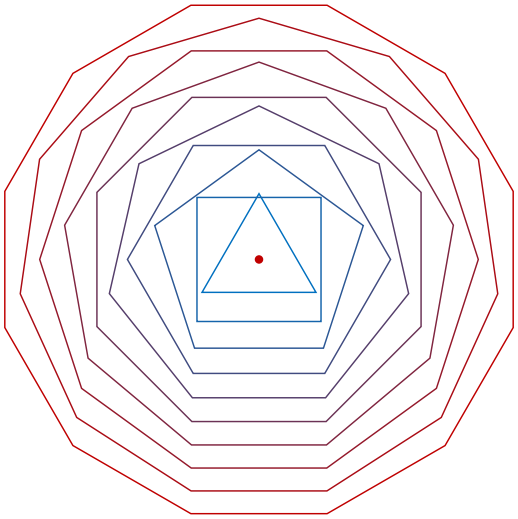
Liste des premiers groupes finis

Les vingt-quatre groupes d'ordre inférieur ou égal à douze



Je ne sais si je n'ai pas déjà dit quelque part que la mathématique est l'art de donner le même nom à des choses différentes.

Henri Poincaré, *Science et méthode*, Flammarion, 1908, livre I, chapitre II (« L'avenir des mathématiques »), texte d'une conférence lue par Gaston Darboux au Congrès international des mathématiciens de Rome en avril 1908.

Ce document décrit, un par un, les vingt-quatre groupes d'ordre inférieur ou égal à douze. Pour chacun : une fiche signalétique, une présentation par générateurs et relations, le treillis complet de ses sous-groupes avec l'indication de ceux qui sont distingués, une réalisation géométrique explicite et un ou deux points d'ancrage en algèbre. Les classifications sont démontrées, non admises. Toutes les tables, tous les ordres d'éléments et tous les treillis ont été recalculés par ordinateur avant rédaction.

Document de référence — M. Jourdain

Table des matières

Introduction : ce que l'on entend par « lister les groupes » **3**

1 Ordre 1 **7**
1.1 Le groupe trivial $\{e\}$ . . . 7

2 Ordre 2 **9**
2.1 Le groupe $\mathbb{Z}/2\mathbb{Z}$ . . . 9

3 Ordre 3 **11**
3.1 Le groupe $\mathbb{Z}/3\mathbb{Z}$ . . . 11

4 Ordre 4 **13**
4.1 Le groupe cyclique $\mathbb{Z}/4\mathbb{Z}$ . . . 13
4.2 Le groupe de Klein $\mathcal{V}$ . . . 13
4.3 Comparaison des deux groupes d'ordre 4 . . . 14

5 Ordre 5 **16**
5.1 Le groupe $\mathbb{Z}/5\mathbb{Z}$ . . . 16

6 Ordre 6 **17**
6.1 Le groupe cyclique $\mathbb{Z}/6\mathbb{Z}$ . . . 17
6.2 Le groupe symétrique $\mathfrak{S}_3 \simeq \mathcal{D}_3$ . . . 18

7 Ordre 7 **20**
7.1 Le groupe $\mathbb{Z}/7\mathbb{Z}$ . . . 20

8 Ordre 8 **21**
8.1 Le groupe cyclique $\mathbb{Z}/8\mathbb{Z}$ . . . 21
8.2 Le groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . . . 22
8.3 Le groupe $(\mathbb{Z}/2\mathbb{Z})^3$ . . . 23
8.4 Le groupe diédral $\mathcal{D}_4$ . . . 24
8.5 Le groupe des quaternions $\mathcal{Q}_8$ . . . 25
8.6 Comparaison des cinq groupes d'ordre 8 . . . 26

9 Ordre 9 **27**
9.1 Le groupe cyclique $\mathbb{Z}/9\mathbb{Z}$ . . . 27
9.2 Le groupe $(\mathbb{Z}/3\mathbb{Z})^2$ . . . 27

10 Ordre 10 **29**
10.1 Le groupe cyclique $\mathbb{Z}/10\mathbb{Z}$ . . . 29
10.2 Le groupe diédral $\mathcal{D}_5$ . . . 29

11 Ordre 11 **31**
11.1 Le groupe $\mathbb{Z}/11\mathbb{Z}$ . . . 31

12 Ordre 12 **32**
12.1 Le groupe cyclique $\mathbb{Z}/12\mathbb{Z}$ 33
12.2 Le groupe $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 33
12.3 Le groupe diédral $\mathcal{D}_6$ 34
12.4 Le groupe alterné $\mathfrak{A}_4$ 35
12.5 Le groupe dicyclique Dic_3 37
12.6 Comparaison des cinq groupes d'ordre 12 38

Conclusion : au-delà de l'ordre 12 **39**

Introduction : ce que l'on entend par « lister les groupes »

Le sens de la question

Combien existe-t-il de groupes à huit éléments ? La question paraît absurde tant qu'on ne précise pas ce qu'on accepte d'appeler « le même groupe ». Les rotations du carré, les puissances de i dans $\mathbb{C}$, et les restes modulo 4 munis de l'addition sont trois objets que rien ne rapproche : l'un est fait de mouvements du plan, le deuxième de nombres complexes, le troisième de classes d'entiers. Pourtant, dès qu'on remplace la rotation d'un quart de tour par i, et i par la classe de 1, les trois tables de multiplication deviennent identiques. Le mathématicien décide alors de ne pas les distinguer, et la citation de Poincaré placée en exergue décrit exactement ce geste.

> **Définition :** Soient $(G, *)$ et $(H, \cdot)$ deux groupes. Un **isomorphisme** de G sur H est une bijection $\varphi : G \to H$ telle que $\varphi(x * y) = \varphi(x) \cdot \varphi(y)$ pour tous $x, y \in G$. Lorsqu'il en existe un, on dit que G et H sont **isomorphes** et l'on note $G \simeq H$.

> *Remarque :* L'isomorphie est une relation d'équivalence sur les groupes : l'identité est un isomorphisme, la réciproque d'un isomorphisme en est un, et la composée de deux isomorphismes en est un. « Lister les groupes d'ordre n » signifie donc décrire les classes d'équivalence pour cette relation, et non pas décrire tous les groupes à n éléments, qui sont en nombre infini dès que $n \geqslant 1$.

Dans tout ce document, l'**ordre** d'un groupe G, noté $|G|$, est son nombre d'éléments, et l'**ordre** d'un élément x, noté $\mathrm{o}(x)$, est le plus petit entier $k \geqslant 1$ tel que $x^k = e$. Ces deux emplois du même mot ne sont pas un abus : l'ordre de x est précisément l'ordre du groupe $\langle x \rangle$ qu'il engendre.

Le résultat

Il y a exactement vingt-quatre classes d'isomorphisme de groupes d'ordre au plus douze. Le tableau ci-dessous les récapitule ; chacune fait l'objet d'une section du document.

Ordre	Nombre	Les groupes
1	1	$\{e\}$
2	1	$\mathbb{Z}/2\mathbb{Z}$
3	1	$\mathbb{Z}/3\mathbb{Z}$
4	2	$\mathbb{Z}/4\mathbb{Z}$; $\mathcal{V} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
5	1	$\mathbb{Z}/5\mathbb{Z}$
6	2	$\mathbb{Z}/6\mathbb{Z}$; $\mathfrak{S}_3 \simeq \mathcal{D}_3$
7	1	$\mathbb{Z}/7\mathbb{Z}$
8	5	$\mathbb{Z}/8\mathbb{Z}$; $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z})^3$; $\mathcal{D}_4$; $\mathcal{Q}_8$
9	2	$\mathbb{Z}/9\mathbb{Z}$; $(\mathbb{Z}/3\mathbb{Z})^2$
10	2	$\mathbb{Z}/10\mathbb{Z}$; $\mathcal{D}_5$
11	1	$\mathbb{Z}/11\mathbb{Z}$
12	5	$\mathbb{Z}/12\mathbb{Z}$; $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; $\mathcal{D}_6$; $\mathfrak{A}_4$; Dic_3

Remarque : Les ordres 1, 2, 3, 5, 7 et 11 ne portent qu'un seul groupe, et l'on verra au chapitre 2 pourquoi : ce sont des nombres premiers. En revanche 4 en porte deux et 8 en porte cinq, alors que 6, 10 et 9 n'en portent que deux : la richesse ne croît pas avec n, elle croît avec la façon dont n se factorise. Les ordres 8 et 12 sont les deux sommets de notre parcours.

Les cinq outils employés

Quatre théorèmes et une construction suffisent à établir toute la liste. Ils sont rappelés ici sans démonstration lorsque celle-ci est classique, et réemployés au fil des chapitres.

Théorème 1 (Lagrange, 1771) : Si G est un groupe fini et H un sous-groupe de G, alors $|H|$ divise $|G|$. En particulier, l'ordre de tout élément de G divise $|G|$.

∘ *Démonstration :* Pour $g \in G$, la classe à gauche $gH = \{gh,\ h \in H\}$ est en bijection avec H par $h \mapsto gh$, donc $|gH| = |H|$. Deux classes sont égales ou disjointes : si $z \in gH \cap g'H$, alors $gH = zH = g'H$. Comme tout g appartient à gH, les classes forment une partition de G en parts de cardinal $|H|$, d'où $|G| = [G : H]\,|H|$ où $[G : H]$ désigne le nombre de classes. □

Théorème 2 (Cauchy, 1845) : Si p est un nombre premier divisant $|G|$, alors G possède un élément d'ordre p.

Théorème 3 (Sylow, 1872) : Soit $|G| = p^a m$ avec p premier ne divisant pas m. Alors G possède des sous-groupes d'ordre p^a, dits **p-sous-groupes de Sylow** ; ils sont tous conjugués entre eux ; et leur nombre n_p vérifie

$$n_p \equiv 1 \pmod{p} \qquad \text{et} \qquad n_p \mid m.$$

En particulier, $n_p = 1$ équivaut à ce que l'unique p-Sylow soit distingué dans G.

Théorème 4 (classification des groupes abéliens finis) : Tout groupe abélien fini est isomorphe à un produit $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$ avec $d_1 \mid d_2 \mid \cdots \mid d_r$, et cette suite de **facteurs invariants** est unique.

Remarque : On peut aussi décomposer en facteurs de la forme $\mathbb{Z}/p^k\mathbb{Z}$: le nombre de groupes abéliens d'ordre $n = p_1^{a_1} \cdots p_s^{a_s}$ vaut alors $P(a_1) \times \cdots \times P(a_s)$, où $P(a)$ est le nombre de partitions de l'entier a. Pour $n = 8 = 2^3$ on trouve $P(3) = 3$ groupes abéliens, ce que le chapitre 8 confirmera.

Enfin, la construction qui produit presque tous les groupes non abéliens de la liste :

Définition : Soient N et H deux groupes et $\varphi : H \to \mathrm{Aut}(N)$ un morphisme. Le **produit semi-direct** $N \rtimes_\varphi H$ est l'ensemble $N \times H$ muni de

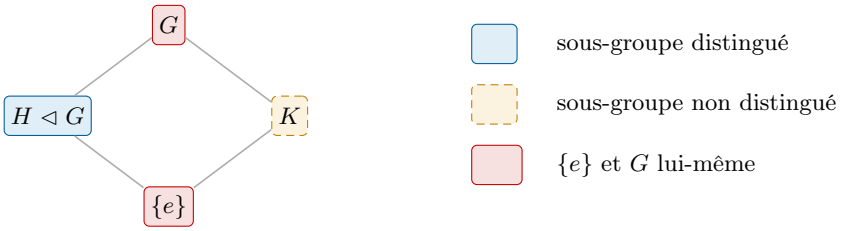
$$(n, h) \cdot (n', h') = \big(n\,\varphi(h)(n'),\ hh'\big).$$

Lorsque φ est trivial, on retrouve le produit direct $N \times H$.

Remarque : Tout l'intérêt du procédé tient dans le choix de φ. C'est pourquoi le calcul du groupe $\mathrm{Aut}(N)$ revient sans cesse : il mesure de combien de manières H peut « tordre » N. On retiendra $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, de cardinal $\varphi(n)$ (indicatrice d'Euler) ; en particulier $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ et $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ sont d'ordre 2, tandis que $\mathrm{Aut}(\mathcal{V}) \simeq \mathfrak{S}_3$ est d'ordre 6.

Comment lire les treillis de sous-groupes

Chaque groupe est accompagné de son **treillis de sous-groupes** : un diagramme de Hasse dont les sommets sont les sous-groupes et où l'on relie H à K dès que $H \subsetneq K$ *sans sous-groupe intermédiaire*. Les inclusions non dessinées se lisent par transitivité. Le groupe entier est en haut, le sous-groupe trivial $\{e\}$ en bas.



Lecture du diagramme : un trait montant signifie « est contenu dans, sans intermédiaire ». Le remplissage bleu continu signale un sous-groupe *distingué* ($gHg^{-1} = H$ pour tout g), c'est-à-dire un sous-groupe par lequel on peut quotienter ; le contour orange pointillé signale un sous-groupe non distingué, qui possède alors des conjugués distincts de lui-même, tous de même ordre. Dans un groupe abélien, tous les sous-groupes sont distingués et le diagramme est entièrement bleu et rouge.

Remarque : Le treillis n'est pas un invariant complet : deux groupes non isomorphes peuvent avoir des treillis de même forme. Le cas le plus frappant est celui de $\mathfrak{S}_3$ (ordre 6) et de $(\mathbb{Z}/3\mathbb{Z})^2$ (ordre 9) : tous deux ont un treillis à six sommets fait d'un plancher, d'un plafond et de quatre sous-groupes propres deux à deux incomparables, alors que l'un est non abélien et l'autre abélien, et qu'ils n'ont même pas le même cardinal. On comparera les chapitres 6 et 9. Inversement, deux groupes dont les treillis diffèrent ne sont certainement pas isomorphes : c'est l'usage que nous en ferons le plus souvent.

Remarque : Les tables de Cayley, les ordres des éléments et les treillis présentés dans ce document ont été recalculés par ordinateur avant rédaction. Les nombres de sous-groupes annoncés — notamment les 16 sous-groupes de $\mathcal{D}_6$ et de $(\mathbb{Z}/2\mathbb{Z})^3$, souvent mal recopiés dans la littérature — sont donc fiables.

Ordre 1

1.1 Le groupe trivial $\{e\}$

Notations	$\{e\}$, 1, $\mathbb{Z}/1\mathbb{Z}$, $\mathfrak{S}_1$, $\mathfrak{A}_1$, $\mathfrak{A}_2$
Présentation	$\langle \mid \rangle$: aucun générateur, aucune relation
Ordres des éléments	1 élément d'ordre 1
Sous-groupes	un seul : lui-même

Il n'y a qu'un seul élément, le neutre, et une seule façon de le multiplier par lui-même : $e \cdot e = e$. Les axiomes de groupe sont vérifiés sans rien vérifier. Ce groupe est abélien, cyclique, et engendré par la partie vide.

Remarque : On hésite parfois à l'appeler un groupe, comme on hésite à appeler 1 un produit vide. C'est pourtant la même convention, et elle est indispensable : sans elle, l'énoncé « le noyau d'un morphisme injectif est trivial » n'aurait pas de sens, et l'intersection de deux sous-groupes d'intersection réduite au neutre ne serait pas un sous-groupe.

Sous-groupes

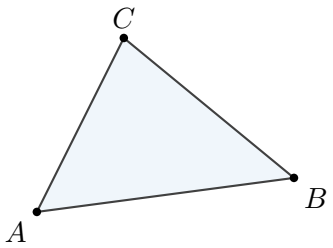
Le seul sous-groupe de $\{e\}$ est $\{e\}$. Le treillis se réduit à un sommet.



Le treillis le plus simple possible. C'est aussi le seul cas où le sommet $\{e\}$ et le sommet G sont confondus ; dans tous les chapitres suivants ils seront distincts.

Lien avec la géométrie

Un groupe de symétries se réduit au groupe trivial exactement quand la figure étudiée n'admet aucune symétrie autre que l'identité : aucune rotation, aucune réflexion ne la laisse globalement invariante. C'est le cas générique — une figure prise au hasard n'a aucune symétrie — et c'est pourquoi les figures symétriques nous frappent.



$AB \neq BC \neq CA$: les trois côtés sont deux à deux distincts, donc aucune isométrie non triviale ne conserve le triangle.

Un triangle scalène : son groupe d'isométries est $\{e\}$. Une isométrie qui le conserve permute ses sommets en préservant les longueurs ; comme les trois côtés ont des longueurs distinctes, chaque sommet est caractérisé par les deux longueurs qui l'encadrent et doit donc rester fixe. L'isométrie fixe trois points non alignés : c'est l'identité.

Lien avec l'algèbre

Le groupe trivial est l'élément neutre du produit direct : $G \times \{e\} \simeq G$ pour tout groupe G. Il apparaît comme noyau de tout morphisme injectif, comme groupe de Galois $\mathrm{Gal}(K/K)$ d'une extension triviale, et comme groupe fondamental $\pi_1(X)$ d'un espace simplement connexe.

> *Remarque :* C'est le seul groupe qui soit à la fois *initial* et *final* : pour tout groupe G, il existe exactement un morphisme $\{e\} \to G$ et exactement un morphisme $G \to \{e\}$. Cette double propriété fait de lui l'« objet nul » de la théorie des groupes, et c'est elle qui rend possible la notion de suite exacte $1 \to N \to G \to Q \to 1$, dont nous ferons usage à partir du chapitre 6.

Ordre 2

Le chapitre est court, mais il installe le théorème qui règle d'un coup les ordres 2, 3, 5, 7 et 11.

Théorème 5 : Si $|G| = p$ avec p premier, alors G est cyclique, donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Il n'y a donc, à isomorphisme près, qu'un seul groupe d'ordre p.

∘ *Démonstration :* Comme $p \geqslant 2$, choisissons $x \in G$ avec $x \neq e$. Le sous-groupe $\langle x \rangle$ contient e et x, donc $|\langle x \rangle| \geqslant 2$. Par le théorème de Lagrange, $|\langle x \rangle|$ divise p ; les seuls diviseurs de p étant 1 et p, on a $|\langle x \rangle| = p$, c'est-à-dire $\langle x \rangle = G$. Le morphisme $\mathbb{Z}/p\mathbb{Z} \to G$, $\overline{k} \mapsto x^k$, est alors bien défini et bijectif. □

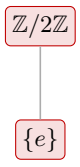
Remarque : La démonstration montre davantage : dans un groupe d'ordre premier, *tout* élément distinct du neutre est un générateur. C'est une propriété très rigide, et elle explique la pauvreté du treillis de ces groupes. On dit d'ailleurs que ces groupes sont **simples** : ils n'ont aucun sous-groupe distingué autre que $\{e\}$ et eux-mêmes.

2.1 Le groupe $\mathbb{Z}/2\mathbb{Z}$

Notations	$\mathbb{Z}/2\mathbb{Z}$, $\mathbb{F}_2$, $\{\pm 1\}$, $\mathfrak{S}_2$, $\mathcal{D}_1$
Présentation	$\langle s \mid s^2 = e \rangle$
Ordres des éléments	1 élément d'ordre 1, 1 élément d'ordre 2
Sous-groupes	2 sous-groupes, tous distingués

L'élément non trivial s est son propre inverse : c'est une **involution**. La table de Cayley tient en quatre cases.

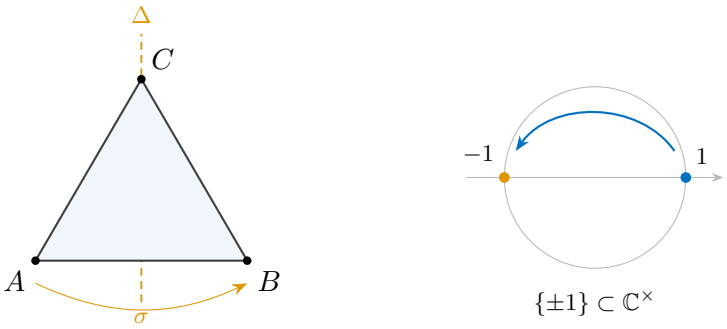
$\cdot$	e	s
e	e	s
s	s	e



À gauche la table de Cayley, à droite le treillis. Le treillis d'un groupe d'ordre premier est toujours cette « arête » à deux sommets : il n'y a pas de place pour un sous-groupe intermédiaire, puisque son ordre devrait diviser strictement 2 tout en étant strictement supérieur à 1.

Lien avec la géométrie

C'est le groupe d'une **réflexion**. Une figure du plan qui possède un axe de symétrie et rien d'autre a pour groupe d'isométries $\{\mathrm{id}, \sigma\}$, où σ est la réflexion d'axe Δ. On a bien $\sigma \circ \sigma = \mathrm{id}$: appliquer deux fois le miroir rend la figure inchangée.



Deux incarnations du même groupe. À gauche, le triangle isocèle et sa réflexion σ d'axe Δ : σ échange A et B et fixe C. À droite, les racines carrées de l'unité dans $\mathbb{C}$: la multiplication par -1 échange 1 et -1. Les deux tables de Cayley coïncident quand on pose $\sigma \leftrightarrow -1$.

Lien avec l'algèbre

Ce groupe est omniprésent parce qu'il code toutes les alternatives binaires stables par composition.

Exemple : La **signature** $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est un morphisme surjectif dès que $n \geqslant 2$; son noyau est le groupe alterné $\mathfrak{A}_n$. Le déterminant restreint au groupe orthogonal donne de même $\det : \mathrm{O}(n) \to \{\pm 1\}$, dont le noyau est $\mathrm{SO}(n)$: c'est la distinction entre isométries directes et indirectes, que nous retrouverons à chaque groupe diédral.

Exemple : $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, z \mapsto \overline{z}\} \simeq \mathbb{Z}/2\mathbb{Z}$. Plus généralement, toute extension quadratique $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ a pour groupe de Galois $\mathbb{Z}/2\mathbb{Z}$, l'élément non trivial envoyant $\sqrt{d}$ sur $-\sqrt{d}$.

Remarque : Une conséquence du théorème de Cauchy mérite d'être retenue telle quelle : *tout groupe d'ordre pair contient un élément d'ordre* 2. On peut aussi le voir sans Cauchy, en appariant chaque élément avec son inverse : les éléments x tels que $x \neq x^{-1}$ vont par paires, donc ceux qui vérifient $x = x^{-1}$ sont en nombre pair ; comme e en fait partie, il y en a au moins un autre.

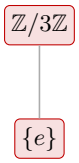
Ordre 3

3.1 Le groupe $\mathbb{Z}/3\mathbb{Z}$

Notations	$\mathbb{Z}/3\mathbb{Z}$, $\mathbb{F}_3$, μ_3, $\mathfrak{A}_3$
Présentation	$\langle r \mid r^3 = e \rangle$
Ordres des éléments	1 élément d'ordre 1, 2 éléments d'ordre 3
Sous-groupes	2 sous-groupes, tous distingués

Par le théorème 5, il n'y a qu'un groupe d'ordre 3. Ses deux éléments non triviaux sont r et $r^2 = r^{-1}$: chacun engendre le groupe, et ils sont inverses l'un de l'autre.

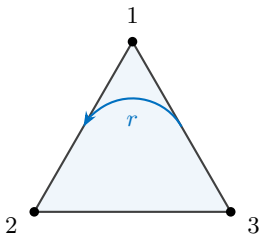
$\cdot$	e	r	r^2
e	e	r	r^2
r	r	r^2	e
r^2	r^2	e	r



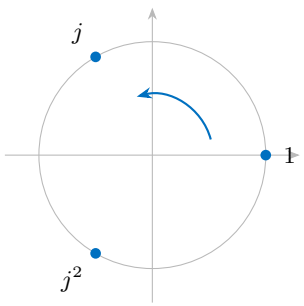
Chaque ligne de la table est la précédente décalée d'un cran : c'est la signature visuelle d'un groupe cyclique. Le treillis, comme pour tout ordre premier, ne comporte que deux sommets.

Lien avec la géométrie

C'est le groupe des rotations qui conservent un triangle équilatéral : rotation d'un tiers de tour, de deux tiers de tour, et identité. Il s'identifie aussi au groupe multiplicatif $\mu_3 = \{1, j, j^2\}$ des racines cubiques de l'unité, où $j = e^{2i\pi/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.



rotations du triangle



racines cubiques de 1

Les sommets du triangle sont numérotés 1, 2, 3 dans le sens direct ; la rotation r les envoie sur 2, 3, 1. À droite, la multiplication par j fait tourner le triangle $\{1, j, j^2\}$ d'un tiers de tour. Les sommets du triangle équilatéral inscrit dans le cercle unité *sont* les racines cubiques de l'unité : les deux figures sont la même, lue une fois avec des mouvements et une fois avec des nombres.

Lien avec l'algèbre

$\mathbb{Z}/3\mathbb{Z}$ est le groupe additif du corps $\mathbb{F}_3$, et le groupe alterné $\mathfrak{A}_3$ des permutations paires de trois lettres. En théorie de Galois, c'est le groupe de l'extension cyclique $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}$ de degré 3, ou encore celui du corps de décomposition de $X^3 - 3X + 1$, dont le discriminant 81 est un carré.

Remarque : L'erreur la plus répandue à ce stade est de croire qu'un groupe d'ordre impair ne peut contenir d'involution « parce qu'il n'y a pas de symétrie ». La raison est autre, et purement arithmétique : l'ordre d'une involution vaut 2, qui devrait diviser un nombre impair.

Ordre 4

C'est le premier ordre qui porte deux groupes. La bifurcation tient à une seule question : existe-t-il un élément d'ordre 4 ?

Théorème 6 : Tout groupe d'ordre 4 est abélien, et il est isomorphe soit à $\mathbb{Z}/4\mathbb{Z}$, soit au groupe de Klein $\mathcal{V} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

∘ *Démonstration :* Soit $|G| = 4$. Par Lagrange, l'ordre de tout élément divise 4, donc vaut 1, 2 ou 4. *Premier cas :* il existe x d'ordre 4 ; alors $\langle x \rangle = G$ et $G \simeq \mathbb{Z}/4\mathbb{Z}$. *Second cas :* tout élément $x \neq e$ est d'ordre 2, donc $x^2 = e$, c'est-à-dire $x = x^{-1}$ pour tout $x \in G$. Pour $x, y \in G$ on a alors

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

donc G est abélien. En posant $G = \{e, a, b, c\}$, le produit ab ne peut valoir ni e (sinon $b = a^{-1} = a$), ni a (sinon $b = e$), ni b (sinon $a = e$) : donc $ab = c$. Les neuf autres produits s'en déduisent, et $G \simeq \mathcal{V}$. □

Remarque : Ce raisonnement contient un lemme réutilisable : *un groupe dans lequel tout élément est son propre inverse est abélien.* Il servira encore au chapitre 8 pour $(\mathbb{Z}/2\mathbb{Z})^3$.

4.1 Le groupe cyclique $\mathbb{Z}/4\mathbb{Z}$

Notations	$\mathbb{Z}/4\mathbb{Z}$, $\mu_4 = \{1, i, -1, -i\}$, $\mathbb{Z}/4\mathbb{Z}$
Présentation	$\langle r \mid r^4 = e \rangle$
Ordres des éléments	1 élément d'ordre 1, 1 élément d'ordre 2, 2 éléments d'ordre 4
Sous-groupes	3 sous-groupes, tous distingués, formant une chaîne

L'élément r engendre tout le groupe : e, r, r^2, r^3. On remarquera que r^2 est la *seule* involution, et que r et r^3 sont les deux générateurs.

Lien avec la géométrie

C'est le groupe des rotations du carré : identité, quart de tour, demi-tour, trois quarts de tour. Il s'identifie à $\mu_4 = \{1, i, -1, -i\}$, où la multiplication par i *est* le quart de tour direct.

4.2 Le groupe de Klein $\mathcal{V}$

Notations	$\mathcal{V}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{F}_2)^2$, *Vierergruppe*
Présentation	$\langle a, b \mid a^2 = b^2 = e,\ ab = ba \rangle$
Ordres des éléments	1 élément d'ordre 1, 3 éléments d'ordre 2
Sous-groupes	5 sous-groupes, tous distingués

Les trois éléments non triviaux a, b, $c = ab$ jouent des rôles parfaitement symétriques : le produit de deux d'entre eux est le troisième, et chacun est sa propre inverse. C'est le plus petit groupe non cyclique.

4.3 Comparaison des deux groupes d'ordre 4

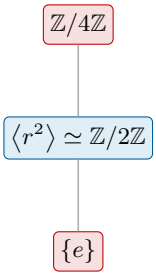
Les deux tables de Cayley

$\cdot$	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

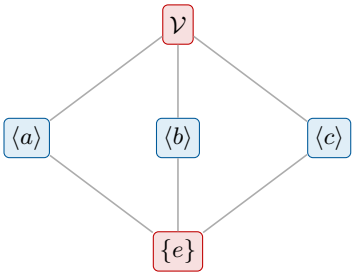
$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Les tables de $\mathbb{Z}/4\mathbb{Z}$ (à gauche) et de $\mathcal{V}$ (à droite). Elles se distinguent au premier coup d'œil par leur diagonale : celle de $\mathcal{V}$ ne contient que e, puisque tout élément y est involutif, alors que celle de $\mathbb{Z}/4\mathbb{Z}$ contient r^2 deux fois. C'est le test le plus rapide pour reconnaître lequel des deux groupes on a sous les yeux.

Les deux treillis



$\mathbb{Z}/4\mathbb{Z}$: une chaîne

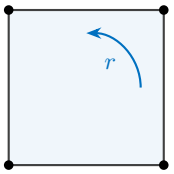


$\mathcal{V}$: un diamant

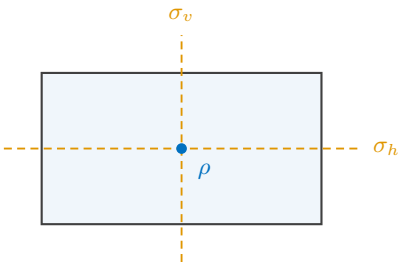
Les deux groupes d'ordre 4 ont des treillis de formes incompatibles : $\mathbb{Z}/4\mathbb{Z}$ a un unique sous-groupe propre, $\mathcal{V}$ en a trois. Cela suffit à prouver qu'ils ne sont pas isomorphes, sans même examiner leurs tables. Les cinq sommets de $\mathcal{V}$ sont tous bleus ou rouges : le groupe étant abélien, tous ses sous-groupes sont distingués.

Lien avec la géométrie

Le groupe de Klein est le groupe d'isométries d'un rectangle non carré : identité, réflexion d'axe horizontal, réflexion d'axe vertical, et demi-tour autour du centre. Le carré, lui, a huit isométries et fournira $\mathcal{D}_4$ au chapitre 8 ; en n'en gardant que les rotations on obtient $\mathbb{Z}/4\mathbb{Z}$.



carré : 4 rotations
$\Rightarrow \mathbb{Z}/4\mathbb{Z}$



rectangle : $\mathrm{id}, \sigma_h, \sigma_v, \rho$
$\Rightarrow \mathcal{V}$

À gauche, les quatre rotations du carré engendrées par le quart de tour r. À droite, les quatre isométries du rectangle : les deux réflexions σ_h, σ_v d'axes les médiatrices, et le demi-tour ρ de centre le centre du rectangle. On vérifie sur la figure que $\sigma_h\sigma_v = \rho$: réfléchir selon les deux axes revient à faire un demi-tour. Aucune de ces trois transformations n'est d'ordre 4, ce qui confirme que le groupe du rectangle n'est pas $\mathbb{Z}/4\mathbb{Z}$.

Lien avec l'algèbre

$\mathcal{V}$ est le plan vectoriel $(\mathbb{F}_2)^2$: ses trois sous-groupes d'ordre 2 sont ses trois droites vectorielles, et le treillis en diamant ci-dessus est exactement le treillis des sous-espaces de ce plan. C'est aussi le sous-groupe $\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ de $\mathfrak{S}_4$, dont nous verrons au chapitre 12 qu'il est distingué dans $\mathfrak{A}_4$: cette copie de $\mathcal{V}$ est la clé de la résolution des équations du quatrième degré.

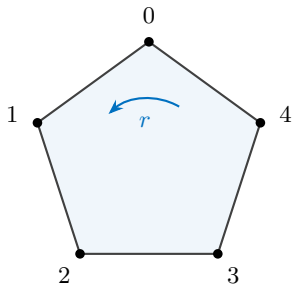
Exemple : $\mathrm{Gal}\big(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\big) \simeq \mathcal{V}$: un automorphisme est déterminé par les signes qu'il donne à $\sqrt{2}$ et $\sqrt{3}$, soit quatre possibilités, et chacun est involutif. Les trois sous-groupes d'ordre 2 correspondent aux trois sous-corps quadratiques $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ et $\mathbb{Q}(\sqrt{6})$. En revanche $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \simeq (\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z}$, qui est cyclique : c'est cette différence qui rend le pentagone régulier constructible à la règle et au compas.

Ordre 5

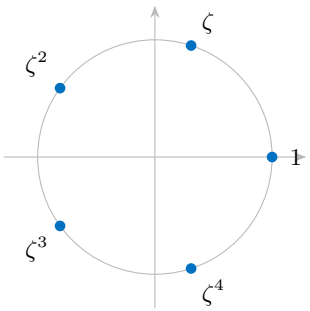
5.1 Le groupe $\mathbb{Z}/5\mathbb{Z}$

Notations	$\mathbb{Z}/5\mathbb{Z}$, $\mathbb{F}_5$, μ_5
Présentation	$\langle r \mid r^5 = e \rangle$
Ordres des éléments	1 élément d'ordre 1, 4 éléments d'ordre 5
Sous-groupes	2 sous-groupes, tous distingués

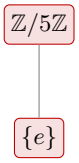
Le théorème 5 s'applique : 5 étant premier, il n'y a qu'un groupe d'ordre 5, et chacun de ses quatre éléments non triviaux l'engendre.



rotations du pentagone



μ_5, racines 5-ièmes de 1



Les sommets du pentagone régulier inscrit dans le cercle unité sont les racines cinquièmes de l'unité $\zeta^k = e^{2ik\pi/5}$; la rotation r d'un cinquième de tour correspond à la multiplication par ζ. Comme 5 est premier, toute puissance ζ^k avec $k \not\equiv 0$ est encore une racine *primitive* : on peut parcourir les cinq sommets en partant de n'importe lequel d'entre eux, ce que traduit le treillis à deux étages placé à droite.

Lien avec l'algèbre

$\mathbb{Z}/5\mathbb{Z}$ est le groupe additif de $\mathbb{F}_5$. On le rencontre comme sous-groupe distingué d'indice 2 dans $\mathcal{D}_5$ (chapitre 10) et comme unique 5-Sylow de tout groupe d'ordre 10 ou 20. En théorie de Galois, c'est le groupe de l'unique sous-extension de degré 5 de $\mathbb{Q}(\zeta_{11})$, dont le groupe de Galois est cyclique d'ordre 10.

Remarque : Il ne faut pas confondre ce groupe très docile avec $\mathfrak{A}_5$, d'ordre 60, qui est le premier groupe simple non abélien et dont la non-résolubilité interdit la résolution par radicaux de l'équation générale du cinquième degré. L'ordre 5 et le degré 5 jouent ici deux rôles sans rapport.

Ordre 6

L'ordre 6 est celui où apparaît la non-commutativité. Un théorème général règle d'un coup les ordres 6 et 10.

Théorème 7 : Soit p un nombre premier impair. Tout groupe d'ordre $2p$ est isomorphe soit à $\mathbb{Z}/2p\mathbb{Z}$, soit au groupe diédral $\mathcal{D}_p$.

∘ *Démonstration :* Soit $|G| = 2p$. Par le théorème de Cauchy, G contient un élément a d'ordre p et un élément b d'ordre 2. Le sous-groupe $\langle a \rangle$ est d'indice 2, donc distingué : pour $g \notin \langle a \rangle$, les deux classes à gauche sont $\langle a \rangle$ et $g\langle a \rangle$, et il en va de même à droite, donc $g\langle a \rangle = \langle a \rangle g$. Ainsi $bab^{-1} \in \langle a \rangle$, disons $bab^{-1} = a^k$. En conjuguant deux fois,

$$a = b^2ab^{-2} = b(a^k)b^{-1} = (bab^{-1})^k = a^{k^2},$$

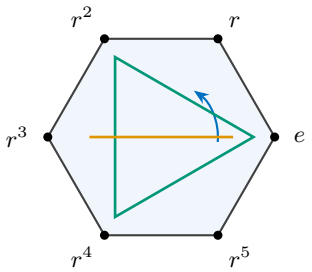
donc $k^2 \equiv 1 \pmod{p}$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, $X^2 - 1$ y a au plus deux racines, qui sont 1 et -1 : donc $k \equiv 1$ ou $k \equiv -1$. Si $k \equiv 1$, alors a et b commutent, ab est d'ordre $2p$ et $G \simeq \mathbb{Z}/2p\mathbb{Z}$. Si $k \equiv -1$, alors $bab^{-1} = a^{-1}$: c'est la relation de présentation de $\mathcal{D}_p$, et $G = \langle a, b \mid a^p = b^2 = e,\ bab^{-1} = a^{-1} \rangle$. □

Remarque : La conjugaison $bab^{-1} = a^{-1}$ mérite une lecture géométrique : si a est une rotation et b une réflexion, alors regarder la rotation « dans le miroir » l'inverse. C'est la relation fondamentale de tous les groupes diédraux, et elle réapparaîtra aux chapitres 8, 10 et 12.

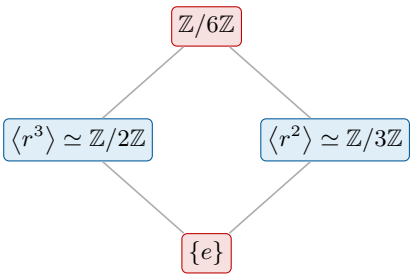
6.1 Le groupe cyclique $\mathbb{Z}/6\mathbb{Z}$

Notations	$\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, μ_6, $(\mathbb{Z}/7\mathbb{Z})^\times$
Présentation	$\langle r \mid r^6 = e \rangle$
Ordres des éléments	1 d'ordre 1, 1 d'ordre 2, 2 d'ordre 3, 2 d'ordre 6
Sous-groupes	4 sous-groupes, tous distingués

L'isomorphisme $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est le théorème des restes chinois : 2 et 3 étant premiers entre eux, se donner un reste modulo 6 revient à se donner un reste modulo 2 et un reste modulo 3. C'est la raison pour laquelle $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ne figure pas comme groupe supplémentaire dans notre liste.



$\langle r^2 \rangle \simeq \mathbb{Z}/3\mathbb{Z}$ en vert,
$\langle r^3 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ en orange



Les six sommets de l'hexagone portent les six puissances de r. En reliant un sommet sur deux on obtient le triangle vert $\{e, r^2, r^4\}$, qui est le sous-groupe d'ordre 3 ; en reliant les deux sommets diamétralement opposés e et r^3 on obtient le sous-groupe d'ordre 2. Le treillis à droite est un diamant, mais il ne faut pas le confondre avec celui de $\mathcal{V}$: ici les deux sous-groupes intermédiaires ont des ordres *différents*, 2 et 3, et leur intersection triviale jointe à $2 \times 3 = 6$ redonne l'isomorphisme $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

6.2 Le groupe symétrique $\mathfrak{S}_3 \simeq \mathcal{D}_3$

Notations	$\mathfrak{S}_3$, $\mathcal{D}_3$, $\mathrm{GL}_2(\mathbb{F}_2)$, $\mathrm{Aut}(\mathcal{V})$
Présentation	$\langle r, s \mid r^3 = s^2 = e,\ srs^{-1} = r^{-1} \rangle$
Ordres des éléments	1 d'ordre 1, 3 d'ordre 2, 2 d'ordre 3
Sous-groupes	6 sous-groupes, dont 3 non distingués

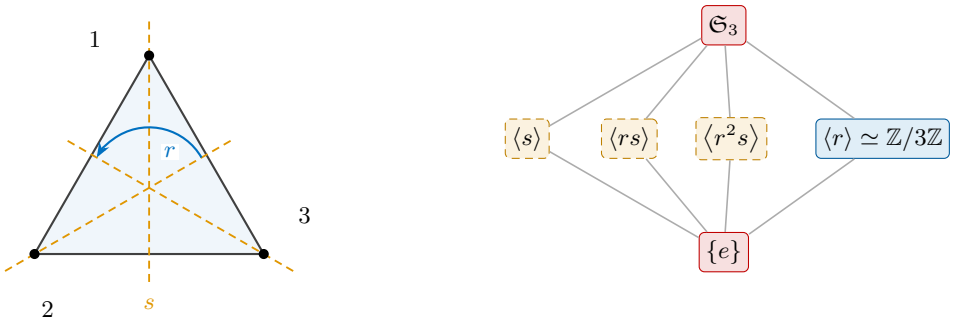
C'est le plus petit groupe non abélien, et le plus petit groupe possédant un sous-groupe non distingué. Ses six éléments sont e, r, r^2 (les rotations) et s, rs, r^2s (les réflexions). La relation $srs^{-1} = r^{-1}$, équivalente à $sr = r^2s$, suffit à réduire tout mot en r et s à la forme $r^i s^j$.

$\cdot$	e	r	r^2	s	rs	r^2s
e	e	r	r^2	s	rs	r^2s
r	r	r^2	e	rs	r^2s	s
r^2	r^2	e	r	r^2s	s	rs
s	s	r^2s	rs	e	r^2	r
rs	rs	s	r^2s	r	e	r^2
r^2s	r^2s	rs	s	r^2	r	e

Table de Cayley de $\mathfrak{S}_3$, les rotations d'abord, les réflexions ensuite. Les deux blocs diagonaux ne contiennent que des rotations et les deux blocs anti-diagonaux que des réflexions : c'est la traduction de « rotation × rotation = rotation » et « rotation × réflexion = réflexion ». On lit la non-commutativité en comparant $r \cdot s = rs$ (ligne r, colonne s) et $s \cdot r = r^2s$ (ligne s, colonne r) : les deux résultats diffèrent.

Lien avec la géométrie

$\mathfrak{S}_3$ est le groupe complet des isométries du triangle équilatéral : trois rotations et trois réflexions, dont les axes sont les trois médiatrices. C'est aussi, et c'est la même chose, le groupe de toutes les permutations des trois sommets : une isométrie du triangle est déterminée par l'image des sommets, et les six permutations sont toutes réalisées.



À gauche, le triangle équilatéral, ses trois axes de symétrie en orange pointillé et la rotation r en bleu. À droite, le treillis : le sous-groupe des rotations $\langle r \rangle$, seul sous-groupe d'ordre 3, est distingué (il est d'indice 2), tandis que les trois sous-groupes engendrés par une réflexion sont *conjugués entre eux* et donc non distingués. On vérifie d'ailleurs sur la table que $r \cdot s \cdot r^{-1} = r^2 s \notin \langle s \rangle$. C'est ici qu'apparaît pour la première fois la couleur orange pointillée.

Lien avec l'algèbre

Trois identifications valent d'être retenues. D'abord $\mathfrak{S}_3 \simeq \mathrm{GL}_2(\mathbb{F}_2)$: le plan $(\mathbb{F}_2)^2$ a trois vecteurs non nuls, qu'une application linéaire inversible permute arbitrairement. Ensuite $\mathfrak{S}_3 \simeq \mathrm{Aut}(\mathcal{V})$, pour la même raison lue du côté des groupes : un automorphisme du groupe de Klein permute ses trois involutions, et toute permutation convient. Enfin, en théorie de Galois, $\mathfrak{S}_3$ est le groupe du corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$, à savoir $\mathbb{Q}(\sqrt[3]{2}, j)$, de degré 6.

Remarque : L'erreur la plus répandue consiste à écrire $\mathfrak{S}_3 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ au prétexte que $6 = 2 \times 3$. C'est faux : ce produit est abélien, donc isomorphe à $\mathbb{Z}/6\mathbb{Z}$. Le produit correct est le produit *semi-direct* $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, où $\mathbb{Z}/2\mathbb{Z}$ agit sur $\mathbb{Z}/3\mathbb{Z}$ par $x \mapsto -x$. Le seul morphisme non trivial $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$ étant l'identité, ce produit semi-direct est unique, ce qui redonne le théorème 7.

Ordre 7

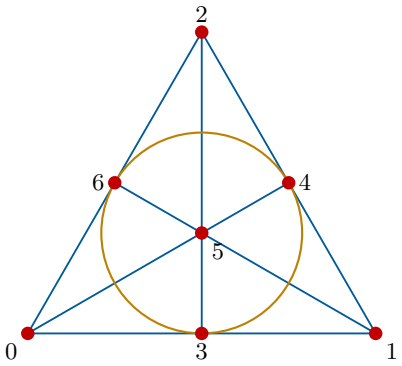
7.1 Le groupe $\mathbb{Z}/7\mathbb{Z}$

Notations	$\mathbb{Z}/7\mathbb{Z}$, $\mathbb{F}_7$, μ_7
Présentation	$\langle r \mid r^7 = e \rangle$
Ordres des éléments	1 élément d'ordre 1, 6 éléments d'ordre 7
Sous-groupes	2 sous-groupes, tous distingués

Le théorème 5 s'applique encore. Ce groupe est engendré par n'importe lequel de ses six éléments non triviaux, et son treillis ne comporte que deux sommets.

Lien avec la géométrie

Outre les rotations de l'heptagone régulier, $\mathbb{Z}/7\mathbb{Z}$ apparaît de façon plus surprenante comme groupe de symétries du **plan de Fano**, la plus petite géométrie projective : sept points, sept droites, trois points sur chaque droite, trois droites par chaque point.



Les sept droites sont les ensembles $\{i,\ i{+}1,\ i{+}3\}$ pour $i = 0, \ldots, 6$:

$\{0,1,3\}$ $\{1,2,4\}$ $\{2,3,5\}$
$\{3,4,6\}$ $\{4,5,0\}$ $\{5,6,1\}$
$\{6,0,2\}$

$i \mapsto i+1$ permute circulairement les sept points et conserve les sept droites.

Le plan de Fano, étiqueté de sorte que la translation $i \mapsto i+1$ modulo 7 en soit une symétrie. Les « droites » sont les trois côtés du triangle, les trois médianes, et le cercle passant par les trois milieux, dessiné en orange : ce cercle est une droite du plan de Fano au même titre que les autres, la courbure n'étant qu'un artifice de dessin. On vérifie par exemple que le côté $[0,1]$ porte aussi le point 3, milieu de $[AB]$, et que $\{0,1,3\}$ figure bien dans la liste. L'étiquetage a été déterminé par recherche exhaustive des bijections compatibles.

Remarque : Le groupe complet des symétries du plan de Fano est $\mathrm{GL}_3(\mathbb{F}_2)$, d'ordre 168 ; $\mathbb{Z}/7\mathbb{Z}$ n'en est qu'un sous-groupe, engendré par la permutation circulaire dessinée ci-dessus. C'est néanmoins $\mathbb{Z}/7\mathbb{Z}$ qui rend l'étiquetage possible, et la liste $\{0,1,3\}$ s'appelle pour cette raison un **ensemble de différences parfait** modulo 7.

Lien avec l'algèbre

$\mathbb{Z}/7\mathbb{Z}$ est le groupe additif de $\mathbb{F}_7$. Il apparaît aussi comme l'unique sous-groupe d'ordre 7 du groupe $(\mathbb{Z}/29\mathbb{Z})^\times$, qui est cyclique d'ordre 28, et comme unique 7-Sylow de tout groupe d'ordre 14 ou 21. Il faut enfin noter que $(\mathbb{Z}/7\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z}$: le groupe *multiplicatif* de $\mathbb{F}_7$ est le groupe cyclique d'ordre 6 étudié au chapitre précédent, ce qui illustre le théorème selon lequel le groupe multiplicatif d'un corps fini est toujours cyclique.

Ordre 8

Avec cinq groupes, l'ordre 8 est le premier sommet du parcours. Trois de ces groupes sont abéliens — la classification des groupes abéliens finis les donne d'emblée, puisque $8 = 2^3$ et que 3 admet trois partitions 3, $2+1$, $1+1+1$ — et deux sont non abéliens.

Théorème 8 : Tout groupe d'ordre 8 est isomorphe à l'un des cinq groupes suivants, deux à deux non isomorphes :

$$\mathbb{Z}/8\mathbb{Z}, \qquad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \qquad (\mathbb{Z}/2\mathbb{Z})^3, \qquad \mathcal{D}_4, \qquad \mathcal{Q}_8.$$

∘ *Démonstration :* Soit $|G| = 8$. Les ordres des éléments valent 1, 2, 4 ou 8.

Cas 1 : un élément est d'ordre 8, et $G \simeq \mathbb{Z}/8\mathbb{Z}$.

Cas 2 : tout élément non trivial est d'ordre 2. Par le lemme du chapitre 4, G est abélien ; c'est alors un $\mathbb{F}_2$-espace vectoriel de cardinal 8, donc de dimension 3, et $G \simeq (\mathbb{Z}/2\mathbb{Z})^3$.

Cas 3 : l'ordre maximal est 4. Choisissons a d'ordre 4. Le sous-groupe $\langle a \rangle$ est d'indice 2, donc distingué. Prenons $b \notin \langle a \rangle$. Alors $b^2 \in \langle a \rangle$, et b^2 ne peut valoir a ni a^3 (sinon b serait d'ordre 8) : donc $b^2 = e$ ou $b^2 = a^2$. Par ailleurs bab^{-1} engendre $\langle a \rangle$ et est d'ordre 4, donc $bab^{-1} = a$ ou $bab^{-1} = a^{-1}$. Quatre combinaisons se présentent :

- $bab^{-1} = a$ et $b^2 = e$: G est abélien, $G = \langle a \rangle \times \langle b \rangle \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- $bab^{-1} = a$ et $b^2 = a^2$: G est encore abélien, et $c = ab$ vérifie $c^2 = a^2b^2 = a^4 = e$ avec $c \notin \langle a \rangle$; on est ramené au cas précédent, donc $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- $bab^{-1} = a^{-1}$ et $b^2 = e$: c'est la présentation de $\mathcal{D}_4$.
- $bab^{-1} = a^{-1}$ et $b^2 = a^2$: c'est la présentation de $\mathcal{Q}_8$.

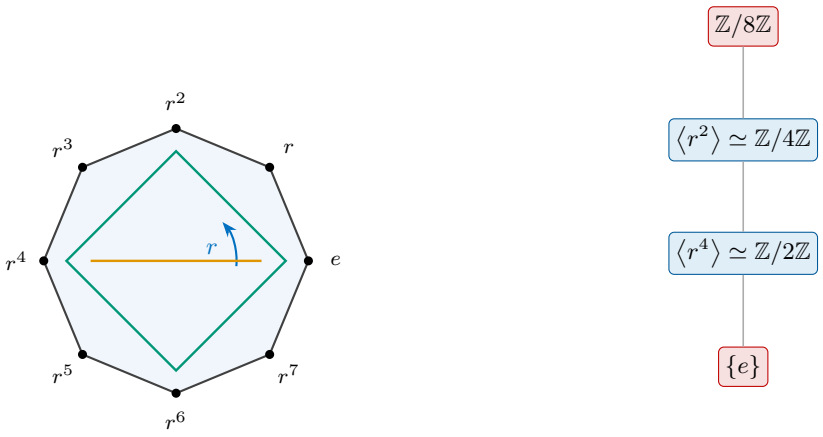
Les cinq groupes sont deux à deux non isomorphes : leurs nombres d'éléments d'ordre 2 valent respectivement 1, 3, 7, 5 et 1, et $\mathbb{Z}/8\mathbb{Z}$ se distingue de $\mathcal{Q}_8$ par l'existence d'un élément d'ordre 8. □

Remarque : La dernière ligne du tableau est la plus instructive : $\mathcal{D}_4$ et $\mathcal{Q}_8$ ne diffèrent que par la valeur de b^2. C'est un changement minuscule dans la présentation, et pourtant il fait passer de cinq involutions à une seule.

8.1 Le groupe cyclique $\mathbb{Z}/8\mathbb{Z}$

Notations	$\mathbb{Z}/8\mathbb{Z}$, μ_8
Présentation	$\langle r \mid r^8 = e \rangle$
Ordres des éléments	1 d'ordre 1, 1 d'ordre 2, 2 d'ordre 4, 4 d'ordre 8
Sous-groupes	4 sous-groupes, tous distingués, formant une chaîne

Un groupe cyclique possède, pour chaque diviseur d de son ordre, un *unique* sous-groupe d'ordre d. Comme les diviseurs de 8 forment la chaîne $1 \mid 2 \mid 4 \mid 8$, le treillis de $\mathbb{Z}/8\mathbb{Z}$ est une chaîne. C'est le seul groupe d'ordre 8 dont le treillis soit totalement ordonné, et cela le caractérise.



L'octogone régulier et ses huit rotations. Le carré vert joint un sommet sur deux : c'est le sous-groupe $\langle r^2 \rangle$ d'ordre 4. Le diamètre orange joint e à r^4 : c'est le sous-groupe d'ordre 2. L'emboîtement visuel carré $\subset$ octogone et diamètre $\subset$ carré *est* la chaîne du treillis dessinée à droite.

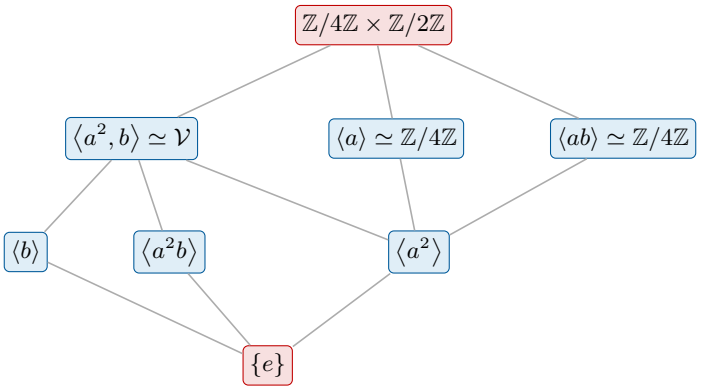
Lien avec la géométrie et l'algèbre

C'est le groupe des rotations de l'octogone régulier, et le groupe μ_8 des racines huitièmes de l'unité. En arithmétique, $(\mathbb{Z}/17\mathbb{Z})^\times$ est cyclique d'ordre 16 et contient donc un unique sous-groupe d'ordre 8, isomorphe à $\mathbb{Z}/8\mathbb{Z}$; le sous-corps de degré 8 de $\mathbb{Q}(\zeta_{17})$ a pour groupe de Galois sur $\mathbb{Q}$ ce même $\mathbb{Z}/8\mathbb{Z}$. C'est la cyclicité de $(\mathbb{Z}/17\mathbb{Z})^\times$ qui a permis à Gauss, à dix-neuf ans, de construire le polygone régulier à 17 côtés à la règle et au compas.

8.2 Le groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Notations	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/16\mathbb{Z})^\times$, $(\mathbb{Z}/15\mathbb{Z})^\times$
Présentation	$\langle a, b \mid a^4 = b^2 = e,\ ab = ba \rangle$
Ordres des éléments	1 d'ordre 1, 3 d'ordre 2, 4 d'ordre 4
Sous-groupes	8 sous-groupes, tous distingués

C'est le groupe abélien « intermédiaire » : il possède un élément d'ordre 4, ce qui le distingue de $(\mathbb{Z}/2\mathbb{Z})^3$, mais aucun élément d'ordre 8, ce qui le distingue de $\mathbb{Z}/8\mathbb{Z}$. Ses trois involutions sont a^2, b et a^2b ; la première joue un rôle particulier, car c'est la seule à être un carré.



Le treillis de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: huit sommets, tous bleus ou rouges puisque le groupe est abélien. Ce qu'il faut y lire est la position privilégiée de $\langle a^2 \rangle$: ce sous-groupe d'ordre 2 est contenu dans les *trois* sous-groupes d'ordre 4, alors que $\langle b \rangle$ et $\langle a^2 b \rangle$ ne sont contenus que dans le seul $\langle a^2, b \rangle$. La raison est que a^2 est le carré d'un élément d'ordre 4, tandis que b et $a^2 b$ ne sont carrés de personne.

Lien avec l'algèbre

Ce groupe apparaît naturellement en arithmétique modulaire : $(\mathbb{Z}/16\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, engendré par 3 (d'ordre 4) et -1 (d'ordre 2) ; de même $(\mathbb{Z}/15\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ par le théorème des restes chinois, puisque $(\mathbb{Z}/3\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$ et $(\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z}$. Le fait que $(\mathbb{Z}/2^k\mathbb{Z})^\times$ ne soit pas cyclique pour $k \geqslant 3$ est la principale exception au théorème sur les racines primitives, et c'est ici qu'on la rencontre pour la première fois.

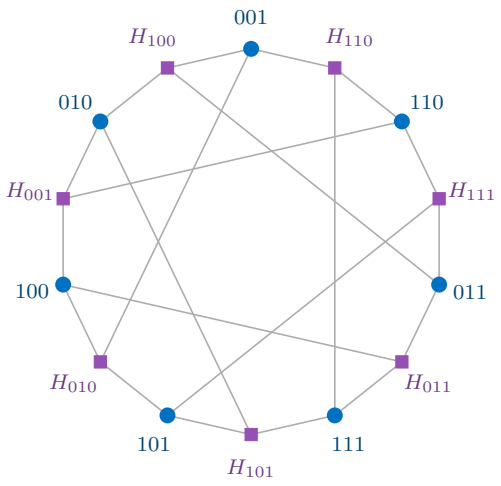
8.3 Le groupe $(\mathbb{Z}/2\mathbb{Z})^3$

Notations	$(\mathbb{Z}/2\mathbb{Z})^3$, $(\mathbb{F}_2)^3$, $(\mathbb{Z}/24\mathbb{Z})^\times$, groupe de Boole
Présentation	$\langle a, b, c \mid a^2 = b^2 = c^2 = e,\ ab = ba,\ ac = ca,\ bc = cb \rangle$
Ordres des éléments	1 d'ordre 1, 7 d'ordre 2
Sous-groupes	16 sous-groupes, tous distingués

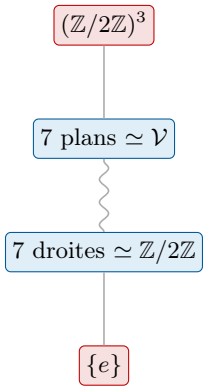
Tous les éléments non triviaux sont involutifs : le groupe est l'espace vectoriel $(\mathbb{F}_2)^3$ et sa loi est le « ou exclusif » bit à bit. C'est le groupe d'un tableau de trois interrupteurs indépendants : chaque élément est un sous-ensemble d'interrupteurs à basculer, et basculer deux fois le même ne fait rien.

Sous-groupes : la géométrie de Fano revient

Les sous-groupes d'ordre 2 sont les sept droites vectorielles, c'est-à-dire les sept vecteurs non nuls ; les sous-groupes d'ordre 4 sont les sept plans vectoriels. Un vecteur appartient à trois plans, un plan contient trois vecteurs non nuls : c'est exactement l'incidence du plan de Fano rencontré au chapitre 7. Le treillis complet a donc $1 + 7 + 7 + 1 = 16$ sommets, et son étage central est le graphe d'incidence points-droites du plan de Fano, appelé **graphe de Heawood**.



7 disques bleus : sous-groupes d'ordre 2
7 carrés violets : sous-groupes d'ordre 4



21 arêtes, dessinées à gauche

Le graphe de Heawood. Chaque disque bleu v représente le sous-groupe $\{0, v\}$; chaque carré violet H_ℓ représente le plan $\{x : \ell \cdot x = 0\}$, sous-groupe d'ordre 4 isomorphe à $\mathcal{V}$. Une arête relie v à H_ℓ exactement quand $\ell \cdot v = 0$, c'est-à-dire quand le sous-groupe d'ordre 2 est contenu dans celui d'ordre 4. Chaque sommet a exactement trois voisins : trois plans contiennent une droite donnée, trois droites sont contenues dans un plan donné. L'étiquetage a été obtenu par recherche exhaustive et vérifié. À droite, le treillis résumé : il faudrait y ajouter 7 arêtes vers le bas et 7 vers le haut, soit 35 arêtes en tout, ce qui rendrait le dessin illisible — d'où ce découpage.

Remarque : Ce groupe a le treillis le plus riche des cinq groupes d'ordre 8, avec ses seize sommets, et c'est aussi le plus « plat » : tous ses éléments non triviaux sont interchangeables par un automorphisme. Son groupe d'automorphismes est $\mathrm{GL}_3(\mathbb{F}_2)$, d'ordre 168, ce qui en fait le groupe d'ordre 8 le plus symétrique — alors que $\mathbb{Z}/8\mathbb{Z}$, qui n'a que quatre automorphismes, est le plus rigide.

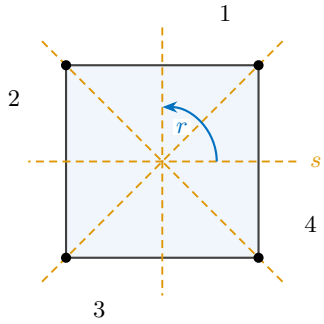
Lien avec l'algèbre

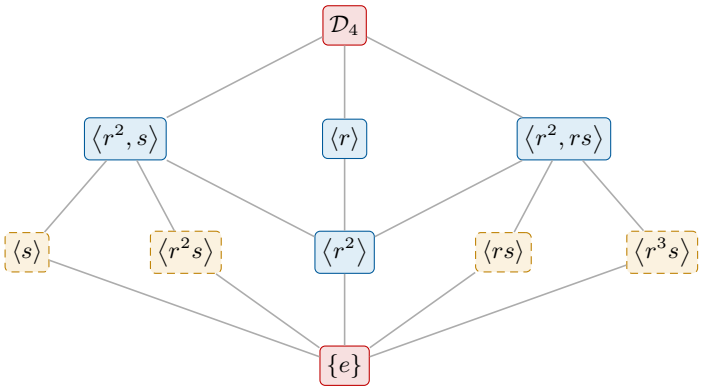
On a $(\mathbb{Z}/24\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z})^3$: les huit inversibles modulo 24 sont $1, 5, 7, 11, 13, 17, 19, 23$, et le carré de chacun vaut 1 modulo 24. C'est aussi $\mathrm{Gal}\big(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}\big)$, un automorphisme étant déterminé par les trois signes qu'il attribue aux trois radicaux.

8.4 Le groupe diédral $\mathcal{D}_4$

Notations	$\mathcal{D}_4$, D_8 (notation anglo-saxonne), groupe du carré
Présentation	$\langle r, s \mid r^4 = s^2 = e,\ srs^{-1} = r^{-1} \rangle$
Ordres des éléments	1 d'ordre 1, 5 d'ordre 2, 2 d'ordre 4
Sous-groupes	10 sous-groupes, dont 4 non distingués

C'est le groupe complet des isométries du carré : quatre rotations e, r, r^2, r^3 et quatre réflexions s, rs, r^2s, r^3s, dont deux ont pour axes les médiatrices des côtés et deux les diagonales. Son centre est $\{e, r^2\}$: le demi-tour est la seule isométrie non triviale qui commute à toutes les autres.





2 axes diagonaux, 2 axes médians

À gauche le carré avec ses quatre axes de symétrie ; à droite le treillis complet. Les quatre sous-groupes engendrés par une réflexion sont non distingués et se répartissent en *deux* classes de conjugaison : $\{\langle s\rangle, \langle r^2 s\rangle\}$, les axes médians, et $\{\langle rs\rangle, \langle r^3 s\rangle\}$, les diagonales. C'est pourquoi les deux sous-groupes de Klein $\langle r^2, s\rangle$ et $\langle r^2, rs\rangle$ sont distincts : le premier réunit les deux réflexions médianes, le second les deux réflexions diagonales. Tous deux contiennent le centre $\langle r^2\rangle$, qui est le seul sous-groupe d'ordre 2 distingué.

Remarque : Le treillis de $\mathcal{D}_4$ est la traduction fidèle du treillis des sous-corps de $\mathbb{Q}(\sqrt[4]{2}, i)$ sur $\mathbb{Q}$: cette extension est de degré 8, de groupe de Galois $\mathcal{D}_4$, et la correspondance de Galois renverse les inclusions. Les dix sous-groupes donnent les dix corps intermédiaires, et les trois sous-groupes d'indice 2 donnent les trois sous-corps quadratiques $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ et $\mathbb{Q}(i\sqrt{2})$.

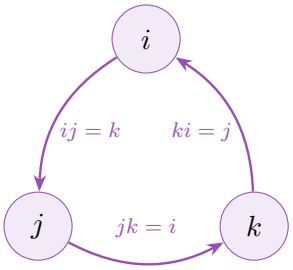
8.5 Le groupe des quaternions $\mathcal{Q}_8$

Notations	$\mathcal{Q}_8$, $\{\pm 1, \pm i, \pm j, \pm k\}$, groupe quaternionique
Présentation	$\langle a, b \mid a^4 = e,\ b^2 = a^2,\ bab^{-1} = a^{-1} \rangle$
Ordres des éléments	1 d'ordre 1, 1 d'ordre 2, 6 d'ordre 4
Sous-groupes	6 sous-groupes, *tous* distingués

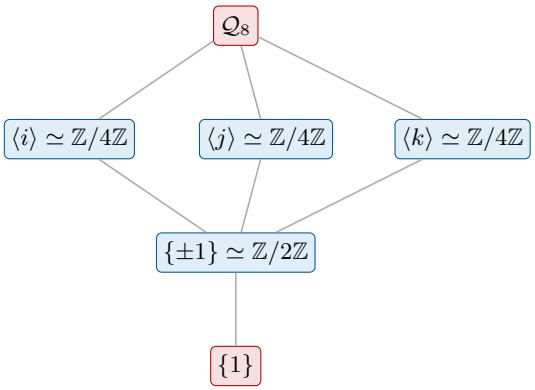
Ses huit éléments sont $\pm 1, \pm i, \pm j, \pm k$, avec les relations découvertes par Hamilton en 1843 :

$$i^2 = j^2 = k^2 = ijk = -1, \qquad ij = k, \quad jk = i, \quad ki = j,$$

et donc $ji = -k$, $kj = -i$, $ik = -j$. L'élément -1 est central et c'est la *seule* involution : six éléments sur huit sont d'ordre 4, ce qui ne se produit dans aucun autre groupe d'ordre 8.



dans le sens de la flèche : produit = suivant
à contresens : produit = opposé du suivant



À gauche le triangle mnémotechnique de Hamilton : parcouru dans le sens des flèches, le produit de deux éléments consécutifs donne le troisième ; parcouru à l'envers, il donne son opposé. À droite le treillis : il n'a que six sommets et *tous* sont bleus ou rouges, alors que le groupe n'est pas abélien. Le sous-groupe $\{\pm 1\}$ est contenu dans les trois sous-groupes d'ordre 4 : c'est l'unique sous-groupe d'ordre 2, puisque -1 est la seule involution.

Remarque : $\mathcal{Q}_8$ est le plus petit groupe **hamiltonien** : non abélien, mais dont tous les sous-groupes sont distingués. La raison tient en une ligne : tout sous-groupe propre non trivial contient -1 ou vaut $\{\pm 1\}$, et ceux d'ordre 4 sont d'indice 2 donc automatiquement distingués. Ce phénomène est rare, et un théorème de Dedekind affirme que tout groupe hamiltonien contient une copie de $\mathcal{Q}_8$.

Lien avec la géométrie

$\mathcal{Q}_8$ est le groupe des huit quaternions unitaires « entiers » $\pm 1, \pm i, \pm j, \pm k$, c'est-à-dire un sous-groupe fini de la sphère unité $\mathbb{S}^3$ des quaternions de norme 1, elle-même isomorphe à $\mathrm{SU}(2)$. Le morphisme de revêtement $\mathrm{SU}(2) \to \mathrm{SO}(3)$, de noyau $\{\pm 1\}$, envoie $\mathcal{Q}_8$ sur le groupe de Klein : les images de i, j, k sont les trois demi-tours autour des trois axes de coordonnées. Autrement dit, $\mathcal{Q}_8$ est le **revêtement double** du groupe du rectangle, et $\mathcal{Q}_8/\{\pm 1\} \simeq \mathcal{V}$.

Remarque : C'est ici l'écart le plus instructif entre $\mathcal{D}_4$ et $\mathcal{Q}_8$. Les deux groupes ont le même quotient $\mathcal{V}$ par leur centre, la même présentation à un signe près, et pourtant $\mathcal{D}_4$ se réalise dans le plan tandis que $\mathcal{Q}_8$ ne se réalise pas du tout comme groupe d'isométries d'une figure plane ou spatiale : il n'a qu'une involution, alors qu'un groupe d'isométries de l'espace contenant des rotations d'ordre 4 en aurait plusieurs. $\mathcal{Q}_8$ vit dans la sphère de dimension 3, et c'est de là que vient le spin des physiciens.

8.6 Comparaison des cinq groupes d'ordre 8

Groupe	Abélien	Élém. d'ordre 2	Élém. d'ordre 4	Centre	Sous-gr.
$\mathbb{Z}/8\mathbb{Z}$	oui	1	2	tout	4
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	oui	3	4	tout	8
$(\mathbb{Z}/2\mathbb{Z})^3$	oui	7	0	tout	16
$\mathcal{D}_4$	non	5	2	$\mathbb{Z}/2\mathbb{Z}$	10
$\mathcal{Q}_8$	non	1	6	$\mathbb{Z}/2\mathbb{Z}$	6

Le nombre d'éléments d'ordre 2 suffit à lui seul à séparer $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$ et $\mathcal{D}_4$; il ne sépare pas $\mathbb{Z}/8\mathbb{Z}$ de $\mathcal{Q}_8$, qui ont tous deux une unique involution, mais l'existence d'un élément d'ordre 8 tranche. C'est la méthode générale : on compare les *profils d'ordres* avant de chercher un isomorphisme.

Remarque : L'erreur la plus répandue est de croire que $\mathcal{D}_4 \simeq \mathcal{Q}_8$ parce que leurs présentations se ressemblent et que leurs quotients par le centre coïncident. Le tableau ci-dessus la corrige en une ligne : $\mathcal{D}_4$ a cinq involutions, $\mathcal{Q}_8$ une seule. Une erreur voisine consiste à écrire $\mathcal{D}_4 \simeq \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ *et* $\mathcal{Q}_8 \simeq \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$: la première écriture est correcte, la seconde est fausse, car $\mathcal{Q}_8$ n'est pas un produit semi-direct non trivial — aucun sous-groupe d'ordre 2 ne le complète, puisque le seul candidat $\{\pm 1\}$ est contenu dans tous les autres sous-groupes.

Ordre 9

L'ordre $9 = 3^2$ est le carré d'un nombre premier. Un théorème général affirme qu'un tel ordre ne peut porter que des groupes abéliens ; il n'y en a donc que deux, comme à l'ordre $4 = 2^2$.

Théorème 9 : Si $|G| = p^2$ avec p premier, alors G est abélien, et $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $G \simeq (\mathbb{Z}/p\mathbb{Z})^2$.

La démonstration repose sur deux lemmes que l'on retrouvera au chapitre 12.

Propriété 10 : *(a)* Si $G/Z(G)$ est cyclique, alors G est abélien.
(b) Si $|G| = p^n$ avec $n \geqslant 1$, alors $Z(G) \neq \{e\}$.

∘ *Démonstration : (a)* Soit gZ un générateur de G/Z, où $Z = Z(G)$. Tout $x \in G$ appartient à une classe $g^a Z$, donc s'écrit $x = g^a z$ avec $z \in Z$. Pour $x = g^a z$ et $y = g^b z'$, les éléments z et z' commutent à tout, donc $xy = g^{a+b} zz' = g^{b+a} z'z = yx$.

(b) L'équation aux classes s'écrit $|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$, la somme portant sur des représentants des classes de conjugaison non réduites à un point. Chaque indice $[G : C_G(x_i)]$ divise p^n et est strictement supérieur à 1, donc est divisible par p. Comme p divise $|G|$, il divise aussi $|Z(G)|$, qui est donc au moins égal à p. □

∘ *Démonstration : (Théorème 9.)* Par (b), $|Z(G)| \in \{p, p^2\}$. Si $|Z(G)| = p$, alors $G/Z(G)$ est d'ordre p, donc cyclique par le théorème 5, donc G est abélien par (a) : mais alors $Z(G) = G$ serait d'ordre p^2, contradiction. Donc $|Z(G)| = p^2$ et G est abélien. Si G contient un élément d'ordre p^2 il est cyclique ; sinon tout élément non trivial est d'ordre p et G est un $\mathbb{F}_p$-espace vectoriel de dimension 2. □

9.1 Le groupe cyclique $\mathbb{Z}/9\mathbb{Z}$

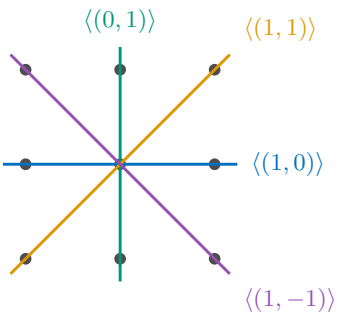
Notations	$\mathbb{Z}/9\mathbb{Z}$, μ_9, $(\mathbb{Z}/19\mathbb{Z})^\times$ en sous-groupe
Présentation	$\langle r \mid r^9 = e \rangle$
Ordres des éléments	1 d'ordre 1, 2 d'ordre 3, 6 d'ordre 9
Sous-groupes	3 sous-groupes, tous distingués, formant une chaîne

Les diviseurs de 9 forment la chaîne $1 \mid 3 \mid 9$: le treillis est donc une chaîne à trois sommets, comme celui de $\mathbb{Z}/4\mathbb{Z}$. L'unique sous-groupe propre est $\langle r^3 \rangle = \{e, r^3, r^6\}$.

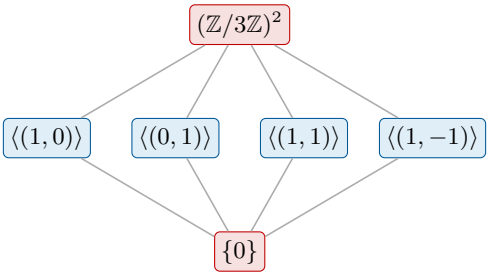
9.2 Le groupe $(\mathbb{Z}/3\mathbb{Z})^2$

Notations	$(\mathbb{Z}/3\mathbb{Z})^2$, $(\mathbb{F}_3)^2$, plan affine d'ordre 3
Présentation	$\langle a, b \mid a^3 = b^3 = e,\ ab = ba \rangle$
Ordres des éléments	1 d'ordre 1, 8 d'ordre 3
Sous-groupes	6 sous-groupes, tous distingués

C'est le plan vectoriel sur le corps $\mathbb{F}_3$. Ses quatre sous-groupes d'ordre 3 sont ses quatre droites vectorielles, et le treillis a la même forme que celui de $\mathfrak{S}_3$: un plancher, un plafond, et quatre sous-groupes propres deux à deux incomparables. Cette coïncidence, annoncée en introduction, montre bien que le treillis seul ne détermine pas le groupe — ici il ne détermine même pas son ordre.



les quatre droites vectorielles



Les neuf éléments de $(\mathbb{Z}/3\mathbb{Z})^2$, représentés par les couples de coordonnées prises dans $\{-1, 0, 1\}$: avec ce choix de représentants, les quatre sous-groupes d'ordre 3 deviennent les quatre alignements de trois points passant par le centre, et le dessin est exact. Chacun contient l'origine et deux points opposés, conformément à $-x = 2x$ dans $\mathbb{F}_3$. À droite le treillis correspondant : quatre sous-groupes propres, tous d'ordre 3, tous incomparables.

Lien avec la géométrie

Le groupe $(\mathbb{Z}/3\mathbb{Z})^2$ *est* le plan affine d'ordre 3 : neuf points, douze droites de trois points chacune, réparties en quatre directions de trois droites parallèles. Les quatre droites passant par l'origine sont les sous-groupes ; les huit autres sont leurs classes latérales. On vérifie le compte : $4 \times 3 = 12$ droites, et chaque point appartient à quatre d'entre elles.

> *Remarque :* Le jeu de cartes *SET* est une réalisation exacte de cette géométrie, en dimension 4 : chaque carte porte quatre caractères à trois valeurs, ce qui en fait un point de $(\mathbb{F}_3)^4$, et un « set » de trois cartes est précisément une droite affine, c'est-à-dire un triplet de somme nulle. Le fait qu'à partir de toute paire de cartes il existe exactement une troisième qui complète le set traduit l'axiome d'incidence : par deux points passe une unique droite.

Lien avec l'algèbre

Trois apparitions méritent d'être signalées. C'est d'abord le groupe des translations du plan affine $\mathrm{AG}(2, 3)$ décrit ci-dessus. C'est ensuite le 3-sous-groupe de Sylow de $\mathfrak{S}_3 \times \mathfrak{S}_3$, groupe d'ordre $36 = 2^2 \times 3^2$. C'est enfin, en théorie de Galois, le groupe du compositum de deux extensions cycliques cubiques indépendantes de $\mathbb{Q}$: par exemple le sous-corps réel de $\mathbb{Q}(\zeta_7)$ et celui de $\mathbb{Q}(\zeta_9)$, qui sont de degré 3 et de conducteurs distincts, engendrent une extension de degré 9 et de groupe $(\mathbb{Z}/3\mathbb{Z})^2$. Plus généralement, le groupe des points de n-torsion d'une courbe elliptique sur un corps algébriquement clos de caractéristique ne divisant pas n est $(\mathbb{Z}/n\mathbb{Z})^2$: pour $n = 3$, c'est exactement notre groupe, et ses quatre sous-groupes d'ordre 3 correspondent aux quatre isogénies de degré 3 issues de la courbe.

Ordre 10

Le théorème 7, démontré au chapitre 6, s'applique avec $p = 5$: il y a exactement deux groupes d'ordre 10, le cyclique et le diédral.

10.1 Le groupe cyclique $\mathbb{Z}/10\mathbb{Z}$

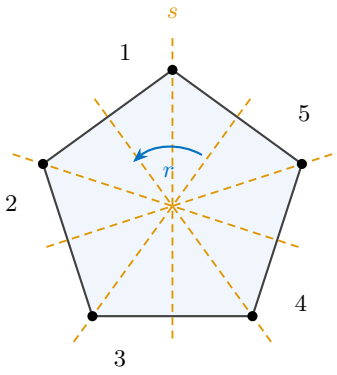
Notations	$\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, μ_{10}, $(\mathbb{Z}/11\mathbb{Z})^\times$
Présentation	$\langle r \mid r^{10} = e \rangle$
Ordres des éléments	1 d'ordre 1, 1 d'ordre 2, 4 d'ordre 5, 4 d'ordre 10
Sous-groupes	4 sous-groupes, tous distingués

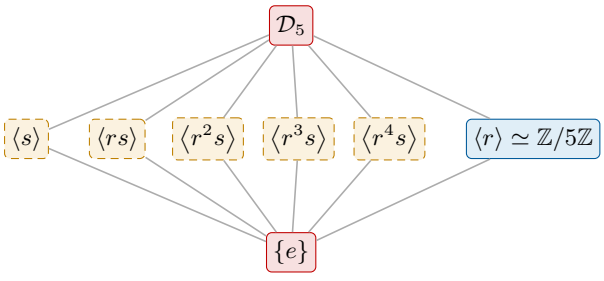
Les diviseurs de 10 sont $1, 2, 5, 10$: le treillis est un diamant, comme celui de $\mathbb{Z}/6\mathbb{Z}$. L'isomorphisme $\mathbb{Z}/10\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ est encore le théorème des restes chinois. Le groupe $(\mathbb{Z}/11\mathbb{Z})^\times$, d'ordre 10, est cyclique : 2 en est un générateur, car ses puissances successives $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$ parcourent tous les inversibles modulo 11.

10.2 Le groupe diédral $\mathcal{D}_5$

Notations	$\mathcal{D}_5$, D_{10} (notation anglo-saxonne), groupe du pentagone
Présentation	$\langle r, s \mid r^5 = s^2 = e,\ srs^{-1} = r^{-1} \rangle$
Ordres des éléments	1 d'ordre 1, 5 d'ordre 2, 4 d'ordre 5
Sous-groupes	8 sous-groupes, dont 5 non distingués

C'est le groupe des dix isométries du pentagone régulier : cinq rotations et cinq réflexions. Contrairement au carré, le pentagone n'a qu'une seule famille d'axes, chacun passant par un sommet et par le milieu du côté opposé — conséquence directe de l'imparité de 5. Les cinq réflexions sont donc toutes conjuguées entre elles, ce qui explique que les cinq sous-groupes d'ordre 2 forment une unique classe de conjugaison.





Le pentagone régulier, ses cinq axes de symétrie et la rotation r ; à droite le treillis. Comme pour $\mathfrak{S}_3$, ce treillis n'a que deux étages : tout sous-groupe propre non trivial est d'ordre 2 ou 5, donc premier, donc à la fois minimal et maximal. Seul $\langle r \rangle$, d'indice 2, est distingué. On notera la différence avec $\mathcal{D}_4$ du chapitre 8, dont le treillis avait trois étages : c'est que 4 n'est pas premier et que le carré possède deux familles d'axes, alors que le pentagone n'en a qu'une.

Lien avec la géométrie et l'algèbre

Outre le pentagone, $\mathcal{D}_5$ est le groupe de symétrie de l'étoile à cinq branches et du pentagramme, ainsi que le groupe des symétries planes d'une face du dodécaèdre régulier. En théorie de Galois, c'est le groupe de certains polynômes de degré 5 résolubles par radicaux, par exemple $X^5 - 5X + 12$: le groupe $\mathcal{D}_5$ est résoluble, puisque $\{e\} \lhd \langle r \rangle \lhd \mathcal{D}_5$ a des quotients cycliques d'ordres 5 et 2. Ce sont les quintiques de groupe $\mathfrak{S}_5$ ou $\mathfrak{A}_5$ qui échappent aux radicaux.

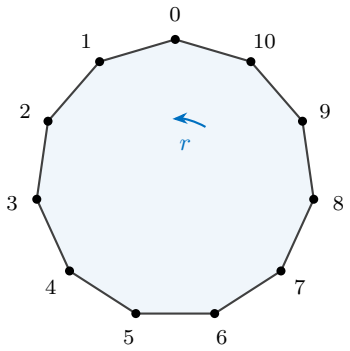
Remarque : Il vaut la peine de comparer $\mathbb{Z}/10\mathbb{Z}$ et $\mathcal{D}_5$ par leurs éléments d'ordre 2 : le premier en a un, le second en a cinq. C'est le critère le plus rapide, et il se généralise : $\mathbb{Z}/2p\mathbb{Z}$ a une seule involution, $\mathcal{D}_p$ en a p.

Ordre 11

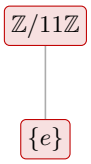
11.1 Le groupe $\mathbb{Z}/11\mathbb{Z}$

Notations	$\mathbb{Z}/11\mathbb{Z}$, $\mathbb{F}_{11}$, μ_{11}
Présentation	$\langle r \mid r^{11} = e \rangle$
Ordres des éléments	1 élément d'ordre 1, 10 éléments d'ordre 11
Sous-groupes	2 sous-groupes, tous distingués

Dernier ordre premier de notre parcours, dernier groupe sans structure interne : le théorème 5 donne l'unicité, et les dix éléments non triviaux sont autant de générateurs.



les onze rotations de l'hendécagone



aucun sous-groupe intermédiaire possible : 11 est premier

L'hendécagone régulier et ses onze rotations. Ce polygone a une particularité que les précédents n'avaient pas : il n'est *pas* constructible à la règle et au compas. Le critère de Gauss–Wantzel exige que le nombre de côtés soit un produit d'une puissance de 2 et de nombres premiers de Fermat distincts ; or 11 n'est pas un nombre de Fermat, contrairement à 3, 5 et 17. Le dessin ci-dessus a donc été obtenu par calcul d'angles, non par construction géométrique.

Lien avec l'algèbre

$\mathbb{Z}/11\mathbb{Z}$ est le groupe additif de $\mathbb{F}_{11}$. Il apparaît comme unique sous-groupe d'ordre 11 du groupe cyclique $(\mathbb{Z}/23\mathbb{Z})^\times$, d'ordre 22, et comme groupe de Galois de l'unique sous-extension de degré 11 de $\mathbb{Q}(\zeta_{23})$.

Remarque : L'ordre 11 clôt la liste des ordres « sans histoire ». Le chapitre suivant, consacré à l'ordre 12, rassemble au contraire toutes les techniques accumulées : théorèmes de Sylow, produits semi-directs, et le premier exemple d'un groupe où la réciproque du théorème de Lagrange est en défaut.

Ordre 12

Second sommet du parcours, et le plus riche en enseignements : les cinq groupes d'ordre 12 se laissent tous décrire comme produits semi-directs, et l'un d'eux, $\mathfrak{A}_4$, fournit le contre-exemple classique à la réciproque du théorème de Lagrange.

Théorème 11 : Tout groupe d'ordre 12 est isomorphe à l'un des cinq groupes suivants, deux à deux non isomorphes :

$$\mathbb{Z}/12\mathbb{Z}, \qquad \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \qquad \mathcal{D}_6, \qquad \mathfrak{A}_4, \qquad \mathrm{Dic}_3.$$

∘ *Démonstration :* Soit $|G| = 12 = 2^2 \times 3$. Les théorèmes de Sylow imposent $n_3 \equiv 1 \pmod 3$ et $n_3 \mid 4$, donc $n_3 \in \{1, 4\}$.

Cas $n_3 = 4$. Deux 3-Sylow distincts sont d'ordre premier 3, donc s'intersectent trivialement : les quatre 3-Sylow fournissent $4 \times 2 = 8$ éléments d'ordre 3. Il reste $12 - 8 = 4$ éléments, dont aucun n'est d'ordre 3 ; or tout 2-Sylow est formé de 4 tels éléments, donc il n'y en a qu'un, noté P, et il est distingué. Comme $|P| = 4$ et $|Q| = 3$ pour un 3-Sylow Q, on a $P \cap Q = \{e\}$ et $|PQ| = 12$, donc $G = P \rtimes Q$. L'action de $Q \simeq \mathbb{Z}/3\mathbb{Z}$ sur P est non triviale, sinon $G = P \times Q$ n'aurait qu'un seul 3-Sylow. Si $P \simeq \mathbb{Z}/4\mathbb{Z}$, alors $\mathrm{Aut}(P) \simeq \mathbb{Z}/2\mathbb{Z}$ ne contient aucun élément d'ordre 3 et l'action serait triviale : donc $P \simeq \mathcal{V}$. Comme $\mathrm{Aut}(\mathcal{V}) \simeq \mathfrak{S}_3$, les morphismes non triviaux $\mathbb{Z}/3\mathbb{Z} \to \mathfrak{S}_3$ ont pour image l'unique sous-groupe d'ordre 3, et les deux tels morphismes diffèrent par un automorphisme de $\mathbb{Z}/3\mathbb{Z}$: ils donnent le même groupe, à savoir $\mathcal{V} \rtimes \mathbb{Z}/3\mathbb{Z} \simeq \mathfrak{A}_4$.

Cas $n_3 = 1$. L'unique 3-Sylow $Q \simeq \mathbb{Z}/3\mathbb{Z}$ est distingué, et le même argument donne $G = Q \rtimes P$ avec $|P| = 4$. L'action est un morphisme $\varphi : P \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$.

- $P \simeq \mathbb{Z}/4\mathbb{Z}$ et φ trivial : $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z}$.
- $P \simeq \mathbb{Z}/4\mathbb{Z}$ et φ surjectif, de noyau l'unique sous-groupe d'ordre 2 : $G \simeq \mathrm{Dic}_3$.
- $P \simeq \mathcal{V}$ et φ trivial : $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathcal{V} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- $P \simeq \mathcal{V}$ et φ surjectif : le noyau est l'un des trois sous-groupes d'ordre 2 de $\mathcal{V}$, mais $\mathrm{Aut}(\mathcal{V})$ les permute transitivement, donc les trois choix donnent des groupes isomorphes : $G \simeq \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z} \simeq \mathcal{D}_6$.

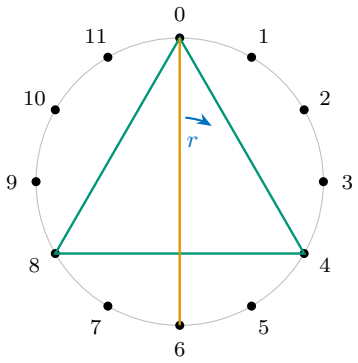
Les cinq groupes sont deux à deux distincts : leurs profils d'ordres d'éléments, donnés dans le tableau de la section 12.6, sont tous différents. □

> *Remarque :* On retiendra la ligne de force : *c'est* $\mathrm{Aut}(N)$ *qui décide.* À chaque étape, le nombre de groupes obtenus est le nombre de morphismes $P \to \mathrm{Aut}(N)$, comptés à conjugaison près. Ce schéma de preuve, appliqué à l'ordre 8 au chapitre précédent et à l'ordre 12 ici, est celui qu'on reprend pour tous les ordres de la forme p^2q.

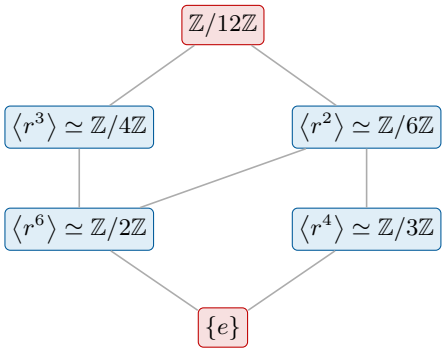
12.1 Le groupe cyclique $\mathbb{Z}/12\mathbb{Z}$

Notations	$\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, μ_{12}, $(\mathbb{Z}/13\mathbb{Z})^\times$ en sous-groupe
Présentation	$\langle r \mid r^{12} = e \rangle$
Ordres des éléments	1 d'ordre 1, 1 d'ordre 2, 2 d'ordre 3, 2 d'ordre 4, 2 d'ordre 6, 4 d'ordre 12
Sous-groupes	6 sous-groupes, tous distingués

Un sous-groupe par diviseur de 12, soit $1, 2, 3, 4, 6, 12$: le treillis des sous-groupes *est* le treillis des diviseurs de 12, ordonné par divisibilité. C'est le seul des cinq groupes d'ordre 12 à posséder un élément d'ordre 12.



$\langle r^4 \rangle \simeq \mathbb{Z}/3\mathbb{Z}$ en vert
$\langle r^6 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ en orange

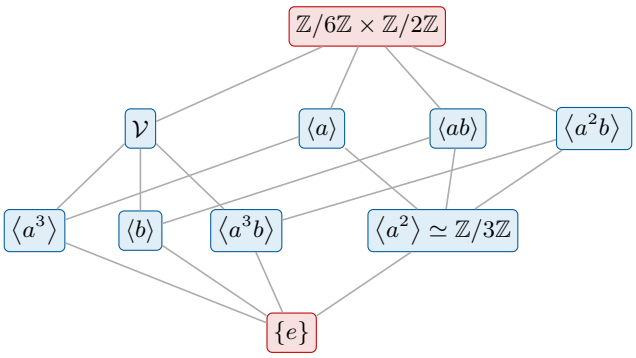


Le cadran de l'horloge est la réalisation la plus familière de $\mathbb{Z}/12\mathbb{Z}$, et les douze hauteurs de la gamme tempérée en sont une autre : transposer d'un demi-ton, c'est ajouter 1 modulo 12. Le triangle vert joint les multiples de 4, sous-groupe d'ordre 3 ; le diamètre orange joint 0 et 6, sous-groupe d'ordre 2. À droite, le treillis : on notera que $\langle r^4 \rangle \simeq \mathbb{Z}/3\mathbb{Z}$ n'est *pas* contenu dans $\langle r^3 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$, car 3 ne divise pas 4 — le treillis des sous-groupes reproduit exactement celui des diviseurs.

12.2 Le groupe $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Notations	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathcal{V} \times \mathbb{Z}/3\mathbb{Z}$
Présentation	$\langle a, b \mid a^6 = b^2 = e,\ ab = ba \rangle$
Ordres des éléments	1 d'ordre 1, 3 d'ordre 2, 2 d'ordre 3, 6 d'ordre 6
Sous-groupes	10 sous-groupes, tous distingués

C'est l'unique groupe abélien non cyclique d'ordre 12. La classification des groupes abéliens finis le donne sous la forme des facteurs invariants $2 \mid 6$, et le théorème des restes chinois le récrit $\mathcal{V} \times \mathbb{Z}/3\mathbb{Z}$, écriture beaucoup plus commode : ses sous-groupes sont exactement les produits d'un sous-groupe de $\mathcal{V}$ par un sous-groupe de $\mathbb{Z}/3\mathbb{Z}$, soit $5 \times 2 = 10$.



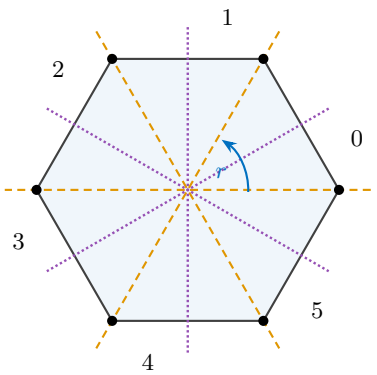
Le treillis de $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathcal{V} \times \mathbb{Z}/3\mathbb{Z}$. Il se lit comme deux copies superposées du diamant de $\mathcal{V}$: l'étage du bas ($\{e\}$, les trois sous-groupes d'ordre 2, $\mathcal{V}$) et l'étage du haut obtenu en multipliant chacun par $\langle a^2 \rangle$ ($\langle a^2 \rangle$, les trois sous-groupes d'ordre 6, le groupe entier). Les arêtes qui montent de $\langle a^3 \rangle$ vers $\langle a \rangle$, de $\langle b \rangle$ vers $\langle ab \rangle$ et de $\langle a^3 b \rangle$ vers $\langle a^2 b \rangle$ réalisent cette superposition. Les quelques croisements de traits sont inévitables : on vérifie que ce graphe n'est pas planaire, il n'existe donc aucun dessin sans croisement.

Remarque : Ce groupe et $\mathfrak{A}_4$ ont tous deux dix sous-groupes, ce qui montre une fois encore qu'un simple comptage ne suffit pas. Mais leurs treillis diffèrent profondément : celui-ci a quatre sous-groupes minimaux, celui de $\mathfrak{A}_4$ en a sept.

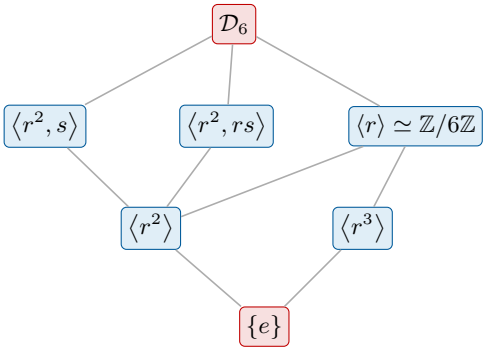
12.3 Le groupe diédral $\mathcal{D}_6$

Notations	$\mathcal{D}_6$, D_{12} (notation anglo-saxonne), $\mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$
Présentation	$\langle r, s \mid r^6 = s^2 = e,\ srs^{-1} = r^{-1} \rangle$
Ordres des éléments	1 d'ordre 1, 7 d'ordre 2, 2 d'ordre 3, 2 d'ordre 6
Sous-groupes	16 sous-groupes, dont 9 non distingués

C'est le groupe des douze isométries de l'hexagone régulier. Son centre est $\{e, r^3\}$, et l'isomorphisme $\mathcal{D}_6 \simeq \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$ s'obtient en écrivant toute isométrie de l'hexagone comme le produit d'une isométrie du triangle $\{1, 3, 5\}$ par l'identité ou par le demi-tour r^3.



tirets orange : 3 axes par deux sommets
pointillés violets : 3 axes par deux milieux



les 7 sous-groupes distingués
(les deux $\langle r^2, \cdot \rangle$ sont des $\mathfrak{S}_3$)

L'hexagone possède *deux* familles d'axes, parce que 6 est pair : trois axes joignant deux sommets opposés et trois axes joignant les milieux de deux côtés opposés. Deux réflexions sont conjuguées si et seulement si leurs axes appartiennent à la même famille, d'où deux classes de trois réflexions — et donc les deux copies de $\mathfrak{S}_3$ du treillis de droite, chacune contenant les trois réflexions d'une famille. On notera qu'un axe orange et un axe violet se coupent à angle droit pour exactement trois couples : les axes orange font avec l'horizontale les angles 0°, 60°, 120° et les axes violets les angles 30°, 90°, 150°, si bien que chaque orange a un unique violet perpendiculaire. Ce sont ces trois couples qui engendrent, avec le demi-tour r^3, les trois sous-groupes de Klein.

Les seize sous-groupes

Le treillis complet de $\mathcal{D}_6$ n'est pas planaire et comporte 33 arêtes : le dessiner d'un seul tenant le rendrait illisible. On en donne donc la liste exhaustive, vérifiée par ordinateur.

Ordre	Nombre	Description	Distingués
1	1	$\{e\}$	1
2	7	les six $\langle r^k s\rangle$, plus le centre $\langle r^3\rangle$	1
3	1	$\langle r^2\rangle$	1
4	3	$\{e, r^3, r^k s, r^{k+3}s\}$ pour $k = 0, 1, 2$, isomorphes à $\mathcal{V}$	0
6	3	$\langle r\rangle \simeq \mathbb{Z}/6\mathbb{Z}$, et les deux $\mathfrak{S}_3$ engendrés par r^2 et une réflexion	3
12	1	$\mathcal{D}_6$	1

Total : 16 sous-groupes, dont 7 distingués. Les trois sous-groupes de Klein sont d'indice 3 et ne sont pas distingués, ce qui surprend souvent : la conjugaison par r envoie $\{e, r^3, s, r^3 s\}$ sur $\{e, r^3, r^2 s, r^5 s\}$, qui est un autre des trois. Les six sous-groupes engendrés par une réflexion ne sont pas distingués non plus, et se répartissent en deux classes de conjugaison de trois éléments, conformément aux deux familles d'axes.

12.4 Le groupe alterné $\mathfrak{A}_4$

Notations	$\mathfrak{A}_4$, groupe du tétraèdre, $\mathcal{V} \rtimes \mathbb{Z}/3\mathbb{Z}$, $\mathrm{PSL}_2(\mathbb{F}_3)$
Présentation	$\langle a, b \mid a^3 = b^2 = (ab)^3 = e\rangle$
Ordres des éléments	1 d'ordre 1, 3 d'ordre 2, 8 d'ordre 3
Sous-groupes	10 sous-groupes, dont 7 non distingués

$\mathfrak{A}_4$ est le groupe des permutations paires de quatre lettres : l'identité, les trois doubles transpositions (12)(34), (13)(24), (14)(23), et les huit 3-cycles. Les trois doubles transpositions et l'identité forment une copie de $\mathcal{V}$, distinguée car stable par conjugaison : conjuguer une double transposition donne une double transposition.

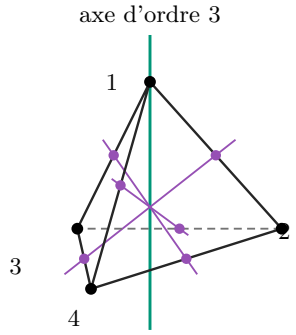
Théorème 12 : $\mathfrak{A}_4$ ne possède aucun sous-groupe d'ordre 6. La réciproque du théorème de Lagrange est donc fausse : un diviseur de $|G|$ n'est pas nécessairement l'ordre d'un sous-groupe.

∘ *Démonstration :* Supposons qu'il existe $H \leqslant \mathfrak{A}_4$ avec $|H| = 6$. Alors $[\mathfrak{A}_4 : H] = 2$, donc H est distingué et le quotient $\mathfrak{A}_4/H$ est d'ordre 2. Soit σ un 3-cycle et $\overline{\sigma}$ son image dans le quotient. On a $\overline{\sigma}^3 = \overline{e}$ puisque $\sigma^3 = e$, et $\overline{\sigma}^2 = \overline{e}$ puisque le quotient est d'ordre 2. Donc $\overline{\sigma} = \overline{\sigma}^{3-2} = \overline{e}$, c'est-à-dire $\sigma \in H$. Cela vaut pour les huit 3-cycles, donc $|H| \geqslant 9$, contradiction avec $|H| = 6$. □

Remarque : $\mathfrak{A}_4$ est le plus petit groupe pour lequel ce phénomène se produit, et c'est l'unique exemple parmi les vingt-quatre groupes de ce document. L'erreur la plus répandue en théorie des groupes consiste précisément à « appliquer Lagrange à l'envers » : il faut retenir que seul le théorème de Cauchy, et plus généralement les théorèmes de Sylow, garantissent l'existence de sous-groupes, et uniquement pour des ordres qui sont des puissances de nombres premiers.

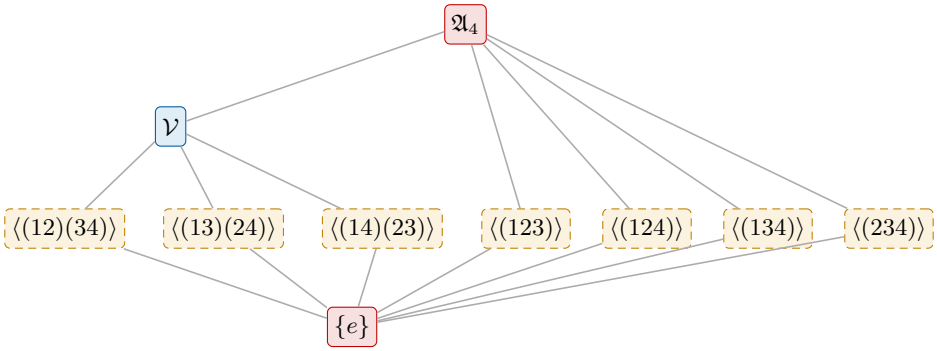
Lien avec la géométrie

$\mathfrak{A}_4$ est le groupe des rotations qui conservent un tétraèdre régulier. Il y a deux sortes d'axes : quatre axes joignant un sommet au centre de la face opposée, autour desquels on tourne d'un tiers ou de deux tiers de tour, ce qui donne $4 \times 2 = 8$ rotations d'ordre 3 ; et trois axes joignant les milieux de deux arêtes opposées, autour desquels on fait un demi-tour, ce qui donne 3 rotations d'ordre 2. Avec l'identité, on retrouve $1 + 8 + 3 = 12$.



en vert, l'un des quatre axes d'ordre 3
en violet, les trois axes d'ordre 2 et les six milieux d'arêtes

Un tétraèdre régulier, posé sur une face horizontale, vu en perspective isométrique. Ses arêtes valent $1{,}2\sqrt{3}$ et sa hauteur 1,697 ; l'arête tracée en pointillé est celle qui passe derrière, choix fait en comparant les profondeurs des six arêtes, non à vue. En vert, l'axe joignant le sommet 1 au centre de la face 234 : la rotation d'un tiers de tour autour de cet axe permute circulairement 2, 3, 4. Il y a quatre axes de ce type, un par sommet, d'où $4 \times 2 = 8$ rotations d'ordre 3. En violet, les trois axes joignant les milieux de deux arêtes opposées, marqués par des points : la rotation d'un demi-tour autour de l'un d'eux échange les deux sommets de chaque arête, ce qui donne la double transposition correspondante. Ces trois demi-tours, joints à l'identité, forment le sous-groupe de Klein distingué de $\mathfrak{A}_4$.



Le treillis de $\mathfrak{A}_4$: dix sous-groupes, et surtout aucun sommet à l'étage « ordre 6 », conformément au théorème 12. Les quatre sous-groupes d'ordre 3 sont les 3-Sylow ; ils sont conjugués, donc non distingués, et leur nombre $n_3 = 4$ est bien congru à 1 modulo 3. Les trois sous-groupes d'ordre 2 ne sont pas distingués individuellement — la conjugaison par (123) les permute circulairement — mais leur réunion avec $\{e\}$ forme $\mathcal{V}$, qui l'est. Ce treillis est planaire, contrairement à ceux de $\mathcal{D}_6$ et de $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Lien avec l'algèbre

$\mathfrak{A}_4 \simeq \mathrm{PSL}_2(\mathbb{F}_3)$, et c'est le groupe de Galois de certains polynômes de degré 4, par exemple $X^4 + 8X + 12$. Dans la résolution des équations du quatrième degré, la suite

$$\{e\} \lhd \mathcal{V} \lhd \mathfrak{A}_4 \lhd \mathfrak{S}_4$$

à quotients successifs $\mathcal{V}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ est exactement ce qui rend l'équation générale de degré 4 résoluble par radicaux ; la copie de $\mathcal{V}$ rencontrée au chapitre 4 correspond à la résolvante cubique.

12.5 Le groupe dicyclique Dic_3

Notations	Dic_3, Q_{12}, $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, groupe diédral binaire $\langle 2,2,3\rangle$
Présentation	$\langle a, b \mid a^6 = e,\ b^2 = a^3,\ bab^{-1} = a^{-1}\rangle$
Ordres des éléments	1 d'ordre 1, 1 d'ordre 2, 2 d'ordre 3, 6 d'ordre 4, 2 d'ordre 6
Sous-groupes	8 sous-groupes, dont 3 non distingués

C'est le moins familier des cinq, et il se construit exactement comme $\mathcal{Q}_8$ se construisait à partir de $\mathcal{D}_4$: on remplace la relation $b^2 = e$ du groupe diédral par $b^2 = a^3$, où a^3 est l'unique involution. Comme pour $\mathcal{Q}_8$, il n'y a qu'un seul élément d'ordre 2, et il est central.

> *Remarque :* La famille $\mathrm{Dic}_{3n} = \langle a, b \mid a^{2n} = e,\ b^2 = a^n,\ bab^{-1} = a^{-1}\rangle$, d'ordre $4n$, généralise cette construction ; pour $n = 2$ elle redonne $\mathcal{Q}_8$. On dit aussi *groupe quaternionique généralisé* lorsque n est une puissance de 2.

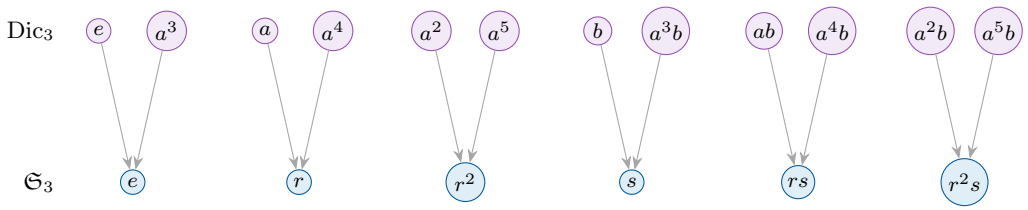
Réalisation concrète

Dans les quaternions unitaires, posons $\zeta = e^{i\pi/3} = \cos(\pi/3) + i\sin(\pi/3)$ et prenons j. Alors ζ est d'ordre 6, $j^2 = -1 = \zeta^3$, et $j\zeta j^{-1} = \overline{\zeta} = \zeta^{-1}$: le groupe $\langle \zeta, j\rangle$ est donc une copie de Dic_3. Matriciellement, dans $\mathrm{SU}(2)$:

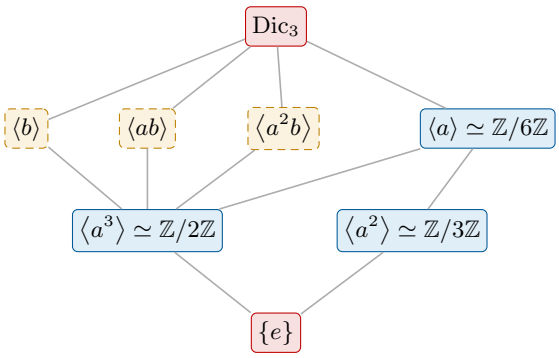
$$a = \begin{pmatrix} e^{i\pi/3} & 0 \\ 0 & e^{-i\pi/3} \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad b^2 = -I_2 = a^3.$$

Lien avec la géométrie

Le revêtement double $\mathrm{SU}(2) \to \mathrm{SO}(3)$ envoie Dic_3 sur le groupe $\mathfrak{S}_3 \simeq \mathcal{D}_3$ des isométries du triangle équilatéral, avec pour noyau $\{\pm I_2\} = \langle a^3\rangle$. C'est pourquoi on appelle Dic_3 le **groupe diédral binaire** d'indice 3 : il est au triangle ce que $\mathcal{Q}_8$ est au rectangle.



Le morphisme $\mathrm{Dic}_3 \to \mathfrak{S}_3$ de noyau $\{e, a^3\}$: chaque isométrie du triangle possède exactement deux antécédents, qui diffèrent par la multiplication par $a^3 = -1$. L'extension ne se scinde pas : Dic_3 ne contient aucun sous-groupe isomorphe à $\mathfrak{S}_3$, car il n'a qu'une seule involution alors que $\mathfrak{S}_3$ en a trois. C'est ce qui distingue Dic_3 de $\mathcal{D}_6 \simeq \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$, qui est l'extension scindée du même quotient par le même noyau.



Le treillis de Dic$_3$: huit sous-groupes. Les trois sous-groupes $\langle b\rangle$, $\langle ab\rangle$ et $\langle a^2b\rangle$ sont cycliques d'ordre 4. Comme dans $\mathcal{Q}_8$, l'unique sous-groupe d'ordre 2 est contenu dans tous les sous-groupes non triviaux sauf $\langle a^2\rangle$; c'est le centre. Les trois sous-groupes cycliques d'ordre 4 sont conjugués entre eux, donc non distingués — leur indice 3 l'autorise, contrairement à l'indice 2. On remarquera l'absence totale de sous-groupe isomorphe à $\mathcal{V}$: un tel sous-groupe exigerait trois involutions, et Dic$_3$ n'en a qu'une.

12.6 Comparaison des cinq groupes d'ordre 12

Groupe	**Ab.**	**ordre 2**	**ordre 3**	**ordre 4**	**ordre 6**	n_3
$\mathbb{Z}/12\mathbb{Z}$	oui	1	2	2	2	1
$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	oui	3	2	0	6	1
$\mathcal{D}_6$	non	7	2	0	2	1
$\mathfrak{A}_4$	non	3	8	0	0	4
Dic$_3$	non	1	2	6	2	1

Les colonnes donnent le nombre d'éléments de chaque ordre, plus le nombre n_3 de 3-sous-groupes de Sylow. Chaque ligne est différente des quatre autres, ce qui redémontre au passage que les cinq groupes sont deux à deux non isomorphes. Le total de chaque ligne vaut bien 12 une fois l'élément neutre ajouté : par exemple pour $\mathfrak{A}_4$, $1+3+8=12$. $\mathfrak{A}_4$ est le seul à avoir $n_3=4$, et le seul sans élément d'ordre 6 ; Dic$_3$ est le seul à avoir des éléments d'ordre 4 ; $\mathcal{D}_6$ est celui qui a le plus d'involutions.

Conclusion : au-delà de l'ordre 12

Chaque fois que vous avez affaire à un objet muni d'une structure, cherchez-en le groupe d'automorphismes, le groupe des transformations élément par élément qui laissent intactes toutes les relations structurelles. Vous pouvez espérer gagner ainsi une compréhension profonde de la constitution de cet objet.

Hermann Weyl, *Symmetry*, Princeton University Press, 1952, p. 144 (traduction ; le texte original dit « *try to determine its group of automorphisms* »).

Ce que la liste a montré

Vingt-quatre groupes, dont dix-sept abéliens et sept non abéliens. Le tableau suivant les récapitule tous, avec les invariants qui ont servi à les distinguer.

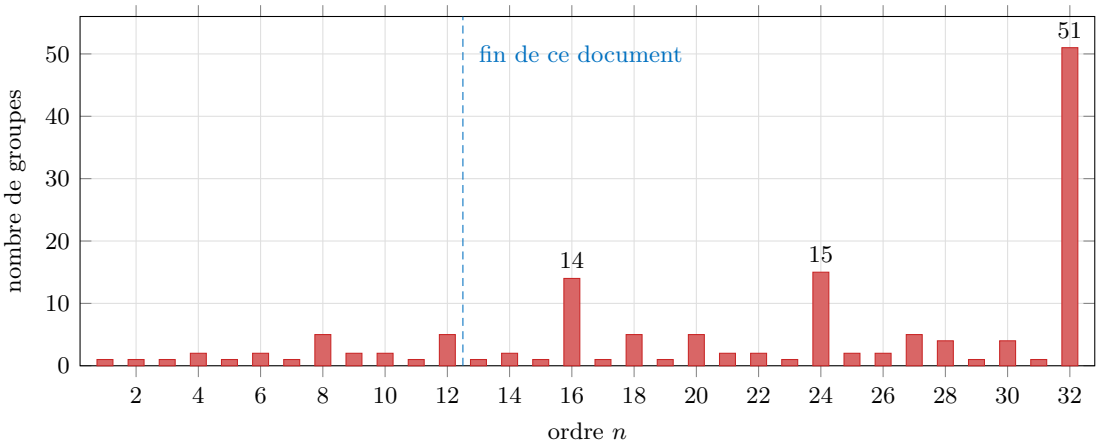
Ordre	Groupe	Ab.	Cycl.	Invol.	S.-gr.	Réalisation typique
1	$\{e\}$	oui	oui	0	1	figure sans symétrie
2	$\mathbb{Z}/2\mathbb{Z}$	oui	oui	1	2	une réflexion
3	$\mathbb{Z}/3\mathbb{Z}$	oui	oui	0	2	rotations du triangle
4	$\mathbb{Z}/4\mathbb{Z}$	oui	oui	1	3	rotations du carré
4	$\mathcal{V}$	oui	non	3	5	isométries du rectangle
5	$\mathbb{Z}/5\mathbb{Z}$	oui	oui	0	2	rotations du pentagone
6	$\mathbb{Z}/6\mathbb{Z}$	oui	oui	1	4	rotations de l'hexagone
6	$\mathfrak{S}_3$	non	non	3	6	isométries du triangle
7	$\mathbb{Z}/7\mathbb{Z}$	oui	oui	0	2	rotations de l'heptagone
8	$\mathbb{Z}/8\mathbb{Z}$	oui	oui	1	4	rotations de l'octogone
8	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	oui	non	3	8	rotations du carré et réflexion du plan
8	$(\mathbb{Z}/2\mathbb{Z})^3$	oui	non	7	16	trois interrupteurs ; plan de Fano
8	$\mathcal{D}_4$	non	non	5	10	isométries du carré
8	$\mathcal{Q}_8$	non	non	1	6	quaternions unitaires de SU(2)
9	$\mathbb{Z}/9\mathbb{Z}$	oui	oui	0	3	rotations de l'ennéagone
9	$(\mathbb{Z}/3\mathbb{Z})^2$	oui	non	0	6	plan affine d'ordre 3
10	$\mathbb{Z}/10\mathbb{Z}$	oui	oui	1	4	rotations du décagone
10	$\mathcal{D}_5$	non	non	5	8	isométries du pentagone
11	$\mathbb{Z}/11\mathbb{Z}$	oui	oui	0	2	rotations de l'hendécagone
12	$\mathbb{Z}/12\mathbb{Z}$	oui	oui	1	6	cadran de l'horloge
12	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	oui	non	3	10	$\mathcal{V} \times \mathbb{Z}/3\mathbb{Z}$
12	$\mathcal{D}_6$	non	non	7	16	isométries de l'hexagone
12	$\mathfrak{A}_4$	non	non	3	10	rotations du tétraèdre
12	Dic_3	non	non	1	8	diédral binaire dans SU(2)

Récapitulatif des vingt-quatre groupes. La colonne « involutions » donne le nombre d'éléments d'ordre 2 ; c'est l'invariant le plus économique. Il sépare la plupart des groupes de même ordre, mais pas $\{\mathbb{Z}/8\mathbb{Z}, \mathcal{Q}_8\}$, ni $\{\mathbb{Z}/9\mathbb{Z}, (\mathbb{Z}/3\mathbb{Z})^2\}$, ni $\{\mathbb{Z}/12\mathbb{Z}, \mathrm{Dic}_3\}$ et $\{\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathfrak{A}_4\}$: il faut alors compter les éléments d'ordre 3, 4 ou 9. Tous ces nombres ont été recalculés par ordinateur.

Remarque : Trois régularités se dégagent. D'abord, un groupe fini a un treillis totalement ordonné — une chaîne — si et seulement s'il est cyclique d'ordre une puissance de nombre premier ; on le vérifie sur les neuf chaînes de la liste. Ensuite, le nombre d'involutions distingue systématiquement un groupe cyclique $\mathbb{Z}/2m\mathbb{Z}$ (une seule) d'un groupe diédral $\mathcal{D}_m$ (m ou $m+1$ selon la parité de m). Enfin, deux groupes seulement de la liste — $\mathcal{Q}_8$ et Dic_3 — sont non abéliens avec une unique involution : ce sont les deux groupes *dicycliques* de la liste, et ils vivent tous deux dans la sphère $\mathrm{SU}(2)$.

La suite immédiate

Au-delà de 12, le paysage se complique brutalement, et de façon très inégale selon l'arithmétique de l'ordre.



Nombre de groupes d'ordre n pour $n \leqslant 32$ (suite A000001 de l'*Encyclopédie en ligne des suites de nombres entiers*). La barre de hauteur 1 aux ordres 13, 17, 19, 23, 29, 31 est le théorème 5 : un seul groupe par ordre premier. Les trois pics sont aux ordres 16, 24 et 32, c'est-à-dire là où la puissance de 2 est la plus élevée. La leçon est claire : la difficulté ne vient pas de la taille de n, mais de la puissance de 2 qu'il contient.

Cette tendance ne fait que s'accentuer. Il y a 51 groupes d'ordre 32, 267 d'ordre 64, 2 328 d'ordre 128, 56 092 d'ordre 256, 10 494 213 d'ordre 512 et 49 487 367 289 d'ordre 1024. Besche, Eick et O'Brien avaient annoncé en 2001 la construction des 49 910 529 484 groupes d'ordre au plus 2000 ; le décompte de l'ordre 1024 a été corrigé en 2021 par David Burrell, ce qui porte le total à 49 910 531 351. Autrement dit, plus de 99 % des groupes d'ordre au plus 2000 sont d'ordre exactement 1024, et l'immense majorité des groupes finis « petits » sont des 2-groupes.

Remarque : Ce constat explique pourquoi la classification générale des groupes finis est hors d'atteinte, alors même que celle des groupes finis *simples* a été achevée. Les groupes simples sont rares et rigides — le plus petit non abélien est $\mathfrak{A}_5$, d'ordre 60, donc au-delà de notre liste — tandis que les p-groupes prolifèrent parce que les extensions successives offrent à chaque étage un grand nombre de choix.

Ce qui manquait à la liste

Aucun groupe simple non abélien n'apparaît parmi nos vingt-quatre : c'est normal, car un théorème de Burnside affirme que tout groupe d'ordre $p^a q^b$ est résoluble, et tous les entiers de 1 à 12 sont de cette forme. Le premier ordre susceptible de porter un groupe simple non abélien est 60, et $\mathfrak{A}_5$ y parvient.
De même, parmi les sept groupes non abéliens de la liste, seuls $\mathfrak{S}_3$, $\mathcal{D}_5$ et $\mathfrak{A}_4$ ont un centre réduit à $\{e\}$: les quatre autres — $\mathcal{D}_4$, $\mathcal{Q}_8$, $\mathcal{D}_6$, Dic_3 — ont un centre d'ordre 2. Pour $\mathcal{D}_4$ et $\mathcal{Q}_8$, qui sont

des 2-groupes, c'est la proposition 10(b) qui l'impose ; pour $\mathcal{D}_6$ et Dic_3, dont l'ordre 12 n'est pas une puissance de 2, l'argument est autre : le centre est engendré par la rotation d'un demi-tour r^3, respectivement a^3, qui commute à tout parce que l'indice 6 est pair.

> *Remarque :* Une dernière observation, qui résume l'esprit du document. Sur les vingt-quatre groupes, vingt-et-un se réalisent comme groupe d'isométries ou de rotations d'une figure explicite : un polygone, un rectangle, un tétraèdre, un plan fini. Les trois exceptions — $\mathcal{Q}_8$, Dic_3 et, dans une moindre mesure, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ — demandent de sortir du plan et de l'espace ordinaire pour aller dans $\mathrm{SU}(2)$, c'est-à-dire dans la sphère de dimension 3. C'est exactement le programme de Weyl cité en exergue, lu à l'envers : partant du groupe, on cherche l'objet dont il est le groupe de symétries, et cette recherche force parfois à agrandir la géométrie.

Pour aller plus loin

— J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, 1967 — pour aborder les mêmes groupes par leurs caractères, invariant beaucoup plus fin que le treillis.

— D. Dummit et R. Foote, *Abstract Algebra*, 3e édition, Wiley, 2004 — les chapitres 4 à 6 contiennent la classification des groupes d'ordre inférieur à 60, avec les treillis dessinés.

— H. U. Besche, B. Eick et E. A. O'Brien, *The groups of order at most 2000*, Electronic Research Announcements of the AMS, vol. 7, 2001 — le décompte cité ci-dessus.

— H. Weyl, *Symmetry*, Princeton University Press, 1952 — l'ouvrage dont est tirée l'épigraphe, et la meilleure introduction au lien entre groupes et géométrie.

