Classification des petits groupes

Table des matières

Dans toute cette étude, on considère un groupe $(G, *)$ (que l'on notera G par la suite) de cardinal (ou d'ordre si l'on préfère) fini (et de neutre noté e_G pour la loi de composition interne $*$ (que l'on ne fera pas apparaître ici)) et un nombre premier p (quelconque lors de l'étude des groupes d'ordre p et p^2 et supérieur ou égal à 3 lors de l'étude des groupes d'ordre $2p$).

Pour mener à bien cette étude, on suppose que les bases de la théorie des groupes sont connues (notions de groupes, sous-groupes, morphismes de groupes, ordre d'un élément et d'un groupe, etc.) ainsi que tout ce qui en découle, mais également les notions de groupe quotient et d'action de groupe et enfin les notions de produits directs et semi-directs. On suppose également connus les "théorèmes classiques" de théorie des groupes : théorème de Lagrange, théorèmes d'isomorphismes, théorèmes de Sylow, etc.

I Motivation de la classification des petits groupes

Lorsque l'on travaille en théorie des groupes avec des groupes qui sont de cardinaux finis et raisonnablement petits (très souvent inférieur ou égal à 15), il est très utile (voire même essentiel) de pouvoir déterminer la structure du groupe pour pouvoir l'identifier (à l'isomorphisme près !) et utiliser toutes les propriétés découlant de cette structure. Une autre utilité de la classification des petits groupes est en théorie de Galois. En effet, lorsque l'on étudie la théorie des corps, la notion centrale est celle d'extension de corps. Ainsi, lorsque l'on travaille avec une extension donnée (de degré fini) on cherche à obtenir le maximum d'information et notamment de connaître les extensions intermédiaires. C'est ici qu'intervient la théorie de Galois : la correspondance de Galois nous donne une correspondance bijective entre l'extension de corps et ses extensions intermédiaires et le groupe de Galois de cette extension et ses sous-groupes (pour une extension galoisienne !). Ainsi, connaître le groupe de Galois nous donne sa structure interne et donc nous permet de trouver toutes les extensions intermédiaires et les liens qui les relient.

Le but de ce document est donc l'étude des groupes finis de cardinal inférieur ou égal à 15 (il est bien sûr possible d'aller plus loin, mais cela devient très vite compliqué dès que le cardinal du groupe dépasse 15) et d'établir une classification à l'isomorphisme près de ces "petits groupes" en guise de conclusion.

II Le cas (très rapide !) du groupe d'ordre 1

Dans toute cette partie, on suppose que le groupe G est d'ordre 1.

Proposition 1 :
Si le groupe G est de cardinal égal à 1, alors $G = \{e_G\}$.

Preuve :

On sait par définition d'un groupe que $\{e_G\} \subseteq G$. De plus, puisque $\text{Card}(G) = \text{Card}(\{e_G\}) = 1$, on en déduit par inclusion et égalité des cardinaux que $G = \{e_G\}$.

Finalement, on a donc $G = \{e_G\}$.

$\blacksquare$

Remarque :
On a ici (et c'est le seul cas dans toute cette étude !) une égalité explicite entre deux ensembles et deux structures algébriques. Dans toute la suite de cette étude, les résultats ne pourront être énoncés que sous la forme de deux structures algébriques isomorphes l'une à l'autre et non égales (d'où l'importance du terme "à l'isomorphisme près" donné en introduction).

Ainsi, il n'existe qu'un seul groupe d'ordre 1 qui est $\{e_G\}$ et tout groupe d'ordre 1 lui est égal. De plus, tous les groupes d'ordre 1 sont donc commutatifs.

III Le cas des groupes d'ordre p et p^2

Le but de cette partie est d'étudier les groupes d'ordre p et p^2, où p est un nombre premier quelconque.

III.1 Étude des groupes d'ordre p

Dans toute cette sous-partie, on suppose que le groupe G est d'ordre p.

Proposition 2 :
Si le groupe G est d'ordre p, alors il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Preuve :

On considère $x \in G \backslash \{e_G\}$ (possible car $\text{Card}(G) \geq 2$).
Comme G est un groupe fini, d'après le théorème de Lagrange, on obtient que $o(x)$ divise $\text{Card}(G)$. Autrement dit, $o(x)$ divise p.

Or, comme $o(x) > 0$ et que p est un nombre premier, alors $o(x) \in \{1; p\}$.
De plus, $x \neq e_G$, donc $o(x) \neq 1$ et ainsi, $o(x) = p$.

Puisque $x \in G$, on a donc $< x > \subseteq G$ et comme x est d'ordre p, $\text{Card}(< x >) = \text{Card}(G) = p$.
On en déduit donc par inclusion et égalité des cardinaux que $G = < x >$.

Finalement, le groupe G est un groupe cyclique d'ordre p, donc on a $G \cong \mathbb{Z}/p\mathbb{Z}$.

$\blacksquare$

Remarque :
Comme tous les groupes d'ordre p sont isomorphes à $\mathbb{Z}/p\mathbb{Z}$, alors en particulier ils sont abéliens et cycliques.

III.2 Étude des groupes d'ordre p^2

Dans toute cette sou-partie, on suppose que le groupe G est d'ordre p^2.

Lemme 3 :
Si le groupe quotient $G/Z(G)$ est un groupe monogène, alors le groupe G est un groupe abélien.

Preuve :

On suppose que le groupe quotient $G/Z(G)$ est un groupe monogène.
Comme $G/Z(G)$ est un groupe monogène, il existe $k \in G/Z(G)$ tel que $G/Z(G) =< k >$. Or, la projection canonique étant surjective, il existe donc $x_0 \in G$ tel que $k = \overline{x_0}$ et ainsi $G/Z(G) = \langle \overline{x_0} \rangle$.

On considère $x, y \in G$.
Il existe $k \in \mathbb{Z}$ et $\ell \in \mathbb{Z}$ tels que $\overline{x} = \overline{x_0}^k = \overline{x_0^k}$ et $\overline{y} = \overline{x_0}^\ell = \overline{x_0^\ell}$.

De plus, il existe $c_x, c_y \in Z(G)$ tels que $x = c_x x_0^k$ et $y = c_0 y_0^\ell$.

On a donc :

$$xy = \left(c_x x_0^k\right)\left(c_y x_0^\ell\right) \underset{c_y \in Z(G)}{=} c_x c_y x_0^k x_0^\ell \underset{c_y \in Z(G)}{=} c_y c_x x_0^\ell x_0^k \underset{c_x \in Z(G)}{=} \left(c_y x_0^\ell\right)\left(c_x x_0^k\right) = yx$$

Finalement, on en déduit que le groupe G est un groupe abélien.

$\blacksquare$

Lemme 4 :
Le nombre premier p divise le cardinal du centre du groupe G.

Preuve :

On sait que $Z(G)$ est un sous-groupe du groupe fini G, donc par le théorème de Lagrange, $\text{Card}(Z(G))$ divise donc $\text{Card}(G)$. Autrement dit, $\text{Card}(Z(G)) \in \{1; p; p^2\}$ (car $\text{Card}(Z(G)) > 0$).

Or, comme G est un p-groupe, d'après l'équation aux classes pour les p-groupes, on a :

$$\text{Card}(G) \equiv \text{Card}(Z(G)) \; [p]$$

Or, comme $\text{Card}(G) = p^2$, on a alors :

$$\text{Card}(Z(G)) \equiv 0 \; [p]$$

C'est-à-dire que $\text{Card}(Z(G))$ est divisible par p.

Finalement, on en conclut que p divise le cardinal du centre du groupe G.

■

On sait donc que le centre du groupe G est divisible par p. Or, comme on sait que $\text{Card}(Z(G)) \in \left\{1; p; p^2\right\}$, on peut donc affirmer que $\text{Card}(Z(G)) \in \left\{p; p^2\right\}$ (autrement dit, $Z(G) \neq \{e_G\}$).

Montrons par disjonction de cas que tout groupe d'ordre p^2 est abélien :
$*$ Si $\text{Card}(Z(G)) = p^2$, alors :
Comme on sait que $Z(G) \subseteq G$ (puisque $Z(G)$ est un sous-groupe de G) et que $\text{Card}(Z(G)) = \text{Card}(G)$, on en déduit donc par inclusion et égalité des cardinaux que $G = Z(G)$. Or, comme $Z(G)$ est un groupe abélien, on en déduit que le groupe G est un groupe abélien.

$*$ Si $\text{Card}(Z(G)) = p$, alors :
Comme G est un ensemble fini, on a :

$$\text{Card}(G/Z(G)) = \frac{\text{Card}(G)}{\text{Card}(Z(G))} = \frac{p^2}{p} = p$$

Donc d'après l'étude des groupes d'ordre p, le groupe $G/Z(G)$ est un groupe isomorphe à $\mathbb{Z}/p\mathbb{Z}$, il est donc cyclique. Ainsi, d'après le lemme 3, on en déduit que le groupe G est un groupe abélien.

On achève ainsi cette étude par une deuxième disjonction de cas :
$*$ S'il existe un élément x d'ordre p^2 dans G, alors on a $< x > \subseteq G$ ainsi que $\text{Card}(< x >) = o(x) = \text{Card}(G)$, on a donc par inclusion et égalité des cardinaux que $G = < x >$.
Ainsi, G est abélien et cyclique (car engendré par x d'ordre p^2), donc $G \cong \mathbb{Z}/p^2\mathbb{Z}$.

$*$ S'il n'existe pas d'élément d'ordre p^2, alors tout élément différent de e_G est d'ordre p (par le théorème de Lagrange). Il existe donc deux éléments $x, y \in G$ tels que $o(x) = o(y) = p$ et $y \in G \setminus < x >$ (car $< x > \subsetneq G$ par cardinalité).

On pose alors $H = < x >$ et $N = < y >$.
Les groupes H et N sont alors des groupes d'ordre p, donc par l'étude précédente sur les groupes d'ordre p on a $H \cong \mathbb{Z}/p\mathbb{Z}$ et $N \cong \mathbb{Z}/p\mathbb{Z}$.

De plus :
- H et N sont distingués dans G (car se sont deux sous-groupes de G et G est un groupe abélien).

- $\mathrm{Card}(G) = \mathrm{Card}(H)\,\mathrm{Card}(N)$.

- $H \cap N = \{e_G\}$. En effet, si ce n'est pas le cas, alors on a par le théorème de Lagrange (puisque $H \cap N$ est un sous-groupe de G et que $H \cap N \subseteq H$) que $\mathrm{Card}(H \cap N) = p$ et par cardinalité que $H \cap N = H$. Donc en particulier on a $y \in H$, ce qui contredit la définition de y.

Ainsi, par la caractérisation du produit direct interne de groupes finis, on a $G \cong H \times N \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Finalement, on obtient que $G \cong \mathbb{Z}/p^2\mathbb{Z}$ ou $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

III.3 Conclusion

D'après les deux études précédentes, on en déduit plusieurs choses :

— Tous les groupes d'ordre p sont abéliens et cycliques, donc isomorphes à $\mathbb{Z}/p\mathbb{Z}$.

— Tous les groupes d'ordre p^2 sont abéliens et isomorphes à $\mathbb{Z}/p^2\mathbb{Z}$ (si $\mathrm{Card}(Z(G)) = p^2$, ou bien s'ils sont cycliques) ou bien à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (si $\mathrm{Card}(Z(G)) = p$, ou bien s'ils ne sont pas cycliques).

Remarque :
Pour distinguer quel cas est le bon lorsque l'on a un groupe d'ordre p^2, on peut essayer de chercher un élément d'ordre p^2 dans ce groupe (si c'est le cas alors le groupe est cyclique et sinon il ne l'est pas).

On peut donc désormais donner en particulier la classification suivante pour les groupes d'ordre p ou p^2 inférieurs ou égaux à 15 :

Ordre du groupe	2	3	4	5	7	9	11	13
Isomorphe à	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/9\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/11\mathbb{Z}$	$\mathbb{Z}/13\mathbb{Z}$

IV Le cas des groupes d'ordre $2p$

Dans toute cette partie, on suppose que le groupe G est d'ordre $2p$, avec $p > 2$ (car pour $p = 2$ on a $2p = p^2$ et donc ce cas a été traité précédemment).

IV.1 Étude des groupes d'ordre $2p$

Lemme 5 :
Il existe deux sous-groupes de G, dont l'un est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et l'autre est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Preuve :

Puisque $\mathrm{Card}(G) = 2p$ et que p est un nombre premier différent de 2, on a que 2 et p sont premiers entre eux et donc par le théorème de Cauchy, il existe un élément $a \in G$ d'ordre p et un élément $b \in G$ d'ordre 2. De plus, puisque 2 et p sont des nombres premiers, alors par l'étude des groupes d'ordre un nombre premier, on a $< a >\cong \mathbb{Z}/p\mathbb{Z}$ et $< b >\cong \mathbb{Z}/2\mathbb{Z}$.

Finalement, il existe deux sous-groupes de G dont l'un est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et l'autre à $\mathbb{Z}/p\mathbb{Z}$.

■

Dans la proposition qui suit, on reprend les notations du lemme précédent.

Proposition 6 :
Si G est d'ordre $2p$, alors G est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ ou à D_{2p}.

Preuve :

Par les théorèmes de Sylow, on a :

$$n_p \equiv 1 \ [p] \text{ et } n_p | 2, \text{ donc } n_p = 1 \text{ (car } p > 2)$$

Ainsi, G contient un unique p-Sylow noté H et de cardinal égal à p (car $\mathrm{Card}(H) = p$ divise $\mathrm{Card}(G) = 2p$ et $\mathrm{PGCD}(2, p) = 1$).

Raisonnons par l'absurde en supposant que ba est d'ordre p :
On a alors $H =< ba >=< a >$ (par unicité du p-Sylow qui est d'ordre p), donc $b = (ba)a^{-1} \in H$. Ainsi, par le théorème de Lagrange, $o(b)$ divise p. Mais puisque $o(b) = 2$ et que 2 est premier avec p (car $p \in \mathcal{P}\backslash\{2\}$), on a alors une contradiction.

Ainsi, par le théorème de Lagrange, on a trois possibilités :
- Si $o(ba) = 1$, alors $ba = e_G$ et ainsi $a = b = e_G$ mais ceci est impossible car a est d'ordre p et b d'ordre 2.

- Si $o(ba) = 2p$, alors puisque l'on a $< ba >\subseteq G$ et $\mathrm{Card}(G) = \mathrm{Card}(< ba >)$, on a par inclusion et égalité des cardinaux que $G =< ba >\cong \mathbb{Z}/2p\mathbb{Z}$.

- Sinon, $o(ba) = 2$ et on a alors $baba = e_G$, c'est-à-dire $bab^{-1} = a^{-1}$ (car b est d'ordre 2). On reconnaît alors la présentation par générateurs et relations du groupe diédral et ainsi $< a, b >\cong D_{2p}$. Enfin, puisque $< a, b >\subseteq G$ et par égalité des cardinaux, on a $G \cong D_{2p}$.

Finalement, on a obtenu deux classes d'isomorphisme.

■

IV.2 Conclusion

D'après l'étude précédente, on en déduit que tous les groupes d'ordre $2p$ (pour p un nombre premier supérieur ou égal à 3) sont isomorphes à $\mathbb{Z}/2p\mathbb{Z}$ ou à D_{2p}. De plus, tous les groupes d'ordre $2p$ ne sont pas commutatifs ! En effet, puisque le groupe D_{2p} n'est pas un groupe commutatif, les groupes d'ordre $2p$ isomorphes à celui-ci ne sont donc pas commutatifs. C'est pourquoi le plus petit groupe non commutatif est d'ordre 6 (lorsque pour $p = 3$, D_6 n'est pas un groupe commutatif).

On peut donc désormais donner en particulier la classification suivante pour les groupes d'ordre $2p$ (où p est un nombre premier supérieur ou égal à 3) inférieurs ou égaux à 15 :

Ordre du groupe	6	10	14
Isomorphe à	$\mathbb{Z}/6\mathbb{Z}$ ou D_6	$\mathbb{Z}/10\mathbb{Z}$ ou D_{10}	$\mathbb{Z}/14\mathbb{Z}$ ou D_{14}

Remarque :
Dans la classification des groupes d'ordre $2p$, on a en réalité "caché" un produit semi-direct. En effet, en reprenant les notations du lemme 5, on a :
- $< a >$ est distingué dans G (car d'indice 2).

- $\text{Card}(G) = \text{Card}(< a >)\,\text{Card}(< b >)$.

- $< a > \cap < b >= \{e_G\}$. En effet, pour $x \in< a > \cap < b >$ on a que $o(x)$ divise à la fois $o(a) = p$ et $o(b) = 2$ et donc en particulier $\text{PGCD}(2, p) = 1$ et par positivité de l'ordre on a ainsi $o(x) = 1$, d'où $x = e_G$. L'inclusion réciproque étant vraie car $< a >$ et $< b >$ sont deux sous-groupes de G donc contient chacun e_G.

Par la caractérisation des produits semi-directs internes, on a $G \cong< a > \rtimes < b >\cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

En général ce produit reste semi-direct et on retrouve bien le groupe diédral D_{2p}, mais celui-ci peut devenir direct lorsque $< b >$ est distingué dans G (par exemple pour G abélien) et donc par le théorème des restes chinois (puisque 2 et p sont premiers entre eux) on retrouve le fait que $G \cong< a > \times < b >\cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2p\mathbb{Z}$.

V Le cas des groupes d'ordre 8

Dans toute cette partie, on suppose que le groupe G est d'ordre 8.

D'après le théorème de Lagrange, l'ordre de tout élément $x \in G$ divise le cardinal de G, donc si $x \in G \backslash \{e_G\}$ (possible car $\mathrm{Card}(G) = 8 > 1$, alors on a $o(x) \in \{2; 4; 8\}$.

On va donc raisonner par disjonction de cas afin de pouvoir étudier les groupes d'ordre 8.

V.1 Existence d'un élément d'ordre 8

Dans toute cette sous-partie, on suppose qu'il existe $x \in G$ d'ordre 8.

Proposition 7 :
Le groupe G est isomorphe à $\mathbb{Z}/8\mathbb{Z}$.

Preuve :

On sait que $x \in G$ et que $o(x) = 8$, on a donc $< x > \subseteq G$ et $\mathrm{Card}(< x >) = \mathrm{Card}(G) = 8$, donc par inclusion et égalité des cardinaux on a $G = < x >$.

Finalement, le groupe G est cyclique et d'ordre 8, donc il est isomorphe à $\mathbb{Z}/8\mathbb{Z}$.

■

V.2 Non-existence d'un élément d'ordre 8

Dans toute cette sous-partie, on suppose que G ne possède pas d'élément d'ordre 8.

V.2.1 Non-existence d'un élément d'ordre 4

Dans tout ce paragraphe, on suppose que G ne possède pas d'élément d'ordre 4 (donc ne possède que e_G ainsi que des éléments d'ordre 2).

Lemme 8 :
Le groupe G est un groupe abélien.

Preuve :

Soient $x, y \in G$. Comme tous les éléments de G sont d'ordre 1 ou 2, on a :

$$yx = y^{-1}x^{-1} = (xy)^{-1} = xy$$

Finalement, le groupe G est un groupe abélien.

■

Remarque :
Nous avons ici montré que tout groupe (fini ou non) ne contenant que des éléments d'ordre 2 (en dehors de e_G) est abélien.

Par le lemme 8, on sait donc que G est un groupe abélien. De plus, si l'on définit la loi externe :

$$* : \left| \begin{array}{ccc} \mathbb{F}_2 \times G & \longrightarrow & G \\ (\overline{m}, g) & \longmapsto & \overline{m} * g = g^{\overline{m}} \end{array} \right.$$

alors elle est bien définie et munit le groupe abélien G d'une structure de $\mathbb{F}_2$-espace vectoriel, nécessairement de dimension finie, puisque G est fini.

Mais alors, si $n = \dim_{\mathbb{F}_2}(G)$, on a un isomorphisme d'espaces vectoriels $G \cong \mathbb{F}_2^n$, qui est en particulier un isomorphisme de groupes abéliens. Et comme G est d'ordre 8, on obtient $n = 3$, soit $G \cong (\mathbb{Z}/2\mathbb{Z})^3$.

V.2.2 Existence d'un élément d'ordre 4

On considère dans ce paragraphe, un élément x d'ordre 4.

V.2.2.1 Cas 1 : Existence de $y \in G$ d'ordre 2 tel que $y \notin < x >$

Puisque $o(x) = 4$, on a que $< x >$ est distingué dans G (car d'indice 2) et ainsi $yxy^{-1} \in < x > = \{e_G, x, x^2, x^{-1}\}$. Or si $yxy^{-1} = e_G$, alors $yx = y$ et donc $x = e_G$, ce qui n'est pas possible. De même, si $yxy^{-1} = x^2$, alors $o\left(yxy^{-1}\right) = o(x^2)$. Or, on a $o\left(yxy^{-1}\right) = o(x) = 4$ et $o\left(x^2\right) = \frac{o(x)}{\mathrm{PGCD}(2, o(x))} = \frac{4}{\mathrm{PGCD}(2,4)} = \frac{4}{2} = 2 \neq 4$, ce qui est contradictoire.

Ainsi, on a que $yxy^{-1} \in \{x, x^{-1}\}$ et on termine notre raisonnement par disjonction de cas :
$*$ Si $yxy^{-1} = x$, alors $xy = yx$ et puisque $y \notin < x >$, on en déduit que G est abélien et en particulier $< y >$ est distingué dans G. Ainsi :
- $< x >$ et $< y >$ sont distingués dans G.

- $\mathrm{Card}(G) = \mathrm{Card}(< x >)\,\mathrm{Card}(< y >)$.

- $< x > \cap < y > = \{e_G\}$ car on a $< x > \cap < y > \subseteq < y > = \{e_G, y\}$ et $y \notin < x >$.

Finalement, par la caractérisation des produits directs internes, on a $G \cong < x > \times < y > \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$*$ Si $yxy^{-1} = x^{-1}$, alors on reconnaît une fois de plus la présentation par générateurs et relations du groupe diédral et ainsi $< x, y > \cong D_8$. Or puisque $< x, y > \subseteq G$ et que $\mathrm{Card}(G) = \mathrm{Card}(< x, y >)$, on en déduit que $G = < x, y > \cong D_8$.

V.2.2.2 Cas 2 : Non existence de $y \in G$ d'ordre 2 tel que $y \notin < x >$

Montrons qu'il existe deux éléments notés i et j d'ordre 4 qui ne commutent pas entre-eux :
$*$ On considère $y \in G \setminus < x >$ d'ordre différent de 2 (par hypothèse).
On a donc $o(y) \in \{4; 8\}$ (par le théorème de Lagrange), mais par hypothèse, y ne peut pas être d'ordre 8 (non existence d'un élément d'ordre 8), on a donc $o(y) = 4$.
Ainsi, $i = x$ et $j = y$ conviennent tous les deux.

$*$ Supposons par l'absurde que $ij = ji$:
On a alors $\left(i^2 j^2\right)^2 = i^4 j^4 = e_G e_G = e_G$.
Donc $i^2 j^2$ est d'ordre 2 dans G (car s'il était d'ordre 1 on aurait $j^{-1} = i$ ce qui est impossible de par la définition de j) et par hypothèse on a alors $i^2 j^2 \in < x > = \{e_G, i, i^2, i^3 = i^{-1}\}$. Ainsi on obtient par un argument d'ordre que $i^2 j^2 = i^2$ et donc que $j^2 = e_G$. On aboutit donc à une contradiction puisque $o(j) = 4$.
Ainsi, ij et ji ne commutent pas entre-eux.

Proposition 9 :

On a dans G les relations suivantes :

$$i^4 = e_G, \; i^2 = j^2 \text{ et } iji^{-1} = j^{-1}$$

Preuve :

Montrons les trois relations :
$*$ Puisque i est d'ordre 4 d'après ce qui précède, on a $i^4 = e_G$.

$*$ On sait que j^2 est d'ordre 2 (car j est d'ordre 4) et donc par hypothèse, $j^2 \in < x > \{e_G, i, i^2, i^{-1}\}$. Par un argument d'ordre similaire à ce qui précède, on a alors $i^2 = j^2$.

$*$ Tout d'abord, on a $iji^{-1} \in < j >$ car $< j >$ est un sous groupe d'indice 2 dans G et donc distingué. Ainsi, $iji^{-1} \in \{e_G, j, j^2, j^{-1}\}$.

Or, $iji^{-1} \neq e_G$ car sinon $ij = i$ et $j = e_G$ (ce qui est impossible car j est d'ordre 4), $iji^{-1} \neq j$ car sinon $ij = ji$ (ce qui est impossible par ce qui précède) et enfin $iji^{-1} \neq j^2$ car sinon $\left(iji^{-1}\right)^2 = ij^2i^{-1} = e_G$ et donc $ij^2 = i$ et $j^2 = e_G$ (ce qui est impossible car j est d'ordre 4).
Finalement, on a donc $iji^{-1} = j^{-1}$.

Ainsi, on a donc les trois relations annoncées.

Finalement, le groupe qui en résulte est un groupe non commutatif d'ordre 8, appelé **groupe des quaternions** et noté $\mathbb{H}_8$.

V.3 Conclusion

D'après l'étude précédente, on en déduit que les groupes d'ordre 8 sont isomorphes à 5 groupes différents suivant leur structure interne. De plus, tous les groupes d'ordre 8 ne sont pas commutatifs (puisque le groupe $\mathbb{H}_8$ ne l'est pas par exemple).

On peut donc désormais donner la classification suivante pour les groupes d'ordre 8 :

<table>
<tr><td rowspan="3">Structure interne</td><td rowspan="3">Élément d'ordre 8</td><td colspan="3">Pas d'élément d'ordre 8</td></tr>
<tr><td colspan="2">Élément d'ordre 4</td><td rowspan="2">Pas d'élément d'ordre 4</td></tr>
<tr><td>Cas 1</td><td>Cas 2</td></tr>
<tr><td>Isomorphe à</td><td>$\mathbb{Z}/8\mathbb{Z}$</td><td>$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
ou D_8</td><td>$\mathbb{H}_8$</td><td>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$</td></tr>
</table>

VI Le cas des groupes d'ordre 12

Dans toute cette partie, on suppose que le groupe G est d'ordre 12.

VI.1 Résultat préliminaire

On écrit $12 = 4\times3 = 2^2\times3$. Par les théorèmes de Sylow, on sait que $n_2 \equiv 1\ [2]$ et $n_2|3$, donc $n_2 \in \{1;3\}$ et ce(s) 2-Sylow(s) est/sont d'ordre 4. De même, on a $n_3 \equiv 1\ [3]$ et $n_3|4$, donc $n_3 \in \{1;4\}$ et ce(s) 3-Sylow(s) est/sont d'ordre 3.

De plus, les ordres des éléments de G peuvent être 1,2,3,4,6 ou 12 (d'après le théorème de Lagrange). Ainsi, si $n_3 = 4$, alors G contient 4 3-Sylow différents, chacun contenant deux éléments d'ordre 3 (par la classification des groupes d'ordre p). Donc G contient 8 éléments d'ordre 3, ainsi que e_G.

Il reste alors seulement 3 éléments dont l'ordre peut être 2 ou 4. Or, si $n_2 = 3$, alors G contient 3 2-Sylows (d'ordre 4) différents et ainsi G posséderait plus que 12 éléments, ce qui n'est pas possible. Ainsi, on en déduit que $n_2 = 1$ ou $n_3 = 1$.

VI.2 Cas où $n_2 = n_3 = 1$

Dans toute cette sous-partie, on suppose que $n_2 = n_3 = 1$ et note P l'unique 2-Sylow de G et Q l'unique 3-Sylow de G.

Proposition 10 :
G est le produit direct interne de P par Q.

Preuve :

$*$ Par les théorèmes de Sylow, on sait que P et Q sont deux sous-groupes distingués de G (car se sont les seuls sous-groupes de Sylow de leur ordre respectif).

$*$ $\mathrm{Card}(G) = \mathrm{Card}(P)\,\mathrm{Card}(Q)$.

$*$ $P \cap Q = \{e_G\}$ car $\mathrm{PGCD}(o(P), o(Q)) = 1$.

Par la caractérisation des produits directs internes, on en déduit que $G \cong P \times Q$.

■

Proposition 11 :
G est isomorphe à $\mathbb{Z}/12\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Preuve :

Puisque P est un groupe d'ordre 4, on sait par l'étude des groupes de cardinal p^2 que $P \cong \mathbb{Z}/4\mathbb{Z}$ ou $P \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et de même on a $Q \cong \mathbb{Z}/3\mathbb{Z}$.

$*$ Premier cas :
Si $P \cong \mathbb{Z}/4\mathbb{Z}$, alors par le théorème des restes chinois, on a :

$$G \cong P \times Q \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$$

$*$ Deuxième cas :
Si $P \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, alors toujours par le théorème des restes chinois, on a :

$$G \cong P \times Q \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

Finalement, on en déduit que G est isomorphe à $\mathbb{Z}/12\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

■

VI.3 Cas où $n_2 = 1$ et $n_3 = 4$

Dans toute cette sous-partie, on suppose que $n_2 = 1$ et $n_3 = 4$.

On fait opérer G par conjugaison sur l'ensemble S de ses 3-Sylow. Plus précisément, on considère l'application :

$$* : \left| \begin{array}{ccc} G \times S & \longrightarrow & S \\ (g, Q) & \longmapsto & gQg^{-1} \end{array} \right.$$

Montrons que $*$ définit une action de G sur S :
$*$ Pour tout $Q \in S$, on a $e_G * Q = e_G Q e_G^{-1} = Q$.

$*$ Pour tout $(g, g') \in G^2$ et $Q \in S$, on a :

$$g * (g' * Q) := g * \left(g'Qg'^{-1}\right) = gg'Qg'^{-1}g^{-1} = (gg')\,Q\,(gg')^{-1} = (gg') * Q$$

Ainsi, $*$ est bien une action de G sur S.

Proposition 12 :
Soit Q un 3-Sylow de G.
$\mathrm{Stab}(Q)$ est un sous-groupe de G de cardinal 3 et $\mathrm{Stab}(Q) = Q$.

Preuve :

Soit Q un 3-Sylow de G.
Comme l'action de G est transitive (car par les théorèmes de Sylow, tous les p-Sylows sont conjugués entre eux), on a pour tout $Q \in S$, $\mathrm{Orb}(Q) = S$.
Donc, par la relation orbite-stabilisateur, on a $\mathrm{Card}(\mathrm{Stab}(Q)) = \dfrac{\mathrm{Card}(G)}{\mathrm{Card}(\mathrm{Orb}(Q))} = \dfrac{\mathrm{Card}(G)}{\mathrm{Card}(S)} = \dfrac{12}{4} = 3$.

De plus, pour tout $g \in Q$, $gQg^{-1} = Q$, donc $Q \subseteq \mathrm{Stab}(Q)$ et par égalité des cardinaux, on en déduit que $\mathrm{Stab}(Q) = Q$.

Finalement, $\mathrm{Stab}(Q)$ est un sous-groupe de G de cardinal 3 et $\mathrm{Stab}(Q) = Q$.

■

Proposition 13 :
L'application :

$$f : \left| \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}_S \\ g & \longmapsto & f_g : \left| \begin{array}{ccc} S & \longrightarrow & S \\ Q & \longmapsto & g * Q \end{array} \right. \end{array} \right.$$

est un morphisme de groupes injectif.

Preuve :

On considère l'application :

$$f : \left| \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}_S \\ g & \longmapsto & f_g : \left| \begin{array}{ccc} S & \longrightarrow & S \\ Q & \longmapsto & g * Q \end{array} \right. \end{array} \right.$$

De manière générale, la donnée d'une action $*$ de G sur un ensemble non vide X est équivalente à la donnée d'un morphisme de groupes φ de G dans $\mathfrak{S}_X$. Donc ici, f est bien un morphisme de groupes de G dans $\mathfrak{S}_S$ car $*$ est une action de G sur S.

De plus :

$$\mathrm{Ker}(f) = \{g \in G \text{ tq } \forall Q \in S,\ g * Q = Q\} = \bigcap_{Q \in S} \mathrm{Stab}(Q)$$

Or les 3-Sylows sont d'ordre 3 et distincts, donc deux-à-deux d'intersection réduite au neutre.
En effet, pour $Q, Q' \in S$, $Q \cap Q'$ est un sous-groupe de Q et par le théorème de Lagrange on obtient que $\mathrm{Card}(Q \cap Q') \in \{1; 3\}$. Or, si $\mathrm{Card}(Q \cap Q') = 3$, alors par inclusion et égalité des cardinaux on a $Q \cap Q' = Q$ et donc $Q = Q'$ (car Q' d'ordre 3) ce qui est contradictoire avec le fait qu'ils sont distincts.

Donc, pour $Q, Q' \in S$ distincts, on a $\mathrm{Stab}(Q) \cap \mathrm{Stab}(Q') = \{e_G\}$ et ainsi $\mathrm{Ker}(f) = \{e_G\}$.

Finalement, f est donc bien un morphisme de groupes injectif.

■

On identifie désormais le groupe $\mathfrak{S}_S$ à $\mathfrak{S}_4$ (ce qui est possible car S est de cardinal 4, donc en bijection avec $[\![1; 4]\!]$).

Avant de pouvoir conclure, remarquons que G possède ici 4 3-Sylow chacun de cardinal 3, donc chaque 3-Sylow est isomorphe à $\mathbb{Z}/3\mathbb{Z}$ (par la classification des groupes d'ordre p). Ainsi, G possède exactement 8 éléments d'ordre 3 ($4 \times 4 - 3 = 12 - 4 = 8$).

Proposition 14 :
$\mathrm{Im}(f) \cap \mathfrak{A}_4$ possède au moins 9 éléments.

Preuve :

Comme G possède exactement 8 éléments d'ordre 3, ceux-ci peuvent être identifiés comme des éléments de $\mathfrak{S}_4$ d'ordre 3 (car $f : G \longrightarrow \mathfrak{S}_4$ est injective) et donc des 3-cycles. Or les 3-cycles ont pour signature 1 et sont donc des éléments de $\mathfrak{A}_4$.

Ainsi, $\mathrm{Im}(f) \cap \mathfrak{A}_4$ possède au moins $\mathrm{Id}_{[\![1;4]\!]}$ et ces 8 3-cycles, c'est-à-dire au moins 9 éléments.

■

Pour conclure, remarquons que $\mathrm{Im}(f) \cap \mathfrak{A}_4$ est un sous-groupe de $\mathfrak{A}_4$, donc par le théorème de Lagrange, $\mathrm{Card}(\mathrm{Im}(f) \cap \mathfrak{A}_4)$ divise $\mathrm{Card}(\mathfrak{A}_4) = \dfrac{24}{2} = 12$. Or, on a $\mathrm{Card}(\mathrm{Im}(f) \cap \mathfrak{A}_4) \geq 9$, ce qui oblige à avoir l'égalité $\mathrm{Card}(\mathrm{Im}(f) \cap \mathfrak{A}_4) = 12 = \mathrm{Card}(\mathfrak{A}_4)$.

Ainsi, on a $\mathrm{Im}(f) \subseteq \mathfrak{S}_4$ et $\mathrm{Im}(f) \cap \mathfrak{A}_4 = \mathfrak{A}_4$, donc on a les inclusions $\mathfrak{A}_4 \subseteq \mathrm{Im}(f) \subseteq \mathfrak{S}_4$.

Donc $\mathrm{Im}(f)$ est d'indice 1 ou 2 dans $\mathfrak{S}_4$ et par le premier théorème d'isomorphisme et par injectivité de f on a :

$$G \cong G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$$

Donc en passant au cardinal on a $\mathrm{Card}(\mathrm{Im}(f)) = \mathrm{Card}(G) = 12$ et donc $\mathrm{Im}(f) = \mathfrak{A}_4$, d'où $G \cong \mathfrak{A}_4$.

VI.4 Cas où $n_2 = 3$ et $n_3 = 1$

Dans toute cette sous-partie, on suppose que $n_2 = 3$ et $n_3 = 1$.

On note Q l'unique 3-Sylow de G et P un 2-Sylow de G (qui est d'ordre 4 car par les théorèmes de Sylow, ils sont tous conjugués entre-eux et l'un d'eux est d'ordre 4).

Montrons tout d'abord le résultat suivant :

Proposition 15 :
G est isomorphe au produit semi-direct interne de Q par P.

Preuve :

$*$ Par les théorèmes de Sylow, Q est le seul 3-Sylow de G, c'est donc un sous-groupe distingué de G.

$*$ $\mathrm{Card}(G) = \mathrm{Card}(P)\,\mathrm{Card}(Q)$.

$*$ $Q \cap P = \{e_G\}$, car si $x \in P \cap Q$, alors $o(x)$ divise $\mathrm{PGCD}(\mathrm{Card}(P), \mathrm{Card}(Q)) = 1$, donc $x = \{e_G\}$ (et réciproquement $e_G \in P \cap Q$).

Finalement, on en déduit par la caractérisation des produits semi-directs internes que $G \cong Q \rtimes P$.

■

Il nous reste désormais à traiter deux cas. En effet, puisque P est un groupe d'ordre 4, on obtient par la classification des groupes d'ordre $2p$ qu'il est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou à $\mathbb{Z}/4\mathbb{Z}$.

VI.4.1 Cas où $P \cong \mathbb{Z}/4\mathbb{Z}$

On considère dans ce paragraphe que P est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

D'après la proposition 18, on a alors directement que $G \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ (ce groupe est non commutatif et d'ordre 12).

VI.4.2 Cas où $P \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

On considère dans ce paragraphe que P est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Montrons tout d'abord le résultat suivant :

Lemme 16 :
Le groupe diédral D_{12} vérifie $n_2 = 3$, $n_3 = 1$ et ne contient aucun élément d'ordre 4.

Preuve :

On sait que $D_{12} := <\rho, \tau> = <\rho> \rtimes <\tau>$, avec ρ un élément d'ordre 6 correspondant à une rotation d'angle $\frac{2\pi}{6} = \frac{\pi}{3}$ dans l'hexagone régulier centré en l'origine et τ un élément d'ordre 2 correspondant à la symétrie par rapport à l'axe des abscisses tels que $\tau \circ \rho \circ \tau = \rho^{-1}$.

On dénombre les éléments de D_{12} :

$$D_{12} = \{\mathrm{Id}, \rho, \rho^2, \rho^3, \rho^4, \rho^5, \tau, \tau \circ \rho, \tau \circ \rho^2, \tau \circ \rho^3, \tau \circ \rho^4, \tau \circ \rho^5\}$$

D_{12} comporte 7 éléments d'ordre 2 qui sont : ρ^3, τ, $\tau \circ \rho$, $\tau \circ \rho^2$, $\tau \circ \rho^3$, $\tau \circ \rho^4$ et $\tau \circ \rho^5$. Il reste donc Id d'ordre 1, ρ d'ordre 6, ρ^2 d'ordre 3, ρ^4 d'ordre 3 et ρ^5 d'ordre 6.

Ainsi D_{12} ne possède pas d'élément d'ordre 4 et la liste de ses 2-Sylows comporte donc au moins :

$$\begin{cases} <\rho^3, \tau> & = \{\mathrm{Id}, \tau, \rho^3, \tau \circ \rho^3\} \\ <\rho^3, \tau \circ \rho> & = \{\mathrm{Id}, \rho^3, \tau \circ \rho, \tau \circ \rho^4\} \\ <\rho^3, \tau \circ \rho^2> & = \{\mathrm{Id}, \rho^3, \tau \circ \rho^2, \tau \circ \rho^5\} \end{cases}$$

Donc D_{12} contient ces 3 2-Sylows et cette liste est exhaustive car par le résultat préliminaire (cf. VI.1) on a $n_2 = 1$ ou $n_2 = 3$. On en déduit ainsi que D_{12} ne possède qu'un seul 3-Sylow étant donné que $n_2 = 3$ (toujours par le même résultat préliminaire).

Finalement, le groupe diédral D_{12} vérifie $n_2 = 3$, $n_3 = 1$ et ne contient aucun élément d'ordre 4.

■

On peut donc désormais conclure :

Proposition 17 :
Le groupe G est isomorphe au groupe diédral D_{12}.

Preuve :

Puisque $P \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, on peut écrire $P \cong \{e_G, x, y, xy\}$ tel que l'on ait $x, y \in G$, $xy = yx$ et $o(x) = o(y) = o(xy) = 2$.
On peut alors définir :

$$\varphi : \left| \begin{array}{ccc} P & \longrightarrow & \mathrm{Aut}(Q) \\ z & \longmapsto & \varphi_z : \left| \begin{array}{ccc} Q & \longrightarrow & Q \\ q & \longmapsto & zqz^{-1} \end{array} \right. \end{array} \right.$$

qui est un morphisme de groupes bien défini (car Q est distingué dans G puisque c'est le seul 3-Sylow de G) non trivial.

Donc, parmi x, y ou xy, il existe un unique élément dans $\mathrm{Ker}(\varphi)$ (par le théorème de Lagrange, la non trivialité de φ et le fait que $\mathrm{Card}(\mathrm{Aut}(Q)) = 2$). Quitte à renommer les variables, on peut supposer que $y \in \mathrm{Ker}(\varphi)$ et $(x, xy) \notin (\mathrm{Ker}(\varphi))^2$.

Soit t un élément d'ordre 3 tel que $Q =< t >$ (possible car $Q \cong \mathbb{Z}/3\mathbb{Z}$).
D'une part, on a $yty = t$ (car $y \in \mathrm{Ker}(\varphi)$ et est d'ordre 2) et d'autre part on a également que $xtx = t^{-1}$.

En effet, on a $xtx \in < t >= \left\{e_G, t, t^{-1}\right\}$ et comme $x \notin \mathrm{Ker}(\varphi)$, on a xtx différent de t. De plus, si $xtx = e_G$, alors $tx = x^{-1}$ et donc $tx^2 = e_G$. Ainsi $x^2 = t^{-1} \in Q$ et comme x est d'ordre 2 on a $t = e_G$, ce qui est contradictoire avec sa définition.

Ainsi, yt est d'ordre 6 car on remarque que $(yt)^2 = (yty)t = t^2$, donc $(yt)^3 = yt(yt)^2 = yt^3 = y$ et donc $(yt)^6 = y^3 = e_G$. Par conséquent, $o(yt)$ divise 6 et puisque $yt, (yt)^2, (yt)^3 \neq e_G$, on en déduit que $o(yt) = 6$ (car $o(yt) > 0$).

De plus comme P est abélien, on a également :

$$x(yt)x = (xy)tx = (yx)tx = y(xtx) = yt^{-1} = y^{-1}t^{-1} = (ty)^{-1}$$

Ainsi, on a $< yt, x >$ d'ordre 12 tel que $o(yt) = 6$, $o(x) = 2$ et $x(yt)x^{-1} = x(yt)x = (yt)^{-1}$. On reconnaît donc la présentation par générateurs et relations du groupe diédral, d'où $< yt, x >\cong D_{12}$.

Ainsi, puisque $< yt, x >\subseteq G$ et par égalité des cardinaux, on a $G =< yt, x >\cong D_{12}$.

■

VI.5 Conclusion

D'après l'étude précédente, on en déduit que les groupes d'ordre 12 sont isomorphes à 5 groupes différents suivant leur structure interne. De plus, tous les groupes d'ordre 12 ne sont pas commutatifs (puisque le groupe D_{12} ne l'est pas par exemple).

On peut donc désormais donner la classification suivante pour les groupes d'ordre 12 :

Structure interne	$n_2 = n_3 = 1$		$n_2 = 1$ et $n_3 = 3$	$n_2 = 3$ et $n_3 = 1$	
	$P \cong \mathbb{Z}/4\mathbb{Z}$	$P \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$		$P \cong \mathbb{Z}/4\mathbb{Z}$	$P \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
Isomorphe à	$\mathbb{Z}/12\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$\mathfrak{A}_4$	$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$	D_{12}

VII Le cas des groupes d'ordre 15

Dans toute cette partie, on suppose que le groupe G est d'ordre 15.

VII.1 Étude des groupes d'ordre 15

Proposition 18 :
Si le groupe G est d'ordre 15, alors il est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Preuve :

Puisque le groupe G est d'ordre $15 = 3 \times 5$, d'après les théorèmes de Sylows on a :

$$\begin{cases} n_3 \equiv 1 \ [3] & \text{et } n_3 \text{ divise } 5 \\ n_5 \equiv 1 \ [5] & \text{et } n_5 \text{ divise } 3 \end{cases}$$

On a donc $n_3 = n_5 = 1$ et on note alors respectivement S_3 et S_5 l'unique 3-Sylow et l'unique 5-Sylow de G.

Montrons que $G \cong S_3 \times S_5$:
$*$ Toujours d'après les théorèmes de Sylow, les sous-groupes S_3 et S_5 sont des sous-groupes distingués de G (car sont uniques).

$*$ $\mathrm{Card}(G) = \mathrm{Card}(S_3)\,\mathrm{Card}(S_5)$.

$*$ On a $S_3 \cap S_5 = \{e_G\}$.
En effet, si $x \in S_3 \cap S_5$, alors d'après le théorème de Lagrange, $o(x)$ divise $\mathrm{Card}(S_3) = 3$ et $\mathrm{Card}(S_5) = 5$, donc $o(x)$ divise $\mathrm{PGCD}(3;5) = 1$, donc $o(x) = 1$ (car $o(x) > 0$), d'où $x = e_G$ (et réciproquement, $e_G \in S_3 \cap S_5$).

Ainsi, d'après la caractérisation des produits directs internes, on a alors $G \cong S_3 \times S_5$.

De plus, S_3 est un groupe d'ordre 3 et S_5 est un groupe d'ordre 5, donc d'après l'étude faite sur les groupes d'ordre p, on en déduit que :

$$S_3 \cong \mathbb{Z}/3\mathbb{Z} \text{ et } S_5 \cong \mathbb{Z}/5\mathbb{Z}$$

On a donc ainsi $G \cong S_3 \times S_5 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ et comme 3 et 5 sont deux nombres premiers entre eux, d'après le théorème des restes chinois, on a $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$.

■

VII.2 Conclusion

D'après l'étude précédente, on en déduit que tous les groupes d'ordre 15 sont isomorphes à $\mathbb{Z}/15\mathbb{Z}$, donc en particulier abéliens et cycliques.

VIII Conclusion générale

Maintenant que notre étude des petits groupes est terminée, nous allons pouvoir résumer les résultats trouvés dans les tableaux ci-dessous. Ces tableaux ne donneront pas tous les cas de figure précis et il faudra se reporter aux parties correspondantes pour savoir exactement à quoi le groupe considéré est isomorphe.

VIII.1 Classification des petits groupes

Nous résumons tout d'abord dans le tableau ci-dessus, pour chaque cardinal allant de 1 à 15, le nombre de groupes abéliens possibles ainsi que le nombre de groupes non abéliens possibles (à l'isomorphisme près) :

Ordre du groupe	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Nombre de groupes abéliens	1	1	1	2	1	1	1	3	2	1	1	2	1	1	1
Nombre de groupes non abéliens	0	0	0	0	0	1	0	2	0	1	0	3	0	1	0
Nombre total de groupes	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1

En ce qui concerne les groupes abéliens d'ordre inférieur ou égal à 15, ceux-ci ont une classification simple. En effet, il est possible de montrer qu'ils sont tous cycliques, ou produits directs de groupes cycliques (comme on a pu le constater) : c'est le théorème de structure des groupes abéliens finis.

On donne ci-dessous les groupes abéliens (à isomorphisme près) de cardinal inférieur ou égal à 15 :

Ordre du groupe	1	2	3	4	5
Groupe	$\{e_G\} \cong \mathfrak{S}_1 \cong \mathfrak{A}_2$	$\mathbb{Z}/2\mathbb{Z} \cong \mathfrak{S}_2 \cong D_2$	$\mathbb{Z}/3\mathbb{Z} \cong \mathfrak{A}_3$	$\mathbb{Z}/4\mathbb{Z}$ ou $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong D_4$	$\mathbb{Z}/5\mathbb{Z}$

Ordre du groupe	6	7	8	9
Groupe	$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$ ou $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/9\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Ordre du groupe	10	11	12
Groupe	$\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/11\mathbb{Z}$	$\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ou $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Ordre du groupe	13	14	15
Groupe	$\mathbb{Z}/13\mathbb{Z}$	$\mathbb{Z}/14\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Enfin, en ce qui concerne les groupes non abéliens, on ne connaît pas de classification complète et il est plus difficile d'avoir des informations sur eux. On sait par exemple que tout groupe simple non abélien est d'ordre pair (théorème de Feit-Thompson) et le plus petit est le groupe $\mathfrak{A}_5$ (d'ordre 60) ou bien encore que le plus petit groupe non abélien d'ordre impair est le groupe de Frobenius F_{21} (d'ordre 21).

On donne ci-dessous les groupes non abéliens (à isomorphisme près) de cardinal inférieur ou égal à 15 :

Ordre du groupe	6	8	10	12	14
Groupe	$\mathfrak{S}_3 \cong D_6$	D_8 ou $\mathbb{H}_8$	D_{10}	$D_{12} \cong D_6 \times \mathbb{Z}/2\mathbb{Z}$ ou $\mathfrak{A}_4$ ou $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$	D_{14}

VIII.2 Pour aller plus loin...

Il est bien évidemment possible d'aller plus loin dans la classification des groupes finis mais cela devient très vite compliqué (surtout lorsque le groupe n'est pas commutatif !) au-delà de 15 (c'est notamment pour cela que l'on s'est arrêté ici). On notera cependant qu'il existe des techniques pour déterminer tous les groupes abéliens d'ordre fini donné (encore une fois grâce au théorème de structure des groupes abéliens finis).

On donne ci-dessous à titre de curiosité mathématique le nombre de groupes (à l'isomorphisme près) d'ordre compris entre 16 et 20 :

Ordre du groupe	16	17	18	19	20
Nombre de groupes abéliens	5	1	2	1	2
Nombre de groupes non abéliens	9	0	3	0	3
Nombre total de groupes	14	1	5	1	5

Pour remédier à ce problème, il est possible de s'intéresser uniquement aux groupes simples. En effet, à l'image des nombres premiers en arithmétique, ceux-ci sont les "briques" fondamentales de la théorie des groupes et comprendre ces groupes permet de comprendre n'importe quel groupe (théorème de Jordan-Hölder).

Dans l'étude de la classification des groupes finis simples, les mathématiciens ont été amenés à découvrir des êtres mathématiques inattendus qu'ils appelèrent des groupes sporadiques pour marquer le fait qu'ils n'apparaissent dans aucune des listes générales. La classification montre que tout groupe fini simple est de l'un des types suivants :
∗ Un groupe cyclique dont l'ordre est un nombre premier.

∗ Un groupe alterné de degré au moins égal à 5.

∗ Un groupe classique (groupe linéaire spécial projectif, symplectique, orthogonal ou unitaire sur un corps fini).

∗ Un groupe de type de Lie exceptionnel ou tordu (on inclut en général le groupe de Tits dans ce cas).

∗ Un des 26 groupes sporadiques.

Cette classification a des applications dans beaucoup de branches des mathématiques, les questions sur les groupes finis pouvant souvent se réduire à des questions sur les groupes finis simples, et donc à une énumération de cas.