Groupes d'ordre pq

Florian BOUGUET

Références :
– PERRIN : Cours d'algèbre (un peu)

Un développement pas trop compliqué sur la structure des groupes d'ordre pq. Il fait cependant appel à la notion de produit semi-direct, qu'il est bon d'avoir revue avant le jour J.

Theorème 1

Considérons G un groupe d'ordre pq, où p et q sont premiers distincts
Alors G n'a que deux structures possibles.

Preuve :

Mon énoncé n'étant peut-être pas le plus clair du monde, prenons le temps de bien le reformuler. En d'autres termes, tous les groupes d'ordre pq non-isomorphes à $\mathbb{Z}/(pq)\mathbb{Z}$ (qui est un groupe évident d'ordre pq) sont isomorphes entre eux.

Soient donc p et q deux nombres premiers distincts ; on peut supposer que $p < q$. Posons G d'élément neutre e un groupe d'ordre (i.e. de cardinal)

$$|G| = pq$$

D'après le théorème de CAUCHY, il existe H et N deux sous-groupes de G d'ordres respectifs p et q (les notations ne sont pas choisies au hasard, on ne va pas tarder à démontrer que N est distingué). Ces sous-groupes sont donc respectivement isomorphes à $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$.

Intéressons-nous aux q-Sylow de G. D'après le théorème de SYLOW, en notant n_q le nombre de q-Sylow de G on a

$$\begin{aligned} n_q &\equiv 1[q] \\ n_q &\text{ divise } p \end{aligned}$$

Puisque $p \leq q$, la seule possibilité est $n_q = 1$. D'autre part, toujours d'après le théorème de SYLOW, les q-Sylow sont d'ordre q et conjugués entre eux. En mettant bout à bout tous les arguments, l'unique q-Sylow de G est N et il est distingué. Enfin $|G| = |N||H|$ et par primalité $N \cap H = e$. On a donc on a un produit semi-direct via le morphisme $\varphi : H \to \text{Aut}(N)$:

$$N \rtimes_\varphi H \approx G$$

On rappelle que la loi d'un tel produit semi-direct est

$$(n, h) \cdot_\varphi (n', h') = \left(n\varphi(h)(n'), hh'\right) \qquad \text{pour } n, n' \in N \text{ et } h, h' \in H$$

Remarquons d'abord que

$$\text{Aut}(N) \approx \text{Aut}(\mathbb{Z}/q\mathbb{Z}) \approx (\mathbb{Z}/q\mathbb{Z})^* \approx \mathbb{Z}/(q-1)\mathbb{Z} \qquad \text{(voir par exemple PERRIN)}$$

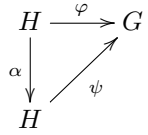
Soit x un élément de H distinct de e. $\text{ord}(x) = p$ car H est d'ordre p. Donc $(\varphi(x))^p = 1$. On en arrive donc aux deux cas suivants :

► 1er cas : si p ne divise pas $(q-1)$
Ce cas est le plus facile, car $\text{ord}(\varphi(x)) = 1$ ou p et p ne divise pas $(q-1)$. Donc $\text{ord}(\varphi(x)) = 1$ pour tout $x \in H$, donc φ est le morphisme trivial. Autrement dit, notre produit semi-direct est direct et

$$G \approx \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{q\mathbb{Z}} \approx \frac{\mathbb{Z}}{(pq)\mathbb{Z}} \qquad \text{par le lemme chinois}$$

► 1er cas : si p divise $(q-1)$
Les choses se compliquent un peu. On peut désormais construire des morphismes non-triviaux réalisant un "vrai" produit semi-direct $N \rtimes_\varphi H$. Attention, cela dépend quand même de la structure du groupe et ne veut pas dire que tous les morphismes sont non-triviaux (pour preuve, $\mathbb{Z}/6\mathbb{Z}$ existe). Terminons alors la preuve du théorème en montrant que si φ et ψ sont non-triviaux, alors ils réalisent le même produit semi-direct.

$\ker\varphi$ est un sous-groupe de H et $\ker\varphi \neq H$ (car φ n'est pas trivial). Donc $\ker\varphi = \{e\}$, et donc $\varphi(H) = G_p$, où G_p est l'unique sous-groupe de N d'ordre p. Le raisonnement s'applique aussi à ψ ce qui nous donne le diagramme commutatif suivant :



α étant un isomorphisme, on a la bijection suivante :

$$\begin{array}{rccc} \theta: & N \rtimes_\varphi H & \to & N \rtimes_\psi H \\ & (n,h) & \mapsto & (n, \alpha(h)) \end{array}$$

Nous arrivons à la dernière partie de la preuve, où il reste à montrer que θ est bien un morphisme :

$$\begin{array}{rcl} \theta\big((n,h) \cdot_\varphi (n',h')\big) & = & \theta\big((n\varphi(h)(n'), hh')\big) \\ & = & (n\varphi(h)(n'), \alpha(hh')) \\ \theta\big((n,h)\big) \cdot_\psi \theta\big((n',h')\big) & = & \big(n, \alpha(h)\big) \cdot_\psi \big(n', \alpha(h')\big) \\ & = & (n\psi(\alpha(h))(n'), \alpha(h)\alpha(h')) \end{array}$$

On a égalité, car $\varphi = \psi \circ \alpha$ et α est un morphisme.

□

Remarques :

On a donc conclut que deux groupes d'ordre pq sont isomorphes si ils ne sont pas isomorphes à $\mathbb{Z}/(pq)\mathbb{Z}$. Un tel résultat peut alors permettre d'affirmer sans autre forme de procès que D_3 et $\mathfrak{S}_3$ sont isomorphes, car ni l'un ni l'autre ne possède d'élément d'ordre 6.