Classification des groupes d'ordre pq

Référence : [Per96] p.27-28.

Théorème 0.1 *Soient p et q deux nombres premiers avec $p < q$. Alors :*

1. *Si p ne divise pas $q-1$, tout groupe d'ordre pq est cyclique et isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.*
2. *Si p divise $q-1$, il y a deux groupes d'ordre pq non isomorphes, le groupe cyclique et un produit semi-direct non commutatif.*

Démonstration Soit G un groupe d'ordre pq.
$\rightsquigarrow$ D'après le théorème de Sylow, on sait qu'il existe des q-Sylow de G, soit Q l'un d'entre eux. On sait aussi d'après le théorème de Sylow, que le nombre n_q de q-Sylow vérifie :

$$\begin{aligned} &n_q = 1[q] \\ &n_q | p \end{aligned}$$

p étant premier, on a $n_q = 1$ ou p, or $n_q = 1[q]$, d'où $n_q = 1$ (car $p < q$).
Ainsi il existe un unique q-Sylow dans G, de plus d'après le théorème de Sylow, tous les q-Sylow sont conjugués entre eux, or Q est tout seul, il est donc distingué dans G.
De plus comme q est premier, on sait que G est isomorphe à $\mathbb{Z}/q\mathbb{Z}$.
$\rightsquigarrow$ De la même façon, on sait que G contient des p-Sylow et leur nombre n_p vérifie :

$$\begin{aligned} &n_p = 1[p] \\ &n_p | q \end{aligned}$$

Donc $n_p = 1$ ou q. Notons P un p-Sylow. On a :

- $P \cap Q = \{e\}$, car sinon il existerait $a \in P \cap Q$, ie $a \in P$ et $a \in Q$, or Q est d'ordre q et P est d'ordre p (d'après le théorème de Sylow), donc l'ordre de a doit diviser p et q (d'après le théorème de Lagrange), ie nécessairement l'ordre de a est 1, ie $a^1 = e$, ie $a = e$.
- $|P| \times |Q| = pq = |G|$.
- Q distingué dans G.

Donc d'après le propriété du produit semi-direct, on sait qu'il va exister un produit semi-direct entre P et Q, ie $Q \rtimes_\phi P$, on a donc l'existence d'un morphisme :

$$\begin{aligned} \phi : P &\longrightarrow Aut(Q) = Aut(\mathbb{Z}/q\mathbb{Z}) \\ \overline{a} &\longmapsto f_a \end{aligned}$$

De plus, comme q est premier, on sait que $Aut(\mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$.
Soit $a \in \mathbb{Z}/p\mathbb{Z}$, alors $pa = 0$, d'où $\phi(ap) = \phi(0) = id$, or $\phi(ap) = \phi(a)^p = id$ (car ϕ est un morphisme de groupes d'un groupe additif $(\mathbb{Z}/p\mathbb{Z})$ dans un groupe multiplicatif $Aut(\mathbb{Z}/q\mathbb{Z})$), donc $\phi(a)$ est d'ordre qui divise p, donc l'ordre de $\phi(a)$ est 1 ou p (car p premier).
De plus, l'ordre de $\phi(a)$ divise aussi l'ordre du groupe $Aut(\mathbb{Z}/q\mathbb{Z})$, qui est $q-1$ d'après le théorème de Lagrange, donc on peut distinguer deux cas :

- Si p ne divise pas $q-1$, alors l'ordre de $\phi(a)$ est 1 pour tout $a \in \mathbb{Z}/p\mathbb{Z}$, ie $\phi(a)^1 = id$, donc ϕ est le morphisme trivial et l'opération du produit semi-direct s'écrit pour $(p,q),(p',q') \in \mathbb{Z}/p\mathbb{Z} \ltimes_\phi \mathbb{Z}/q\mathbb{Z}$:

  $$(p,q).(p',q') = (pp', q\phi(p)(q')) = (pp', qid(q')) = (pp', qq')$$

  on reconnaît alors la loi de groupe du produit direct, d'où G isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ qui est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$ d'après le théorème Chinois.

– Si p divise $q-1$, alors $\mathbb{Z}/(q-1)\mathbb{Z}$ admet un unique sous-groupe d'ordre p, donc $Aut(\mathbb{Z}/q\mathbb{Z})$ aussi, notons son sous-groupe d'ordre p, H.
Considérons maintenant l'image de ϕ, c'est un sous-groupe de $Aut(\mathbb{Z}/q\mathbb{Z})$ et ce sous-groupe est de cardinal 1 ou p (d'après ce qu'on vient de faire sur l'ordre d'un élément du groupe $\mathbb{Z}/p\mathbb{Z}$, qui suggère que soit tous les éléments de $Aut(\mathbb{Z}/q\mathbb{Z})$ sont d'ordre 1, soit il existe un élément d'ordre p dans $Aut(\mathbb{Z}/q\mathbb{Z})$ et cet élément engendre alors un sous-groupe d'ordre p).
De plus on a une surjection de $\mathbb{Z}/p\mathbb{Z} \longrightarrow Im(\phi)$, donc $|Im(\phi)| \leq p$.
On distingue de nouveau deux cas :
– Si $|Im(\phi)| = 1$, alors $Im(\phi) = \{id\}$ car c'est un groupe et on retrouve le morphisme trivial, par conséquent G est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.
– Si $|Im(\phi)| = p$, par unicité du sous-groupe d'ordre p dans $Aut(\mathbb{Z}/q\mathbb{Z})$, on a $H = Im(\phi)$.
On considère un autre morphisme :

$$\psi : \mathbb{Z}/p\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/q\mathbb{Z})$$

ie un autre produit semi-direct, montrons alors que ϕ et ψ sont isomorphes.
De même, on peut montrer que $H = Im(\psi)$, ainsi on peut considérer les morphismes :

$$\overline{\phi} : \mathbb{Z}/p\mathbb{Z} \longrightarrow Im(\phi) = H$$
$$\overline{\psi} : \mathbb{Z}/p\mathbb{Z} \longrightarrow Im(\psi) = H$$

Ce sont des morphismes bijectifs, car surjectifs, puisqu'on a restreint les morphismes ϕ et ψ à leur image et bijectif, car $|\mathbb{Z}/p\mathbb{Z}| = |H| = p$.
Ainsi si on pose $\alpha = \overline{\psi}^{-1} \circ \overline{\phi}$, alors l'application :

$$\begin{aligned} f : \mathbb{Z}/p\mathbb{Z} \ltimes_\phi \mathbb{Z}/q\mathbb{Z} &\longrightarrow \mathbb{Z}/p\mathbb{Z} \ltimes_\psi \mathbb{Z}/q\mathbb{Z} \\ (p,q) &\longmapsto (\alpha(p), q) \end{aligned}$$

est un isomorphisme de groupes ; en effet, soient $(p,q), (p',q') \in \mathbb{Z}/p\mathbb{Z} \ltimes_\phi \mathbb{Z}/q\mathbb{Z}$:
– Montrons que f est un morphisme de groupes :

$$f((p,q).(p',q')) = f(pp', q\phi(p)(q')) = (\alpha(pp'), q\phi(p)(q'))$$
$$f(p,q).f(p',q') = (\alpha(p),q).(\alpha(p'),q') = (\alpha(p)\alpha(p'), q\psi(\alpha(p))(q)q') = (\alpha(pp'), q\phi(p)(q'))$$

– Comme $|\mathbb{Z}/p\mathbb{Z} \ltimes_\phi \mathbb{Z}/q\mathbb{Z}| = |\mathbb{Z}/p\mathbb{Z} \ltimes_\psi \mathbb{Z}/q\mathbb{Z}| = pq$, alors il suffit de montrer l'injectivité de f, soit $(p,q) \in \mathbb{Z}/p\mathbb{Z} \ltimes_\phi \mathbb{Z}/q\mathbb{Z}$ tels que $f(p,q) = (0,0)$. Alors $\alpha(p) = 0$ et $q = 0$, ie $\psi^{-1} \circ \phi(p) = 0$, ie $\phi(p) = \psi(0) = 0$, ie $p = \phi^{-1}(0) = 0$.
D'où l'isomorphisme.

Lemmes utilisés

Lemme 0.1 (Théorème de Sylow) *Soit G un groupe de cardinal $|G| = n = p^\alpha m$ avec p premier et m ne divisant pas p. Alors :*

1. *Si H est un sous-groupe de G qui est un p-groupe alors il existe un p-Sylow S tel que $H \subset S$;*
2. *Les p-Sylow sont tous conjugués dans G (et donc leur nombre k divise n) ;*
3. *On a $k \equiv 1[p]$ (donc k divise m).*

Démonstration cf le développement sur le théorème de Sylow.

Lemme 0.2 (Théorème de Lagrange) *Soit G un groupe fini de cardinal N. Alors $g^N = e$ pour tout $g \in G$ et le plus petit des entiers non nul n tel que $g^n = e$ divise le cardinal de G.*

Démonstration Soit $H = \{g^n, n \in \mathbb{N}\}$. H est un ensemble fini puisque G l'est. Donc $\exists a, b \in \mathbb{N}$ et $a > b$ tels que $g^a = g^b$, ie en multipliant par $(g^{-1})^b$, que $g^{a-b} = e$.
Soit t le plus petit entier tel que $g^t = e$.
Montrons maintenant que H est un sous-groupe de G.
– $H \subset G$, car $\forall g \in G$, $\forall n \in \mathbb{N}$, $g^n \in G$ car G groupe.
– soient $g^a, g^b \in H$, alors $g^a g^b = g^{a+b} \in H$.
– soit $g^a \in H$. Comme t est le plus petit entier tel que $g^t = e$. Alors g^{t-1} est l'inverse de g. D'où $g^{a(t-1)}$ est l'inverse de g^a et cet inverse est dans H.

Montrons que le cardinal de H est t. Soit n un entier, on effectue la division euclidienne de n par t, alors il existe $(q,r) \in \mathbb{N}^2$, tels que $n = tq + r$ et $0 \leq r < t$. Alors $g^n = g^{tq+r} = (g^t)^q g^r = g^r$.
Ainsi $H = \{1, g, g^2, \ldots, g^{t-1}\}$; mais $g^r = g^s$ avec $1 \leq r < s \leq t$, ainsi l'argument donné au début de cette preuve nous donne que $g^{s-r} = e$, ce qui contredit la minimalité de t. Ainsi H a t éléments et on conclut par le fait que le cardinal de H divise le cardinal de G.

Lemme 0.3 (Théorème Chinois) *Soient p et q deux entiers premiers entre eux. Alors :*

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

Démonstration On considère le morphisme :

$$\begin{aligned} \mathbb{Z}/pq\mathbb{Z} &\longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ \overline{n} &\longmapsto (\widehat{n}, \tilde{n}) \end{aligned}$$

Il est injectif car p et q sont premiers entre eux et bijectif par égalité des cardinaux. En effet si $(\widehat{n}, \tilde{n}) = (0,0)$ alors n divise p et n divise q, ie $n = kp = k'q$, or p et q sont premiers entre eux donc n divise pq, ie $n = cpq$, d'où $\overline{n} = 0$.

Lemme 0.4 (Admis, produit direct et semi-direct) *Soit G un groupe. Soient K, H des sous-groupes de G tels que $H \cap K = \{e\}$ et que $|H| \times |K| = |G|$.*

1. *Si H et K sont distingués dans G, alors $G \simeq H \times K$;*
2. *Si H est distingué dans G, alors il existe $\phi : K \longrightarrow Aut(H)$ tel que $G \simeq H \rtimes_\phi K$.*

Lemme 0.5 (Automorphisme de $\mathbb{Z}/n\mathbb{Z}$)

$$Aut(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$$

Démonstration
($\Rightarrow$) Soit $u \in Aut(\mathbb{Z}/n\mathbb{Z})$, alors $u(1)$ est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$. Donc $u(1) \in (\mathbb{Z}/n\mathbb{Z})^*$ et on vérifie que l'application $\tau : u \longmapsto u(1)$ est un morphisme.
($\Leftarrow$) Soit σ défini sur $(\mathbb{Z}/n\mathbb{Z})^*$ par $\sigma(s)(x) = sx$. $\sigma(s)$ est un endomorphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ car $s(x+y) = sx + sy$ et c'est un automorphisme car $sx = 0$ implique que $x = 0$ car s est inversible.
Enfin τ et σ sont réciproques l'un de l'autre.

Lemme 0.6 *$\mathbb{Z}/n\mathbb{Z}$ admet un unique sous-groupe d'ordre $\mathbb{Z}/d\mathbb{Z}$ avec d divisant n.*

Démonstration Comme d divise n, alors il existe $k \in \mathbb{Z}$ tel que $n = kd$, ainsi $k \in \mathbb{Z}/n\mathbb{Z}$ et est d'ordre d, car $kd = 0[n]$ et $\forall q < d$, $kq \neq 0[n]$.
On pose $K =< k >$ le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par k, il est de cardinal d.
Soit $K' =< k' >$ un autre sous-groupe de cardinal d dans $\mathbb{Z}/n\mathbb{Z}$ (il est bien cyclique, car $\mathbb{Z}/n\mathbb{Z}$ l'est). Alors $k'd = 0[n]$ et $\forall q < d$, $k'q \neq 0[n]$.
On a donc : $kd = n$ et $k'd = pn$ avec $p \in \mathbb{Z}$, d'où $k'd = pkd$, ie $k' = pk$ (car $\mathbb{Z}$ est intègre), donc $k' \in K$, d'où l'unicité du sous-groupe d'ordre d.

Références

[Per96] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.