Structure des groupes d'ordre pq

Théorème 1. *Soient p, q deux nombres premiers tels que $p < q$ et G un groupe d'ordre pq. Alors :*

- *Si $p \nmid q-1$, G est cyclique et $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, par exemple pour $pq = 15, 35, 51, \ldots$*
- *Si $p \mid q-1$, il y a (à isomorphisme près) deux groupes d'ordre pq. Le groupe G est soit cyclique avec $G \simeq \mathbb{Z}/pq\mathbb{Z}$, ou bien G est non abélien isomorphe à un produit* semi-direct *non commutatif.*

Corollaire 1. *Pour $p = 2$, on a à isomorphismes près deux groupes d'ordre $2q$, le groupe cyclique $\mathbb{Z}/2q\mathbb{Z}$ et un produit semi-direct qui est isomorphe au groupe diédral D_q.*

Démonstration. :
Etape 1 : commençons par montrer que G est nécessairement isomorphe à un produit semi-direct $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. Comme $p \mid \text{card}(G)$ et $q \mid \text{card}(G)$, G admet un p-Sylow et un q-Sylow. En particulier d'après les théorèmes de Sylow, le nombre de q-sylow k_q vérifie :

$$k_q \equiv 1\,[q] \text{ et } k_q \mid p.$$

Alors, $k_q \neq p$ car sinon on aurait $q \mid p-1$ avec $q > p > p-1$, absurde. D'où nécessairement $k_q = 1$ et il n'y a qu'un seul q-sylow de G noté Q, qui est donc distingué dans G. On en déduit donc que G/Q est muni d'une structure de groupe avec $\text{card}(G/Q) = \frac{\text{card}(G)}{\text{card}(Q)} = p$ soit $G/Q \simeq \mathbb{Z}/p\mathbb{Z}$. On a donc la suite exacte :

$$1 \mapsto Q \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} G/Q \mapsto 1$$

où $i : P \hookrightarrow G$ est l'injection canonique et $\pi : G \twoheadrightarrow G/Q$ la surjection canonique.

Objectif 1. *Trouver un relèvement de la suite exacte à l'aide d'un p-sylow de G.*

On note P un p-sylow de G et $\pi_{|P}$ la restriction à P de la surjection canonique π et on va montrer que $\pi_{|P}$ un un isomorphisme. Pour ce faire comme $\text{card}(P) = \text{card}(G/Q)$, il suffit de montrer que $\pi_{|P}$ est injective. Or, $\text{Ker}(\pi_{|P}) = P \cap \text{Ker}(\pi) = P \cap Q$, il s'agit donc de prouver que $P \cap Q = \{1\}$. Soit $x \in P \cap Q$, on a en particulier $\text{ordre}(x) \mid p$ et $\text{ordre}(x) \mid q$ où $p \wedge q = 1$, d'où $x = 1$. On a donc l'existence d'un sous-groupe P de G tel que $\pi_{|P}$ soit une bijection, ie l'existence d'un relèvement de la suite exacte. Ainsi, G est *isomorphe à un produit semi-direct* de la forme $Q \rtimes_\phi G/Q$ et par cardinalité, on a l'isomorphisme :

$$G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}$$

où $\phi : \mathbb{Z}/p\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ est un morphisme qui détermine la loi de groupe $+$ sur l'ensemble cartésien $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, via $(k_1, l_1) + (k_2, l_2) = (k_1 + \phi(l_1)(k_2), l_1 + l_2)$.

Lemme 1. *Soit $n \in \mathbb{N}^*$, $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$*

Démonstration. $u \in \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ est entièrement déterminé par l'image de $\overline{1}$ qui génère $\mathbb{Z}/n\mathbb{Z}$. Pour construire un automorphisme il suffit d'envoyer $\overline{1}$ sur un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$, *ie* un élément de $(\mathbb{Z}/n\mathbb{Z})^*$. On définit alors l'application $\Phi : \text{Aut}(\mathbb{Z}/n\mathbb{Z}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ associant à u, l'élément $u(\overline{1})$ et on définit $\Psi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ par $\Psi(\overline{k}) : \overline{s} \longrightarrow \overline{k}\overline{s}$. Il est facile de vérifier que Ψ est bien à valeurs dans $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ et ensuite que Ψ et Φ sont des morphismes réciproques l'un de l'autre, ie :

$$\Phi \circ \Psi = \text{Id}_{(\mathbb{Z}/n\mathbb{Z})^*} \text{ et } \Psi \circ \Phi = \text{Id}_{\text{Aut}(\mathbb{Z}/n\mathbb{Z})},$$

□

Etape 2 : étudions les morphismes de $\mathbb{Z}/p\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^* \simeq (\mathbb{Z}/(q-1)\mathbb{Z}, +)$ pour comprendre la structure de produits semi-directs. On distingue alors les cas $q \not\equiv 1[p]$ et $q \equiv 1[p]$.

1) Supposons $q \not\equiv 1[p]$. Le nombre de p-sylow vérifie $k_p \equiv 1[p]$ et $k_p \mid q$ et donc $k_p \neq q \Longrightarrow k_p = 1$. D'où, l'unique p-sylow est distingué, tout comme l'unique q-sylow, ce qui donne une structure de produit direct.

2) Supposons $q \equiv 1[p]$. Un morphisme $\theta : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/(q-1)\mathbb{Z}$ est entièrement déterminé par l'image du générateur $\overline{1}$ qui est d'ordre p et par le théorème de Lagrange $\text{card}(\text{Ker}(\theta)) \mid p$ soit $\text{card}(\text{Ker}(\theta)) \in \{1, p\}$. Alors :

- Si $\text{card}(\text{Ker}(\theta)) = p$, alors $\text{Ker}(\theta) = \mathbb{Z}/p\mathbb{Z}$ et θ est le morphisme trivial, ce qui donne une structure de *produit direct*.
- Si $\text{card}(\text{Ker}(\theta)) = 1$, le morphisme $\theta : \mathbb{Z}/p\mathbb{Z} \longrightarrow \text{Im}(\theta)$ est isomorphisme et donc $\text{Im}(\theta)$ est un sous-groupe de cardinal p de $\mathbb{Z}/(q-1)\mathbb{Z}$. Comme il y a un unique sous-groupe de cardinal p dans $\mathbb{Z}/(q-1)\mathbb{Z}$ noté Γ, le morphisme $\theta : \mathbb{Z}/p\mathbb{Z} \longrightarrow \Gamma$ est un isomorphisme et θ est *entièrement déterminé* par le choix de $\theta(\overline{1})$ que l'on doit choisir parmi les $p-1$ générateurs de Γ.

Objectif 2. *montrer que pour θ_1 et θ_2 deux isomorphismes de $\mathbb{Z}/p\mathbb{Z}$ dans Γ, les produits semi-directs associés sont isomorphes ie : $\mathbb{Z}/q\mathbb{Z} \times_{\theta_1} \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z} \times_{\theta_2} \mathbb{Z}/p\mathbb{Z}$*

On pose $\alpha = \theta_2^{-1} \circ \theta_1 \in \text{Aut}(\mathbb{Z}/p\mathbb{Z})$ et on vérifie alors que :

$$\Theta : \begin{array}{ccc} \mathbb{Z}/q\mathbb{Z} \rtimes_{\theta_1} \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathbb{Z}/q\mathbb{Z} \rtimes_{\theta_2} \mathbb{Z}/p\mathbb{Z} \\ (k_1, l_1) & \longmapsto & (k_1, \alpha(l_1)) \end{array}$$

donne l'isomorphisme attendu. Il suffit de montrer par cardinalité que l'application Θ est un morphisme de groupe, injectif. On a :

$$\begin{aligned} \Theta((k_1,l_1)+(k_2,l_2)) &= \Theta(k_1+\theta_1(l_1)(k_2), l_1+l_2) \\ &= (k_1+\theta_1(l_1)(k_2), \alpha(l_1+l_2)) \\ &= (k_1+\theta_1(l_1)(k_2), \alpha(l_1)+\alpha(l_2)) \\ &= (k_1+\theta_2(\alpha(l_1))(k_2), \alpha(l_1)+\alpha(l_2)) \end{aligned}$$

car $\theta_2 \circ \alpha = \theta_1$ et :

$$\begin{aligned} \Theta((k_1,l_1)) + \Theta((k_2,l_2)) &= (k_1, \alpha(l_1)) + (k_2, \alpha(l_2)) \\ &= (k_1+\theta_2(\alpha(l_1))(k_2), \alpha(l_1)+\alpha(l_2)) \end{aligned}$$

Ce qui donne bien $\Theta((k_1,l_1)+(k_2,l_2)) = \Theta((k_1,l_1)) + \Theta((k_2,l_2))$ pour les lois $+$ des deux produits semi-directs. Enfin l'injectivité est immédiate, on a en effet :

$\Theta(k_1,l_1) = (0,0) \Longleftrightarrow (k_1, \alpha(l_1)) = (0,0) \Longleftrightarrow k_1 = 0, l_1 = 0$ car α est un automorphisme.

Ce qui prouve bien le résultat attendu. □

Rappel 1. *Tout sous-groupe d'un groupe cyclique est cyclique. Plus précisément pour $n > 1$:*
- *Tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique engendré par la classe $\overline{b}$ d'un élément b tel que $b \mid n$ et $< \overline{b} >$ est d'ordre $\frac{n}{d}$.*
- *Pour $a > 0$ un diviseur de n, on note $b = \frac{n}{a}$. Il existe alors un et un seul sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre a. Ce sous-groupe est engendré par $\overline{b}$ et est formé de l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ dont l'ordre divise a.*

Rappel 2. *Soit G un groupe de cardinal $n = p^\alpha m$ où $p \nmid m$. Alors :*
- *Les p-sylow de G sont tous conjugués.*
- *Le nombre k_p de p-sylow vérifie $k_p \equiv 1\,[p]$ et $k_p \mid m$.*
- *P est l'unique p-sylow de $G \Longleftrightarrow k_p = 1 \Longleftrightarrow P$ est distingué dans G.*

Rappel 3. *Soient N, G et H des groupes tels qu'il existe une suite exacte :*

$$1 \mapsto N \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} H \mapsto 1$$

S'il existe un sous-groupe de G noté $\overline{H}$ tel que $\pi_{|\overline{H}} : \overline{H} \longrightarrow H$ soit un isomorphisme, alors G est isomorphe à un produit semi-direct $N \rtimes_\phi H$ où ϕ désigne un morphisme de H sur $Aut(N)$ qui permet de définir la loi de groupe sur l'ensemble produit $N \times H$ par :

$$(n,h).(n',h') = (n\phi(h)(n'), hh').$$

Références :
- Cours d'algèbre. Daniel Perrin. Page 27-28 pour le développement mais beaucoup moins détaillé et page 19, 22 et 24 pour les rappels sur les théorèmes de Sylow et le produit semi-direct.
- Combes pour le développement.
- Boyer et Risler : algèbre pour la licence 3, pour le rappel sur les sous-groupes des groupes cycliques.