كلية العلوم و التقنيات فاس
ⵜⴰⵖⵡⵍⵍⴰⵜ ⵏ ⵜⵓⵙⵙⵏⵉ ⴷ ⵜⵓⵣⵔⴼⵜ
Faculté des Sciences et Techniques de Fès

جامعة سيدي محمد بن عبد الله
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵙⵉⴷⵉ ⵎⵓⵃⴰⵎⴻⴷ ⴱⵏ ⵄⴱⴷⵍⵍⴰⵀ
Université Sidi Mohamed Ben Abdellah

Licence Sciences et Techniques (LST)

MATHEMATIQUES ET APPLICATIONS

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du Diplôme de Licence Sciences et Techniques

Groupes commutatifs finis

Présenté par :

- **Fatima zahrae Hakimi.**

Encadrés par :

- **Encadrant : Najib Mahdou.**
- **Co-Encadrant: Abdelhaq ElKhalfi.**

Soutenu le 08 juillet 2021 devant le jury composé de :

- **Najib Mahdou.**
- **Abdelhaq ElKhalfi.**
- **Abdelmajid Hilali.**
- **Lahcen Oukhtite.**

Stage effectué à la Faculté des Sciences et Technique de Fès

Année Universitaire 2020/2021

FACULTE DES SCIENCES ET TECHNIQUES FES – SAISS
B.P. 2202 – Route d'Imouzzer – FES
212 (0)5 35 61 16 86 – Fax : 212 (0)5 35 60 82 14
Site web : http://www.fst-usmba.ac.ma

Dédicace

A mes chers parents,
Je dédis tous mes moments de labeur à mes très chers parents qui n'ont guère cessé de me soutenir et de m'apporter toute l'assurance et l'épaulement, que Dieu les protèges et les honores.
A mon adorable frère Ibrahim,
A ma chère sœur Hajar,
Votre affection et vos encouragements ont toujours été pour moi des plus précieux, que ce travail soit pour vous le gage de mon profond amour.
A toute ma famille, mes amis (es) et A ceux qui se dévouent sans cesse pour nous éclaircir la voie et les immenses horizons du savoir et dont leurs efforts méritent largement notre respect.
Je prie Dieu de vous procurer santé, bonheur et longue vie afin que vous puissiez exhausser tous vos rêves.

Remerciements

Au terme de ce travail, je tiens à remercier Dieu avant tout, Je tiens à remercier tous ceux qui ont participé à la réalisation de ce projet de fin d'étude et qui n'a été possible que grâce au soutien de nombreuses personnes, que chacune trouve dans les premières phrases de ce mémoire l'expression de ma profonde et sincère reconnaissance. Je tiens tout d'abord à exprimer mes remerciements au Mr.Najib Mahdou professeur à la Faculté de Sciences et techniques, qui a bien accepté de me faire bénéficier de son savoir, son expérience et de ses compétences, et aussi spécialement pour sa rigueur scientifique manifesté toute au long de la réalisation de ce travail. Mes remerciements sont adressés aussi à tous ceux qui ont participé de près ou de loin et dont leurs noms ne figurent pas sur cette liste.

Table des matières

Introduction :

La structure de groupe est commune à de nombreux ensembles de nombres par exemple les nombres entiers relatifs, munis de la loi d'addition. Mais cette structure se retrouve aussi dans de nombreux autres domaines, notamment en algèbre, ce qui en fait une notion centrale des mathématiques modernes.

La structure de groupe possède un lien étroit avec la notion de symétrie. Un groupe de symétrie décrit les symétries d'une forme géométrique : il consiste en un ensemble de transformations géométriques qui laissent l'objet invariant, l'opération consistant à composer de telles transformations, c'est-à-dire à les appliquer l'une après l'autre. De tels groupes de symétrie, en particulier les groupes de Lie continus, jouent un rôle important dans de nombreuses sciences. Ces derniers, par exemple, sont les groupes de symétries utilisés dans le modèle standard de la physique des particules. Les groupes généraux linéaires sont, quant à eux, utilisés en physique fondamentale, afin de comprendre les lois de la relativité restreinte et les phénomènes liés à la symétrie des molécules en chimie.

Le concept de groupe fit son apparition dans l'étude des équations polynomiales. En effet, c'est Évariste Galois qui, durant les années 1830, utilisa pour la première fois le terme « groupe » dans un sens technique similaire à ce qui est utilisé de nos jours, faisant de lui un des fondateurs de la théorie des groupes. Suite à des contributions d'autres domaines des mathématiques, comme la théorie des nombres et la géométrie, la notion de groupe fut généralisée et plus fermement établie autour des années 1870.

La théorie des groupes moderne, une branche des mathématiques toujours active, se concentre donc sur la structure de groupes abstraits, indépendamment de leur utilisation extra-mathématique. Ce faisant, les mathématiciens ont défini, au fil des années, plusieurs notions permettant de fragmenter des groupes en des objets plus petits et plus compréhensibles ; les sous-groupes, groupes quotients, sous-groupes normaux et les groupes simples en sont quelques exemples. En plus d'étudier ces types de structures, les théoriciens de groupes s'intéressent aussi aux différentes façons dont un groupe peut être exprimé concrètement, autant du point du vue de la théorie des représentations que du point de vue computationnel. La théorie des groupes finis fut développée avec, comme point culminant, la classification des groupes finis simples, la théorie géométrique des groupes, qui s'intéresse aux groupes de type fini en tant qu'objectes géométriques, est devenue un champ particulièrement actif de la théorie des groupes.

Le but du premier chapitre est de pouvoir écrire la structure des groupes commutatifs finis, et pour avoir une aidée plus claire on a traiter dans le deuxième chapitre d'exercices d'application.

Chapitre 1

Groupes commutatifs finis

Dans ce chapitre, tous les groupes sont considérés commutatifs et finis.

1.1 Somme directe de groupes commutatifs

Définition 1.1.1
Soit G un groupe commutatif et H *un sous-groupe de G. On dit que H est un facteur direct de* G*, s'il existe un sous-groupe K de G tel que* $\mathbf{G = H \oplus K}$.

On a la caractérisation suivante :

Proposition 1.1.2
Étant donné un groupe G et un sous-groupe H*, notons q l'injection canonique de* H *dans* G*. Alors* H *est un facteur direct de* G*, si et seulement s'il existe* $p \in \mathrm{Hom(G, H)}$ *tel que* $p \circ q = \mathrm{id_H}$.

Preuve:
Si $\mathrm{G = H \oplus K}$, alors l'injection canonique $q : \mathrm{H} \to \mathrm{G}$ et la projection canonique $p : \mathrm{G} \to \mathrm{H}$ vérifient la condition $p \circ q = \mathrm{id_H}$.

Réciproquement, supposons qu'il existe $p \in \mathrm{Hom}(G, H)$ tel que $p \circ q = \mathrm{id_H}$ on remarque que p est surjectif, où $p\,(x_H + x_k) = x_H$ (avec $x_H \in \mathrm{H}$ *et* $x_K \in \mathrm{K}$).

Soit $g \in G$ et posons $p(g) = h$. On a :

$$\begin{aligned} p(g) &= h \\ &= p \circ q(h) \\ &= p(h) \end{aligned}$$

de sorte que $(g-h) \in \operatorname{Ker} p$. D'où $\mathrm{G} = \mathrm{H} + \operatorname{Ker} p$.
Montrons que cette somme est directe, et soit $x \in \mathrm{H} \cap \operatorname{Ker} p$. Puisque $x \in \mathrm{H}$, alors on a :

$$\begin{aligned} x &= p \circ q(x) \\ &= p(x) \\ &= 0 \end{aligned}$$

car $x \in \operatorname{Ker} p$. D'où $\mathrm{H} \cap \operatorname{Ker} p = 0$, de sorte qu'on a :

$$\mathrm{G} = \mathrm{H} \oplus \operatorname{Ker} p.$$

■

1.2 p-groupe

Définition 1.2.1
Soit $p > 0$ un entier premier. On dit que G est un p-groupe si tous les éléments de G ont pour ordre une puissance de p.

Exemple 1.2.2
1) $\mathbb{Z}/4\mathbb{Z}$ est un 2-groupe d'ordre 4.
2) $\mathbb{Z}/6\mathbb{Z}$ n'est pas p-groupe car il y a des éléments d'ordre 2, 3 ou 6.
3) $\mathbb{Z}/8\mathbb{Z}$ est un 2-groupe d'ordre 8.
4) Le groupe de Klein $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ est un 2-groupe d'ordre 4.
5) $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/27\mathbb{Z})$ est un 3-groupe d'ordre 81.

1.2.1 p-composante d'un groupe

Définition et Proposition 1.2.3
Soit $p > 0$ un entier premier divisant l'ordre d'un groupe G. L'ensemble G_p des éléments de G dont l'ordre est une puissance de p est un sous-groupe de G appelé p-composante de G.

Preuve: Laisser au lecteur.

Exemple 1.2.4
Soit $G = \mathbb{Z}/120\mathbb{Z}$ et $p = 2$. On a $120 = 2^3.3.5$ de sorte que la 2-composante de G

est :

$$\begin{aligned} G_2 &\simeq 15\mathbb{Z}/120\mathbb{Z} \\ &\simeq 15\mathbb{Z}/15\cdot 8\mathbb{Z} \\ &\simeq \mathbb{Z}/8\mathbb{Z}. \end{aligned}$$

Exemple 1.2.5
Soit $G = (\mathbb{Z}/150\mathbb{Z}) \times (\mathbb{Z}/160\mathbb{Z}) \times (\mathbb{Z}/120\mathbb{Z})$.
1)*Donner la 2-composante* G_2 *de* G.
2)*Donner la 3-composante* G_3 *de* G.
3)*Donner la 5-composante* G_5 *de* G.

Solution :
1)*Cherchons d'abord la 2-composante* G_2 *de* G. *On a* $150 = 2.3.5^2$, *donc la 2-composante de* $(\mathbb{Z}/150\mathbb{Z})$ *est* $75\mathbb{Z}/150\mathbb{Z}$. *Elle est isomorphe à* $\mathbb{Z}/2\mathbb{Z}$.

D'autre part, $160 = 2^5.5$ *donc la 2-composante de* $(\mathbb{Z}/160\mathbb{Z})$ *est* $5\mathbb{Z}/160\mathbb{Z}$. *Elle est isomorphe à* $\mathbb{Z}/32\mathbb{Z}$.

On a aussi $120 = 2^3.3.5$ *et la 2-composante de* $(\mathbb{Z}/120\mathbb{Z})$ *est* $15\mathbb{Z}/120\mathbb{Z}$. *Elle est isomorphe à* $\mathbb{Z}/8\mathbb{Z}$.

Finalement, la 2-composante G_2 *de* G *est isomorphe à :*

$$(75\mathbb{Z}/150\mathbb{Z}) \times (5\mathbb{Z}/160\mathbb{Z}) \times (15\mathbb{Z}/120\mathbb{Z})$$

et elle est isomorphe à :

$$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/32\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z}).$$

2) *Cherchons maintenant la 3-composante* G_3 *de* G. *On a* $150 = 2.3.5^2$ *et donc la 3-composante de* $(\mathbb{Z}/150\mathbb{Z})$ *est* $50\mathbb{Z}/150\mathbb{Z}$. *Elle est isomorphe à* $\mathbb{Z}/3\mathbb{Z}$.

On a aussi $160 = 2^5.5$ *et donc la 3-composante de* $(\mathbb{Z}/160\mathbb{Z})$ *est* $160\mathbb{Z}/160\mathbb{Z} \simeq 0$.

Finalement, on a $120 = 2^3.3.5$ *et donc la 3-composante de* $\mathbb{Z}/120\mathbb{Z}$ *est* $40\mathbb{Z}/120\mathbb{Z}$. *Elle est isomorphe à* $\mathbb{Z}/3\mathbb{Z}$.

Ainsi, la 3-composante G_3 *de* G *est isomorphe à :*

$$(50\mathbb{Z}/150\mathbb{Z}) \times (160\mathbb{Z}/160\mathbb{Z}) \times (40\mathbb{Z}/120\mathbb{Z})$$

et elle est isomorphe à :

$$(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}).$$

3) *Cherchons d'abord la 5-composante G_5 de G. On a $150 = 2.3.5^2$ et donc la 5-composante de $(\mathbb{Z}/150\mathbb{Z})$ est $6\mathbb{Z}/150\mathbb{Z}$. Elle est isomorphe à $\mathbb{Z}/25\mathbb{Z}$.*

On a $160 = 2^5.5$, donc la 5-composante de $(\mathbb{Z}/160\mathbb{Z})$ est $32\mathbb{Z}/160\mathbb{Z}$. Elle est isomorphe à $\mathbb{Z}/5\mathbb{Z}$.
On a aussi $120 = 2^3.3.5$, donc la 5-composante de $(\mathbb{Z}/120\mathbb{Z})$ est $24\mathbb{Z}/120\mathbb{Z}$. Elle est isomorphe à $\mathbb{Z}/5\mathbb{Z}$.

Finalement, la 5-composante G_5 de G est isomorphe à :

$$(6\mathbb{Z}/150\mathbb{Z}) \times (32\mathbb{Z}/160\mathbb{Z}) \times (24\mathbb{Z}/120\mathbb{Z})$$

et elle est isomorphe à :

$$(\mathbb{Z}/25\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}).$$

1.3 Décomposition d'un groupe en p-groupes non nécessairement cycliques

Nous allons donner maintenant un premier théorème de décomposition d'un groupe commutatif fini G.

Définition 1.3.1 (Somme directe d'une famille de sous-groupes)
Soit G un groupe commutatif, $(H_i)_{i\in I}$ une famille quelconque de sous-groupes de G. On dit que G est somme directe des H_i et on note $G = \oplus H_i$ si $G = \sum_{i\in I} H_i$ et si $\forall j \in I, H_j \bigcap \left(\sum_{i\in I, i\neq j} H_i\right) = (0)$ Dans ce cas on peut écrire : $\oplus H_i$ $i \in I$

Théorème 1

Tout groupe commutatif fini G est somme directe de p-groupes, où p parcourt l'ensemble des diviseurs premiers de l'ordre de G noté D :

$$G = \oplus_{p\in D} G_p.$$

Pour la preuve du théorème, on a besoin du lemme suivant :

Lemme 1.3.2
Soient $H_1, H_2, \ldots, H_n$ des sous-groupes d'un groupe G. Le groupe G est la somme directe des H_i, si et seulement si :

a) $G = \sum_{i=1}^{n} H_i$,
b) $H_j \cap \left(\sum_{i \neq j} H_i\right) = 0$, *pour tout* $j = 1, 2, \ldots, n$.

Preuve:

Supposons que G est la somme directe des H_i. Puisque tout $x \in G$ peut s'écrire $x = h_1 + h_2 + \ldots + h_n$, avec $h_i \in H_i$, on a $G = \sum_{i=1}^{n} H_i$. Si $x \in H_j \cap \left(\sum_{i \neq j} H_i\right)$, on a $x = \sum_{i \neq j} h_i$, avec $h_i \in H_i$, donc $0 = \left(\sum_{i \neq j} h_i\right) - x$. L'écriture étant unique par hypothèse, et $-x \in H_j$, on obtient $h_i = 0$ pour tout $i \neq j$, et donc $x = 0$.

Inversement supposons a) et b)du lemme et vrai. Puisque $G = \sum_{i=1}^{n} H_i$, si $x \in G, x$ peut s'écrire $x = \sum_{i=1}^{n} h_i$ avec $h_i \in H$. Cette écriture est unique car si $k_i \in H_i$ et si $\sum_{x=1}^{n} h_i = \sum_{i=1}^{n} k_i$, on a :

$$h_j - k_j = \sum_{i \neq j} (k_i - h_i) \in H_j \cap \left(\sum_{j \neq i} H_i\right) = \{0\}$$

Ainsi, pour tout $j = 1, \ldots, n, h_j = k_j$.
■

Preuve du théorème :
Montrons que les H_i vérifient les conditions (a) et (b) de lemme précédent.

- Condition (a) :

Soient $x \neq 0$ un élément de G, n l'ordre de G et $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ la décomposition de |G| en facteurs premiers (puissances de nombres premiers) distincts. On définit n_i par $n = n_i p_i^{\alpha_i}$. Les n_i étant par définition premiers dans leur ensemble, i1 existe, d'après le théorème de Bézout, des entiers $m_1, m_2, \ldots, m_k$ tels que $1 = \sum_{i=1}^{k} m_i n_i$, de sorte qu'on a : $x = \sum_{i=1}^{k} m_i n_i x$.
Puisque $n = |G|$ est un multiple de est l'ordre de x, on a :

$$\begin{aligned} p_i^{\alpha_i} (m_i n_i x) &= m_i (nx) \\ &= 0 \end{aligned}$$

ce qui montre que $m_i n_i x \in G_{p_i}$ pour tout $i = 1, \ldots, k$,et que finalement $x \in \sum_{i=1}^{k} G_{p_i}$. D'où $\sum_{i=1}^{k} G_{p_i}$

- Condition (b)

Soient $p \in D$, avec D l'ensemble des diviseurs premiers de l'ordre de G :, et $x \in G_p \cap \sum_{\substack{q\in D \\ q\neq p}} G_q$. Par définition de chacun des termes de cette intersection, il existe $\alpha \in \mathbb{N}, p^\alpha x = 0$ et $x = \sum_{\substack{q\in D \\ q\neq p}} x_q$, avec $x_q \in G_q$. Mais $x_q \in G_q$ implique l'existence d'un $\alpha_q \in \mathbb{N}$ tel que $q^{\alpha q} x_q = 0$. Posons :

$$s = \sum_{\substack{q\in D \\ q\neq p}} q^{\alpha_q}.$$

On a évidemment $sx = 0$. Par construction, s et p^α sont premiers entre eux et il existe,d'après l'identité de Bézout, $\gamma, \delta \in \mathbb{Z}$ tels que :

$$s\gamma + p^\alpha \delta = 1.$$

Donc, on a :

$$\begin{aligned} x &= s\gamma x + p^\alpha \delta x \\ &= 0 \end{aligned}$$

Ce théorème est un théorème d'existence des décompositions premiers en ce sens que si G est un groupe fini d'ordre $n = p_1^{\alpha_1} p_2^{a_2} \dots p_k^\alpha k$, il permet d'affirmer que :

$$G = G_{p_1} \oplus G_{p_2} \oplus \dots \oplus G_{p_k}.$$

■

Dans le cas particulier d'un groupe cyclique fini qui est naturellement commutatif, on obtient :

Corollaire 1.3.3
Tout groupe cyclique G d'ordre $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots . {p_k}^{\alpha_k}$ (isomorphe à $\mathbb{Z}/n\mathbb{Z}$) est somme directe des groupes p_i-composante de G : $G_{p_i} \simeq \mathbb{Z}/{p_i}^{\alpha_i}\mathbb{Z}$.

Preuve:
D'après le théorème précèdent, et comme le sous-groupe d'un groupe cyclique est cyclique il reste à montrer que $|G_{p_i}| = {p_i}^{\alpha_i}$. D'après ce qui précède, il existe un sous-groupe H de G tel que $|H| = {p_i}^{\alpha_i}$. Les ordres des éléments de H divisent ${p_i}^{\alpha_i}$ et donc des puissances de p_i, d'où $H \subseteq G_{p_i}$.
Inversement, soit $x \in G_{p_i}$. Par définition de G_{p_i}, x est d'ordre ${p_i}^{\beta_i}$. Puisque le sous groupe engendré par x est un sous-groupe de G et d'après le théorème de Lagrange, son ordre ${p_i}^{\beta_i}$ divise $n = |G|$, ce qui montre que $\beta_i \leq \alpha_i$. Puisque $|H| = {p_i}^{\alpha_i}, H$ contient un unique sous-groupe L d'ordre ${p_i}^{\beta_i}$, de sorte que le sous groupe engendré

par x est L. Dés hors on a $x \in L \subseteq H$ et par suite $G_{p_i} \subseteq H$. Finalement $G_{p_i} = H$ et donc on a :

$$\begin{aligned} |G_{p_i}| &= |H| \\ &= {p_i}^{\alpha_i} \end{aligned}$$

Le sous-groupe cyclique G_{p_i}, d'ordre ${p_i}^{\alpha_i}$, est isomorphe a $\mathbb{Z}/{p_i}^{\alpha_i}\mathbb{Z}$.

■

Exemple 1.3.4
Comme on a $24 = 2^3.3$, *alors on a d'après le corollaire précédent :*

$$\mathbb{Z}/24\mathbb{Z} \simeq \mathbb{Z}/8\mathbb{Z} \bigoplus \mathbb{Z}/3\mathbb{Z}$$

Si on considère $\mathbb{Z}/27\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, on constate que ces 3 -groupes vérifient respectivement $3(\mathbb{Z}/24\mathbb{Z}) \neq 0$ *et* $3(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) = \{0\}$, cela nous amène à considérer les p-groupes G tels que :
$\mathrm{pG} = \{\mathrm{px}, \mathrm{x} \in \mathrm{G}\} = \{0\}$, c'est-à-dire dont tous les éléments non nuls sont d'ordre p puisque p est premier.

1.4 Les p-groupes élémentaires

Définition 1.4.1
Soit G un groupe commutatif fini et $p > 0$ un entier premier. Supposons que $pG = \{px; x \in G\} = \{0\}$. On dit que G est un p-groupe élémentaire.

Proposition 1.4.2
Dans un groupe G, si $p > 0$ est un entier premier, $G_p = \{x \in G; px = 0\}$ est un p-groupe élémentaire de G. Si $px = 0$, comme p est premier, x est nul ou x est d'ordre p.

Exemple 1.4.3
Cette proposition permet de déterminer d'explicitement G_p :
S par exemple, $G = \mathbb{Z}/30\mathbb{Z}$, on a $G_2 = \{0, 15\}; G_5 = \{0, 6, 12, 18, 24\}$ si $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, on a $G_2 = G$

Cas particulier *dans $\mathbb{Z}/n\mathbb{Z}$, si $p > 0$ est un diviseur premier de n, un élément d'ordre p engendre un sous-groupe cyclique dont tous les éléments non nuls sont d'ordre p. Comme dans $\mathbb{Z}/n\mathbb{Z}$ il existe un unique sous-groupe d'ordre p (celui engendre par $\frac{n}{p}$), nous voyons que*
1) Si p divise n : $(\mathbb{Z}/n\mathbb{Z})_p = \frac{n}{p}\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z}$.
2) Si p ne divise pas n : $(\mathbb{Z}/n\mathbb{Z})[p] = \{0\}$.

1.5 Décomposition d'un p-groupe élémentaire

Définition 1.5.1
Soit $p > 0$ un entier premier, considérons le corps $\mathbb{Z}/p\mathbb{Z}$ et un p-groupe élémentaire G.
Soient d'une part $h, k \in \mathbb{Z}$ tels que $h \equiv k \bmod p$ c'est-a-dire il existe $\alpha \in \mathbb{Z}$ tel que $h - k = \alpha p \in p\mathbb{Z}$; soit d'autre part $x \in G$. Puisque $(h-k)x = \alpha p x = 0$, on a $hx = kx$. Le calcul précédent permet de définir une $(\mathbb{Z}/p\mathbb{Z})$-loi externe sur G, c'est-à-dire une application de $(\mathbb{Z}/p\mathbb{Z}) \times G$ dans G en posant, pour tout $\bar{k} \in \mathbb{Z}/p\mathbb{Z}$ et tout $x \in G$

$$\bar{k} \cdot x = kx$$

Théorème 2

Un p-groupe élémentaire G, de cardinal n, est somme directe de n groupes cycliques isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Preuve:
Soit

$$\{x_1, x_2, \ldots, x_n\}$$

une base du $(\mathbb{Z}/p\mathbb{Z})$-espace vectoriel G et soit $G_i =< x_i >$. Par définition de la loi externe sur G et pour tout $x \in G$, on a :

$$\begin{aligned} x &= \sum_{i=1}^{n} \bar{k}_i x_i \\ &= \sum_{i=1}^{n} k_i x_i. \end{aligned}$$

Avec $\sum_{i=1}^{n} k_i x_i \in \sum_{i=1}^{n} G_i$. Montrons qu'il s'agit d'une somme directe.
Soit $x \in G_j \cap \sum_{i \neq j}^{n} G_i$. Cet x peut s'écrire

$$\begin{aligned} x &= k_j x_j \\ &= \sum_{i \neq j}^{n} k_i x_i, \end{aligned}$$

avec $k_i \in \mathbb{Z}$. Comme $\{x_1, x_2, \ldots, x_n\}$ est une base du $(\mathbb{Z}/p\mathbb{Z})$-espace vectoriel G, $\sum_{i \neq j} \bar{k}_i x_i - k_j \cdot x_j = \sum_{i \neq j} k_i x_i - k_j x_j$. Alors pour tout $i = 1, \ldots\ldots n$, on a $\overline{k_i} = \overline{0}$, ou encore $k_i = \alpha_i p$, ce qui montre que $G = \oplus_{i=0}^{n} G_i$, avec $n = d(G)$. Reste à prouver que pour $i = 1, \ldots, n$

$G_i = \mathbb{Z}/p\mathbb{Z}$. Mais $G_i =< x_i >$ est cyclique et comme G est un p-groupe élémentaire, x_i est d'ordre p.

1.6 Décomposition d'un groupe commutatif fini

Nous allons donner maintenant le théorème de décomposition des groupes commutatifs finis en somme directe de p-groupes cycliques.

Théorème 3

Tout groupe commutatif fini d'ordre n est somme directe de k p-groupes cycliques Γ_i, avec $\mathrm{n} = \prod_{i=1}^{k} |\Gamma_i|$.

Ce théorème repose sur le lemme suivant :

Lemme 1.6.1
Soit G un p-groupe et $\mathrm{y}_1, \mathrm{y}_2, \ldots, \mathrm{y}_\mathrm{n}$ des éléments de G tels que $\sum_{i=1}^{n} < y_i >= \bigoplus_{i=1}^{n} . < y_i >$. Soient $z_1, \ldots, z_n$ des éléments de G tels que, pour tout $i = 1, \ldots, n, pz_i = y_i$, alors $\sum_{i=1}^{n} < z_i >= \bigoplus_{i=1}^{n} < z_i >$.

Preuve:
Un élément $x \in < z_j > \cap \sum_{i \neq j} < z_i >$ peut s'écrire comme suit :

$$\begin{aligned} x &= m_j z_j \\ &= \sum_{i \neq j} m_i z_i. \end{aligned}$$

Par suite,

$$\begin{aligned} px &= m_j y_j \\ &= \sum_{i \neq j} m_i y_i \end{aligned}$$

Comme $\sum_{i=1}^{n} < y_j >= \bigoplus_{i=1}^{n} < y_j >, px = 0$, donc $m_i y_j = 0$, pour $i = 1, \ldots,$ n. Si $p^{\alpha_i} (\alpha_i \geq 1)$ est l'ordre de y_i, m_i est un multiple de p^{α_i} et s'écrit $\gamma_i \, p^{\alpha_i}$,où $\gamma_i \in \mathbb{Z}$. Il s'ensuit

$$\begin{aligned} x &= \gamma_j p^{\alpha_j} z_j \\ &= \sum_{i \neq j} \gamma_i p^{\alpha_i} z_i \end{aligned}$$

et

$$\begin{aligned} x &= \left(\gamma_j p_j^{-1}\right) y_j \\ &= \sum_{i\neq j} \left(r_j p^{\alpha_i - 1}\right) y_i \in < y_j > \cap \sum_{i\neq 1} < y_j > \end{aligned}$$

par conséquent, x=0.

■

Preuve du théorème 3 :

$G = \oplus_{\mathrm{p}} G_{\mathrm{p}}$, où les $\mathrm{G_p}$ sont les p-composantes de G. Puisque G est fini, il en est de même de G_p, et il existe $m \geqslant 1$ tel que

$$p^m G_p = 0.$$

Nous allons montrer, par récurrence sur $m \geqslant 1$, que G_p est somme directe de groupes cycliques p-groupe.
Si $m = 1$:
Supposons que $m \geqslant 1$, l'assertion démontrée à l'ordre m et $p^{m+1} G_p = 0$.
Posons $H = pG_p$, on a $p^m H = 0$. D'après l'hypothèse de récurrence, $H \bigoplus_{i=1}^{n} H_{\mathrm{i}}$, où H_i est un groupe cyclique p-groupe, pour tout i.
Un générateur $\mathrm{y}_i (\mathrm{H}_i =< y_j >)$ s'écrit, comme tous les éléments de $\mathrm{H_i}, \mathrm{y_i} = \mathrm{pz_i}$, où $z_i \in G_p$. D'après le lemme précédent :

$$\sum_{i=1}^{n} < z_i >= \bigoplus_{i=1}^{n} < z_i >$$

Posons $L = \bigoplus_{i=1}^{n} < z_i >$ et montrons, en le construisant, qu'il existe un sous-groupe M de G_p tel que $G_p = L \oplus M$. $Gp = \{x \in G, px = 0\}$ est un p-sous-groupe élémentaire de $G, 11$ est donc canoniquement muni d'une structure de $(\mathbb{Z}/p\mathbb{Z})$-espace vectoriel.

Si $k_i = \theta(y_j)$, puisque $y_j = pz_i$, on a $pk_i z_i = k_i(pz_i) = k_i y_i = 0$, et par suite $k_i z_i \in Gp$.
Montrons que $\sum_{i=1}^{n} < k_i z_i >$ est une somme directe :
$< k_j z_j > \cap \sum_{i\neq j} < k_i z_i > \subset < z_j > \cap \sum_{i\neq j} < z_i >= \{0\}$. On a donc

$\sum_{i=1}^{n} < k_i z_i >= \bigoplus_{i=1}^{n} < z_i >$.
Cela revient à dire que les éléments $k_1 z_1, k_2 z_2, \ldots, k_n z_n$ du $(\mathbb{Z}/p\mathbb{Z})$-espace vectoriel G_p sont linéairement indépendants. On admet qu'il existe dans Gp, des éléments $x_1, \ldots, x_s$ tels que :

$$\{k_1 z_1, k_2 z_2, \ldots, k_n z_n, x_1, x_2, \ldots, x_s\}$$

soit une base de Gp. Posons :

$$M = \bigoplus_{i=1}^{S} < x_i >$$

et achevons la démonstration en prouvant que $G_p = L \oplus M$. Tout $x \in L \cap M$, s'écrit $\sum_{i=1}^{n} b_i z_i = \sum_{j=1}^{s} a_j x_j$. Puisque $x \in M \subset G_p, px = 0$ et $\sum_{i=1}^{n} p b_i z_j = 0$; du fait que la somme des $< z_i >$ est directe, nous pouvons affirmer que $b_j y_i = p b_j z_i = 0$, pour tout $i = 1, 2, \ldots, n$.
Comme exposant de y_i, b_i vérifie $b_i = b_i' \theta(y_i) = b_j' k_i$ et il vient

$$0 = \sum_{i=1}^{n} b_i' k_i z_i - \sum_{j=1}^{s} a_j x_j.$$

Comme $k_1 z_1, \ldots, k_n z_n, x_1, \ldots, x_s$ est une base du $(\mathbb{Z}/p\mathbb{Z})$ -espace vectoriel G_p, tous les b_i' (pour $i \in [1, n]$) sont nuls dans $(\mathbb{Z}/p\mathbb{Z})$, i.e. $b_i'\ p \in \mathbb{Z}$. Ces b_i' de $p\mathbb{Z}$ annulent les produits de la forme $b_i' z_i$ parce que les z_i appartiennent par hypothèse à un p-groupe élémentaire : il en résulte que, pour tout $i \in [1, n], b_i z_1 = 0$, d'où $x = 0$. La démonstration est bien avancée. Il nous reste a vérifier que G_p est somme de L et de M.
Pour tout $x \in G_p, px \in H = pG$, et $px = \sum_{i=1}^{n} c_i y_i = \sum_{i=1}^{n} c_i p z_i$.
Il s'ensuit $p(x - \sum_{i=1}^{n} c_i z_i) = 0$, relation prouvant que $x - \sum_{i=1}^{n} c_i z_i \in G_p$ et cet élément, comme tel, s'écrit $x - \sum_{i=1}^{n} c_i z_i = \sum_{j=1}^{S} a_j x_j + \sum_{i=1}^{n} b_i k_i z_i$.
Finalement $x = \sum_{i=1}^{n} (c_i + b_i k_i) z_i + \sum_{j=1}^{s} a_j x_j \in L + M$ et on a bien $G_P = (\bigoplus_{i=1}^{n} < z_i >) \oplus (\bigoplus_{i=1}^{S} < x_i >)$. Tous les sous-groupes de cette somme sont cycliques par définition et p-groupe comme sous-groupes de p-groupe.

■

Remarque 1.6.2

Il ne faut pas confondre le théorème 1 *de décomposition des groupes commutatifs finis en p-groupe non nécessairement cycliques (en p-composantes) et le théorème* 3 *de décomposition en p-groupes cycliques.*

Remarque 1.6.3

Le théorème 4 *affirme que tout groupe fini G est de la forme* $G = \bigoplus_{i=1}^{n} \Gamma_i$, *où les* Γ_i *sont eux-mêmes isomorphes à des groupes cycliques de la forme* $\mathbb{Z}/{p_i}^{\alpha_i}\mathbb{Z}$..
Mais attention :
1) Le groupe de Klein est de la forme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *; donc, dans cette décomposition, les* p_i *ne sont pas nécessairement distincts.*

Exemple 1.6.4

Pour $G = \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ *(qui est d'ordre* $n = 360 = 2^3 \times 3^2 \times 5$ *) la décomposition de G en p-groupe est de la forme :* $G = \Gamma_8 \oplus \Gamma_2 \oplus \Gamma_3 \oplus \Gamma_3 \oplus \Gamma_5$ *avec* $G = \Gamma_8 \simeq \mathbb{Z}/8\mathbb{Z}, \quad \Gamma_2 \simeq \mathbb{Z}/2\mathbb{Z}; \Gamma_3 = \Gamma_3 \simeq \mathbb{Z}/3\mathbb{Z}; \Gamma_5 \simeq \mathbb{Z}/5\mathbb{Z}$.

Chapitre 2

Exemples corrigés

Exercice 2.0.1
Montrer qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

Solution :
Le groupe G est isomorphe à un produit $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$, avec $d_i \geq 2$ et $d_i \mid d_{i+1}$. Comme G n'est pas cyclique, on a $r \geq 2$. Il existe un facteur premier p de d_1, alors p divise tous les d_i, et $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à un sous-groupe de chacun des $\mathbb{Z}/d_i\mathbb{Z}$ (c'est le sous-groupe de p -torsion). Alors le sous-groupe de p -torsion de G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^r$, qui contient clairement un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 2.0.2
1) Combien y a-t-il de groupes commutatif de cardinal 360? *Faire la liste complète de ces groupes.*
2) Plus généralement, pour tout entier n, combien y a-t-il de groupes commutatifs de cardinal n ?

Solution :
1) On écrit la décomposition en facteurs premiers de $360 = 2^3.3^2.5$. Alors si G est un groupe de cardinal $360, G_2$ est un groupe commutatifs de cardinal 2^3, il y a donc 3 classes d'isomorphisme de tels groupes, à savoir $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^3$. De même, il y a exactement deux classes d'isomorphisme possibles pour G_3, à savoir $\mathbb{Z}/9\mathbb{Z}$ et $(\mathbb{Z}/3\mathbb{Z})^2$, et G_5 est isomorphe à $\mathbb{Z}/5\mathbb{Z}$.

Par conséquent, il y a exactement $3.2 = 6$ classes d'isomorphisme de groupes commutatifs d'ordre 360, dont les décompositions p-primaires et en facteurs invariants sont les suivantes :

$$\begin{gathered}\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/360\mathbb{Z},\\ (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z},\\ (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z},\\ \mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z},\\ (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z},\\ (\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}.\end{gathered}$$

2) On utilise la classification des classes d'isomorphisme de groupes commutatifs finis. Notons $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers. Alors on sait que la classe d'isomorphisme d'un groupe abélien d'ordre n est caractérisée par ses facteurs invariants $(d_1, \dots, d_s)$ qui sont des entiers > 1 tels que $d_i \mid d_{i+1}$ et $d_1 \dots d_s = n$. Par conséquent, chaque d_i se décompose $d_i = p_1^{\alpha_{i,1}} \dots p_1^{\alpha_{i,r}}$, avec les contraintes suivantes : pour tout $j, \alpha_{i,j} \leq \alpha_{i+1,j}($ pour tout $i)$ et $\sum_{i=1}^{s} \alpha_{i,j} = \alpha_j$ Par conséquent, le nombre de choix possibles pour les a_i est exactement $\prod_{j=1}^{r} p(\alpha_j)$, où $p(\alpha)$ désigne le nombre de partitions de α, le nombre de façons d'écrire l'entier α comme une somme croissante d'entiers strictement positifs.

Exercice 2.0.3
Soit G un groupe abélien fini. Montrer qu'il existe dans G un élément d'ordre égal à l'exposant de G (c'est-à-dire au ppcm des ordres des éléments de G).

Solution :
Montrons d'abord que pour tous $x, y \in G$ d'ordres respectifs m et n premiers entre eux, le produit xy est d'ordre $m.n$. Il est clair que $(xy)^{mn} = 1$ donc l'ordre de xy divise mn. Soit maintenant $k \geq 1$ tel que $(xy)^k = 1$. En élevant à la puissance n, on obtient $x^{kn} = 1$, donc m divise kn. Or m et n sont premiers entre eux, donc m divise k. Par symétrie, on a aussi que n divise k, donc mn divise k, donc xy est d'ordre mn. On décompose l'exposant de G en facteurs premiers : $\exp(G) = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, avec les p_i premiers distincts. Par définition de l'exposant de G, pour tout $1 \leq i \leq r$, il existe $g_i \in G$ dont l'ordre est divisible par $p_i^{\alpha_i}$, disons égal à $p_i^{\alpha_i} \cdot m_i$. Alors $g_i^{m_i}$ est d'ordre $p_i^{\alpha_i}$, et on a vu qu'alors l'élément $g := g_1^{m_1} \dots g_r^{m_r} \in G$ est d'ordre exactement $p_1^{\alpha_1} \dots p_r^{\alpha_r} = \exp(G)$

Exercice 2.0.4
Étude des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$:
1) Montrez que tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

2) Montrez que tout sous-groupe d'un groupe cyclique est cyclique.
3) Montrez que pour $d \mid n$, il existe un unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$.
4) Donnez le cardinal du sous-groupe engendré par k dans $\mathbb{Z}/n\mathbb{Z}$.
5) Montrez que $n = \sum_{d|n} \varphi(d)$ où $\phi(d)$ est l'indicatrice d'Euler, c'est à dire le nombre de générateurs de $\mathbb{Z}/d\mathbb{Z}$.
6) Montrez que tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

Solution :

1) Soit G un groupe cyclique de cardinal n et g un générateur. On note la loi de G multiplicativement. Par définition tout élément de G est de la forme g^k. On considère alors le morphisme $\phi : \mathbb{Z} \longrightarrow G$ défini par $\phi(k) = g^k$, c'est clairement un morphisme de groupe et surjectif par définition d'un groupe cyclique. Étudions son noyau, qui est un sous-groupe de $\mathbb{Z}$, donc de la forme $m\mathbb{Z}$. Ainsi ϕ induit un isomorphisme $\mathbb{Z}/m\mathbb{Z}$ sur G, par cardinalité on en déduit $m = n$.
2) Soit H un sous-groupe de G et $\varphi : \mathbb{Z} \longrightarrow G \longrightarrow G/H$, l'application composée de ϕ et du morphisme de réduction $G \longrightarrow G/H$. On rappelle que G étant commutatif, H est forcément distingué et G/H est alors naturellement muni d'une structure de groupe (cf. le cours). Le noyau de φ est un sous-groupe de $\mathbb{Z}$ donc de la forme $d\mathbb{Z}$, contenant Ker $\phi = n\mathbb{Z}$, on en déduit donc que d divise n. Ainsi H est cyclique, un générateur étant g^d, son ordre est ainsi n/d.
3) Soit donc H un sous-groupe de G d'ordre d; il est cyclique d'après (2), on note $h = g^k$ avec $0 \leqslant k < n$, un générateur. D'après la relation de Bezout H contient le groupe engendré par g^δ où $\delta = (n, k)$ et il est clairement contenu dans celui-ci. En outre ce dernier est évidement d'ordre $n/\delta = d$. En résumé H est isomorphe au sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par n/d.
4) On vient de voir dans le point précédent que l'ordre du sous-groupe engendré par k est égal à $n/(n, k)$.
5) Chaque élément de $\mathbb{Z}/n\mathbb{Z}$ engendre un sous-groupe, soit $n = \sum_H g(H)$ où la somme est indexée par les sous-groupes H de $\mathbb{Z}/n\mathbb{Z}$ et $g(H)$ est le cardinal des générateurs de H. D'après ce que l'on vient de voir, l'ensemble des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ est indexée par les diviseurs d de n, où à un diviseur d on associe le sous-groupe H engendré par n/d. D'après (4), l'ensemble des générateurs de (n/d) est en bijection avec l'ensemble $0 \leqslant \lambda < n$ tel que $(\lambda, n) = n/d$, soit en divisant par n/d, avec l'ensemble des $0 \leqslant \alpha < d$ premier avec d, i.e l'ensemble des générateurs de $\mathbb{Z}/d\mathbb{Z}$, d'où le résultat.
6) Soit donc G un sous-groupe fini du groupe multiplicatif d'un corps K (commutatif), et soit n le cardinal de G. Si $g \in G$, son ordre est un diviseur de n car le sous-groupe engendré par g est de cardinal son ordre, et le cardinal d'un sous-groupe divise le cardinal du groupe . Ainsi pour d divisant n, on note A_d (resp. H_d) l'ensemble des éléments de G d'ordre d (reps. divisant d) : en particulier on a $H_d = \left\{g \in G / g^d = 1\right\}$. Le corps K étant commutatif, on a $|H_d| \leqslant d$, car le polynôme $X^d - 1$ y a au plus d racines. En outre si $A_d \neq$, alors $|H_d| = d$ car tout élément de A_d

engendre un sous-groupe d'ordre d dans lequel tout élément g est tel que $g^d = 1$. Or $A_d \subset H_d$ soit $|A_d| \leqslant \varphi(d)$, l'inégalité $|A_d| \geqslant \varphi(d)$ étant évidente. En résumé soit A_d est vide soit son cardinal est égal à $\varphi(d)$. En reprenant le comptage de la question précédente, $G = \coprod_{d|n} A_d$, on obtient :

$$n = \sum_{d|n} \epsilon(d)\varphi(d).$$

où $\epsilon(d)$ est nul si A_d est vide, et égal à 1 sinon. En comparant cette égalité avec celle de (5), on en déduit que $\epsilon(d) = 1$ pour tout $d \mid n$, soit A_d non vide et en particulier A_n.

Exercice 2.0.5
Donnez les morphismes de groupe $\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$ puis ceux de $\mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$. Trouvez une condition nécessaire et suffisante sur m et n pour que tout morphisme $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ soit nul.

Solution :

On rappelle qu'un morphisme f d'un groupe cyclique $(G =< x >, +)$ d'ordre n vers un groupe cyclique $(H =< y >, +)$ d'ordre m est bien déterminé par l'image du générateur x de G.

Comme $f(x) \in H$ et H est d'ordre m, alors l'ordre de $f(x)$ divise m. D'autre part, l'ordre de $f(x)$ divise aussi n car l'ordre de x est n ($nx = 0$ et donc $nf(x) = 0$). Dés lors, l'ordre de $f(x)$ divise $pgcd(n, m)$.

En particulier, si $pgcd(n, m) = 1$, alors $|f(x)| = 1$ de sorte que $f(x) = 0_H$ et f est le morphisme nul.

Ainsi comme $pgcd(3, 4) = 1$, le seul morphisme $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ est le morphisme nul.

Pour les morphismes de groupes de $f : \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$, l'ordre de $f(1_{\mathbb{Z}/12\mathbb{Z}})$ divise $pgcd(12, 15) = 3$. Dés lors on a trois cas, à savoir $f(1_{\mathbb{Z}/12\mathbb{Z}}) = 0_{\mathbb{Z}/15\mathbb{Z}}$, $f(1_{\mathbb{Z}/12\mathbb{Z}} = 5\mathbb{Z}/15\mathbb{Z}$, ou bien $f(1_{\mathbb{Z}/12\mathbb{Z}}) = 10\mathbb{Z}/15\mathbb{Z}$.
Il y'a donc trois morphismes distincts.
par Enfin, c'est claire d'après ce qui précède, que la condition nécessaire et suffisante sue m et n pour que tout morphisme $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ soit nul est que $pgcd(n, m) = 1$.

Bibliographie

[1] A. Bouvier et D. Rihard, Groupes, Hermann, 1974.

[2] J. Calais, Eléments de théorie des groupes, Presses universitaires de France (1984).

[3] N. Mahdou, Structure algébrique, Faculté des Science Technique Fés,Université Sidi Mohamed Ben Abdellah