être abélien, ce résultat est bien connu ; en fait, on a même un énoncé plus fort (Théorème 3.3), que nous utiliserons d'ailleurs dans notre démonstration.

Les notations sont des plus usuelles : $|A|$ désigne le cardinal de l'ensemble fini A, Z_n le groupe cyclique d'ordre n et ϕ la fonction indicatrice d'Euler. Pour G un groupe, on note $Z(G)$ son centre :

$$Z(G) := \{x \in G | (\forall y \in G) xy = yx\} \ ,$$

et, pour $(a, b) \in G^2$:

$$a^b := b^{-1}ab \ ,$$

$$[a, b] := a^{-1}a^b = a^{-1}b^{-1}ab$$

(**commutateur** de a et b) et

$$G^{'} :=< [a, b]|(a, b) \in G^2 >$$

(**groupe dérivé** de G).

L'ordre d'un élément x de G est noté $\omega(x)$.

2. Sur les groupes abéliens finis

Pour deux groupes finis abéliens A et B, $Hom(A, B)$ désignera l'ensemble des homomorphismes de A dans B. Nous le munirons de la multiplication évidente :

$$\forall(\varphi, \psi) \in Hom(A, B)^2 \ \forall a \in A$$
$$(\varphi.\psi)(a) = \varphi(a)\psi(a) \ .$$

Il est visible que cette opération fait de $Hom(A, B)$ un groupe abélien.

Théorème 3. *Si A et B sont deux groupes abéliens finis, alors*

$$Hom(A, B) \simeq Hom(B, A) \ .$$

Démonstration D'après le théorème de structure des groupes abéliens finis, on peut écrire A comme produit direct de groupes cycliques

$$A = A_1 \times ... \times A_r \ ,$$

et de même

$$B = B_1 \times ... \times B_s \ .$$

Soit $\varphi \in Hom(A, B)$; alors, pour $i \in \{1, ..., r\}$ et $a \in A_i$, posons (l'élément a étant situé à la i–ème place)

$$\varphi((1, ..., 1, a, ..., 1)) = (\psi_{1,i}(a), ..., \psi_{s,i}(a)).$$

Il apparaît que

$$\psi_{j,i} \in Hom(A_i, B_j) \ ;$$

de plus, si $a = (a_1, ..., a_r) \in A$,

$$\varphi(a) = \prod_{i=1}^{r} (\psi_{1,i}(a_i), ..., \psi_{s,i}(a_i)).$$

Il en résulte que l'application

$$\begin{aligned} Hom(A,B) \to & \prod_{1\leqslant i\leqslant r;1\leqslant j\leqslant s} Hom(A_i,B_j) \\ \varphi \mapsto & \quad (\psi_{j,i})_{1\leqslant i\leqslant r;1\leqslant j\leqslant s} \end{aligned}$$

est un isomorphisme ; donc

$$Hom(A,B) \simeq \prod_{1\leqslant i\leqslant r;1\leqslant j\leqslant s} Hom(A_i,B_j).$$

De même

$$Hom(B,A) \simeq \prod_{1\leqslant j\leqslant s;1\leqslant i\leqslant r} Hom(B_j,A_i).$$

Il suffit donc d'établir que, pour tous i et j, l'on a

$$Hom(A_i,B_j) \simeq Hom(B_j,A_i)\ ;$$

en d'autres termes, nous nous sommes ramené au cas où A et B sont cycliques.

Soient donc $A =< a >$ d'ordre m, et $B =< b >$ d'ordre n, et posons

$d = pgcd(m,n)$. En vertu du Théorème de Bachet–Bezout, il existe $(x,y) \in \mathbf{Z}^2$ tel que $d = xm + yn$.

Soit alors $\varphi \in Hom(A,B)$; écrivons $\varphi(a) = b^s$. Il suit

$$\begin{aligned} b^{sm} &= (b^s)^m \\ &= \varphi(a)^m \\ &= \varphi(a^m) \\ &= \varphi(1) \\ &= 1\ , \end{aligned}$$

d'òu

$$\begin{aligned} b^{sd} &= b^{s(xm+yn)} \\ &= b^{sxm}b^{syn} \\ &= (b^{sm})^x(b^n)^{ys} \\ &= 1\ , \end{aligned}$$

donc $n = \omega(b)$ divise sd, et $\dfrac{n}{d}$ divise s.

Soit $s = \frac{n}{d}t$; alors, pour tout $r \in \mathbf{N}$

$$\varphi(a^r) = \varphi(a)^r = b^{sr} = b^{\frac{n}{d}tr} \ (*).$$

Réciproquement, pour chaque $t \in \mathbf{Z}$, la relation

$$\varphi_t(a^r) := b^{\frac{n}{d}tr}$$

définit une application $\varphi_t : A \to B$; en effet, $a^r = a^{r'}$ entraîne $m|r-r'$, soit $r-r' = mr''$; mais alors

$$\begin{aligned} \frac{n}{d}tr - \frac{n}{d}tr' &= \frac{n}{d}t(r-r') \\ &= \frac{n}{d}tmr'' \\ &= n(t\frac{m}{d}r'') \ , \end{aligned}$$

lequel est divisible par n, donc

$$b^{\frac{n}{d}tr} = b^{\frac{n}{d}tr'} \ .$$

Ce φ_t est donc un morphisme de A dans B, ne dépendant que de la classe de t modulo d. On a donc

$$Hom(A,B) = \{\varphi_0, ..., \varphi_{d-1}\}.$$

De plus, pour chaque t, $\varphi_t = (\varphi_1)^t$ dans $Hom(A,B)$; $Hom(A,B)$ est donc cyclique d'ordre $d = pgcd(m,n)$.

De même $Hom(B,A)$ est cyclique d'ordre $pgcd(n,m) = d$. ***cqfd***

Remarque Une autre démonstration du Théorème 2.1 peut être donnée au moyen de la théorie de la dualité : A est isomorphe (non canoniquement) à son groupe dual A^*, et de même B à son groupe dual B^*. $Hom(A,B)$ est donc isomorphe à $Hom(A^*,B^*)$, lequel s'identifie, *via* transposition, à $Hom(B,A)$.

Lemme 1. *Soit G un groupe fini abélien ; alors $|G|$ divise $|Hom(G,G)|$.*

Démonstration Reprenons la démonstration du Théorème 2.1 ; on peut écrire G comme produit direct de groupes cycliques

$$G = G_1 \times ... \times G_r$$

($|G_i| = g_i$) ; comme il a été vu, on a, en prenant $s = r$ et $B_i = A_i = G_i$:

$$Hom(G,G) \simeq \prod_{1 \leqslant i \leqslant r; 1 \leqslant j \leqslant r} Hom(G_i, G_j).$$

De ce fait, $Hom(G,G)$ contient le sous–groupe "diagonal "

$$H := \prod_{1 \leqslant i \leqslant r} Hom(G_i, G_i) \ .$$

Mais nous avons constaté que $Hom(G_i, G_i)$ était isomorphe à $Z_{pgcd(g_i,g_i)} = Z_{g_i}$, donc à G_i ; H est donc isomorphe à

$$\prod_{1 \leqslant i \leqslant r} G_i,$$

donc à G lui–même.

Il existe donc un sous–groupe de $Hom(G,G)$ isomorphe à G, d'où le résultat en vertu du Théorème de Lagrange. ***cqfd***

Corollaire 1. *Soient A et B deux groupes abéliens finis, C un sous–groupe de A et D un sous–groupe de B tels que $\dfrac{B}{D} \simeq C$; alors $|C|$ divise $|Hom(A,B)|$.*

Démonstration (Inspirée de [1], Theorem 4) Soit $\varphi \in Hom(\dfrac{B}{D}, C)$; pour $b \in B$, posons

$$i_\varphi(b) := \varphi(\bar{b}) \ ;$$

alors

$$i_\varphi(b) \in C \subseteq A \ .(**)$$

Il est clair d'après $(**)$ que $i_\varphi \in Hom(B,A)$, et que l'application

$$\begin{aligned} &Hom(\frac{B}{D}, C) \to Hom(B,A) \\ &\varphi \mapsto i_\varphi \end{aligned}$$

est un morphisme de groupes, injectif ; $Hom(B,A)$ contient donc un sous–groupe isomorphe à $Hom(\dfrac{B}{D}, C)$, donc à $Hom(C,C)$.

Mais $Hom(A,B) \simeq Hom(B,A)$ (Théorème 2.1) donc $Hom(A,B)$ contient un sous–groupe isomorphe à $Hom(C,C)$. Il en résulte que $|Hom(C,C)|$ divise $|Hom(A,B)|$; mais $|C|$ divise $|Hom(C,C)|$(Lemme 2.3), donc $|C|$ divise $|Hom(A,B)|$. ***cqfd***

3. Quatre résultats préliminaires

Proposition 1. *Soit G un groupe tel que $\dfrac{G}{Z(G)}$ soit d'ordre fini m ; alors*

$$|G'| \leqslant m^{2m^3}.$$

Démonstration Ce résultat est implicite dans la démonstration de [2],(33.9), pp. 168–169.

Posons $\bar{G} := \dfrac{G}{Z(G)}$, et soit, pour $a \in G$, $\bar{a} := aZ(G) \in \dfrac{G}{Z(G)}$. Supposons $\bar{c} = \bar{a}$ et $\bar{d} = \bar{b}$; alors il existe $(z, z') \in (\dfrac{G}{Z(G)})^2$ tel que $c = az$ et $d = bz^{'}$. Mais alors

$$\begin{aligned}
[c,d] &= c^{-1}d^{-1}cd \\
&= z^{-1}a^{-1}(z^{'})^{-1}b^{-1}azbz' \\
&= z^{-1}(z^{'})^{-1}zz^{'}a^{-1}b^{-1}ab \text{ (car } z \text{ et } z^{'} \text{ sont centraux)} \\
&= a^{-1}b^{-1}ab \\
&= [a,b].
\end{aligned}$$

Le commutateur de deux éléments de G ne dépend donc que de leurs classes dans $\dfrac{G}{Z(G)}$; vu que $|\dfrac{G}{Z(G)}| = m$, il y a au plus m^2 commutateurs distincts dans G. Pour établir le résultat, il suffit donc de faire voir que chaque élément de $G^{'}$ peut s'exprimer comme le produit de m^3 commutateurs.

Soit $x \in G^{'}$, et soit n le nombre minimal de termes dans une représentation de x comme produit de commutateurs :

$$x = c_1 ... c_n.$$

Si $n \leqslant m^3$, en complétant au besoin par $m^3 - n$ occurrences du commutateur $1 = [1,1]$ on obtient bien la représentation voulue. Supposons donc $n \geqslant m^3 + 1$; nous allons obtenir une contradiction. Comme vu ci–dessus, il y a en tout au plus m^2 commutateurs dans $G^{'}$; d'après le "principe des tiroirs", un commutateur (notons–le c) apparaît donc au moins $m + 1$ fois parmi les c_i.

Soient y et z deux commutateurs, $y = [a,b]$; alors

$$\begin{aligned}
yz &= zy^z \\
&= z[a,b]^z \\
&= z[a^z, b^z].
\end{aligned}$$

Au moyen de cette identité, il est possible de faire glisser vers la gauche dans l'expression de x les $m + 1$ occurrences de c susmentionnées ; on obtient donc une expression de la forme

$$x = c^{m+1}c_1^{'} ... c_{n-m-1}^{'}$$

où les $c_i^{'}$ sont des commutateurs. Nous allons faire voir que l'on peut exprimer c^{m+1} comme produit de m commutateurs, et donc x comme produit de $m + (n - m - 1) = n - 1$ commutateurs, contredisant ainsi la minimalité de n.

Soit $c = [u, v]$; du fait que $|\frac{G}{Z(G)}| = m$, on a $(cZ(G))^m = 1$ dans $\frac{G}{Z(G)}$, soit $c^m \in Z(G)$; mais alors

$$\begin{aligned} c^{m+1} &= c^m c \\ &= u^{-1}uc^m c \\ &= u^{-1}c^m uc \text{ (car } c^m \in Z(G)) \\ &= u^{-1}c^{m-1}cu[u,v] \\ &= u^{-1}c^{m-1}u^{-1}v^{-1}uvuu^{-1}v^{-1}uv \\ &= u^{-1}c^{m-1}u^{-1}v^{-1}u^2v \\ &= u^{-1}c^{m-1}uu^{-2}v^{-1}u^2v \\ &= (u^{-1}cu)^{m-1}[u^2,v] \end{aligned}$$

est le produit de $m-1$ commutateurs, car $u^{-1}cu = c^u = [u,v]^u = [u,v^u]$ est un commutateur. ***cqfd***

Théorème 4. *Soit G un groupe fini n'ayant aucun facteur direct abélien $\neq \{1\}$; alors $Aut(G)$ contient un sous–groupe d'ordre $|Hom(\frac{G}{G'}, Z(G))|$.*

Démonstration ([1], Théorème 1, p. 137)

Les automorphismes de G agissant trivialement sur $\frac{G}{Z(G)}$ forment un sous–groupe A_c de $Aut(G)$. Soit $\alpha \in A_c$; pour chaque $x \in G$ on a

$$\alpha(x) = x\theta_\alpha(x)$$

avec

$$\theta_\alpha(x) \in Z(G)\ ,$$

et il est visible que θ_α est un morphisme de G dans $Z(G)$. L'application

$$\begin{aligned} A_c &\to Hom(G, Z(G)) \\ \alpha &\mapsto \theta_\alpha \end{aligned}$$

est évidemment injective ; nous allons faire voir qu'elle est bijective.

Soit donc $\varphi \in Hom(G, Z(G))$; il s'agit de montrer que l'application

$$\begin{aligned} \alpha \ : \ & G \to G \\ & x \mapsto x\varphi(x) \end{aligned}$$

est un automorphisme de G ; on aura alors $\theta_\alpha = \varphi$.

Il est clair qu'il s'agit d'un morphisme de groupes ; G étant fini, il nous suffit d'établir son injectivité. Supposons donc $\mathrm{Ker}(\alpha) \neq \{1\}$; nous allons obtenir une contradiction.

Le noyau $\mathrm{Ker}(\alpha)$ contient un élément x d'ordre premier p ; on a alors

$$x\varphi(x) = \alpha(x) = 1 \ ,$$

soit $\varphi(x) = x^{-1}$. Notons $\bar{G} := \dfrac{G}{G'}$, et

$$\begin{array}{rcl} \pi & : & G \to \dfrac{G}{G'} \\ & & x \mapsto xG' \end{array}$$

la projection canonique.

$\bar{G}$ étant abélien, on peut le décomposer en

$$\bar{G} = A \times B$$

où A est d'ordre une puissance de p ($|A| = p^r$) et l'ordre de B n'est pas divisible par p. On a

$$\bar{x}^p = \bar{x^p} = \bar{1} \ ;$$

de plus l'homomorphisme φ de G dans $Z(G)$ est trivial sur G' (car $Z(G)$ est abélien) et

$$\varphi(x) = x^{-1} \neq 1 \ ,$$

d'où $x \notin G'$, $\bar{x} \neq \bar{1}$ et $\omega(\bar{x}) = p$.

Soit k le plus grand entier positif ou nul tel que $\bar{x}$ soit une puissance p^k–ème dans A ; il est apparent que $0 \leqslant k \leqslant r-1$. Ecrivons $\bar{x} = a^{p^k}$ ($a \in A$), et $a = \bar{z}$ ($z \in G$) ; alors $\bar{x} = \bar{z}^{p^k} = \bar{z^{p^k}}$, soit $x = z^{p^k} u$ pour un $u \in G'$. Mais alors

$$\begin{array}{rcl} x^{-1} & = & \varphi(x) \\ & = & \varphi(z^{p^k} u) \\ & = & (\varphi(z))^{p^k} \varphi(u) \\ & = & \varphi(z)^{p^k}. \end{array}$$

Soit $y := \varphi(z) \in Z(G)$; alors

$$x = y^{-p^k} \ ,$$

$$y^{p^{k+1}} = x^{-p} = 1$$

et

$$y^{p^k} = x^{-1} \neq 1 \ ,$$

d'où $\omega(y) = p^{k+1}$. De plus

$$\bar{y}^{p^{k+1}} = \bar{1}$$

(en particulier, $\bar{y} \in A$) et

$$\bar{y}^{p^k} = \bar{y^{p^k}} = \bar{x^{-1}} \neq \bar{1} \ ,$$

d'où $\omega(\bar{y}) = p^{k+1}$.

Dans ce qui suit, nous nous inspirons de [3], pp. 14-21.

Posons $u = \bar{y}$, soit $\bar{A} := \dfrac{A}{< u >}$, et écrivons $\bar{A}$ comme produit direct de groupes cycliques :

$$\bar{A} =< \bar{a_1} > \times ... \times < \bar{a_r} >$$

avec $\omega(\bar{a_i}) = p^{n_i}$. On a donc $a_i^{p^{n_i}} \in < u >$, soit

$$a_i^{p^{n_i}} = u^{p^{m_i} s_i}$$

pour un $m_i \geqslant 0$ et un s_i non divisible par p.

Si $m_i \geqslant k+1$, alors $u^{p^{m_i}} = 1$ et donc $a_i^{p^{n_i}} = 1$; nous supposerons donc dorénavant que $m_i \leqslant k$.

Soit t_i tel que $s_i t_i \equiv 1[p]$. On a

$$\begin{aligned}
\bar{x}^{-1} &= (\bar{y})^{p^k} \\
&= u^{p^k} \\
&= u^{p^k s_i t_i} \\
&= (u^{p^{m_i} s_i})^{p^{k-m_i} t_i} \\
&= (a_i^{p^{n_i}})^{p^{k-m_i} t_i} \\
&= a_i^{p^{n_i} p^{k-m_i} t_i} \\
&= (a_i^{t_i})^{p^{n_i+k-m_i}}
\end{aligned}$$

d'où, par définition de k, $n_i + k - m_i \leqslant k$, et $n_i \leqslant m_i$. En remplaçant a_i par $a_i u^{-p^{m_i-n_i} s_i}$ (ce qui ne change pas la classe de a_i modulo $< u >$), on peut donc supposer que $a_i^{p^{n_i}} = 1$, donc que $\omega(a_i)$ divise p^{n_i}. Mais $p^{n_i} = \omega(\bar{a_i})$ divise $\omega(a_i)$, d'où $\omega(a_i) = \omega(\bar{a_i}) = p^{n_i}$.

Mais alors de

$$a_1^{m_1} ... a_r^{m_r} = 1$$

suit

$$\bar{a_1}^{m_1} ... \bar{a_r}^{m_r} = 1 \ ;$$

donc chaque $\bar{a_j}^{m_j}$ vaut $\bar{1}$, soit $p^{n_j} \mid m_j$; mais alors $a_j^{m_j} = 1$. Soit $C :=< a_1, ..., a_r >$; il apparaît que, d'une part, le groupe C est le produit direct des groupes $< a_i >$:

$$C =< a_1 > \times ... \times < a_r > \ ,$$

(d'où $|C| = p^{n_1+\ldots+n_r} = |\bar{A}|$) et d'autre part que $C \cap < u >= \{1\}$; il s'ensuit que

$$A =< u > \times C =< \bar{y} > \times C \ .$$

Soient $M := \pi^{-1}(C)$ et $N := \pi^{-1}(B)$; alors M et N sont des sous–groupes distingués de G, donc

$$H = MN := \{uv | u \in M, v \in N\}$$

est un sous–groupe (distingué) de G.

Soit $g \in G$; alors $\pi(g) \in \bar{G}$, donc $\pi(g)$ est représentable sous la forme ab ($a \in A$, $b \in B$) ; écrivons $a = (\bar{y})^m c$ pour $m \in \mathbf{Z}$ et $c \in C$. Soit $r \in G$ tel que $\pi(r) = b$; en particulier, $r \in \pi^{-1}(B) = N$. Il apparaît que

$$\begin{aligned} \pi(g) &= ab \\ &= \pi(y)^m cb \\ &= \pi(y^m)c\pi(r) \end{aligned}$$

et

$$\pi(y^{-m}gr) = c \in C \ ,$$

soit $y^{-m}gr \in \pi^{-1}(C) = M$ et

$$g = y^m(y^{-m}gr)r^{-1} \in < y > MN =< y > H;$$

donc

$$G =< y > H \ .$$

Supposons maintenant que $y^s \in H$ pour un $s \in \mathbf{Z}$; alors

$$\bar{y}^s = \bar{y^s} = \pi(y^s) \in \pi(MN) \subseteq BC = C \times B \subseteq A \times B \ ,$$

d'où $\bar{y}^s \in C$ (car l'ordre de $\bar{y}^s$ est une puissance de p), puis $\bar{y}^s = \bar{1}$. Mais cela signifie que $\omega(y) = \omega(\bar{y})$ divise s, donc $y^s = 1$.

Nous venons de montrer que

$$< y > \cap H = \{1\} \ ;$$

y étant central dans G, il s'ensuit que

$$G =< y > \times H$$

et $< y >$ est un facteur direct abélien non–trivial de G, contrairement à l'hypothèse.

Nous avons établi que $Aut(G)$ contenait un sous–groupe d'ordre $|Hom(G, Z(G))|$; mais, comme précédemment observé, un homomorphisme de G dans $Z(G)$ doit être trivial sur G', et $Hom(G, Z(G))$ s'identifie donc à $Hom(\frac{G}{G'}, Z(G))$. ***cqfd***

Théorème 5. *Soit G un groupe fini abélien ; alors*

$$|Aut(G)| \geqslant \phi(|G|)$$

Démonstration

Nous suivrons le raisonnement de Wilson ([4], p.2).

Supposons d'abord $|G| = p^n$ (p premier, $n \geqslant 1$), et soit $p^r = e(G)$ l'*exposant* de G :

$$p^r = \max\{\omega(x) | x \in G\}.$$

Si x et y sont deux éléments de G d'ordre p^r, il résulte du théorème de structure des groupes commutatifs finis l'existence de deux sous–groupes H_1 et H_2 de G tels que $G =< x > \times H_1$, $G =< y > \times H_2$ et $H_1 \cong H_2$. Soit $\psi : H_1 \xrightarrow{\sim} H_2$ un isomorphisme ; alors $\beta : G \to G$ défini par

$$\forall n \in \mathbf{Z}\ \forall h_1 \in H_1\ \beta(x^m h_1) = y^m \psi(h_1)$$

définit un automorphisme de G tel que $\beta(x) = y$.

Le groupe $Aut(G)$ agit donc transitivement sur l'ensemble

$$\mathcal{O} := \{x \in G | \omega(x) = p^r\}\ .$$

Mais

$$G \setminus \mathcal{O} = \{x \in G | x^{p^{r-1}} = 1\}$$

est un sous–groupe strict de G, donc $|G \setminus \mathcal{O}| \leqslant \dfrac{|G|}{p}$, et

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

Soit $\mathcal{A} = C_{Aut(G)}(x)$; on a donc

$$\begin{aligned} \frac{|Aut(G)|}{|\mathcal{A}|} &= |\mathcal{O}| \\ &\geqslant p^{n-1}(p-1)\ , \end{aligned}$$

d'où

$$|Aut(G)| \geqslant p^{n-1}(p-1)|\mathcal{A}| \geqslant p^{n-1}(p-1)\ .$$

Soit maintenant G d'ordre $n = \prod_{i=1}^{k} p_i^{a_i}$ (les p_i étant premiers et deux à deux distincts, $a_i \geqslant 1$) ; alors on peut écrire G comme produit direct de sous–groupes

$$G = \prod_{i=1}^{r} G_i$$

avec $|G_i| = p_i^{a_i}$.

Alors

$$Aut(G) = Aut(\prod_{i=1}^{r} G_i)$$

contient (en fait, il coïncide avec) un sous–groupe isomorphe à

$$\prod_{i=1}^{r} Aut(G_i) \ .$$

Il en résulte que

$$\begin{aligned} |Aut(G)| &\geqslant |\prod_{i=1}^{r} Aut(G_i)| \\ &= \prod_{i=1}^{r} |Aut(G_i)| \\ &\geqslant \prod_{i=1}^{r} p_i^{a_i - 1}(p_i - 1) \end{aligned}$$

(d'après le résultat ci–dessus)

$$\begin{aligned} &= \phi(n) \\ &= \phi(|G|) \ . \end{aligned}$$

cqfd

Remarque Il est assez facile de voir que l'inégalité du Théorème 3.3 est stricte, sauf lorsque G est cyclique.

Corollaire 2. *Il existe une fonction croissante $h : \mathbf{N}^* \to \mathbf{N}^*$ telle que, pour tout groupe fini abélien G, l'on ait*

$$|G| \leqslant h(|Aut(G)|).$$

Démonstration Soit $n = |Aut(G)|$; d'après le Théorème 3.3,

$$\phi(|G|) \leqslant n.$$

Or, pour chaque $k \geqslant 1$, l'ensemble

$$\mathcal{E}_k := \{m \in \mathbf{N}^* | \phi(m) = k\}$$

est fini ; soit

$$e_k := \begin{cases} \max(\mathcal{E}_k) \text{ si } \mathcal{E}_k \neq \emptyset \\ 0 \text{ sinon} \ . \end{cases}$$

Il est clair que la fonction h définie par

$$h(n) = \max(e_1, ..., e_n)$$

convient.

cqfd

4. Démonstration du Théorème

Soit donc G un groupe fini, $|Aut(G)| = m$. Choisissons un facteur direct abélien E de G d'ordre maximal ; alors il existe un sous–groupe H de G tel que G soit le produit direct de E et de H. Par construction, H n'a aucun facteur direct abélien non trivial ; en conséquence (Théorème 3.2), l'ordre de $Hom(\frac{H}{H'}, Z(H))$ divise l'ordre de $Aut(H)$.

De plus, $Aut(G) = Aut(E \times H)$ contient un sous–groupe isomorphe à

$$Aut(E) \times Aut(H),$$

d'où

$$|Aut(E)||Aut(H)| \leqslant |Aut(G)| = m \ (***).$$

En particulier, $|Aut(E)| \leqslant m$, d'où (Corollaire 3.4), $|E| \leqslant h(m)$; de plus, $\frac{H}{Z(H)}$ est isomorphe au groupe $Int(H)$ des automorphismes intérieurs de H, lequel est un sous–groupe de $Aut(H)$. Il en résulte que $|\frac{H}{Z(H)}| \leqslant m$, donc, en vertu de la Proposition 3.1, $|H^{'}| \leqslant m^{2m^3}$. De plus

$$|H| \leqslant m|Z(H)| \ .$$

Appliquons maintenant le Corollaire 2.4 avec $A = \frac{H}{H'}$, $C = \frac{Z(H)H^{'}}{H'}$,

$B = Z(H)$ et $D = Z(H) \cap H^{'}$; il s'avère que

$$|\frac{Z(H)}{Z(H) \cap H'}| = |\frac{Z(H)H^{'}}{H'}|$$

divise $|Hom(\frac{H}{H'}, Z(H))|$, donc divise $|Aut(H)|$. En particulier

$$\begin{aligned} \frac{|Z(H)|}{|Z(H) \cap H'|} &\leqslant |Aut(H)| \\ &= m(\text{d'après (***)}) \ , \end{aligned}$$

et

$$\begin{aligned} |Z(H)| &\leqslant m|Z(H) \cap H^{'}| \\ &\leqslant m|H^{'}| \\ &\leqslant m.m^{2m^3} \\ &= m^{2m^3+1}. \end{aligned}$$

Donc $|H| \leqslant m^{2m^3+2}$, et

$$|G| = |E||H| \leqslant h(m)m^{2m^3+2} \ .$$

D'où le résultat avec

$$f(m) := m^{2m^3+2} h(m) \ .$$

cqfd

Remarque Il est facile d'établir l'existence d'une constante C telle que

$$\forall m \geqslant 2 \ h(m) \leqslant Cm \ln(m) \ ;$$

cela fournit une estimation du type

$$f(m) \leqslant Cm^{2m^3+3} \ln(m) \ .$$

Références

[1] J. E. Adney and Ti Yen *Automorphisms of a p–group*, Illinois J. Math. 9(1), 1965, 137–143.

[2] M. Aschbacher *Finite group theory*, Cambridge University Press, 1986.

[3] I. Kaplansky *Infinite abelian groups*, Ann Arbor, 1969.

[4] R. A. Wilson *Finite groups with small automorphism groups*, 2004 ; disponible à http ://www.maths.qmul.ac.uk/ raw/.