Quelques propriétés de certains groupes finis

Lemme 1

Si G un groupe fini non abélien dont tous les sous-groupes propres sont abéliens, G n'est pas simple.

Démonstration :

Dans la suite, si A désigna une partie de G, on notera $< A >_G$ le sous-groupe de G engendré par A.

On procède par l'absurde et on se donne un sous-groupe H de G maximal (comme on a supposé G non abélien, on en déduit que $\{1\} \subsetneq H$). Comme on a supposé G simple, on en déduit que H coincide avec son normalisateur (maximalité de H). Soit alors $x \in G \backslash H$. En utilisant le caractère abélien de H, on constate facilement que $xHx^{-1} \cap H$ est distingué dans $< xHx^{-1} \cup H >_G$. Comme $x \notin H$ et $N_G(H) = H$, on a

$$H \subsetneq < xHx^{-1} \cup H >_G \subset G$$

et à nouveau par maximalité de H, on a donc $< xHx^{-1} \cup H >_G = G$. Le sous-groupe $xHx^{-1} \cap H$ étant distingué dans G, on en déduit :

$$\forall x \notin H,\ xHx^{-1} \cap H = \{1\} \tag{1}$$

Considérons maintenant le sous-ensemble

$$S_H = \bigcup_{x \in G} xHx^{-1}$$

Si N désigne le nombre de conjugués de H, on a alors (avec (1)) :

$$\text{card}(S_H) = (|H| - 1)N + 1$$

et comme $N_G(H) = H$, on en déduit que $N = |G| \,/\, |H|$ et donc :

$$\text{card}(S_H) = |G| - |G| \,/\, |H| + 1. \tag{2}$$

Comme H est un sous-groupe propre de G, on a ainsi $\text{card}(S_H) < |G|$.

On se donne donc un élément $z \notin S_H$ et K un sous-groupe maximal de G contenant z. A nouveau, on constate facilement (caractère abélien de H et K) que $yKy^{-1} \cap xHx^{-1}$ est distingué dans $< yKy^{-1} \cup xHx^{-1} >_G$ et ce pour tout $(x, y) \in G$. Comme $z \notin y^{-1}xHx^{-1}y$, on a encore $< yKy^{-1} \cup xHx^{-1} >_G = G$ par maximalité de H et ainsi :

$$\forall (x, y) \in G,\ yKy^{-1} \cap xHx^{-1} = \{1\} \tag{3}$$

On va déduire de (3) une contradiction ; en effet, avec les mêmes notations que ci-dessus :

$$\begin{aligned}\operatorname{card}(S_K \cup S_H) &= \operatorname{card}(S_K) + \operatorname{card}(S_H) - \operatorname{card}(S_K \cap S_H) \\ &= (|G| - |G| / |K| + 1) + (|G| - |G| / |H| + 1) - 1 \text{ d'après (3)} \\ &= 2\,|G| - |G| / |K| - |G| / |H| + 1 \\ &\geq |G| + 1 \qquad (4)\end{aligned}$$

car H et K ne sont pas réduits à $\{1\}$. L'inégalité (4) étant manifestement absurde, on en déduit que G nest pas simple. □

Proposition 1
Soit G un groupe fini dont tous les sous-groupes propres sont abéliens. Le groupe G est alors résoluble.

Démonstration :

On procède par récurrence sur le cardinal de G. En effet, d'après le lemme 1 ci-dessus, le groupe G n'est pas simple si il n'est pas abélien (auquel cas il est trivialement résoluble). Soit donc H un sous-groupe distingué de G avec $1 \subsetneq H \subsetneq G$. Comme H est un sous-groupe propre de G, H est abélien donc en particulier résoluble. De plus, le groupe G/H vérifie encore les hypothèses de l'énoncé et il est de cardinal strictement inférieur à celui de G : il est donc également résoluble et G avec lui. □

Proposition 2
Soit G un groupe fini de cardinal n. Si n et $\varphi(n)$ sont premiers entre eux, G est cyclique.

Exemple :
Tout groupe d'ordre 15, 33, 35, 51, 95, 255,... est cyclique.

Démonstration :

On remarque que l'hypothèse faite sur n entraine facilement :

$$n = p_1 p_2 \dots p_r.$$

De plus, tout entier m s'écrivant

$$m = p_{i_1} \dots p_{i_l} \text{ avec } \{i_1, \dots, i_l\} \subset \{1, \dots, r\}$$

vérifie également $m \wedge \varphi(m) = 1$. On va donc raisonner par récurrence sur r (le cas $r = 1$ étant trivial). Soit donc G un groupe de cardinal n. Par

hypothèse de récurrence, tous les sous-groupes propres de G sont cycliques et, en appliquant la proposition 1, on en déduit que G est résoluble. Il admet donc un quotient strict Q et, avec la remarque ci-dessus, ce dernier est donc cyclique (par hypothèse de récurrence). En particulier, Q admet $\mathbb{Z}/p_i\mathbb{Z}$ (pour au moins un indice i) comme quotient ; pour fixer les idées, on supposera que $i = r$. Comme Q est lui-même un quotient de G, on a donc une suite exacte :

$$1 \longrightarrow H \longrightarrow G \longrightarrow \mathbb{Z}/p_r\mathbb{Z} \longrightarrow 1 \tag{5}$$

dans laquelle H est un groupe de cardinal $p_1 \dots p_{r-1}$; ce dernier est donc encore cyclique. En utilisant à nouveau le théorème de Cauchy, on peut trouver un élément g_r d'ordre p_r dans G qui fournit donc une section pour la projection $G \longrightarrow \mathbb{Z}/p_r\mathbb{Z}$. La suite exacte (5) montre que G s'écrit alors comme un produit semi-direct :

$$G \simeq H \rtimes_\psi \mathbb{Z}/p_r\mathbb{Z} \tag{6}$$

correspondant à un morphisme

$$\psi : \mathbb{Z}/p_r\mathbb{Z} \longrightarrow \mathrm{Aut}(H).$$

Comme H est isomorphe à $\mathbb{Z}/(p_1 \dots p_{r-1})\mathbb{Z}$, $\mathrm{Aut}(H)$ est de cardinal

$$\mathrm{Card}(\mathrm{Aut}(H)) = (p_1 - 1) \dots (p_{r-1} - 1)$$

et comme p_r et $(p_1 - 1) \dots (p_{r-1} - 1)$ sont premiers entre eux, le morphisme ψ est nécessairement trivial. Le produit semi-direct (6) est donc direct et l'application du théorème chinois montre que :

$$G \simeq H \times \mathbb{Z}/p_r\mathbb{Z} \simeq \mathbb{Z}/(p_1 \dots p_{r-1})\mathbb{Z} \times \mathbb{Z}/p_r\mathbb{Z} \simeq \mathbb{Z}/(p_1 \dots p_r)\mathbb{Z}$$

et G est donc cyclique. □

Remarque 1
On constate facilement que si n n'est pas de la forme ci-dessus (sans facteur carré et p_i ne divise pas $p_j - 1$ pour tout (i, j)), il existe des groupes de cardinal n non cycliques. En effet, si n admet un facteur carré p^2, on construit un produit avec un facteur de la forme $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Si $p < q$ sont deux entiers premiers avec p diviseur de $q-1$, on a alors un morphisme non trivial

$$\psi : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/(q-1)\mathbb{Z} \simeq \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$$

qui donne un produit semi-direct non abélien.

Proposition 3
Soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ un entier. On suppose que n vérifie :

$$\begin{cases} \forall 1 \leq i \leq r,\ \alpha_i = 1 \text{ ou } 2 \\ \forall (i,j),\ p_i \text{ ne divise pas } p_j - 1 \\ \alpha_i = 2 \Longrightarrow \forall j,\ p_j \text{ ne divise pas } p_i + 1 \end{cases}$$

Tout groupe G d'ordre n est alors abélien.

Démonstration :

On procède par récurrence en remarquant que tout sous-groupe et tout quotient d'une tel groupe G a un cardinal qui répond encore à l'énoncé. En particulier, tous les sous-groupes propre de G sont abéliens et, d'après la proposition 1, ce dernier est résoluble. Si Q désigne un quotient strict de G, Q est abélien et est en particulier le produit direct de ses sous-groupes de Sylow. Comme ceux-ci sont de la forme $\mathbb{Z}/p^\alpha\mathbb{Z}$ ou $(\mathbb{Z}/p\mathbb{Z})^\alpha$ (avec $\alpha = 1$ ou 2), on peut à nouveau supposer que G a $\mathbb{Z}/p_r\mathbb{Z}$ pour quotient. Si H désigne le noyau de la projection $G \longrightarrow \mathbb{Z}/p_r\mathbb{Z}$, G est encore le produit semi-direct de H par $\mathbb{Z}/p_r\mathbb{Z}$. Ce produit est associé à un morphisme :

$$\psi : \mathbb{Z}/p_r\mathbb{Z} \longrightarrow \mathrm{Aut}(H).$$

En utilisant à nouveau le fait que H est abélien et le théorème chinois, on se ramène à l'étude de

$$\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}),\ \mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \text{ et } \mathrm{Aut}\big((\mathbb{Z}/p\mathbb{Z})^2\big)$$

Ces groupes sont respectivement isomorphes à

$$\mathbb{Z}/(p-1)\mathbb{Z},\ \mathbb{Z}/p(p-1)\mathbb{Z} \text{ et } GL_2(\mathbb{Z}/p\mathbb{Z})$$

et sont donc de cardinaux respectifs $p-1$, $p(p-1)$ et $p(p-1)^2(p+1)$. Comme p_r ne divise aucun de ces nombres, le morphisme ψ est nécessairement trivial : le produit est donc direct et le groupe G abélien. □

Remarque 2
A nouveau, on constate que si n n'est pas de cette forme, il existe des groupes d'ordre n qui ne sont pas abéliens. En effet, si $n = p^3$, on peut considérer le groupe G formé par les matrices de la forme :

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \text{ avec } (x,y,z) \in (\mathbb{Z}/p\mathbb{Z})^3$$

Le groupe G est un sous-groupe non abélien de $GL_3(\mathbb{Z}/p\mathbb{Z})$. De même, si $n = pq$ avec p diviseur de $q - 1$, il existe un produit semi-direct non trivial (donc non abélien). Enfin, si $n = p^2q$ avec q diviseur de $p + 1$, il existe un groupe G réalisé comme produit semi-direct :

$$1 \longrightarrow (\mathbb{Z}/p\mathbb{Z})^2 \longrightarrow G \longrightarrow \mathbb{Z}/q\mathbb{Z} \longrightarrow 1$$

non abélien.

Remarque 3
Dans le style "botanique", on peut donc dire que tout groupe G d'ordre

$$\begin{aligned}|G| =& 2, 3, 4, 5, 7, 9, 11, 13, 15, 17, 19, 23, 25, 29, 31, 33, 35, 37, 41, 43, 45,\\ & 47, 49, 51, 53, 57, 59, 65, 69, 77, 79, 83, 85, 87, 89, 91, 95, 97, 99\end{aligned}$$

est abélien.