GROUPES D'ORDRE pq.

par

Luc Abergel et Sylvain Arnt

On note Z_p le groupe $\mathrm{Z}/p\mathrm{Z}$. On veut construire les groupes d'ordre pq non monogènes (à isomorphisme près bien sûr). Dans toute la suite, on va considérer un groupe G d'ordre pq avec p, q premiers vérifiants $p \leq q$. On supposera également que G n'est pas cyclique. Il n'admet donc pas d'élément d'ordre pq.

1. Généralités.

On a déjà signalé que les éléments x de G avaient pour ordre 1 (si $x = 1$), p ou q mais jamais pq.

Proposition 1. — *Intersection de sous-groupes.*
Si x, y sont dans G avec x d'ordre p et y d'ordre q, alors :

- *Si $p \neq q$ alors $< x > \cap < y >= \{1\}$.*
- *Si $p = q$ alors soit $< x > \cap < y >= \{1\}$, soit $< x >=< y >$.*

Démonstration. —

- Pour le premier point, si $z \in < x > \cap < y >$, alors l'ordre de z divise p et q, il est donc égal à 1, ce qui montrer bien $z = 1$.
- Si $p = q$ et $z \in < x > \cap < y >$ avec $z \neq 1$. Alors z est d'odre p. Comme $< z > \subset < x >$ on conclut $< z >=< x >$ et de même $< z >=< y >$.

□

Proposition 2. — *G en tant qu'ensemble.*
Si x et y sont dans G d'ordre n et m avec $< x > \cap < y >= \{1\}$, alors G contient un sous-ensemble en bijection avec $Z_n \times Z_m$.

Démonstration. — Soit f l'application de $\mathrm{Z}_n \times \mathrm{Z}_m$ qui à (i, j) associe $x^i y^j$. Cette application est bien déinie du fait des relations $x^n = 1$ et $y^m = 1$. De plus elle est injective : si $x^i y^j = x^{i'} y^{j'}$ alors $x^{i-i'} = y^{j'-j} \in < x > \cap < y >= \{1\}$, donc $x^{i-i'} = y^{j'-j} = 1$ puis $i = i' \mod n$ et $j = j' \mod m$, ce qui donne bien l'inclusion souhaitée. □

Proposition 3. — *Unicité d'un sous-groupe d'ordre q si $p < q$.*
Si $p < q$ alors un éventuel sous-groupe d'ordre q est unique.

Démonstration. — Ceci se déduit des propositions précédentes. Si en effet $< x >$ et $< y >$ sont deux sous-groupes distincts d'ordre q, alors par la proposition 1, $< x > \cap < y >= \{1\}$ puis par la proposition 2, G contient une copie de $\mathrm{Z}_q \times \mathrm{Z}_q$ qui est de cardinal $q^2 > pq$. □

Proposition 4. — *G contient un élément d'odre p.*

Démonstration. — Si G n'en contenait pas alors comme il contient au plus un sous-groupe d'ordre q, il serait de cardinal au plus q ce qui est impossible. □

Proposition 5. — *Un cas simple où on peut conclure que G contient un élément d'ordre q.*
On suppose $p < q$. Si $p-1$ ne divise pas $q-1$ alors G contient un élément d'ordre q.

Démonstration. — En effet, sinon, G serait une union de sous-groupes d'ordre p n'ayant que 1 comme élément commun à deux d'entre eux. Ceci donnerait donc $\mathrm{card}(G) = k(p-1)+1 = pq$ et $p-1$ diviserait $pq-1$, soit $pq - 1 = 0 \mod p-1$ ou encore $q = 1 \mod p-1$. □

On va admettre que dans tous les cas il existe bien un élément d'odre q, ce qui est un résultat classique.

2. Construction de ces groupes.

2.1. Le cas $p < q$. — On se donne un groupe d'ordre pq avec p et q premiers et $p < q$. On sait que G contient un élément x d'ordre p, un élément y d'ordre q et surtout qu'il contient un unique sous-groupe d'ordre q, à savoir $< y >$. On va donc définir G par générateurs et relations.

- $G =< x, y >$.
- $x^p = 1$.
- $y^q = 1$.
- $xy = y^k x$ pour un $k \in \mathrm{Z}_q^*$.

Vérifions cette relation :

Du fait qu'il existe un unique sous-groupe d'ordre q et que xyx^{-1} est d'ordre divisant q, celui-ci est dans $< y >$ et il existe bien $k \in \mathbb{Z}_q^*$ tel que $xyx^{-1} = y^k$. Car si on avait $k = 0 \mod q$, alors on aurait $xy = x$, soit $y = 1$.

On vérifie alors les relations suivantes :

- $xy^\alpha = y^{k\alpha}x$ (par récurrence sur α).
- $x^\alpha y = y^{k^\alpha}x$ (par récurrence sur α).
- $x^\alpha y^\beta = y^{\beta k^\alpha}x^\alpha$ (par récurrence sur β).

De ce fait, en tant que groupe, G est isomorphe à $\mathrm{Z}_q \times \mathrm{Z}_p$ muni de la loi définie par

$$(\alpha, \beta) + (\alpha', \beta') = (\alpha + \alpha' k^\beta, \beta + \beta')$$

Cela provient des relations précédentes :

$$y^{\alpha}[x^{\beta}y^{\alpha'}]x^{\beta'} = y^{\alpha}y^{\alpha' k^{\beta}}x^{\beta+\beta'} = y^{\alpha+\alpha' k^{\beta}}x^{\beta+\beta'}$$

On peut aisement vérifier que cela confère bien une structure de groupe à G mais le point essentiel est de vérifier qu'elle est bien définie. Le fait de remplacer α par $\alpha + q$ ne change clairement pas la définition de la loi $+$. Par contre, pour que β et $\beta + p$ définissent la même opération, on doit avoir $k^p = 1 \mod q$. Comme $k \in \mathrm{Z}_q^*$, on en déduit que si p ne divise pas $q-1$, alors $k = 1$ et G n'est autre que le groupe $\mathbb{Z}_p \times \mathrm{Z}_q \simeq \mathrm{Z}_{pq}$ muni de la sa loi usuelle. Sinon, il y a p éléments $k \in \mathrm{Z}_q$ vérifiant $k^p = 1$, ce qui donne *a priori* p groupes possibles. Il reste à voir s'ils sont isomorphes ou non ce qui va être fait juste en dessous.

2.2. Le cas $p = q$. — On adapte la méthode précédente et on établit les mêmes résultats, à savoir

- $G =< x, y >$.
- $x^p = 1$.
- $y^p = 1$.
- $< x > \cap < y >= \{1\}$.
- $xy = y^k x$ pour un $k \in \mathrm{Z}_p^*$.

Démontrons l'existence de ce $k \in \mathrm{Z}_p^*$: On suppose par l'absurde que $xyx^{-1} \notin < y >$. Posons $z = xyx^{-1}$. Alors $z \neq 1$ donc z est d'ordre p et $< y > \cap < z >= \{1\}$ car $z \notin < y >$. Par suite, d'après la proposition 1, $G =< y, z >= \{y^i z^j \mid (i,j) \in \mathbb{Z}_p \times \mathbb{Z}_p\}$. Ainsi, comme $x^{-1} \in G$, il existe $i, j \in \mathbb{Z}_p$ tels que $x^{-1} = y^i z^j = y^i x y^j x^{-1}$ d'oú $x = y^{-i-j} \in < x > \cap < y >= \{1\}$, contradiction. Ainsi, il existe bien $k \in \mathbb{Z}_q$ tel que $xyx^{-1} = y^k$. Comme dans le cas $p < q$, $k = 0 \Rightarrow y = 1$ ce qui est impossible. Ainsi on a bien $k \in \mathbb{Z}_q^*$.

On a donc $G =< x, y >$ avec x et y d'ordre p. Là encore on dispose d'une relation $xy = y^k x$. Et de même $k^p = 1 \mod p$ ce qui donne $k = 1$. Le groupe est donc $\mathbb{Z}_p^2$. On retrouve ici le résultat classique disant qu'un groupe d'ordre p^2 est abelien.

3. Unicité.

On reprend ici la notation multiplicative d'un tel groupe qu'on suppose non monogène. On a donc $G =< x, y >$ avec x d'odre p, y d'ordre q. Le groupe est entièrement déterminé par la connaissance de k tel que $xy = y^k x$. Si on remplace x par x^{α} (avec α non nul mod p sinon $x^{\alpha} = 1$), alors par la relation devient $x^{\alpha}y = y^{k^{\alpha}}x^{\alpha}$, ce qui veut dire que k est remplacé par k^{α}. Autrement dit, si on choisit k d'ordre exactement p dans $\mathbb{Z}_q$ (qui est cyclique), alors les autres éléments k' de $\mathbb{Z}_q$ vérifiants $k'^p = 1$ sont $k' = k^{\alpha}$ avec $\alpha \in \mathbb{Z}_p$ et ils proviennent du remplacement de x par x^{α} qui est un autre générateur de $< x >$. Les deux groupes $< x, y >$ et $< x^{\alpha}, y >$ sont égaux (une inclusion est évidente et ils ont même cardinal). D'où la proposition suivante :

Proposition 6. — *Groupes d'ordre pq.*
Si p et q sont des premiers distincts ou non avec $p \leq q$, les groupes d'ordre pq sont

Z_{pq}, $Z_p \times Z_q$ et, uniquement si p divise $q-1$, un unique groupe non commutatif d'ordre pq. Dans le cas où p ne divise pas $q-1$ et $p \neq q$, on peut conclure que G est cyclique.

On remarque que ce travail s'étend au cas d'un groupe d'ordre pq avec $p \leq q$ sans supposer p et q premiers mais en supposant que le groupe étudié contient un élément x d'ordre p et un élément y d'ordre q avec $< x > \cap < y >= \{1\}$ (pour assurer le cas $p = q$). À savoir que de tels groupes sont commutatifs si p et $\varphi(q)$ (indicatrice d'Euler) sont premiers entre eux. Si au contraire ils ne le sont pas, on note H le sous-groupe de $\mathbb{Z}/q\mathbb{Z}^*$ consitué des éléments vérifiant $z^p = 1$. Ce groupe est abélien et en tant que tel, il est produit de groupes cycliques : $H \simeq \prod_{1 \leq i \leq n} G_i^{a_i}$ où les ordres des G_i sont tous distincts. On doit pouvoir rédiger qu'il y a alors exactement n groupes non commutatifs d'ordre pq (en raisonnant à isomorphisme près bien sûr).

Post scriptum de Luc Abergel: il a été publiée sur le bulletin vert de l'UPS une version modifiée par Mr Patte au prétexte d'une rédaction qui lui plaisait davantage. Cette réécriture ne correspond en aucun cas à l'esprit de ce que j'ai voulu apporter dans ce travail rédigé avec Sylvain Arnt et validé par Florent Nicaise que nous remercions tous les deux pour ses précieux conseils. C'est donc cette version qui prévaut et non celle appropriée par d'autres.

Je me permets par ailleurs de préciser qu'on peut émettre un avis sur une proposition mathématique sans pour autant en être certain, comme le disait Mr Riemann lorsqu'il a parlé de la fonction ζ.

Luc Abergel[3] et Sylvain Arnt[4]

---

[3] https://jds-mpstar1.e-monsite.com et lucabergel@cegetel.net
[4] https://arnt-sylvain-maths.com et arnt.sylvain@gmail.com