Théorie des groupes
Automorphismes de $\mathbb{Z}/n\mathbb{Z}$, Groupes d'ordre pq

AFFALOU Étienne

Octobre 2023

Table des matières

Dans cet article, on va classifier les groupes d'ordre pq où p et q sont deux nombres premiers distincts. La démonstration nécessite la connaissance du groupe des automorphismes de $\mathbb{Z}/q\mathbb{Z}$ pour q premier seulement, mais on va donner les automorphismes de $\mathbb{Z}/n\mathbb{Z}$ pour tout $n \in \mathbb{N}^* \setminus \{1\}$ au passage. L'article suit la preuve donnée dans **[1]**. On trouve aussi cette classification dans **[2]**.
Dans ce qui suit $n \in \mathbb{N}^* \setminus \{1\}$ et p et q sont deux nombres premiers distincts tels que $p < q$.

1 Automorphismes de $\mathbb{Z}/n\mathbb{Z}$

En fait, au lieu de calculer $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, on va calculer l'ensemble $(\mathbb{Z}/n\mathbb{Z})^*$ des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

1.1 Lien entre $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ et $(\mathbb{Z}/n\mathbb{Z})^*$

PROPOSITION $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

PREUVE :
On définit l'application

$$\begin{array}{ccccc} \sigma & : & (\mathbb{Z}/n\mathbb{Z})^* & \longrightarrow & \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \\ & & s & \longmapsto & \sigma(s) \end{array} \quad : \quad \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & sx \end{array}$$

Montrons que σ est bien définie. Si $s \in (\mathbb{Z}/n\mathbb{Z})^*$, on a $\forall (x,y) \in (\mathbb{Z}/n\mathbb{Z})^2$,

$$\sigma(s)(x+y) = s(x+y) = sx + sy = \sigma(s)(x) + \sigma(s)(y)$$

Donc $\sigma(s)$ est un endomorphisme de $\mathbb{Z}/n\mathbb{Z}$ et si $sx = 0$, on a bien entendu $x = 0$ car s est inversible.
Ainsi, $\sigma(s) \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ et σ est bien définie.
Montrons que σ est un morphisme de groupes. Soient $s, s' \in (\mathbb{Z}/n\mathbb{Z})^*$. $\forall x \in \mathbb{Z}/n\mathbb{Z}$,

$$\sigma(ss')(x) = ss'x = s(s'x) = \sigma(s)(s'x) = \sigma(s)(\sigma(s')(x))$$

Ceci étant vrai pour tout x de $\mathbb{Z}/n\mathbb{Z}$, on a $\sigma(ss') = \sigma(s) \circ \sigma(s')$ et σ est un morphisme de groupes.
Pour montrer que σ est un isomorphisme on va donner son inverse. Définissons

$$\begin{array}{ccccc} \tau & : & \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^* \\ & & u & \longmapsto & u(1) \end{array}$$

Tout d'abord, τ est bien définie car 1 étant un générateur de $\mathbb{Z}/n\mathbb{Z}$ et u étant un automorphisme de $\mathbb{Z}/n\mathbb{Z}$, $u(1)$ engendre encore $\mathbb{Z}/n\mathbb{Z}$ et donc $u(1) \in (\mathbb{Z}/n\mathbb{Z})^*$ (voir **[1]** pour la preuve que $s \in (\mathbb{Z}/n\mathbb{Z})^*$ ssi s engendre $\mathbb{Z}/n\mathbb{Z}$).
Et τ est un morphisme car si $(u,v) \in (\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}))^2$,

$$\tau(u \circ v) = (u \circ v)(1) = u(v(1)) = u(v(1) \times 1) = v(1)u(1) = u(1)v(1) = \tau(u)\tau(v)$$

en voyant $v(1)$ comme un multiple de 1 et en utilisant le fait que u est un morphisme de groupes.
Montrons que $\sigma \circ \tau = \tau \circ \sigma = \mathrm{id}$. Si $u \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, on a $\forall x \in \mathbb{Z}/n\mathbb{Z}$,

$$(\sigma \circ \tau)(u)(x) = \sigma(\tau(u))(x) = \sigma(u(1))(x) = u(1)x = xu(1) = u(x \times 1) = u(x)$$

Ceci étant vrai pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, on a $(\sigma \circ \tau)(u) = u$. Ceci étant vrai pour tout $u \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, $\sigma \circ \tau = \mathrm{id}$.
De plus, si $s \in (\mathbb{Z}/n\mathbb{Z})^*$, on a par définition de τ et de σ que

$$(\tau \circ \sigma)(s) = \tau(\sigma(s)) = s$$

C'est vrai pour tout $s \in (\mathbb{Z}/n\mathbb{Z})^*$ donc $\tau \circ \sigma = \mathrm{id}$. Finalement, σ et τ sont réciproques l'un de l'autre. Ce sont des morphismes de groupes donc on a bien

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

car σ et τ sont des isomorphismes.

On a donc ramené la recherche des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ au calcul de $(\mathbb{Z}/n\mathbb{Z})^*$.

1.2 Calcul de $(\mathbb{Z}/p\mathbb{Z})^*$

On pourrait utiliser le fait que $\mathbb{Z}/p\mathbb{Z}$ est un corps fini pour démontrer que $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique (voir le chapitre 3 de [**1**]), mais on donne ici une preuve qui n'utilise pas ce résultat.

> PROPOSITION $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

PREUVE :
On note r le ppcm des ordres des éléments de $(\mathbb{Z}/p\mathbb{Z})^*$. Montrons qu'il existe un élément d'ordre r dans $(\mathbb{Z}/p\mathbb{Z})^*$.
Décomposons r en produit de facteurs premiers :

$$r = \prod_{i=1}^{k} p_i^{\alpha_i}$$

où les α_i sont des entiers naturels non nuls et les p_i sont distincts deux à deux.
Par définition du ppcm, $\forall i \in \{1, \cdots, k\}$, on a l'existence d'un élément $x_i \in (\mathbb{Z}/p\mathbb{Z})^*$ dont l'ordre est un multiple de $p_i^{\alpha_i}$. On a donc x_i d'ordre $n_i p^{\alpha_i}$, puis $x_i^{n_i}$ d'ordre p^{α_i}. Donc, en posant

$$x = \prod_{i=1}^{k} x_i^{n_i}$$

on obtient que x est d'ordre r (l'ordre du produit de deux éléments dont les ordres sont premiers entre eux vaut le produit des ordres et on obtient le résultat par récurrence).
Rappelons que $|(\mathbb{Z}/p\mathbb{Z})^*| = p-1$ (les éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$ sont ceux qui sont premiers avec p et p est premier).
Par le théorème de Lagrange, $r \mid p-1$ et donc $r \leqslant p-1$. Montrons que $p-1 \leqslant r$.
Le polynôme $P = X^r - 1$ est de degré r donc a au plus r racines. Mais

$$\forall x \in (\mathbb{Z}/p\mathbb{Z})^*, P(x) = 0$$

car r est le ppcm des ordres des éléments de $(\mathbb{Z}/p\mathbb{Z})^*$. Donc, $p-1 \leqslant r$. Ainsi, $r = p-1$.
Cela montre que x est un élément de $(\mathbb{Z}/p\mathbb{Z})^*$ qui est d'ordre $p-1$. $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$ donc on a bien

$$(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$$

par théorème de classification des groupes monogènes.

Maintenant, calculons $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ en distinguant le cas où $p = 2$.

1.3 Calcul de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$

On commence par le cas $p \neq 2$. Ici, α est un entier naturel non nul.

> PROPOSITION Si $p \neq 2$ et $\alpha \geqslant 2$, alors $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \cong \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

PREUVE :
On commence par montrer par récurrence sur k que $\forall k \in \mathbb{N}^*$, $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ avec λ non divisible par p.

— $k = 1$. On sait que

$$(1+p)^p = \sum_{i=0}^{p} \binom{p}{i} p^i$$

Or, pour $1 \leqslant i < p$, $p \mid \binom{p}{i}$ donc pour $i \geqslant 2$, $p^3 \mid \binom{p}{i} p^i$. On a aussi $p^3 \mid p^p$. Donc,

$$(1+p)^p = 1 + p^2 + up^3 = 1 + p^2(1+up)$$

et $1+up$ n'est pas divisible par p. Le résultat est donc prouvé pour $k = 1$.

— Soit $k \in \mathbb{N}^*$. Supposons que $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ avec λ non divisible par p. On a alors

$$(1+p)^{p^{k+1}} = (1+\lambda p^{k+1})^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} \lambda^i p^{(k+1)i} + \lambda^p p^{(k+1)p}$$

Dans la somme, le terme en $i = 1$ vaut λp^{k+2} et pour $i > 1$, on a comme dans le cas $k = 1$ que $p^{k+3} \mid \binom{p}{i}\lambda^i p^{(k+1)i}$. On a aussi $p^{k+3} \mid \lambda^p p^{(k+1)p}$ donc

$$(1+p)^{p^{k+1}} = 1 + \lambda p^{k+2} + up^{k+3} = 1 + p^{k+2}(\lambda + up)$$

avec $\lambda + up$ non divisible par p. On a donc le résultat en posant $\lambda' = \lambda + up$.

Ce que l'on vient de démontrer nous permet de trouver un élément d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha Z)^*$.
En effet, $(1+p)^{p^{\alpha-1}} = 1 + \lambda p^\alpha \equiv 1\ [p^\alpha]$ et pour tous autres les diviseurs stricts de p^α (qui sont les seules autres possibilités pour l'ordre de $1+p$ par le théorème de Lagrange), $(1+p)^{p^k} \not\equiv 1\ [p^\alpha]$ pour $k < \alpha - 1$.
Donc $1+p$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$. À ce stade, rappelons que $|(\mathbb{Z}/p^\alpha\mathbb{Z})^*| = p^{\alpha-1}(p-1)$ (indicatrice d'Euler).
On a déjà un élément d'ordre $p^{\alpha-1}$. Pour montrer notre proposition, il s'agit de trouver un élément d'ordre $p^{\alpha-1}(p-1)$.
On définit l'application

$$\begin{array}{rccc} \psi & : & (\mathbb{Z}/p^\alpha\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^* \\ & & \overline{k} & \longmapsto & \tilde{k} \end{array}$$

où $\overline{k}$ est la classe de k modulo p^α et $\tilde{k}$ est la classe de k modulo p. D'après le **1.2**, par surjectivité de ψ, on peut prendre $y \in (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ tel que $\psi(y)$ est d'ordre $p-1$. De cette façon, $p-1$ divise l'ordre de y. On trouve un élément d'ordre $p-1$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ en trouvant un sous-groupe cyclique du groupe cyclique $< \{y\} >$ étant donné que $p-1$ divise l'ordre de y. Soit x cet élément d'ordre $p-1$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$.
On a $x(1+p) \in (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ et $x(1+p)$ est d'ordre $p^{\alpha-1}(p-1)$ car $p^{\alpha-1}$ et $p-1$ sont premiers entre eux. Donc,

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^* \cong \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$$

d'après le théorème de classification des groupes monogènes.

Il ne nous reste plus que le cas $p = 2$.

PROPOSITION $(\mathbb{Z}/2\mathbb{Z})^* \cong \{1\}$, $(\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$ et pour tout $\alpha \geqslant 3$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z})$.

PREUVE :
La connaissance des cardinaux de $(\mathbb{Z}/2\mathbb{Z})^*$ et de $(\mathbb{Z}/4\mathbb{Z})^*$ permet d'obtenir les deux premiers isomorphismes.
Dans le cas où $\alpha \geqslant 3$, on commence par montrer par récurrence sur k que $\forall k \in \mathbb{N}^*$, $5^{2^k} = 1 + \lambda 2^{k+2}$ où λ est impair.

- $k = 1$. On a $5^2 = 25 = 1 + 24 = 1 + 3 \times 8 = 1 + 3 \times 2^3$. Donc le résultat est vrai pour $k = 1$.
- Soit $k \in \mathbb{N}^*$. Supposons que $5^{2^k} = 1 + \lambda 2^{k+2}$ où λ est impair. Alors,

$$5^{2^{k+1}} = (1 + \lambda 2^{k+2})^2 = 1 + \lambda 2^{k+3} + \lambda^2 2^{2k+4} = 1 + (\lambda + \lambda^2 2^{k+1})2^{k+3}$$

et λ est impair donc λ^2 aussi et donc $\lambda^2 2^{k+1}$ est pair, puis $\lambda + \lambda^2 2^{k+1}$ est impair. D'où le résultat.

Ce résultat nous donne un élément de $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ d'ordre $2^{\alpha-2}$. Or, $|(\mathbb{Z}/2^\alpha\mathbb{Z})^*| = 2^{\alpha-1}(2-1) = 2^{\alpha-1}$. donc le sous-groupe engendré par 5 est d'indice 2 dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ (en particulier, on a $< \{5\} > \trianglelefteq (\mathbb{Z}/2^\alpha\mathbb{Z})^*$).
De plus, $-1 \notin < \{5\} >$. En effet, si $-1 = 5^k + \lambda 2^\alpha$, alors on obtient $3 = 1$ modulo 4 ce qui est faux.
Donc, $< \{-1\} > \cap < \{5\} > = \{1\}$, et $< \{1\} >< \{5\} > = (\mathbb{Z}/2^\alpha\mathbb{Z})^*$. -1 commute avec tous les éléments de $< \{5\} >$, donc comme $< \{5\} > \cong (\mathbb{Z}/2^{\alpha-2}\mathbb{Z})$,

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z})$$

avec $< \{-1\} > \cong \mathbb{Z}/2\mathbb{Z}$.

1.4 Calcul de $(\mathbb{Z}/n\mathbb{Z})^*$

Maintenant qu'on a trouvé les inversibles de $\mathbb{Z}/p^\alpha\mathbb{Z}$, le calcul de $(\mathbb{Z}/n\mathbb{Z})^*$ est rapide.

PROPOSITION On décompose n en produit de facteurs premiers

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

Alors, on a

$$(\mathbb{Z}/n\mathbb{Z})^* \cong \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$$

Preuve :
D'après le théorème chinois,

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$

Donc,

$$(\mathbb{Z}/n\mathbb{Z})^* \cong \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$$

en prenant les éléments inversibles des deux cotés.

On en déduit immédiatement les automorphismes de $\mathbb{Z}/n\mathbb{Z}$.

1.5 Conclusion

Proposition On décompose n en produit de facteurs premiers

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

Alors, on a

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$$

Preuve :
D'après **1.1**, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. D'où le résultat par **1.4**.

En fait, pour donner la structure des groupes d'ordre pq, on a seulement besoin de la structure de $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Cependant, pour des groupes finis d'ordre p^2q par exemple, une classification exhaustive peut être utile (voir par exemple le I.35 de [**3**]).

2 Les groupes d'ordre pq

On commence par montrer un lemme qui nous sera utile pour démontrer le résultat.

2.1 Un lemme

Lemme Soient H et N deux groupes, $\varphi : H \to \mathrm{Aut}(N)$ et $\alpha \in \mathrm{Aut}(H)$.
Soit ψ tel que le diagramme suivant soit commutatif ($\varphi = \psi \circ \alpha$).

$$\begin{array}{ccc} H & \xrightarrow{\varphi} & \mathrm{Aut}(N) \\ {\scriptstyle\alpha}\downarrow & \nearrow_{\psi} & \\ H & & \end{array}$$

Alors, $N \rtimes_\psi H \cong N \rtimes_\varphi H$.

Preuve :
On introduit l'application

$$\begin{array}{rccc} f & : & N \rtimes_\varphi H & \longrightarrow & N \rtimes_\psi H \\ & & (n,h) & \longmapsto & (n, \alpha(h)) \end{array}$$

C'est bien entendu une bijection (on peut donner son inverse). Montrons que c'est un morphisme.
Soient $(n,n') \in N^2$ et $(h,h') \in H^2$. On a d'une part

$$f((n,h)(n',h')) = f(n\varphi(h)(n'), hh') = (n\varphi(h)(n'), \alpha(hh'))$$

Et d'autre part,

$$f(n,h)f(n',h') = (n,\alpha(h))(n',\alpha(h')) = (n\psi(\alpha(h))(n'),\alpha(h)\alpha(h')) = (n\varphi(h)(n'),\alpha(hh'))$$

Donc f est bien un isomorphisme de groupes, et $N \rtimes_\psi H \cong N \rtimes_\varphi H$.

2.2 Classification des groupes d'ordre pq

Le résultat est le suivant.

> PROPOSITION Soit G un groupe d'ordre pq.
> — Si $p \mid q-1$, alors $G \cong \mathbb{Z}/pq\mathbb{Z}$ ou $G \cong (\mathbb{Z}/q\mathbb{Z}) \rtimes_\alpha (\mathbb{Z}/p\mathbb{Z})$ où $\alpha : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est non trivial.
> — Sinon, $G \cong \mathbb{Z}/pq\mathbb{Z}$.

PREUVE :
D'après le premier théorème de Sylow, G admet au moins un q-Sylow.
En utilisant le second théorème de Sylow, on obtient que le nombre n_q de q-Sylow de G vérifie

$$n_q \equiv 1\ [q] \text{ et } n_q \mid p$$

Donc $n_q = 1$ et G a un unique q-Sylow, qui est donc distingué dans G. Notons le Q.
Q étant de cardinal premier, $Q \cong \mathbb{Z}/q\mathbb{Z}$. Or, $p \mid |G|$ donc G a un élément d'ordre p par le théorème de Cauchy.
Le sous-groupe N qu'il engendre est donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On a donc

- $Q \trianglelefteq G$.
- $Q \cap N = \{e\}$ car si $x \in Q \cap N$, son ordre divise q et p par le théorème de Lagrange, donc vaut 1.
- Montrons que $G = QN$. QN est un sous-groupe de G étant donné que $Q \trianglelefteq G$.
  De plus, le second théorème d'isomorphisme donne

  $$QN/Q \cong N/(Q \cap N)$$

  donc $|QN|/q = p/1$ puis $|QN| = pq$ ($NQ = QN$ car $Q \trianglelefteq G$). Ainsi, $G = QN$.

Ces trois points assurent que G s'écrit comme un produit semi-direct

$$G \cong Q \rtimes_\alpha N$$

où $\alpha : N \to \mathrm{Aut}(Q)$ est un morphisme de groupes, avec $N \cong \mathbb{Z}/p\mathbb{Z}$ et $\mathrm{Aut}(Q) \cong \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$.
Les deux sous-cas de la proposition apparaissent naturellement :

1. Si p ne divise pas $q-1$, alors pour tout $x \in N$, l'ordre de $\alpha(x)$ divise $q-1$.
   Or, l'ordre de x étant égal à p, l'ordre de $\alpha(x)$ vaut 1 ou p. Donc l'ordre de $\alpha(x)$ vaut 1 et α est trivial.
   Le produit est donc direct, et

   $$G \cong (\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/pq\mathbb{Z}$$

   par le théorème chinois.
2. Dans le second cas, $p \mid q-1$ et comme $\mathbb{Z}/(q-1)\mathbb{Z}$ est cyclique, il admet un unique sous-groupe d'ordre p.
   On a donc toujours la possibilité où α est trivial, mais α peut également être non trivial, ce qui donne des produits semi-directs isomorphes par le lemme démontré en **2.1**. Ainsi, on a bien

   $$G \cong \mathbb{Z}/pq\mathbb{Z} \text{ ou } G \cong (\mathbb{Z}/q\mathbb{Z}) \rtimes_\alpha (\mathbb{Z}/p\mathbb{Z})$$

   avec $\alpha : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ non trivial.

D'où le résultat annoncé.

2.3 Application au cas $p = 2$

On note D_p le groupe diédral d'indice p (et d'ordre $2p$).

> PROPOSITION Soit G un groupe fini d'ordre $2p$.
> — Si $p = 2$, alors $G \cong \mathbb{Z}/4\mathbb{Z}$ ou $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
> — Si p est impair, $G \cong \mathbb{Z}/2p\mathbb{Z}$ ou $G \cong D_p$.

PREUVE :
Traitons d'abord le cas $p = 2$.

1. Si $p = 2$, alors G est d'ordre 4. Si G a un élément d'ordre 4, alors G est cyclique donc
$$G \cong \mathbb{Z}/4\mathbb{Z}$$
d'après le théorème de classification des groupes monogènes.
Sinon, les trois éléments de G différents du neutre sont d'ordre 2.
Donc $\forall (x, y) \in G^2$, $e = (xy)^2 = xyxy$ donc $xy = y^{-1}x^{-1} = yx$ car $y^{-1} = y$ et $x^{-1} = x$ ($x^2 = y^2 = e$).
Cela montre que G est abélien donc
$$G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$
d'après le théorème de structure des groupes abéliens finis.
2. Si p est impair, alors $p > 2$ et notre classification **2.2** s'applique. Comme p est impair, $2 \mid q - 1$.
D_p est un groupe non abélien d'ordre $2p$, donc il n'est pas isomorphe à $\mathbb{Z}/2p\mathbb{Z}$.
Il est donc nécessairement isomorphe à $G \cong (\mathbb{Z}/p\mathbb{Z}) \rtimes_\alpha (\mathbb{Z}/2\mathbb{Z})$ où $\alpha : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ est non trivial.
Finalement,
$$G \cong \mathbb{Z}/2p\mathbb{Z} \text{ ou } G \cong D_p$$
en utilisant le **2.2**.

On a donc bien le résultat annoncé.

Remarque : On peut aussi classifier les groupes d'ordre $2p$ sans utiliser le **2.2**, mais la preuve est plus fastidieuse.

Références :

— [**1**] Cours d'algèbre, *Daniel Perrin*
— [**2**] Algèbre et géométrie, *François Combes*
— [**3**] Exercices d'algèbre, *Pascal Ortiz*