GROUPES ABÉLIENS FINIS

CHAPITRE 3

Contents

Pour tout entier $n > 0$, on notera $\mathbb{Z}_n$ l'ensemble $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}$.

1. Groupes monogènes, groupes cycliques

Nous rappelons ici la notion de groupe monogène définie au chapitre 1. Un groupe G engendré par un élément $a \in G$ est appelé groupe monogène, on écrit

$$G = \langle a \rangle = \{a^k \ ; \ k \in \mathbb{Z}\}.$$

En notation additive, on écrit

$$G = \langle a \rangle = \{ka \ ; \ k \in \mathbb{Z}\}$$

Il existe des groupes monogènes infinis, tels que $\mathbb{Z}$ et des groupes monogènes finis tels que $\mathbb{Z}_n$.

Définition 1.1. *On dit qu'un groupe G est* **cyclique** *lorsqu'il est monogène et fini. Tout élément a de G tel que $G = \langle a \rangle$ est appelé un* **générateur** *de G. On a donc, si $|G| = n$,*

$$G = \{e, a, a^2, \dots, a^{n-1}\}, \text{ avec } o(a) = n.$$

En notation additive, on écrit

$$G = \{0, a, 2a, \dots, (n-1)a\}, \text{avec } o(a) = n.$$

Proposition 1.2. *Si G est un groupe monogène et si f est un morphisme de groupes de G dans un autre groupe G', alors $f(G)$ est monogène*

Proof. En effet, si $G = \langle a \rangle$ avec $a \in G$, alors $f(G) = \langle f(a) \rangle$, puisque f est un morphisme de groupes. □

Exemples 1.3. (1) Pour tout entier $n > 0$, le groupe additif $\mathbb{Z}_n$ est cyclique. En effet, $(\mathbb{Z}, +)$ et monogène engendré par 1. Le morphisme (projection canonique) $\pi : \mathbb{Z} \to \mathbb{Z}_n$ est surjectif, donc $\mathbb{Z}_n$ est monogène, engendré par $\pi(1) = \bar{1}$. Comme le groupe $\mathbb{Z}_n$ est fini d'ordre n, il est cyclique,

$$\mathbb{Z}_n = \langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

(2) Le groupe multiplicatif $\mathbb{U}_n = \{z \in \mathbb{C}\ ;\ z^n = 1\}$ des racines $n^{\text{ièmes}}$ de l'unité dans $\mathbb{C}$, est groupe cyclique d'ordre n engendré par par $\zeta = e^{\frac{2i\pi}{n}}$. En effet, considérons le morphisme de groupes $\pi(\mathbb{Z},+) \to (\mathbb{C}^\times, \times)$ tel que $\pi(k) = e^{2ik\pi/n}$. Son image $\pi(\mathbb{Z}) = \mathbb{U}_n$ est un groupe cyclique d'ordre n, engendré par $\xi := \pi(1) = e^{2i\pi/n}$,

$$\mathbb{U}_n = \langle \xi \rangle = \{1, \xi, \dots \xi^{n-1}\}.$$

Proposition 1.4. *Si $G = \langle a \rangle$ est un groupe cyclique d'ordre n, alors*

$$(k \in \mathbb{Z} \text{ et } a^k = e) \iff k \in n\mathbb{Z}$$

et n est le plus petit entier strictement positif tel que $a^n = e$.

Proof. En effet, l'element a est dordre n (voir Proposition 9.1 du chapitre 1). □

Pour $n \geq 2$, on note $\varphi(n)$ le cardinal de l'ensemble des entiers k tels que $1 \leq k \leq n-1$ et $\operatorname{pgcd}(k,n) = 1$ (c-à-d. n et k premiers entre eux). On convient que $\varphi(1) = 1$. La fonction $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ ainsi définie est appelée la **fonction d'Euler** ou **caractéristique d'Euler**. Les propriétés de la fonction d'Euler sont étudiées dans l'exercice 16 de la feuille 3.

Proposition 1.5. *Soient G un groupe cyclique d'ordre n et $a \in G$ un générateur de G.*

a) Pour tout $k \in \mathbb{Z}$, l'ordre de $a^k \in G$ est $o(a^k) = \frac{n}{\operatorname{pgcd}(n,k)}$. En particulier, a^k est un générateur de G si et seulement si $\operatorname{pgcd}(n,k) = 1$.

b) Il existe $\varphi(n)$ générateurs distincts dans G.

Proof. Soit $k \in \mathbb{Z}$. Posons $d = \operatorname{pgcd}(n,k) \in \mathbb{N}^*$. Alors $n = dn'$ et $k = dk'$ avec $\operatorname{pgcd}(n',k') = 1$. Pour tout $m \in \mathbb{N}$, on a $(a^k)^m = e \iff a^{km} = e \iff n|km \iff n'|k'm \iff n'|m$. Ainsi n' est le plus petit entier non nul tel que $(a^k)^{n'} = e$ et par suite $n' = o(a^k)$.

□

Exemple 1.6. (a) Le groupe additif $\mathbb{Z}_n$ est cyclique d'ordre n et engendré par $\bar{1}$. Ses générateurs sont de la forme $\bar{k} = k\bar{1}$ avec $0 \leq k \leq n-1$ et $k \wedge n = 1$.

(b) Le groupe multiplicatif $\mathbb{U}_n$ est cyclique d'ordre n et engendré par $\xi = e^{2i\pi/n}$. Ses générateurs sont de la forme ξ^k avec $0 \leq k \leq n-1$ et $k \wedge n = 1$.

(c) Soit $a \in \mathbb{U}_{30}$. Alors il existe un entier k tel que $0 \leq k \leq 29$ tel que $a = \xi^k$ avec $\xi = e^{2i\pi/30} = e^{i\pi/15}$.

$$\begin{aligned} o(a) = 6 \quad &\iff \frac{30}{\operatorname{pgcd}(k,30)} = 6 \\ &\iff \frac{5}{\operatorname{pgcd}(k,30)} = 1 \\ &\iff \operatorname{pgcd}(k,30) = 5 \\ &\iff k = 5, 25 \end{aligned}$$

On en déduit $\mathbb{U}_{30}$ admet deux éléments d'ordre 6 qui sont $\xi^5 = e^{i\pi/3}$ et $\xi^{25} = e^{5i\pi/3}$.

Lemme 1.7. *Soient G un groupe cyclique d'ordre n. Alors G est isomorphe au groupe $\mathbb{Z}/n\mathbb{Z}$. En particulier, G est abélien.*

Proof. Soit $a \in G$ un générateur de G. L'homomrphisme $f_a : k \mapsto a^k$ de $\mathbb{Z}$ dans G est surjectif car $\langle a \rangle = G$. Son noyau est $n\mathbb{Z}$ où $n = o(a)$ est l'ordre de a. Par factorisation, on déduit un isomorphisme $\overline{f}_a : \bar{k} \mapsto a^k$ de $\mathbb{Z}/n\mathbb{Z}$ sur G.

□

2. Morphismes de groupes cycliques

Proposition 2.1. *Soient G un groupe cyclique et $a \in G$ un générateur de G.*

(1) *Soit f un homomorphisme surjectif de G sur un autre groupe G'. Alors G' est cyclique, $a' = f(a)$ engendre G' et $|G'|$ divise $|G|$. En particulier, tout groupe quotient de G est cyclique.*
(2) *Soit G' un groupe cyclique tel que $|G'|$ divise $|G|$. Soit $a' \in G'$. Il existe un unique homomorphisme f de G dans G' tel que $f(a) = a'$. Pour que f soit surjectif, il faut et il suffit que a' soit un générateur de G'.*

Proof. 1. Puisque f est surjectif, pour tout $y \in G'$ il existe $x \in G$ tel que $f(x) = y$. Or il existe k, $0 \leq k \leq n-1$ tel que $x = a^k$, et donc $y = f(a^k) = f(a)^k$ et par suite $f(a)$ engendre G'. De plus, comme f est surjectif, G' est isomorphe à $G/\mathrm{Ker}(f)$ et donc $|G'|$ divise $|G|$.

2. Posons $|G| = n$ et $|G'| = n'$. D'après le théorème de Lagrange, $m := o(a')$ divise n'. Or n' divise n, donc $n\mathbb{Z} \subset m\mathbb{Z}$. Considérons l'homomorphisme canonique $g : k \mapsto a'^k$ de $\mathbb{Z}$ sur $\langle a' \rangle$. Son noyau est $m\mathbb{Z}$. Par (restriction à $\mathbb{Z}/n\mathbb{Z}$) factorisation, il existe un homomorphisme $\bar{g}$ de $\mathbb{Z}/n\mathbb{Z}$ sur $\langle a' \rangle$ tel que $\bar{g}(\bar{k}) = a'^k$ pour tout $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$. Soit f_a l'isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur G donné par le Lemme 1.7. Alors $f = \bar{g} \circ f_a^{-1} \in \mathrm{Hom}(G, G')$ est tel que $f(a) = \bar{g}(f_a^{-1}(a)) = \bar{g}(\bar{1}) = a'$. Il est unique car la donnée de $f(a) = a'$ détermine $f(a^k) = a'^k$ pour tout $k \in \mathbb{Z}$. Pour que f soit surjective, il faut et il suffit que a' engendre G' car $\mathrm{Im}(f) = \mathrm{Im}(g) = \langle a' \rangle$. □

Corollaire 2.2. *Deux groupes cycliques G et G' sont isomorphes si et seulement s'ils ont le même ordre. Supposons cette condition vérifiée. Soit $a \in G$ un générateur de G. Alors l'application $\theta : f \mapsto f(a)$ est une bijection de l'ensemble $Isom(G, G')$ des isomorphismes de G dans G', sur l'ensemble des générateurs de G'.*

Proof. Si G et G sont isomorphes, alors ils ont le même ordre. Réciproquement, s'il G et G' ont le même cardinal, alors d'après le Lemme 1.7, ils sont isomorphes. □

Si m est un entier et si G est un groupe, alors on note f_m l'application de G dans G donnée par $f_m : x \mapsto x^m$.

Exemple 2.3.
(1) Le groupe $\mathbb{Z}/7\mathbb{Z}$ est cyclique engendré par $\bar{1}$. Un élément $\bar{k} = k\bar{1} \in \mathbb{Z}/7\mathbb{Z}$ est un autre générateur si et seulement si $k \wedge 7 = 1$ et $k < 7$. Donc $k = 1$, 2, 3, 4, 5, 6. D'où l'ensemble des générateurs $\Delta_7 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \}$
(2) Si $f : \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ est un endomorphismes de groupes, alors pour tout $\bar{k} \in \mathbb{Z}/7\mathbb{Z}$, $f(\bar{k}) = f(k\bar{1}) = kf(\bar{1})$. On en déduit que f est complètement déterminé par la donnée de $f(1)$.
(3) Remarquons que si $g : \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ est un endomorphisme injectif ou surjectif, alors il est bijectif. Soit $f : \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ un endomorphisme. D'après la Proposition 2.1 $f(\bar{1})$ engendre le groupe cyclique d'arrivée $\mathbb{Z}/7\mathbb{Z}$, si et seulement si f est surjectif et donc bijectif.
(4) On déduit de la question précédente, que le nombre d'automorphismes de $\mathbb{Z}/7\mathbb{Z}$ est égal au cardinal de l'ensemble des générateurs de $\mathbb{Z}/7\mathbb{Z}$. Donc $\mathrm{Card}(\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})) = \mathrm{Card}(\Delta_7) = 6$.
(5) Les éléments de $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$ associés aux divers choix de l'image de $\bar{1}$ sont les f_k tels que $f_k(\bar{1}) = \overline{k}$ pour tout $k = 1, 2, 3, 4, 5, 6$:

$$\begin{array}{lll} f_1 : \overline{n} = n\overline{1} \mapsto n\overline{1} = \overline{n} & f_2 : \overline{n} = n\overline{1} \mapsto n\overline{2} = \overline{2n} & f_3 : \overline{n} = n\overline{1} \mapsto n\overline{3} = \overline{3n} \\ f_4 : \overline{n} = n\overline{1} \mapsto n\overline{4} = \overline{4n} & f_5 : \overline{n} = n\overline{1} \mapsto n\overline{5} = \overline{6n} & f_6 : \overline{n} = n\overline{1} \mapsto n\overline{6} = \overline{6n} \end{array}$$

Remarquons que $f_1 = \text{Id}$. Posons $g = f_3$. On a

- $g^2(\overline{1}) = g(\overline{3}) = \overline{9} = \overline{2} = f_2(\overline{1})$. Donc $g^2 = f_2$ car $\overline{1}$ engendre $\mathbb{Z}/7\mathbb{Z}$.
- $g^3(\overline{1}) = g(g^2(\overline{1})) = g(\overline{2}) = \overline{6} = f_6(\overline{1})$. Donc $g^3 = f_6$.
- $g^4(\overline{1}) = g(g^3(\overline{1})) = g(\overline{6}) = \overline{18} = \overline{4} = f_4(\overline{1})$. Donc $g^4 = f_4$.
- $g^5(\overline{1}) = g(g^4(\overline{1})) = g(\overline{4}) = \overline{12} = \overline{5} = f_5(\overline{1})$. Donc $g^5 = f_5$.
- $g^6(\overline{1}) = g(g^5(\overline{1})) = g(\overline{5}) = \overline{15} = \overline{1}$. Donc $g^6 = \text{Id}$. On en déduit que l'ordre de g est 6.

Regroupons :

$$\text{Aut}(\mathbb{Z}/7\mathbb{Z}) = \{f_1, f_2, f_3, f_4, f_5, f_6\} = \{\text{Id}, g, g^2, g^3, g^4, g^5\} = \langle g \rangle.$$

Le groupe $\text{Aut}(\mathbb{Z}/7\mathbb{Z})$ est donc cyclique d'ordre 6 engendré par $g = f_3$.
Comme $\varphi(6) = 2$ ce groupe cyclique a 2 générateurs qui sont $g(= f_3)$ et $g^5(= f_5)$ puisque 1 et 5 sont les seuls entiers $k < 6$ et $k \wedge 6 = 1$.

D'une façon générale, on a :

Lemme 2.4. *Soit G un groupe cyclique d'ordre n. Le groupe $Aut(G)$ est d'ordre $\varphi(n)$ et ses éléments sont les applications f_k avec k un entier $0 \leq k \leq n-1$ premier avec n.*

Proof. Soit $a \in G$ un générateur de G. D'après le Corollaire 2.2, les automorphismes de G sont déterminer par le choix d'un générateur a' de G. Or d'après la Proposition 1.5 les générateurs de G sont de la forme a^k avec $0 \leq k \leq n-1$ et $k \wedge n = 1$. On a donc $\varphi(n)$ automorphismes. Comme les applications f_k sont des automorphismes (car G étant cyclique est abélien) et qu'ils sont au nombre de $\varphi(n)$ on déduit qu'ils forment le groupe $Aut(G)$. Ils sont donc au nombre de $|\mathbb{Z}_n^\times| = \varphi(n)$. □

Remarque 2.5. En notation additive, les éléments de $Aut(G)$ sont les applications $f_k : G \to G$ telles que $f_k(x) = kx$.

3. Sous-groupes d'un groupe cyclique

Proposition 3.1. *Soient G un groupe cyclique d'ordre n et a un générateur de G. Tout sous-groupe de G est cyclique et pour tout diviseur d de n, il existe un unique sous-groupe H_d de G d'ordre d. En posant $\delta = n/d$, ce sous-groupe est caractérisé par*

$$\begin{aligned} H_d &= \mathbf{Ker}(f_d) = \{x \in G \ : \ x^d = e\} \\ &= \mathbf{Im}(f_\delta) = \{x \in G \ : \ \exists y \in G, \ y^\delta = x\} \\ &= \langle a^\delta \rangle \end{aligned}$$

Proof. Comme G est abélien, pour tout $k \in \mathbb{N}$, $f_k : x \mapsto x^k$ est un endomorphisme de G. Soit d un diviseur de n et posons $\delta = n/d$. Pour tout $x \in G$, on a $(x^d)^\delta = (x^\delta)^d = x^n = e$ et donc $\mathbf{Im}(f_d) \subset \mathbf{Ker}(f_\delta)$ et $\mathbf{Im}(f_\delta) \subset \mathbf{Ker}(f_d)$. Or $o(a^\delta) = d$ et $o(a^d) = \delta$, donc $\langle a^\delta \rangle$ est un sous-groupe d'ordre d et $\langle a^d \rangle$ est un sous-groupe d'ordre δ de G. On a $\mathbf{Im}(f_d) = \{(a^k)^d \ : \ 0 \leq k \leq n-1\} = \{(a^d)^k \ : \ 0 \leq k \leq n-1\} = \langle a^d \rangle$. De même $\mathbf{Im}(f_\delta) = \langle a^\delta \rangle$. Ainsi $|\,\mathbf{Im}(f_d)| = \delta$ et $|\,\mathbf{Im}(f_\delta)| = d$. Or d'après le théorème de l'isomorphisme, $|\,\mathbf{Im}(f_d)| = \frac{|G|}{|\,\mathbf{Ker}(f_d)|}$, donc $|\,\mathbf{Ker}(f_d)| = d$. De même $|\,\mathbf{Ker}(f_\delta)| = \delta$. Les inclusions précédentes sont donc des égalités puisque les cardinaux des deux membres sont égaux. Nous avons donc montré que $\langle a^\delta \rangle = \mathbf{Ker}(f_d) = \mathbf{Im}(f_\delta)$. Ce sous-groupe de G noté H_d est cyclique d'ordre d, et vérifie les relations demandées. Si H est un sous-groupe cyclique de G d'ordre d, alors $H = \langle b \rangle$ où $b \in H$ est un élément d'ordre d. Comme $b^d = e$, $b \in \mathbf{Ker}(f_d)$, et par suite $H = \mathbf{Ker}(f_d)$ car les deux groupes ont le même ordre. D'où l'unicité.

$\square$

Remarque 3.2. En notation additive,

$$\begin{aligned} H_d &= \mathbf{Ker}(f_d) = \{x \in G \;:\; dx = 0\} \\ &= \mathbf{Im}(f_\delta) = \{x \in G \;:\; \exists y \in G,\ \delta y = x\} \\ &= \langle \delta a \rangle \end{aligned}$$

Exemple 3.3. (a) Le groupe $\mathbb{Z}_{12}$ est cyclique d'ordre 12 engendré par $\bar{1}$. Les sous-groupes H_d sont en correspondances avec les diviseurs d de $12 = 2^2 \cdot 3$, qui sont $1, 2, 4 = 2^2, 3, 6 = 2 \cdot 3$ et $12 = 2^2 \cdot 3$:

- $H_1 = \{\bar{0}\}$, d'ordre 1.
- H_2 le sous-groupe d'ordre 2 est engendré par $\frac{12}{2}\bar{1} = \bar{6}$,
$$H_2 = \{\bar{0}, \bar{6}\}$$
- H_4 le sous-groupe d'ordre 4 est engendré par $\frac{12}{4}\bar{1} = \bar{3}$,
$$H_4 = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$$
- H_6 le sous-groupe d'ordre 6 est engendré par $\frac{12}{6}\bar{1} = \bar{2}$,
$$H_6 = \{\bar{0}, \bar{2}, \bar{4}, \bar{}, \bar{8}, \overline{10}\}$$
- H_{12} le sous-groupe d'ordre 12, c'est donc $\mathbb{Z}_{12}$.

(b) Le groupe $\mathbb{U}_{20}$ est cyclique d'ordre 20 engendré par $\xi = e^{2i\pi/20} = e^{i\pi/10}$. Ses sous-groupes H_d sont en correspondance avec les diviseurs de 20 qui sont $1, 2, 4 = 2^2, 5, 10 = 2 \cdot 5$ et $20 = 2^2 \cdot 5$:

- $H_1 = \{1\}$ est d'ordre 1.
- H_2 le sous-groupe d'ordre 2 est engendré par $\xi^{20/2} = \xi^{10} = e^{i\pi} = -1$,
$$H_2 = \{1, -1\}$$
- H_4 le sous-groupe d'ordre 4 est engendré par $\xi^{20/4} = \xi^5 = e^{i\pi/2}$,
$$H_4 = \{1, \xi^5, \xi^{10}, \xi^{15}\} = ...$$
- H_5 le sous-groupe d'ordre 5 est engendré par $\xi^{20/5} = \xi^4 = e^{2i\pi/5}$,
$$H_5 = \{1, \xi^4, \xi^8, \xi^{12}, \xi^{16}\}$$
- H_{10} le sous-groupe d'ordre 10 est engendré par $\xi^{20/10} = \xi^2 = e^{i\pi/5}$,
$$H_{10} = \{1, \xi^2, \xi^4, \xi^6, \xi^8, \xi^{10}, \xi^{12}, \xi^{14}, \xi^{16}, \xi^{18}\}$$
- H_{20} le sous-groupe d'ordre 20, c'est donc $\mathbb{U}_{20}$.

  On donne ici une autre manière, autre que celle de l'Exemple 1.6, pour trouver des éléments d'un groupe cyclique d'un ordre donné. Par exemple si un élément $a \in \mathbb{U}_{20}$ est d'ordre 4, il engendre un sous-groupe d'ordre 4 qui admet $\varphi(4) = 2$ générateurs. Ce sous-groupe est H_4. Il est engendré par $\omega = \xi^5$. L'autre générateur est de la forme ω^k avec $0 \leq k \leq 3$ et $k \wedge 4 = 1$ c,'est-à-dire $k = 3$. Ainsi les générateurs de H_4 sont ξ^5 et ξ^{15} et ce sont les seuls éléments de $\mathbb{U}_{20}$ d'ordre 4.

Proposition 3.4. *Le produit $G_1 \times G_2$ de deux groupes cycliques est cyclique si et seulement si G_1 et G_2 sont cycliques d'ordre m et n premiers entre eux. Dans ce cas, $(a, b) \in G_1 \times G_2$ est un générateur de $G_1 \times G_2$ si et seulement si a et b sont des générateurs de G_1 et G_2 respectivement.*

Proof. Supposons que $G_1 \times G_2$ est un groupe cyclique engendré par (a, b). Les projections canoniques $p_1 : G_1 \times G_2 \to G_1$ et $p_2 : G_1 \times G_2 \to G_2$ étant des morphismes surjectifs, d'après la Proposition 2.1, $G_1 = p_1(G_1 \times G_2)$ et $G_2 = p_2(G_1 \times G_2)$ sont cycliques, engendrés par $a = p_1(a, b)$ et $b = p_2(a, b)$ respectivement. De plus, $mn = |G_1|\,|G_2| = |G_1 \times G_2| = o(a, b) = \mathrm{ppcm}(m, n)$ d'après le corollaire 9.6 du chapitre 1.

Réciproquement, supposons que G_1 et G_2 sont cycliques d'ordre m et n premiers entre eux. Soient a et b des générateurs de G_1 et G_2 respectivement. D'après le corollaire 9.6 du chapitre 1, on a $o(a, b) = \mathrm{ppcm}(o(a), o(b)) = \mathrm{ppcm}(m, n) = mn = |G_1 \times G_2|$ Donc $G_1 \times G_2$ est cyclique puisqu'il est engendré par (a, b). □

Corollaire 3.5. *Soient $G_1, \ldots, G_k$ des groupes cycliques d'ordre respectivement $n_1, \ldots, n_k$. Alors le produit $G_1 \times \cdots \times G_k$ est un groupe cyclique si et seulement si $n_1, \ldots, n_k$ sont deux à deux premiers entre eux.*

Proof. Le raisonnement se fait par récurrence sur k. D'après la Proposition 3.4, le résultat est vrai pour $k = 2$. Supposons ce résultat vrai pour $k - 1$ groupes cycliques. Considérons k groupes cycliques $G_1, \ldots, G_k$ d'ordre $n_1, \ldots, n_k$.

Supposons $n_1, \ldots, n_k$ deux à deux premiers entre eux. D'après l'hypothèse de récurrence, $G' = G_1 \times \cdots \times G_{k-1}$ est cyclique. De plus, son ordre $n_1 \cdots n_{k-1}$ et premier avec l'ordre n_k de G_k. D'après la Proposition 3.4, $G_1 \times \cdots \times G_{k-1} \times G_k = G' \times G_k$ est cyclique.

Réciproquement, si $G_1 \times \cdots \times G_k$ est cyclique, alors $G' = G_1 \times \cdots \times G_{k-1}$ et G_k sont cycliques car la projection de G sur G' est un morphisme surjectiff. D'après l'hypothèse de récurrence, $n_1, \ldots, n_{k-1}$ sont premiers entre eux. Or d'après la proposition prod-gp-cycliques, n_k est premier avec $|G'| = n_1 \cdots n_{k-1}$ et donc avec $n_1, \ldots, n_{k-1}$.

□

4. Groupes d'ordre premier

Proposition 4.1. *Soit G un groupe non réduit à l'élément neutre. Alors G n'a pas d'autre sous-groupe que G et $\{e\}$, si et seulement si G est cyclique d'ordre premier.*

Proof. Soit G un groupe cyclique d'ordre premier p. Comme $p > 1$, alors $G \neq \{e\}$. D'après le théorème de Lagrange, l'ordre d'un sous-groupe de G ne peut être que 1 ou p, donc G n'a pas d'autre sous-groupe que $\{e\}$ et G.

Réciproquement, considérons un groupe $G \neq \{e\}$ dont les seuls sous-groupes sont G et $\{e\}$. Soit $x \neq e$ un élément de G. Donc $\langle x \rangle = G$ et G est monogène.

Si G était infini, G serait isomorphe à $\mathbb{Z}$ donc aurait d'autres sous-groupes que G et$\{e\}$. Par conséquent G est fini et donc cyclique. G n'ayant pas d'autres sous-groupes que G et $\{e\}$, l'ordre de G n'a pas, dans $\mathbb{N}^*$, d'autres diviseurs que lui même et 1, c'est donc un nombre premier. □

Lemme 4.2. *Soit G un groupe fini. Supposons qu'il existe un sous-groupe H du centre $Z(G)$ de G tel que G/H soit un groupe cyclique. Alors G est abélien.*

Proof. Tout sous-groupe du centre étant distingué, G/H est un groupe. Puisque G/H est cyclique, il existe $a \in G$, tel que $\bar{a}$ engendre G/H. Soient $x, y \in G$. Il existe $k, \ell \in \mathbb{N}$ tels que $\bar{x} = \bar{a}^k$ et $\bar{y} = \bar{a}^\ell$. Il existe alors $z, z' \in H \subset Z(H)$ tels que $x = a^k z$ et $y = a^\ell z'$. D'où $xy = (a^k z)(a^\ell z') = a^k a^\ell z z' = a^{k+\ell}(zz')$ puisque $z \in Z(G)$. On vérifie de même que $yx = a^{k+\ell}(zz')$. Ainsi $xy = yx$ et G est abélien. □

On reprend les théorèmes 3.6 3.7 et du chapitre 2.

Théorème 4.3. *Soient p un nombre premier et G un p-groupe, d'ordre p^α, avec $\alpha \in \mathbb{N}$. Alors le centre $Z(G)$ de G n'est pas réduit à $\{e\}$.*

Proof. On fait agir G sur lui même par automorphismes intérieurs. Alors $x \in G$ a une orbite réduite à un point, si et seulement si $gxg^{-1} = x$ pour tout $g \in G$, c'est-à-dire si $x \in Z(G)$. D'après le corollaire 3.3, chapitre 2, $|Z(G)| \equiv |G| \mod p$, donc $|Z(G)|$ est divisible par p. Comme le centre $Z(G)$ contient l'élément neutre, il possède au moins p éléments.

□

Théorème 4.4. *Tout groupe G d'ordre p^2, avec p premier, alors G est abélien.*

Proof. Nous allons donné ici une autre démonstration différente de celle du théorème 3.7, chapitre 2.

D'après le théorème de Lagrange, $|Z(G)|$ divise $|G| = p^2$. D'après le théorème précédent, $|Z(G)|$ est d'ordre p ou p^2. Supposons que $|Z(G)| = p$. Le groupe quotient $G/Z(G)$, d'ordre $[G : Z(G)] = p$, est cyclique d'après la Proposition 4.1. Le Lemme 4.2 montre que G est abélien et donc $Z(G) = G$ ce qui contredit le fait que $|G| = p^2$. Par conséquent $|Z(G)| = p^2$ et $Z(G) = G$, donc G est abélien. □

5. Décomposition cyclique des groupes abéliens finis

Lemme 5.1. *Soit G un groupe abélien fini et $a \in G$ un élément d'ordre $o(a)$ maximum. Tour tout $y \in G/\langle a\rangle$ il existe $x \in G$ tel que $\bar{x} = y$ et $o(x) = o(y)$.*

Proof. Soit φ le morphisme canonique

$$\varphi : G \to G/\langle a\rangle, \quad g \mapsto \bar{g}$$

et soit s l'ordre de y dans le groupe $G/\langle a\rangle$. Comme φ est surjectif, il existe $x \in G$ tel que $\varphi(x) = y$, c-à-d $\bar{x} = y$. Puisque φ est un morphisme, $\varphi(sx) = sy = 0$ et donc $sx \in \mathbf{Ker}(\varphi) = \langle a\rangle = \{0, a, 2a, \ldots, (o(a)-1)a\}$. Il existe donc un entier k tel que $0 \le k < o(a)$ et $sx = ka$. Par division euclidienne, il existe des entiers q, r tels que

$$k = sq + r \;\text{ et }\; 0 \le r < s, \tag{5.1}$$

d'où $sx = ka = sqa + ra$. Posons $x' = x - qa$. On a $\varphi(x') = \varphi(x) = y$ et par suite $s = o(y)|o(x')$.

Supposons $r \neq 0$. On a $sx' = sx - sqa = ra$. En utilisant la Proposition 1.5 on a $o(sx') = \frac{o(x')}{\mathrm{pgcd}(o(x'),s)}$ soit $o(sx') = \frac{o(x')}{s}$ puisque $s|o(x')$. On en déduit que

$$o(x') = so(sx') = so(ra) = s\frac{o(a)}{\mathrm{pgcd}(o(a),r)}.$$

Comme $o(a)$ est maximum, on a $o(x') \le o(a)$. En utilisant la relation précédente on a alors $s \le \mathrm{pgcd}(o(a), r) \le r$. Cela contredit (5.1), donc $r = 0$ et $sx' = ra = 0$. Par conséquent on a $o(x')|s$ et donc $o(x') = o(y)$. □

Théorème 5.2 (Décomposition cyclique)**.** *Soit G un groupe abélien fini d'ordre $n \geq 2$. Il existe une unique suite d'entiers $q_1, q_2, \ldots, q_k$ telle que*

$$1 < q_1 | q_2 | \cdots | q_k \ \text{ et } \ G \simeq \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}.$$

La suite (q_i) caractérise G à un isomorphisme près, on l'appelle **suite des invariants** *de G.*

Proof. Existence : nous allons raisonner par récurrence sur l'ordre n de G.
Si $n = 2$, alors G est cyclique d'ordre 2 et il est isomorphe à $\mathbb{Z}_2$. Soit G un groupe abélien fini d'ordre $n \geq 2$. Supposons vraie l'existence pour les groupes d'ordre strictement inférieur à n. Soit $a \in G$ tel que $m = o(x)$ est maximal. On a $m > 1$ car $G \neq \{0\}$, donc $G/\langle a \rangle$ est d'ordre strictement inférieur à $|G| = n$. D'après l'hypothèse de récurrence, il existe des sous-groupes cycliques $G'_1 = \langle a'_1 \rangle$, …,$G'_{k-1} = \langle a'_{k-1} \rangle$ d'ordres $q_1, \ldots, q_{k-1}$ vérifiants

$$1 < q_1 | q_2 | \cdots | q_{k-1} \ \text{ et } \ G/\langle a \rangle \simeq G'_1 \times \cdots G'_{k-1} \tag{5.2}$$

D'après le Lemme 5.1, il existe dans G des éléments $a_1, \ldots a_{k-1}$ tels que pour chaque i, $\bar{a}_i = a'_i$ et $o(a_i) = o(a'_i)$. Montrons que G est produit direct des sous-groupes $G_1 = \langle a_1 \rangle, \ldots, G_{k-1} = \langle a_{k-1} \rangle, G_k = \langle a \rangle$. Soit le morphisme canonique $\varphi : G \to G/\langle a \rangle$. Soit $x \in G$, il existe des entiers uniques $n_1, \ldots, n_{k-1}$ avec $0 \leq n_i < o(a_i)$ pour chaque i, tels que $\bar{x} = n_1 a'_1 + \ldots n_{k-1} a'_{k-1}$. Alors

$$\varphi(x) = n_1 a'_1 + \ldots n_{k-1} a'_{k-1} = \varphi(n_1 a_1 + \ldots n_{k-1} a_{k-1})$$

ce qui entraîne que $x - (n_1 a_1 + \ldots n_{k-1} a_{k-1}) \in \mathbf{Ker}(\varphi)$. Il existe donc un élément $n_k a \in \mathbf{Ker}(\varphi) = \langle a \rangle$ avec $0 \leq n_k < m = o(a)$ et tel que

$$x = n_1 a_1 + \ldots n_{k-1} a_{k-1} + n_k a \tag{5.3}$$

ce qui montre que $G = G_1 + \ldots + G_k$. Pour montrer que G est produit direct des sous-groupes $G_1, \ldots, G_k$, il suffit de montrer que la décomposition (5.3) est unique. Supposons que x admet une autre décomposition $x = m_1 a_1 + \ldots + m_{k-1} a_{k-1} + m_k a$. Alors $\bar{x} = \varphi(x) = n_1 a'_1 + \ldots n_{k-1} a'_{k-1} = m_1 a'_1 + \ldots m_{k-1} a'_{k-1}$ (car $\varphi(a) = 0$). Comme $G/\langle a \rangle$ est produit direct de $G'_1, \ldots, G'_{k-1}$, on a $n_1 = m_1, \ldots, n_{k-1} = m_{k-1}$. On en déduit que $n_k a = m_k a$ ou encore $(n_k - m_k) a = 0$ ce qui entraîne que $n_k = m_k$ puisque $0 \leq |n_k - m_k| < o(a)$. Ainsi $G = G_1 \times \cdots G_k$. il reste à montrer que $q_1 | q_2 | \cdots | q_k$.

D'après le corollaire 9.6 du chapitre 1, l'ordre de $x_0 = (a_1, \ldots, a_{k-1}, a) \in G_1 \times \cdots \times G_k$ est le ppcm de $o(a_1), \ldots, o(a_{k-1}), o(a)$. Donc $o(x_0) \geq o(a)$. Comme $o(a)$ est le maximum des ordres des éléments de G, on en déduit que $o(a) = o(x_0) = \text{ppcm}(o(a_1), \ldots, o(a_{k-1}), o(a))$ et donc $o(a_1) | \cdots | o(a_{k-1}) | o(a)$ en tenant compte de (5.2).

Unicité : Nous allons montrer l'unicité de la suite $q_1, \ldots, q_k$ par récurrence sur l'ordre n de G.

Si $n = 2$, la suite est unique, et elle est réduite à 2. Supposons l'unicité vraie pour les groupes d'ordre strictement inférieurs à n. Soit G un groupe d'ordre $n > 2$. Considérons deux décompositions

$$G = G_1 \times \cdots \times G_k = G'_1 \times \cdots \times G'_h$$

avec $G_i \simeq \mathbb{Z}_{q_i}$, $G_i \simeq \mathbb{Z}_{q'_i}$, $1 < q_1 | \cdots | q_k$ et $1 < q'_1 | \cdots | q'_h$.

Soit p un facteur premier de q_1 et donc de $q_2, \ldots, q_k$. Comme G est abélien, $f : x \mapsto px$ est un endomorphisme de G. Il laisee stable chacun des sous-groupes G_i, *i.e.* $f(G_i) \subset G_i$. D'après la proposition 3.1, $f(G_1) \subset G_1$ est l'unique sous-groupe de G_1 d'ordre $\frac{q_1}{p}$. De même $f(G_2) \subset G_2, \ldots, f(G_k)$ sont d'ordres $\frac{q_2}{p}, \ldots, \frac{q_k}{p}$.On a pour tout $i = 1, \ldots, k-1$,

$$[\sum_{j=1}^{i} f(G_k)] \cap f(G_{i+1}) \subset [\sum_{j=1}^{i} G_k] \cap G_{i+1} = \{0\}$$

car G est produit direct $G_1, \ldots, G_k$. Donc $f(G)$ est produit direct de $f(G_1), \ldots, f(G_k)$ et on a $|f(G)| = \frac{q_1 \cdots q_k}{p^k} = \frac{|G|}{p^k}$.

De même, on a $f(G'_j) \subset G'_j$ pour $j = 1, \ldots, m$ et $f(G) = f(G'_1) \times \cdots \times f(G'_m)$. Puisque $q'_1| \cdots |q'_m$, il existe r tel que p ne divise pas $q'_1, \ldots, q'_r$ et p divise $q'_{r+1}, \ldots, q'_m$. On a alors $f(G'_1) = G'_1$ car $f : x \mapsto px$ est un autmorphisme de G'_1. De même $f(G'_2) = G'_2, \ldots, f(G'_r) = G'_r$. Par contre, les ordres de $f(G'_{r+1}), \ldots, f(G'_m)$ sont $\frac{q'_{r+1}}{p}, \ldots, \frac{q'_m}{p}$, donc

$$|f(G)| = q'_1 \cdots q'_r \frac{q'_{r+1} \cdots q'_m}{p^{m-r}} = \frac{|G|}{p^{m-r}}$$

En comparant les deux valeurs de $|f(G)|$ obtenues, on voit que $k = m-r \leq m$. En échangeant les rôles on obtient de même $m \leq k$ et donc $m = k$. On en déduit que $r = 0$ et que p divise $q'_1, \ldots, q'_k$. D'après l'hypothèse de récurrence, la décomposition cyclique de $f(G)$ est unique. Les deux suites $\frac{q_1}{p}, \ldots, \frac{q_k}{p}$ et $\frac{q'_1}{p}, \ldots, \frac{q'_k}{p}$ sont donc égales et les suites $q_1, \ldots, q_k$ et $q'_1, \ldots, q'_k$ sont égales. □

Corollaire 5.3. *Soit G un groupe abélien d'ordre p^α avec p premier. Alors il existe une partition $(\beta_1, \ldots, \beta_k)$ de α avec $\beta_1 \leq \ldots \leq \beta_k$, $\beta_1 + \ldots + \beta_k = \alpha$ telle que*

$$G \simeq \mathbb{Z}_{p^{\beta_1}} \times \cdots \times \mathbb{Z}_{p^{\beta_k}}.$$

Corollaire 5.4. *Soit G un groupe abélien fini. Il existe un élément a de G dont l'ordre est le ppcm des ordres des éléments de G.*

Proof. Posons $n = |G|$. Si $n = 1$, le résultat est évident. Si $n \geq 2$, il existe dans G des sous-groupes cycliques $G_1, \ldots, G_k$ tels que $G = G_1 \times \cdots \times G_k$ d'ordres $q_1, \ldots, q_k$ tels que $q_1|q_2 \cdots |q_k$. Soit a un générateur de G_k. Pour tout $x = (x_1, \ldots, x_k) \in G_1 \times \cdots \times G_k = G$ on a $o(x) = \mathrm{ppcm}(o(x_1), \ldots, o(x_k))$, avec $o(x_1)|q_1 \cdots |q_k$, $o(x_2)|q_2| \cdots |q_k$, ect... Donc $o(x)$ divise $q_k = o(a)$ et $o(a)$ est le ppcm des ordres $o(x)$ des éléments $x \in G$. □

Théorème 5.5 (Décomposition primaire)**.** *Soit G un groupe abélien fini d'ordre $n \geq 2$. Soit $n = p_1^{k_1} \cdots p_r^{k_r}$ la décomposition en facteurs premiers de n.*

(a) Pour tout diviseur d de l'ordre n de G, il existe un sous-groupe de G d'ordre d.

(b) Pour chacun des diviseurs $p_i^{k_i}$ où $i = 1, \ldots, k$, il existe un seul sous-groupe G_{p_i} d'ordre $p_i^{k_i}$ et $G_{p_i} = \{x \in G, ; \exists \alpha \mid o(x) = p_i^\alpha\}$. De plus

$$G = G_{p_1} \times \cdots \times G_{p_r}. \tag{5.4}$$

Un sous-groupe G_{p_i} est appelé **composante** p_i**-primaire** *et la décomposition (5.4) est appelée* **décomposition primaire** *de G.*

Proof. (a) D'après le Théorème 5.2, G est produit direct $G_1 \times \cdots \times G_k$ de sous-groupes cycliques. On a $|G| = |G_1| \times \cdots \times |G_k|$. Si d divise $|G|$, en répartissant autant de fois que l'on peut chacun de ses facteurs premiers dans $|G_1|$, puis dans $|G_2|$, etc.. on peut écrire $d = d_1 \cdots d_k$ où d_i divise $|G_i|$ pour $i = 1, \ldots, k$. Pour chaque i il existe un sous-groupe K_i d'ordre d_i dans le groupe cyclique G_i. Alors $K_1 \times \cdots \times K_k \subset G_1 \times \cdots \times G_k = G$ est d'ordre d.

(b) D'après (a), il existe dans G des sous-groupes $G_{p_1}, \dots, G_{p_r}$ d'ordre $p_1^{k_1}, \dots, p_1^{k_r}$. Comme $\mathrm{pgcd}(p_1^{k_1}, p_2^{k_2}) = 1$, on a $G_{p_1} \cap G_{p_2} = \{0\}$. De plus $G_{p_1}G_{p_2}$ est un sous-groupe de G isomorphe $G_{p_1} \times G_{p_2}$ d'ordre $p_1^{k_1}p_2^{k_2}$. De même $(G_{p_1}G_{p_2})G_{p_3}$, est isomorphe $(G_{p_1} \times G_{p_2}) \times G_{p_3}$, d'ordre $p_1^{k_1}p_2^{k_2}p_3^{k_3}$. Par récurrence finie, on montre que $G_{p_1} \times \cdots \times G_{p_r}$ est un sous-groupe de G d'ordre $p_1^{k_1} \cdots p_r^{k_r} = n$ il est donc égal à G. Soit $x = (x_1, \dots, x_k) \in G_{p_1} \times \cdots \times G_{p_r}$, d'après le théorème de Lagrange, il existe $\alpha_1, \dots, \alpha_r$ tels que $o(x_1) = p_1^{\alpha_1}, \dots, o(x_r) = p_r^{\alpha_r}$. On a $o(x) = \mathrm{ppcm}(o(x_1), \dots, o(x_r)) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Si $o(x)$ est une puissance p_1^{α} de p_1, alors $\alpha_2 = \cdots = \alpha_r = 0$ et $x \in G_{p_1}$. Il résulte de cela deux choses. D'abord $G_{p_1} = \{x \in G \ ; \ \exists \alpha \ o(x) = p_1^{\alpha}\}$. Ensuite, si G'_{p_1} est un autre sous-groupe de G d'ordre $p_1^{k_1}$, l'ordre de tout élément de G'_{p_1} divisant $p_1^{k_1}$ on a $G'_{p_1} \subset G_{p_1}$ et donc $G'_{p_1} = G_{p_1}$. Il existe donc un seul sous-groupe d'ordre $p_1^{k_1}$ dans G. Il en va de même pour les autres facteurs premiers de n. $\square$

Exemple 5.6. (1) Le groupe $G = \mathbb{Z}_{12} \times \mathbb{Z}_{90}$ est abélien et d'ordre $12 \times 90 = 2^3 \cdot 3^3 \cdot 5$. D'où sa décomposition primaire $G = G_2 \times G_3 \times G_5$.

La composante primaire G_2 associé au facteur premier 2 est un sous-groupe d'ordre $2^3 = 8$, donné par

$$\begin{aligned} G_2 &= \{(\bar{k}, \tilde{h}) \in \mathbb{Z}_{12} \times \mathbb{Z}_{90} \mid o(\bar{k}, \tilde{h}) \text{ est un ordre de } 2\} \\ &= \{(\bar{k}, \tilde{h}) \in \mathbb{Z}_{12} \times \mathbb{Z}_{90} \mid 2^3(\bar{k}, \tilde{h}) = (\bar{0}, \tilde{0})\} \end{aligned}$$

Or,

$$\left\{ \begin{array}{ll} 2^3k & \equiv 0[12 = 2^2 \cdot 3] \\ 2^3h & \equiv 0[90 = 3^3 \cdot 2 \cdot 5] \end{array} \right. \iff \left\{ \begin{array}{ll} 2k & \equiv 0[3] \\ 2^2h & \equiv 0[45] \end{array} \right. \iff \left\{ \begin{array}{ll} k & \equiv 0[3] \\ h & \equiv 0[45] \end{array} \right.$$

Donc

$$G_2 = 3\mathbb{Z}/12\mathbb{Z} \times 45\mathbb{Z}/90\mathbb{Z} \simeq \mathbb{Z}_4 \times \mathbb{Z}_2.$$

On montre de même que la composante primaire G_3 associée au facteur premier 3 est

$$G_3 = 4\mathbb{Z}/12\mathbb{Z} \times 10\mathbb{Z}/90\mathbb{Z} \simeq \mathbb{Z}_3 \times \mathbb{Z}_9.$$

Enfin, la composante primaire G_5 est

$$G_5 = 12\mathbb{Z}/18\mathbb{Z} \times 18\mathbb{Z}/90\mathbb{Z} \simeq \{\bar{0}\} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/5\mathbb{Z}$$

On peut prévoir ce résultat, car G_5 est un groupe cyclique d'ordre premier 5, donc isomorphe à $\mathbb{Z}_5$. Ainsi

$$\mathbb{Z}_{12} \times \mathbb{Z}_{90} \simeq (\mathbb{Z}_4 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_9) \times \mathbb{Z}_5$$

Or un produit de deux groupes cycliques d'ordres premiers entre eux est un groupe cyclique. On va donc regrouper les différents groupes cyclique pour former une décomposition cyclique :

$$\begin{aligned} G &\simeq (\mathbb{Z}_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5) \\ &\simeq \mathbb{Z}_6 \times \mathbb{Z}_{180} \end{aligned}$$

Ainsi $\mathbb{Z}_6 \times \mathbb{Z}_{180}$ est la décomposition cyclique de $\mathbb{Z}_{12} \times \mathbb{Z}_{90}$ et $(6, 180)$ est sa suite des invariants.

(2) Déterminons tous les groupes abéliens d'ordre 3240.

Si G est un groupe abélien d'ordre $3240 = 2^3 \cdot 3^4 \cdot 5$, alors sa décomposition primaire est $G = G_2 \times G_3 \times G_5$.

$|G_2| = 2^3$ et 3 admet trois partitions qui sont (3), $(1, 2)$ et $(1, 1, 1)$. Donc G_2 est isomorphe à l'un des groupes

$$\begin{array}{l} \mathbb{Z}_{2^3} \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^2} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \end{array}$$

$|G_3| = 3^4$ et 4 admet cinq partitions qui sont (4), $(1,3)$, $(2,2)$, $(1,1,2)$ et $(1,1,1,1)$. Donc G_3 est isomorphe à l'un des groupes

$$\begin{array}{l}
\mathbb{Z}_{3^4} \\
\mathbb{Z}_3 \times \mathbb{Z}_{3^3} \\
\mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2} \\
\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{3^2} \\
\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3
\end{array}$$

Enfin G_5 est un groupe d'ordre 5 (donc cyclique), il est isomorphe à

$$\mathbb{Z}_5.$$

Il y a donc au total à isomorphisme près $3 \times 5 \times 1 = 15$ groupes abéliens d'ordre 3240 :

$$\begin{array}{rl}
\mathbb{Z}_{2^3} \times \mathbb{Z}_{3^4} \times \mathbb{Z}_5 & \simeq \mathbb{Z}_{3240} \\
\mathbb{Z}_{2^3} \times (\mathbb{Z}_3 \times \mathbb{Z}_{3^3}) \times \mathbb{Z}_5 & \simeq \mathbb{Z}_3 \times (\mathbb{Z}_{2^3} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_5) \\
 & \simeq \mathbb{Z}_3 \times \mathbb{Z}_{1080} \\
\mathbb{Z}_{2^3} \times (\mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2}) \times \mathbb{Z}_5 & \simeq \mathbb{Z}_{3^2} \times (\mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5) \\
 & \simeq \mathbb{Z}_9 \times \mathbb{Z}_{360} \\
\mathbb{Z}_{2^3} \times (\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{3^2}) \times \mathbb{Z}_5 & \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \\
 & \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{360} \\
\mathbb{Z}_{2^3} \times (\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_5 & \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times (\mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_5) \\
 & \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{120} \\
\textit{etc...} \text{ (à compléter par l'étudiant).} &
\end{array}$$

D'où les listes des invariants possible pour G :

$$(2340), (3, 1080), (9, 360), (3, 3, 360), (3, 3, 3, 120), \textit{etc...} \text{ (à compléter par l'étudiant).}$$