CLASSIFICATION DES GROUPES D'ORDRE 12

G.BERHUY

Le but de cet article est de donner une classification complète des groupes d'ordre 12.

1. Quelques résultats techniques

On commence par démontrer quelques résultats techniques, qui sont d'un intérêt propre.

Lemme 1.1. *Soient G_1, G_2 deux groupes finis, et soit $\rho : G_1 \longrightarrow G_2$ un morphisme de groupes. Pour tout $g \in G_1$, $o(\rho(g))$ divise $|G_1|$ et $|G_2|$.*

En particulier, si G_1 et G_2 sont deux groupes finis dont les ordres sont premiers entre eux, alors tout morphisme de groupes $G_1 \longrightarrow G_2$ est trivial.

Démonstration. Soit $\rho : G_1 \longrightarrow G_2$ un morphisme de groupes. Soit n_1 l'ordre de G_1, et soit n_2 l'ordre de G_2, et soit $g \in G_1$. Alors, on a $g^{n_1} = 1_{G_1}$, et par conséquent

$$\rho(g)^{n_1} = \rho(g^{n_1}) = \rho(1_{G_1}) = 1_{G_2}.$$

Ainsi, $o(\rho(g)) \mid n_1$. Mais, puisque $\rho(g) \in G_2$, on a aussi $o(\rho(g)) \mid n_2$. En particulier, si n_1 et n_2 sont premiers entre eux, on obtient alors $o(\rho(g)) = 1$, soit $\rho(g) = 1_{G_2}$, et ρ est donc trivial. □

Soit $n \geq 1$ un entier, et soit G un groupe. Pour tout $g \in G$ tel que $o(g) \mid n$, le morphisme de groupes

$$\begin{aligned} h_g \colon \mathbb{Z} &\longrightarrow G \\ m &\longmapsto g^m \end{aligned}$$

induit par passage au quotient un morphisme de groupes

$$\begin{aligned} \overline{h}_g \colon \mathbb{Z}/n\mathbb{Z} &\longrightarrow G \\ \overline{m} &\longmapsto g^m \end{aligned},$$

puisque $n\mathbb{Z} \subset \mathrm{Ker}(h_g)$ par hypothèse sur g. On a alors le résultat suivant.

Lemme 1.2. *Soit $n \geq 1$ un entier, et soit G un groupe. Alors, l'ensemble des morphismes $\mathbb{Z}/n\mathbb{Z} \longrightarrow G$ est en bijection avec l'ensemble des éléments $g \in G$ tels que $o(g) \mid n$. Plus précisément, tout morphisme $\rho : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ est de la forme $\overline{h}_g$, pour un unique $g \in G$ tel que $o(g) \mid n$.*

De plus, $g = \rho(\overline{1})$.

Démonstration. Si $\rho : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ est un morphisme de groupes, posons $g = \rho(\overline{1})$. Alors, pour tout $m \in [\![0, n-1]\!]$, on a

$$\rho(\overline{m}) = \rho(\overline{1} + \cdots + \overline{1}) = \rho(\overline{1})^m = \overline{h}_g(\overline{m}),$$

Date: 10 novembre 2019.

et donc $\rho = \overline{h}_g$, avec $g = \rho(\overline{1})$. Notons que $o(g) \mid n$, d'après le lemme 1.1.

Si maintenant $\rho = \overline{h}_{g_1} = \overline{h}_{g_2}$, où $g_1, g_2 \in G$ sont deux éléments de G dont l'ordre divise n, en appliquant $\overline{1}$ à cette égalité, on obtient $g_1 = g_2$, d'où le résultat. □

Lemme 1.3. *Soit $n \geq 1$. Alors, pour tout $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, l'application*

$$\begin{array}{rccc} \mu_{\overline{a}} \colon & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & \overline{x} & \longmapsto & \overline{a}\cdot\overline{x} \end{array}$$

est un automorphisme de $\mathbb{Z}/n\mathbb{Z}$, et l'application

$$\begin{array}{rccc} \varphi \colon & (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \\ & \overline{a} & \longmapsto & \mu_{\overline{a}} \end{array}$$

est un isomorphisme de groupes.

Démonstration. Pour tout $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, il est clair que $\mu_{\overline{a}}$ est un morphisme de groupes, et de plus, pour tous $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, on a

$$\mu_{\overline{a}} \circ f_{\overline{b}} = f_{\overline{a}\overline{b}}.$$

Comme $f_{\overline{1}} = \mathrm{Id}_{\mathbb{Z}/n\mathbb{Z}}$, on en déduit en particulier que si $\overline{a}$ est inversible, d'inverse $\overline{b}$, alors $f_{\overline{a}}$ est inversible, d'inverse $f_{\overline{b}}$. On obtient aussi grâce à l'égalité ci-dessus que φ est un morphisme de groupes.

Soit $f \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. D'après le lemme 1.2, on a $f = \mu_{\overline{a}}$ pour un unique $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ (remarquer que $\mu_{\overline{a}} = \overline{h}_{\overline{a}}$, avec les notations du lemme) . Il reste à vérifier que $\overline{a}$ est inversible. Or, f étant un automorphisme, il est surjectif, et il existe $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ tel que $f(\overline{b}) = \overline{1}$. Mais alors

$$\overline{1} = f(\overline{b}) = \mu_{\overline{a}}(\overline{b}) = \overline{a}\overline{b},$$

et $\overline{a}$ est bien inversible. Ceci achève la démonstration. □

Lemme 1.4. *Soit p un nombre premier, et soit $n \geq 1$. Alors, les morphismes de groupes de $(\mathbb{Z}/p\mathbb{Z})^n$ dans lui-même sont exactement les endomorphismes du $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_p^n$. En particulier, pour tout $M \in \mathrm{GL}_n(\mathbb{F}_p)$, l'application*

$$\begin{array}{rccc} f_M \colon & (\mathbb{Z}/p\mathbb{Z})^n & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^n \\ & X & \longmapsto & MX \end{array}$$

est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$, et l'application

$$\begin{array}{rccc} \varphi \colon & \mathrm{GL}_n(\mathbb{F}_p) & \longrightarrow & \mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n) \\ & M & \longmapsto & f_M \end{array}$$

est un isomorphisme de groupes.

Démonstration. Il suffit de démontrer le premier point, le reste du lemme étant alors un résultat connu d'algèbre linéaire.

Puisque le groupe sous-jacent à $\mathbb{F}_p^n$ est le groupe $(\mathbb{Z}/p\mathbb{Z})^n$, un endomorphisme de $\mathbb{F}_p$-espace vectoriel de $\mathbb{F}_p^n$ est en particulier un morphisme de groupes de $(\mathbb{Z}/p\mathbb{Z})^n$ dans lui-même. Réciproquement, soit $f : (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n$ un

morphisme de groupes. Il reste à voir que f est $\mathbb{F}_p$-linéaire. Or, pour tout $m \in [\![0, p-1]\!]$, et tout $X = \begin{pmatrix} \overline{x}_1 \\ \cdots \\ \overline{x}_n \end{pmatrix} \in (\mathbb{Z}/p\mathbb{Z})^n$, on a

$$\overline{m}\cdot X = \begin{pmatrix} \overline{m}\cdot\overline{x}_1 \\ \cdots \\ \overline{m}\cdot\overline{x}_n \end{pmatrix} = \begin{pmatrix} \overline{mx_1} \\ \cdots \\ \overline{mx_n} \end{pmatrix} = \begin{pmatrix} \overline{x_1 + \cdots + x_1} \\ \cdots \\ \overline{x_n + \cdots + x_n} \end{pmatrix} = X + \cdots + X.$$

Par conséquent, on a

$$f(\overline{m}\cdot X) = f(X + \cdots + X) = f(X) + \cdots + f(X) = \overline{m}\cdot f(X),$$

d'où le résultat annoncé. □

Lemme 1.5. *Soient H, K deux groupes, et soient $\rho, \rho' : K \longrightarrow \mathrm{Aut}(H)$ deux morphismes de groupes. On suppose qu'il existe $u \in \mathrm{Aut}(H)$ tel que*

$$\rho'_k = u \circ \rho_k \circ u^{-1} \quad \textit{pour tout } k \in K.$$

Alors, l'application

$$\begin{array}{rcl} \varphi\colon H \times_\rho K & \longrightarrow & H \times_{\rho'} K \\ (h, k) & \longmapsto & (u(h), k) \end{array}$$

est un isomorphisme de groupes.

Démonstration. Pour tous $h, h' \in H$, et tous $k, k' \in k$, on a

$$\varphi((h,k)(h',k')) = \varphi(h\rho_k(h'), kk') = (u(h\rho_k(h')), kk') = (u(h)u(\rho_k(h')), kk').$$

Mais on a aussi

$$\varphi((h,k))\varphi(h',k')) = (u(h),k)(u(h'),k') = (u(h)\rho'_k(u(h')), kk').$$

Or, on a $\rho'_k((u(h')) = (u \circ \rho_k \circ u^{-1})(u(h')) = u(\rho_k(h'))$, d'où finalement

$$\varphi((h,k)(h',k')) = \varphi((h,k))\varphi((h',k'))$$

pour tous $h, h' \in H$, et tous $k, k' \in k$. Ainsi, φ est un morphisme de groupes. Si $(h, k) \in H \times_\rho K$ vérifie $\varphi((h,k)) = (u(h), k) = (1_H, 1_K)$, alors $u(h) = 1_H$ et $k = 1_K$. Comme u est un automorphisme de H, il est injectif, et on a $h = 1_H$. Par conséquent, φ est injectif. Il est également surjectif, puisque pour tout $(h, k) \in H \times_{\rho'} K$, on a

$$(h,k) = (u(u^{-1}(h)), k) = \varphi((u^{-1}(h), k)).$$

Ainsi, φ est un isomorphisme de groupes. □

Lemme 1.6. *Soient H, K deux groupes, et soient $\rho, \rho' : K \longrightarrow \mathrm{Aut}(H)$ deux morphismes de groupes. On suppose qu'il existe $\alpha \in \mathrm{Aut}(K)$ tel que $\rho' = \rho \circ \alpha$. Alors, l'application*

$$\begin{array}{rcl} \varphi\colon H \times_{\rho'} K & \longrightarrow & H \times_\rho K \\ (h, k) & \longmapsto & (h, \alpha(k)) \end{array}$$

est un isomorphisme de groupes.

Démonstration. Pour tous $h, h' \in H$, et tous $k, k' \in k$, on a

$$\varphi((h,k)(h',k')) = \varphi(h\rho'_k(h'), kk') = \varphi((h\rho_{\alpha(k)}(h'), kk')),$$

d'où

$$\varphi((h,k)(h',k')) = (h\rho_{\alpha(k)}(h'), \alpha(kk')) = (h\rho_{\alpha(k)}(h'), \alpha(k)\alpha(k')).$$

Mais on a aussi

$$\varphi((h,k))\varphi(h',k')) = (h,\alpha(k))(h',\alpha(k')) = (h\rho_{\alpha(k)}(h'), \alpha(k)\alpha(k')),$$

d'où finalement

$$\varphi((h,k)(h',k')) = \varphi((h,k))\varphi((h',k'))$$

pour tous $h, h' \in H$, et tous $k, k' \in k$. Ainsi, φ est un morphisme de groupes. Si $(h,k) \in H \times_{\rho'} K$ vérifie $\varphi((h,k)) = (h,\alpha(k)) = (1_H, 1_K)$, alors $h = 1_H$ et $\alpha(k) = 1_K$. Comme α est un automorphisme de K, il est injectif, et on a $k = 1_K$. Par conséquent, φ est injectif. Il est également surjectif, puisque pour tout $(h,k) \in H \times_\rho K$, on a

$$(h,k) = (h, \alpha(\alpha^{-1}(k))) = \varphi((h, \alpha^{-1}(k))).$$

Ainsi, φ est un isomorphisme de groupes. □

2. Groupes d'ordre 12

Le but de ce paragraphe est de classifier les groupes d'ordre 12 à isomorphisme. Remarquons que l'on en connait déjà quelques uns :

$$\mathbb{Z}/12\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_6 \ \text{ et } \ \mathfrak{A}_4.$$

La question est de savoir si on les a déjà tous, ou s'il y en a d'autres.

Dans tout ce qui suit, G désigne un groupe d'ordre 12.

Lemme 2.1. *Un 2-Sylow est distingué dans G, ou un 3-Sylow est distingué dans G.*

En particulier, si H_2 est un 2-Sylow et H_3 est un 3-Sylow, on a

$$G \simeq H_2 \rtimes H_3 \ \text{ ou } \ H_3 \rtimes H_2.$$

Démonstration. Le nombre N_4 de 2-Sylow vérifie $N_4 \equiv 1$ [2] et $N_4 \mid 3$. On a donc $N_4 = 1$ ou 3. De plus, le nombre N_3 de 3-Sylow vérifie $N_3 \equiv 1$ [3] et $N_3 \mid 4$. On a donc $N_3 = 1$ ou 4.

Si $N_3 = 1$, alors un 3-Sylow est distingué dans G. Notons maintenant qu'un 3-Sylow est cyclique d'ordre 3. Chaque 3-Sylow contient donc 1_G et deux éléments d'ordre 3. Un élément d'ordre 3 dans un 3-Sylow fixé engendrant ce 3-Sylow, deux 3-Sylow distincts s'intersectent donc trivialement. Si $N_3 = 4$, on a donc au moins 8 éléments d'ordre 3 distincts. Or, un 2-Sylow contient quatre éléments qui sont d'ordre divisant 4. En particulier, ces quatre éléments ne sont pas d'ordre 3. D'après ce qui précède, il y a au plus quatre éléments qui ne sont pas d'ordre 3, et il y a donc au plus un 2-Sylow. Par conséquent, $N_2 = 1$ et un 2-Sylow est distingué dans G.

On a donc $|G| = |H_2|\cdot|H_3|$, $H_2 \cap H_3 = \{1_G\}$ (puisque les ordres de H_2 et H_3 sont premiers entre eux), et H_2 ou H_3 est distingué dans G. On obtient alors la dernière partie du lemme. □

Rappelons qu'il existe seulement deux groupes d'ordre 4 à isomorphisme près, à savoir $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$. D'après le lemme précédent, G est isomorphe à un groupe du type suivant :

$$\mathbb{Z}/3\mathbb{Z} \times_\rho \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \times_\rho (\mathbb{Z}/2\mathbb{Z})^2,\ \mathbb{Z}/4\mathbb{Z} \times_\rho \mathbb{Z}/3\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^2 \times_\rho \mathbb{Z}/3\mathbb{Z},$$

où ρ est un morphisme de groupes approprié.

Le cas $\mathbb{Z}/4\mathbb{Z} \times_\rho \mathbb{Z}/3\mathbb{Z}$. C'est le cas le plus facile. En effet, $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{-1}\}$ est d'ordre 2. Par conséquent, $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ est aussi d'ordre 2, et tout morphisme $\rho : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ est donc trivial d'après le lemme 1.1. On obtient donc le produit direct $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, qui est isomorphe à $\mathbb{Z}/12\mathbb{Z}$, d'après le théorème chinois.

Le cas $\mathbb{Z}/3\mathbb{Z} \times_\rho \mathbb{Z}/4\mathbb{Z}$. On a $(\mathbb{Z}/3\mathbb{Z})^\times = \{\overline{1}, \overline{-1}\} \simeq \mathbb{Z}/2\mathbb{Z}$. Ainsi, $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ est cyclique d'ordre 2. Le lemme 1.3 montre que les deux éléments de $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ sont $\mathrm{Id}_{\mathbb{Z}/3\mathbb{Z}}$ et le morphisme

$$\begin{array}{rccc} \mu_{\overline{-1}}\colon & \mathbb{Z}/3\mathbb{Z} & \longrightarrow & \mathbb{Z}/3\mathbb{Z} \\ & \overline{x} & \longmapsto & \overline{-x}. \end{array}$$

Pour alléger les notations, notons $\mu = \mu_{\overline{-1}}$.

Soit $\rho : \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ un morphisme de groupes. Le lemme 1.2 montre que $\rho = \overline{h}_f$, où $f \in \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ avec $o(f) \mid 4$. Comme $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ est d'ordre 2, ses éléments sont d'ordre 1 ou 2. En particulier, il y a deux morphismes ρ possibles : le morphisme trivial, et le morphisme ρ défini par $\rho(\widehat{m}) = \mu^m$ pour tout $\widehat{m} \in \mathbb{Z}/4\mathbb{Z}$.

Le morphisme trivial donne $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z}$. L'autre groupe est appelé *groupe dicyclique*, et est noté Dic_3. Sa loi de groupe est donnée par

$$(\overline{x}, \widehat{m})(\overline{x'}, \widehat{m'}) = (\overline{x + (-1)^m x'}, \widehat{m + m'}),$$

pour tous $\overline{x}, \overline{x'} \in \mathbb{Z}/3\mathbb{Z}$, et tous $\widehat{m}, \widehat{m'} \in \mathbb{Z}/4\mathbb{Z}$.

Le cas $\mathbb{Z}/3\mathbb{Z} \times_\rho (\mathbb{Z}/2\mathbb{Z})^2$. Soit $\rho : (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ un morphisme de groupes. L'image d'un élément $(\widetilde{m}_1, \widetilde{m}_2) \in (\mathbb{Z}/2\mathbb{Z})^2$ est de la forme μ^k, avec $k = 0$ ou 1. Posons

$$\rho((\widetilde{1}, \widetilde{0})) = \mu^a \quad \text{et} \quad \rho((\widetilde{0}, \widetilde{1})) = \mu^b.$$

On a alors

$$\rho((\widetilde{1}, \widetilde{1})) = \rho((\widetilde{1}, \widetilde{0}) + (\widetilde{0}, \widetilde{1})) = \mu^a \circ \mu^b = \mu^{a+b}.$$

On constate alors que l'on a

$$\rho((\widetilde{m}_1, \widetilde{m}_2)) = \mu^{am_1 + bm_2} \quad \text{pour tout } (\widetilde{m}_1, \widetilde{m}_2) \in (\mathbb{Z}/2\mathbb{Z})^2.$$

Réciproquement, on montre aisément l'application

$$\begin{array}{rccc} \rho_{a,b}\colon & (\mathbb{Z}/2\mathbb{Z})^2 & \longrightarrow & \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \\ & (\widetilde{m}_1, \widetilde{m}_2) & \longmapsto & \mu^{am_1 + bm_2} \end{array}$$

est bien définie et est un morphisme de groupes.

On a donc quatre morphismes possibles. Le morphisme $\rho_{0,0}$ est trivial, et donne le produit direct $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$, qui est isomorphe à $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Nous allons maintenant démontrer que les trois autres morphismes donnent le même groupe à isomorphisme près.

Si $a, b \in \{0, 1\}$ ne sont pas tous les deux nuls, on peut toujours trouver une matrice $M \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ dont la première ligne est $(\widetilde{a}, \widetilde{b})$. Gardons les notations du lemme 1.4. Pour tout $(\widetilde{m}_1, \widetilde{m}_2) \in (\mathbb{Z}/2\mathbb{Z})^2$, on a

$$(\rho_{1,0} \circ f_M)((\widetilde{m}_1, \widetilde{m}_2)) = \rho_{1,0}(\widetilde{am_1 + bm_2}) = \mu^{am_1+bm_2} = \rho_{a,b}((\widetilde{m}_1, \widetilde{m}_2)),$$

d'où $\rho_{a,b} = \phi \circ f_M$. D'après le lemme 1.6, on obtient

$$\mathbb{Z}/3\mathbb{Z} \times_{\rho_{a,b}} (\mathbb{Z}/2\mathbb{Z})^2 \simeq \mathbb{Z}/3\mathbb{Z} \times_{\rho_{1,0}} (\mathbb{Z}/2\mathbb{Z})^2.$$

Notons que la loi de groupe $\mathbb{Z}/3\mathbb{Z} \times_{\rho_{1,0}} (\mathbb{Z}/2\mathbb{Z})^2$ est donnée par

$$(\overline{x}, (\widetilde{m}_1, \widetilde{m}_2))(\overline{x'}, (\widetilde{m'}_1, \widetilde{m'}_2)) = (\overline{x + (-1)^{m_1} x'}, (\widetilde{m_1 + m'_1}, \widetilde{m_2 + m'_2}))$$

pour tous $\overline{x}, \overline{x'} \in \mathbb{Z}/3\mathbb{Z}$, et tous $\widetilde{m}_1, \widetilde{m'}_1, \widetilde{m}_2, \widetilde{m'}_2 \in \mathbb{Z}/2\mathbb{Z}$.

Le cas $(\mathbb{Z}/2\mathbb{Z})^2 \times_\rho \mathbb{Z}/3\mathbb{Z}$. Soit $\rho : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2)$. D'après le lemme 1.2, on a

$$\rho_{\overline{m}} = f^m \quad \text{pour tout } \overline{m} \in \mathbb{Z}/3\mathbb{Z},$$

pour un unique $f \in \mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2)$ d'ordre divisant 3. Un tel automorphisme f est de la forme f_M, avec $M \in \mathrm{GL}_2(\mathbb{F}_2)$, d'après le lemme 1.4. Comme un isomorphisme préserve l'ordre des éléments, M est d'ordre divisant 3.

On a donc $M^3 = I_2$, si bien que le polynôme $X^3 - \widetilde{1} = (X - \widetilde{1})(X^2 + X + \widetilde{1}) \in \mathbb{F}_2[X]$ annule M. Notons que $X^2 + X + \widetilde{1}$ est irréductible, puisqu'il est de degré 2 et n'a pas de racines dans $\mathbb{F}_2$. Le polynôme minimal divise $X^3 - \widetilde{1}$, et est de degré inférieur ou égal 2. Il est donc égal à $X - 1$ ou $X^2 + X + \widetilde{1}$. Dans le premier cas, $M = I_2$ et le morphisme ρ est trivial. Cela donne à nouveau le produit direct $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Supposons maintenant que le polynôme minimal de M soit égal à $X^2 + X + \widetilde{1}$. Nous allons montrer que M est conjuguée à $M_0 = \begin{pmatrix} \widetilde{0} & -\widetilde{1} \\ \widetilde{1} & -\widetilde{1} \end{pmatrix}$. Soit $v \in \mathbb{F}_2^2$ un vecteur non nul arbitraire. Montrons que (v, Mv) est une base de $\mathbb{F}_2^2$. Pour cela, il suffit de vérifier qu'elle est libre, ce qui revient encore à voir que v et Mv ne sont pas proportionnels. Supposons que $Mv = \widetilde{a}v$, avec $\widetilde{a} \in \mathbb{F}_2$. Alors, on a

$$M^2 v = -Mv - v = -(\widetilde{a} + 1)v = \widetilde{a}Mv = \widetilde{a}^2 v,$$

d'où $(\widetilde{a}^2 + \widetilde{a} + 1)v = 0$. Or, $\widetilde{a}^2 + \widetilde{a} + 1$ est non nul pour tout $\widetilde{a} \in \mathbb{F}_2$, d'où la contradiction $v = 0$. Si l'on note $P \in \mathrm{GL}_2(\mathbb{F}_2)$ la matrice de la base (v, Mv) dans la base canonique, on obtient $P^{-1}MP = M_0$, soit encore $M = PM_0P^{-1}$.

Posons alors

$$\begin{array}{rccc} \rho_M \colon & \mathbb{Z}/3\mathbb{Z} & \longrightarrow & \mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2) \\ & \overline{m} & \longmapsto & f_M^m. \end{array}$$

Pour tout $\overline{m} \in \mathbb{Z}/3\mathbb{Z}$, on a alors

$$(\rho_M)_{\overline{m}} = (f_M)^m = (f_P \circ f_{M_0} \circ f_P^{-1})^m = f_P \circ f_{M_0}^m \circ f_P^{-1} = f_P \circ (\rho_{M_0})_{\overline{m}} \circ f_P^{-1}.$$

Par le lemme 1.5, on obtient un isomorphisme

$$(\mathbb{Z}/2\mathbb{Z})^2 \times_{\rho_M} \mathbb{Z}/3\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times_{\rho_{M_0}} \mathbb{Z}/3\mathbb{Z}.$$

Notons que la loi de groupe de $(\mathbb{Z}/2\mathbb{Z})^2 \times_{\rho_{M_0}} \mathbb{Z}/3\mathbb{Z}$ est donnée par

$$((\widetilde{a}, \widetilde{b}), \overline{m})((\widetilde{a'}, \widetilde{b'}), \overline{m'}) = ((\widetilde{a + b'}, \widetilde{b - a' - b'}), \overline{m + m'}),$$

pour tous $\widetilde{a}, \widetilde{a'}, \widetilde{b}, \widetilde{b'} \in \mathbb{Z}/2\mathbb{Z}$ et tous $\overline{m}, \overline{m'} \in \mathbb{Z}/3\mathbb{Z}$.

On a donc obtenu cinq groupes, à savoir

$$G_1 = \mathbb{Z}/12\mathbb{Z},\ G_2 = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ G_3 = \mathrm{Dic}_3,$$

$$G_4 = \mathbb{Z}/3\mathbb{Z} \times_{\rho_{1,0}} (\mathbb{Z}/2\mathbb{Z})^2 \text{ et } G_5 = (\mathbb{Z}/2\mathbb{Z})^2 \times_{\rho_{M_0}} \mathbb{Z}/3\mathbb{Z}.$$

Lemme 2.2. *Les cinq groupes précédents sont deux à deux non isomorphes.*

Démonstration. Commençons par remarquer que, si H et K sont deux groupes abéliens, et si $\rho : K \longrightarrow \mathrm{Aut}(H)$ est un morphisme de groupes, alors $H \times_\rho K$ est abélien si, et seulement si, ρ est trivial.

En effet, si ρ est trivial, $H \times_\rho K = H \times K$ est abélien. Réciproquement, si $H \times_\rho K$ est abélien, tout sous-groupe est distingué dans $H \times_\rho K$. En particulier, $\{1_H\} \times K$ est distingué dans $H \times_\rho K$, et on sait que cela implique que ρ est trivial.

On en déduit que G_3, G_4 et G_5 sont non abéliens, donc non isomorphes à G_1 ou G_2. De plus, G_1 et G_2 ne sont pas isomorphes, car le premier possède un élément d'ordre 12, ce qui n'est pas le cas du second. Il reste donc à constater que les trois derniers groupes sont deux à deux non isomorphes.

Notons que les sous-groupes $H' = H \times \{1_K\}$ et $K' = \{1_H\} \times K$ d'un produit semi-direct $H \times_\rho K$ sont respectivement isomorphes à H et K, les isomorphismes étant donnés par

$$\begin{array}{ccc} H \longrightarrow H' & & K \longrightarrow K' \\ h \longmapsto (h, 1_K) & \text{et} & k \longmapsto (1_H, k). \end{array}$$

Par conséquent, un 2-Sylow de G_3 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ (il en possède au moins un, et tous les 2-Sylow sont conjugués, donc isomorphes), tandis que G_4 et G_5 ont des 2-Sylow isomorphes à $(\mathbb{Z}/2\mathbb{Z})^2$. Ainsi, G_3 n'est pas isomorphe à G_4 ou G_5. Pour conclure, il reste à vérifier que G_4 et G_5 ne sont pas isomorphes. Or, le 2-Sylow $H' = (\mathbb{Z}/2\mathbb{Z})^2 \times \{\overline{0}\}$ de G_5 est distingué dans G_5 (propriété des produits semi-directs externes). Le 2-Sylow $K' = \{\overline{0}\} \times (\mathbb{Z}/2\mathbb{Z})^2$ de G_4 n'est pas contre pas distingué dans G_4, car sinon on sait que le morphisme $\rho_{1,0}$ serait trivial, ce qui n'est pas le cas. Ainsi, G_4 et G_5 ne peuvent être isomorphes, et cela achève la démonstration. □

À ce stade, on pourrait se dire que l'on a terminé : il y a cinq groupes d'ordre 12 à isomorphisme près, donnés par la liste précédente. Oui, mais… où se cachent donc D_6 et $\mathfrak{A}_4$ dans cette liste ?

Le groupe $\mathfrak{A}_4$ est un groupe non abélien, qui possède un sous-groupe distingué d'ordre 4 (constitué de l'identité et des double transpositions). L'analyse précédente montre que le seul groupe dans la liste possédant ces propriétés est le groupe G_5. On a donc $G_5 \simeq \mathfrak{A}_4$. Le groupe D_6 étant non abélien, il est donc nécessairement isomorphe à G_3 ou G_4. Mais D_6 n'a pas d'éléments d'ordre 4 (il est constitué de l'identité, de rotations d'ordre 3, et de symétries orthogonales d'ordre 2). Comme Dic_3 a un élément d'ordre 4 (un 2-Sylow de Dic_3 est cyclique d'ordre 4), D_6 est nécessairement isomorphe à G_5.

On a donc obtenu la classification suivante.

Théorème 2.3. *Il y a cinq groupes d'ordre* 12 *à isomorphisme près (deux abéliens, et trois non abéliens), à savoir*

$$\mathbb{Z}/12\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},\ \mathrm{Dic}_3,\ D_6 \text{ et } \mathfrak{A}_4,$$

où Dic_3 *est le produit semi-direct externe* $\mathbb{Z}/3\mathbb{Z}\times_{\rho_{1,0}}(\mathbb{Z}/2\mathbb{Z})^2$*, dont la loi de groupe est donnée par*

$$(\overline{x},(\widehat{m}_1,\widehat{m}_2))(\overline{x'},(\widehat{m'}_1,\widehat{m'}_2)) = (\overline{x+(-1)^{m_1}x'},(\widehat{m_1+m'_1},\widehat{m_2+m'_2}))$$

pour tous $\overline{x},\overline{x'}\in\mathbb{Z}/3\mathbb{Z}$*, et tous* $\widehat{m}_1,\widehat{m'}_1,\widehat{m}_2,\widehat{m'}_2\in\mathbb{Z}/2\mathbb{Z}$*.*

De plus :

(1) *le groupe* Dic_3 *est le seul groupe non abélien d'ordre* 12 *possédant un* 2*-Sylow cyclique*

(2) *le groupe* D_6 *est le seul groupe non abélien d'ordre* 12 *possédant un* 2*-Sylow non distingué isomorphe à* $(\mathbb{Z}/2\mathbb{Z})^2$

(3) *le groupe* $\mathfrak{A}_4$ *est le seul groupe non abélien d'ordre* 12 *possédant un* 2*-Sylow distingué isomorphe à* $(\mathbb{Z}/2\mathbb{Z})^2$*.*

Finissons par quelques remarques complémentaires.

Remarques 2.4.

(1) Soient $\tau_1 = (1\ 2)(3\ 4), \tau_2 = (1\ 3)(2\ 4)$ et $\sigma = (1\ 2\ 3)$. Le lecteur vérifiera que l'application

$$G_5 \longrightarrow \mathfrak{A}_4$$
$$((\widetilde{a},\widetilde{b}),\overline{m}) \longmapsto \tau_1^a\tau_2^b\sigma^m$$

est bien définie, et est un isomorphisme de groupes.

(2) Soit r la rotation vectorielle d'angle $\dfrac{\pi}{3}$, et soit s la symétrie orthogonale d'axe (Ox). On vérifie que l'application

$$G_4 \longrightarrow D_6$$
$$(\overline{x},(\widetilde{m}_1,\widetilde{m}_2)) \longmapsto r^{4x+3m_2}s^{m_1}$$

est bien définie, et est un isomorphisme de groupes.

(3) Le groupe Dic_3 peut se décrire de manière un peu plus explicite. Soit $j = e^{\frac{2i\pi}{3}}$, et soient $A, B \in \mathrm{GL}_2(\mathbb{C})$ les deux matrices inversibles définies par

$$A = \begin{pmatrix} -j & 0 \\ 0 & -j^2 \end{pmatrix}, \ B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

On vérifie que A est d'ordre 6, que B est d'ordre 4, et que l'on a les égalités

$$A^3 = B^2 = -I_2 \ \text{ et } BAB^{-1} = A^{-1}.$$

Quelques calculs montrent alors que l'ensemble

$$D' = \{A^k B^\ell \mid k \in [\![0,2]\!], \ell \in [\![0,3]\!]\}$$

est un sous-groupe d'ordre 12 de $\mathrm{GL}_2(\mathbb{C})$ (donc égal à $\langle A, B\rangle$), et que l'application

$$\begin{aligned} \mathrm{Dic}_3 &\longrightarrow D' \\ (\overline{x}, \widehat{m}) &\longmapsto A^{4x} B^m \end{aligned}$$

est bien définie, et est un isomorphisme de groupes. Ainsi, Dic_3 peut aussi être défini comme étant le sous groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par les deux matrices A et B.