

Classification des extensions centrales de groupes finis

Cloé Allard

Reçu le 2024-09-11 et accepté le 2025-05-20

RÉSUMÉ Dans cet article on étudie les extensions centrales de groupe en utilisant une approche par les 2-cocycles. On introduit donc les différents concepts qui aideront à définir ce qu'est une extension centrale et un 2-cocycle et comment ceux-ci pourront nous fournir toute l'information nécessaire afin d'être capable d'identifier les classes d'isomorphisme des extensions. On terminera en calculant tous les 2-cocycles dans une classe d'exemples concrets.

1 Introduction

La première théorie de la cohomologie est apparue en 1935 dans un article de JW Alexander [Cor], sur les complexes différentiels et leurs duals. Les origines de la théorie de la cohomologie se trouvent dans la topologie et l'algèbre au début du siècle dernier, mais depuis, elle est devenue un outil important dans presque toutes les branches des mathématiques. Depuis 1935 la théorie de la cohomologie s'est grandement développée. Elle a principalement été étudiée en utilisant les notions de la théorie des catégories. La théorie des catégories étant cependant un sujet normalement abordée lors de cours de cycles supérieurs (maîtrises et doctorats), nous essaierons dans les prochains chapitres d'utiliser principalement les notions enseignées au premier cycle (baccalauréat) afin d'étudier la cohomologie de groupes ainsi que les extensions centrales de groupes. Ces deux sujets semblent indépendants l'un de l'autre, or dans cet article nous montrerons qu'il existe une équivalence entre les extensions centrales de groupes et la cohomologie de groupes.

2 Cohomologie d'un groupe G

Il est à noter que tout au long de cette section nous utiliserons le terme cocycle pour parler de 2-cocycles. De plus G et A seront des groupes et leurs opérations respectives seront notées multiplicativement avec la condition que A soit abélien.

Définition 2.1. Soit une fonction $f : G \times G \rightarrow A$ telle que pour $g, h, k \in G$, $f(h, k)f(g, hk) = f(gh, k)f(g, h)$. On dit alors que f est un cocycle.

Je tiens à remercier professeure Emily Cliff pour son soutien et son encadrement tout au long de mon stage de recherche avec elle ainsi que lors de la rédaction de cet article.

Définition 2.2. Soit un cocycle $f : G \times G \rightarrow A$ tel que pour $g \in G$, $f(g, 1_G) = 1_A$. On dit alors que f est un cocycle normalisé.

Lemme 2.3. Soit un cocycle normalisé $f : G \times G \rightarrow A$. On a alors que pour $g \in G$, $f(1_G, g) = 1_A$.

Démonstration. Soit $g \in G$, prenons le triplet $(g, 1_G, g)$. Comme f est un cocycle on a que $f(1_G, g)f(g, g) = f(g, g)f(g, 1_G)$. Or, comme f est un cocycle normalisé on a que $f(g, 1_G) = 1_A$. On obtient donc que $f(1_G, g) = 1_A$. \square

Proposition 2.4. Soit $\phi : G \rightarrow A$ tel que $\phi(1_G) = 1_A$. On définit $d\phi : G \times G \rightarrow A$ par $d\phi(g, h) := \frac{\phi(g)\phi(h)}{\phi(gh)}$. Alors $d\phi$ est un cocycle normalisé.

Démonstration. Vérifions que cette fonction respecte la condition pour être un cocycle. On observe que

$$d\phi(h, k)d\phi(g, hk) = \frac{\phi(h)\phi(k)}{\phi(hk)} \frac{\phi(g)\phi(hk)}{\phi(ghk)} = \phi(h)\phi(k) \frac{\phi(g)}{\phi(ghk)}.$$

Par contre on a aussi que

$$d\phi(g, h)d\phi(gh, k) = \frac{\phi(g)\phi(h)}{\phi(gh)} \frac{\phi(gh)\phi(k)}{\phi(ghk)} = \phi(h)\phi(k) \frac{\phi(g)}{\phi(ghk)}$$

et donc $d\phi(h, k)d\phi(g, hk) = d\phi(g, h)d\phi(gh, k)$. Nous pouvons ainsi conclure que $d\phi$ est un cocycle.

Vérifions ensuite qu'il s'agit d'un cocycle normalisé. On calcule facilement que

$$d\phi(1_G, h) = \frac{\phi(1_G)\phi(h)}{\phi(1_G \cdot h)} = 1_A \frac{\phi(h)}{\phi(h)} = 1_A.$$

Il suit que $d\phi$ est un cocycle normalisé. \square

Définition 2.5. On dit qu'un cocycle $f : G \times G \rightarrow A$ est trivial si et seulement si $f(g, h) = 1_A$ pour chaque $g, h \in G$.

Proposition 2.6. La fonction $d\phi$ définie à la proposition précédente est triviale si et seulement si ϕ est un homomorphisme.

Démonstration. La fonction est triviale si et seulement si $d\phi(g, h) = 1_A \forall g, h \in G$, on a alors que $\frac{\phi(g)\phi(h)}{\phi(gh)} = 1_A \forall g, h \in G$, ce qui est équivalent à la condition $\phi(g)\phi(h) = \phi(gh) \forall g, h \in G$. Et donc, $d\phi$ est triviale si et seulement si ϕ est un homomorphisme. \square

Notation. Dans cet article la notation \mathbb{Z}_k est utilisée pour représenter le groupe des entiers modulo k .

Exemple 2.7. Soit G le groupe additif \mathbb{Z}_n et A le groupe additif \mathbb{Z}_m . On a que $d\phi = 0$ si et seulement si $\phi(g+n\mathbb{Z}) + \phi(h+n\mathbb{Z}) + m\mathbb{Z} = \phi(g+h+n\mathbb{Z}) + m\mathbb{Z} \forall g, h \in G$, c'est-à-dire si ϕ est un homomorphisme.

Définition 2.8. L'ensemble des applications $\phi : G \rightarrow A$ tel que $\phi(1_G) = 1_A$ est noté $C^1(G,A)$. Il forme un groupe abélien sous la multiplication induite par la multiplication dans A : Pour ϕ, ψ dans $C^1(G,A)$, on a $(\phi\psi)(g) = \phi(g)\psi(g)$.

Définition 2.9. L'ensemble des fonctions $\phi : G \rightarrow A$ tel que ϕ est un homomorphisme forme un sous-groupe de $C^1(G,A)$ noté $Z^1(G,A)$.

Définition 2.10. L'ensemble des cocycles normalisés $f : G \times G \rightarrow A$ forme un groupe abélien noté $Z^2(G,A)$. Encore une fois, la multiplication est induite par la multiplication dans A .

Définition 2.11. L'ensemble des cocycles normalisés qui s'écrivent de la forme $d\phi$ forme un sous-groupe de $Z^2(G,A)$ noté $B^2(G,A)$. Les éléments de $B^2(G,A)$ sont appelés les cobords.

Définition 2.12. On définit la cohomologie de G avec coefficients dans A en degré 2 par $H^2(G,A) = Z^2(G,A)/B^2(G,A)$.

3 Les suites exactes courtes de groupes

Définition 3.1. Soit G un groupe. Le centre de G est

$$Z(G) = \{ z \in G \mid gz = zg \quad \forall g \in G \}.$$

Proposition 3.2. Le centre $Z(G)$ est un sous-groupe normal de G : $Z(G) \trianglelefteq G$.

Démonstration. Posons e_G l'élément neutre de G . Soit g un élément de G . On a $e_G g = g = g e_G$ et donc $e_G \in Z(G)$. Il suit que $Z(G)$ est non vide.

Soient $a, b \in Z(G)$. On veut montrer que $ab \in Z(G)$. Pour $g \in G$ on a $(ab)g = a(bg) = a(gb) = (ag)b = g(ab)$, et ainsi $ab \in Z(G)$.

Soit $a \in Z(G)$. On veut montrer que $a^{-1} \in Z(G)$. Pour $g \in G$ on a $g^{-1} \in G$ et donc $g^{-1}a = ag^{-1}$. Il suit que $a^{-1}g = a^{-1}(g^{-1})^{-1} = (g^{-1}a)^{-1} = (ag^{-1})^{-1} = (g^{-1})^{-1}a^{-1} = ga^{-1}$. Donc $a^{-1} \in Z(G)$ comme désiré. Il suit que $Z(G)$ est un sous-groupe de G .

Il nous reste à démontrer qu'il est normal. Alors prenons $a \in Z(G)$ et $g \in G$, on observe que $gag^{-1} = gg^{-1}a = a \in Z(G)$. Ainsi, $gag^{-1} \in Z(G)$. \square

Définition 3.3. Soient G, H, K et L des groupes et f_i , pour $i \in \{1, 2, 3, 4\}$, des homomorphismes comme suit :

$$\begin{array}{ccc} G & \xrightarrow{f_1} & H \\ \downarrow f_3 & & \downarrow f_2 \\ K & \xrightarrow{f_4} & L. \end{array}$$

On dit que le diagramme est commutatif si et seulement si $f_2 \circ f_1 = f_4 \circ f_3$.

Exemple 3.4. Le diagramme suivant est commutatif

$$\begin{array}{ccc} G & \xrightarrow{f} & G \times G \\ \downarrow id & & \downarrow m \\ G & \xrightarrow{id} & G, \end{array}$$

avec $f : G \rightarrow G \times G$ tel que $f(g) = (1_G, g)$ et $m : G \times G \rightarrow G$ tel que $m(g, h) = gh$, la fonction de multiplication. On a effectivement que $f \circ m = id \circ id = id$.

Exemple 3.5. L'associativité peut être écrite sous la forme d'un diagramme commutatif. Soit m la fonction de multiplication et id la fonction identité. On considère le diagramme suivant :

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m \times id} & G \times G \\ \downarrow id \times m & & \downarrow m \\ G \times G & \xrightarrow{m} & G. \end{array}$$

On a alors $(m \times id)(g, h, k) = (gh, k)$ et $(id \times m)(g, h, k) = (g, hk)$. Le diagramme est commutatif si et seulement si

$$(m \circ (m \times id))(g, h, k) = (m \circ (id \times m))(g, h, k) \forall g, h, k \in G,$$

c'est à dire si et seulement si $(gh)k = g(hk)$. Mais cela est la définition de l'associativité.

Définition 3.6. Soient G, H et K des groupes. Une suite exacte courte de groupes est une suite d'homomorphismes de la forme

$$1 \longrightarrow G \xrightarrow{\phi} H \xrightarrow{\psi} K \longrightarrow 1$$

telle que

1. ϕ est injective ;
2. ψ est surjective ;
3. $Im(\phi) = Ker(\psi)$.

On utilise parfois la notation \hookrightarrow pour représenter une fonction injective et \twoheadrightarrow pour représenter une fonction surjective. On peut donc représenter la suite exacte courte avec le diagramme suivant

$$1 \longrightarrow G \hookrightarrow H \twoheadrightarrow K \longrightarrow 1.$$

Lemme 3.7. Soit la suite exacte courte suivante

$$1 \longrightarrow G \xrightarrow{\phi} H \xrightarrow{\psi} K \longrightarrow 1.$$

Alors $\psi \circ \phi = 1$ où 1 est la fonction qui envoie n'importe quel élément de G à 1_K .

Démonstration. Soit $g \in G$. Alors $\phi(g) \in \text{Im}(\phi) = \text{Ker}(\psi)$ et donc $\psi(\phi(g)) = 1_K$. \square

Exemple 3.8. La suite

$$0 \longrightarrow \mathbb{Z}_2 \xrightarrow{\phi} \mathbb{Z}_2 \times \mathbb{Z}_2 \xrightarrow{\psi} \mathbb{Z}_2 \longrightarrow 0$$

avec

$$\begin{aligned} \phi : \mathbb{Z}_2 &\rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \\ a &\mapsto (0, a) \end{aligned}$$

et

$$\begin{aligned} \psi : \mathbb{Z}_2 \times \mathbb{Z}_2 &\rightarrow \mathbb{Z}_2 \\ (b, a) &\mapsto b \end{aligned}$$

est une suite exacte courte.

4 Les extensions

Définition 4.1. Soit la suite exacte courte de groupes

$$1 \longrightarrow N \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1.$$

On dit que E est une extension de G par N .

De plus, considérons le cas où $N = A$ est abélien. Si $i(A) \subseteq Z(E)$ où $Z(E)$ est le centre de E , alors on dit que E est une extension centrale.

Objectif. On essaie donc de classifier les extensions centrales de G par A .

$$1 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

à isomorphisme près.

On définira bientôt la notion d'isomorphisme d'extensions, mais d'abord donnons quelques exemples d'extensions centrales.

Exemple 4.2. Soit la suite exacte courte de groupes

$$1 \longrightarrow A \xrightarrow{i} A \times G \xrightarrow{\pi} G \longrightarrow 1$$

où A est un groupe abélien. L'homomorphisme $i : A \rightarrow A \times G$ est tel que $i(a) = (a, 1_G)$ et l'homomorphisme $\pi : A \times G \rightarrow G$ est tel que $\pi(a, g) = g$.

De plus, $i(A)$ est tout les éléments de $A \times G$ de la forme $(a, 1_G)$ où $a \in A$.

Calculons maintenant le centre $Z(A \times G)$. Soit $(a, g), (b, h) \in A \times G$. On a que $(a, g)(b, h) = (ab, gh)$ et $(b, h)(a, g) = (ba, hg)$. Comme A est abélien on sait que $(ba, hg) = (ab, hg)$. Ainsi $(a, g) \in Z(A \times G)$ si et seulement si $gh = hg$ pour tout $h \in G$. C'est à dire si et seulement si $g \in Z(G)$. On peut donc conclure que $Z(A \times G) = A \times Z(G)$. Il suit que $i(A) \subseteq Z(A \times G)$. On a ainsi que $A \times G$ est une extension centrale de G par A . On l'appelle l'extension triviale.

Exemple 4.3. Soit la suite exacte courte de groupes

$$0 \longrightarrow \mathbb{Z}_2 \xrightarrow{i} \mathbb{Z}_4 \xrightarrow{\pi} \mathbb{Z}_2 \longrightarrow 0$$

où $i : \mathbb{Z}_2 \rightarrow \mathbb{Z}_4$ est tel que $i(a + 2\mathbb{Z}) = 2(a + 4\mathbb{Z})$ et $\pi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2$ est tel que $\pi(n + 4\mathbb{Z}) = n + 2\mathbb{Z}$.

Le groupe \mathbb{Z}_2 est un groupe abélien. De plus, $i(A) = \{4\mathbb{Z}, 2+4\mathbb{Z}\}$ et $Z(\mathbb{Z}_4) = \mathbb{Z}_4$ car il s'agit d'un groupe abélien. Il en suit que $i(A) \subset Z(\mathbb{Z}_4)$. On peut donc conclure que \mathbb{Z}_4 est une extension centrale de \mathbb{Z}_2 par \mathbb{Z}_2 .

Définition 4.4. Un isomorphisme d'extensions E, E' est un isomorphisme $\phi : E \rightarrow E'$ de groupes tel que le diagramme suivant est commutatif :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \parallel & & \downarrow \phi & & \parallel & & \\ 1 & \longrightarrow & A & \xrightarrow{i'} & E' & \xrightarrow{\pi'} & G & \longrightarrow & 1. \end{array}$$

On a donc

1. $\phi \circ i = i'$;
2. $\pi' \circ \phi = \pi$.

Proposition 4.5 (Court lemme des cinq). *Soient les deux suites exactes courtes suivantes*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G & \xrightarrow{\phi} & H & \xrightarrow{\psi} & K & \longrightarrow & 1 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 1 & \longrightarrow & G' & \xrightarrow{\phi'} & H' & \xrightarrow{\psi'} & K' & \longrightarrow & 1, \end{array}$$

où α, β, γ sont des homomorphismes tels que le diagramme est commutatif. Si α et γ sont des isomorphismes alors β l'est aussi.

Démonstration. Démontrons d'abord que β est surjectif. Soient $h' \in H'$ et $k' = \psi'(h') \in K'$. Comme γ est surjectif,

$$\exists k \in K \text{ tel que } \gamma(k) = k' = \psi'(h'). \quad (1)$$

De plus, comme il s'agit d'une suite exacte courte, ψ est surjectif. Donc

$$\exists h \in H \text{ tel que } \psi(h) = k. \quad (2)$$

Par la commutativité du diagramme on sait que $\gamma(\psi(h)) = \psi'(\beta(h))$. Or, par l'équation (2) on a que $\gamma(\psi(h)) = \gamma(k)$ et par l'équation (1) on a que $\gamma(k) = \psi'(h')$.

En appliquant ψ' à $\beta(h)(h')^{-1}$ on obtient

$$\begin{aligned} \psi'(\beta(h)(h')^{-1}) &= \psi'(\beta(h))\psi'(h')^{-1} = \gamma(\psi(h))\psi'(h')^{-1} \\ &= \gamma(k)\psi'(h')^{-1} = \psi'(h')\psi'(h')^{-1} = 1_{K'}. \end{aligned}$$

C'est-à-dire que $\beta(h)(h')^{-1} \in \text{Ker}(\psi) = \text{Im}(\phi')$. Or, on peut écrire $\text{Im}(\phi')$ comme $\phi'(G') = \phi'(\alpha(G))$ car α est un isomorphisme. Donc $\beta(h)(h')^{-1} \in \phi'(\alpha(G))$, Alors il existe $g \in G$ tel que

$$\phi'(\alpha(g)) = \beta(h)(h')^{-1}. \quad (3)$$

Par la commutativité du diagramme on sait que $\phi' \circ \alpha = \beta \circ \phi$, et donc

$$\phi'(\alpha(g)) = \beta(\phi(g)). \quad (4)$$

Par les équations (3) et (4) on sait que

$$\begin{aligned} \beta(h)(h')^{-1} = \beta(\phi(g)) &\Leftrightarrow h' = \beta(h)\left(\beta(\phi(g))\right)^{-1} \\ &\Leftrightarrow h' = \beta(h\phi(g)^{-1}). \end{aligned}$$

Il suit que β est surjectif, comme désiré.

Maintenant démontrons que β est injectif. Soit $h \in H$ tel que $\beta(h) = 1_{H'}$. Comme ψ' est un homomorphisme, $\psi'(\beta(h)) = 1_{K'}$. Or, par la commutativité du diagramme on sait que $\psi' \circ \beta = \gamma \circ \psi$, et donc $\gamma(\psi(h)) = 1_{K'}$. Comme γ est injective, il suit que $\psi(h) = 1_K$, et donc $h \in \text{Ker}(\psi)$.

Comme $\text{Ker}(\psi) = \text{Im}(\phi)$,

$$\exists g \in G \text{ tel que } \phi(g) = h. \quad (5)$$

1. σ est bijective ;

2. σ est un homomorphisme si et seulement si s est un homomorphisme.

Démonstration.

(1)

Démontrons d'abord que σ est injectif. Soient $(a_1, g_1), (a_2, g_2) \in A \times G$ tels que $\sigma(a_1, g_1) = \sigma(a_2, g_2)$. C'est-à-dire que $i(a_1)s(g_1) = i(a_2)s(g_2)$. Appliquons π ; on obtient : $\pi(i(a_1)s(g_1)) = \pi(i(a_2)s(g_2))$. Comme $\text{Ker}(\pi) = \text{Im}(i)$ et π est un homomorphisme, c'est équivalent à $\pi(s(g_1)) = \pi(s(g_2))$. Mais $\pi \circ s = \text{id}_G$, alors l'équation devient $g_1 = g_2$.

Notre équation originale devient donc $i(a_1)s(g_1) = i(a_2)s(g_1)$, ce qui implique que $i(a_1) = i(a_2)$. Finalement $a_1 = a_2$ car i est injectif. On a donc que $\sigma(a_1, g_1) = \sigma(a_2, g_2)$ si et seulement si $(a_1, g_1) = (a_2, g_2)$, c'est-à-dire que σ est injectif.

Démontrons maintenant que σ est surjectif. Soit $e \in E$, et posons $g = \pi(e)$. On a ainsi que $s(g) = s(\pi(e))$. On observe que $\pi(e \cdot s(\pi(e))^{-1}) = \pi(e) \cdot (\pi \circ s \circ \pi(e))^{-1}$ car π est un homomorphisme. Mais comme $\pi \circ s = \text{id}_G$, on a $\pi(e) \cdot (\pi \circ s \circ \pi(e))^{-1} = \pi(e) \cdot (\pi(e))^{-1} = 1_G$. Alors $e \cdot s(\pi(e))^{-1} \in \text{Ker}(\pi) = \text{Im}(i)$. Donc, il existe $a \in A$ tel que $e \cdot s(\pi(e))^{-1} = i(a)$. Finalement, on voit que $e = i(a)s(\pi(e)) = i(a)s(g) = \sigma(a, g)$, et donc σ est surjectif.

(2)

L'application σ est un homomorphisme si et seulement si

$$\sigma((a_1, g_1) \cdot (a_2, g_2)) = \sigma(a_1, g_1)\sigma(a_2, g_2) \text{ pour tous } (a_i, g_i) \in A \times G.$$

On observe que

$$\sigma((a_1, g_1) \cdot (a_2, g_2)) = i(a_1 a_2)s(g_1 g_2) = i(a_1)i(a_2)s(g_1 g_2)$$

car i est un homomorphisme, tandis que

$$\sigma(a_1, g_1)\sigma(a_2, g_2) = i(a_1)s(g_1)i(a_2)s(g_2) = i(a_1)i(a_2)s(g_1)s(g_2)$$

car E est une extension centrale.

Donc $\sigma((a_1, g_1) \cdot (a_2, g_2)) = \sigma(a_1, g_1)\sigma(a_2, g_2)$ si et seulement si $s(g_1 g_2) = s(g_1)s(g_2)$. On conclut que σ est un homomorphisme si et seulement si s l'est. \square

Théorème 5.3. *Soit*

$$1 \longrightarrow A \xleftarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

une suite exacte courte donnant une extension centrale. L'extension centrale E est isomorphe à l'extension triviale $(A \times G)$ si et seulement s'il existe un homomorphisme $s : G \rightarrow E$ tel que $\pi \circ s = id_G$. On dit alors que s est une section de π .

Démonstration.

Supposons qu'on a une section $s : G \rightarrow E$. De la proposition 5.2(2) on sait que la fonction $\sigma : A \times G \rightarrow E$, $\sigma(a, g) = i(a)s(g)$ est un homomorphisme. On sait également de la proposition 5.2(1) que σ est bijective. On a ainsi que σ est un isomorphisme et donc que $E \cong A \times G$.

Supposons maintenant qu'on a un isomorphisme $\phi : A \times G \rightarrow E$ d'extensions, correspondant au diagramme commutatif suivant :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \parallel & & \uparrow \phi & \swarrow s & \parallel & & \\ 1 & \longrightarrow & A & \xrightarrow{i'} & A \times G & \xrightarrow{\pi'} & G & \longrightarrow & 1 \\ & & & & & \swarrow j & & & \end{array}$$

Si on pose $j : G \rightarrow A \times G$, $j(g) = (1_A, g)$, on peut définir un homomorphisme $s = \phi \circ j : G \rightarrow E$. Par la commutativité du diagramme, on sait que $\pi \circ s = \pi \circ \phi \circ j = \pi' \circ j = id_G$. Donc s est une section comme désiré. \square

Note. En général on veut savoir à quelle "distance" s est d'être un homomorphisme. Pour se faire, on veut comparer $s(g)s(h)$ et $s(gh)$. En appliquant π , on a

$$s(g)s(h) \mapsto \pi(s(g)s(h)) = \pi(s(g))\pi(s(h)) = gh \quad (6)$$

et

$$s(gh) \mapsto \pi(s(gh)) = gh. \quad (7)$$

Par les équations (6) et (7) on peut conclure que $s(g)s(h)s(gh)^{-1} \in Ker(\pi) = Im(i)$. Comme i est injectif, il existe un unique élément $a \in A$ tel que $i(a) = s(g)s(h)s(gh)^{-1}$.

Posons $f(g, h) := a$, on obtient une unique fonction $f : G \times G \rightarrow A$ tel que $s(g)s(h) = i(f(g, h))s(gh)$.

Proposition 5.4. *La fonction $f : G \times G \rightarrow A$ telle que $s(g)s(h) = i(f(g, h))s(gh)$ est triviale si et seulement si s est un homomorphisme.*

Démonstration. La fonction f est triviale, c'est-à-dire $f(g, h) = 1_A$, si et seulement si $i(f(g, h)) = 1_E$, ce qui est équivalent à $s(gh) = s(g)s(h)$. On conclut que f est triviale si et seulement si s est un homomorphisme comme désiré. \square

Lemme 5.5. *La fonction f de la proposition 5.4 est un cocycle normalisé.*

Démonstration. Tout d'abord on observe que

$$i(f(h, k)f(g, hk)) = i(f(h, k))i(f(g, hk)) = s(h)s(k)s(hk)^{-1}s(g)s(hk)s(ghk)^{-1}.$$

Le produit des trois premiers termes étant dans le centre de E , nous obtenons l'égalité

$$i(f(h,k)f(g,hk)) = s(g)s(h)s(k)s(hk)^{-1}s(hk)s(ghk)^{-1} = s(g)s(h)s(k)s(ghk)^{-1}.$$

D'un autre côté nous observons que

$$i(f(g,h)f(gh,k)) = i(f(g,h))i(f(gh,k)) = s(g)s(h)s(gh)^{-1}s(gh)s(k)s(ghk)^{-1}.$$

En simplifiant l'équation nous obtenons

$$i(f(g,h)f(gh,k)) = s(g)s(h)s(k)s(ghk)^{-1}.$$

On a donc que $i(f(h,k)f(g,hk)) = i(f(g,h)f(gh,k))$. Comme i est injectif, la condition pour être un cocycle est respectée.

Vérifions maintenant s'il est normalisé. On remarque que $i(f(1_G, h)) = s(1_G)s(h)s(1_G \cdot h)^{-1} = 1_E \cdot s(h)s(h)^{-1} = 1_E = i(1_A)$. L'injectivité de i implique que $f(1_G, h) = 1_A$.

On peut ainsi conclure que cette fonction f est un cocycle normalisé. \square

On verra maintenant que la fonction f contient l'information nécessaire pour construire une nouvelle opération notée $*_f$ sur $A \times G$ telle que $(A \times G, *_f)$ est une extension centrale de G par A , et la bijection σ de la proposition 5.2 est un isomorphisme d'extensions.

Définition 5.6. Soit une fonction $f : G \times G \rightarrow A$. On définit l'opération $*_f$ sur $A \times G$ par $(a, g) *_f (b, h) := (abf(g, h), gh)$.

Proposition 5.7. Soit $f : G \times G \rightarrow A$ un cocycle normalisé. L'ensemble $A \times G$ muni de l'opération $*_f$ forme un groupe.

Démonstration. Vérifions que le groupe admet un élément neutre.

$$\begin{aligned} (1_A, 1_G) *_f (b, h) &= (1_A b f(1_G, h), 1_G h) = (b, h); \\ (a, g) *_f (1_A, 1_G) &= (a 1_A f(g, 1_G), g 1_G) = (a, g). \end{aligned}$$

Le groupe admet donc l'élément $(1_A, 1_G)$ comme élément neutre.

Vérifions maintenant que l'associativité est respectée. Pour $(a, g), (b, h), (c, k) \in A \times G$ on a

$$(a, g) *_f ((b, h) *_f (c, k)) = (a, g) *_f (bcf(h, k), hk) = (abcf(h, k)f(g, hk), ghk).$$

Pareillement on obtient

$$\begin{aligned} ((a, g) *_f (b, h)) *_f (c, k) &= (abf(g, h), gh) *_f (c, k) = (abf(g, h)cf(gh, k), ghk) \\ &= (abcf(g, h)f(gh, k), ghk). \end{aligned}$$

Comme f est un cocycle, $(abcf(h,k)f(g,hk),ghk) = (abcf(g,h)f(gh,k),ghk)$; ainsi l'associativité est respectée comme désirée.

Vérifions finalement que chaque élément admet un inverse.

$$\begin{aligned} (a,g) *_f (b,h) = (1_A, 1_G) &\Leftrightarrow (abf(g,h), gh) = (1_A, 1_G) \\ &\Leftrightarrow abf(g,h) = 1_A \quad \& \quad gh = 1_G \\ &\Leftrightarrow b = a^{-1}f(g,h)^{-1} \quad \& \quad h = g^{-1} \\ &\Leftrightarrow b = a^{-1}f(g,g^{-1})^{-1} \quad \& \quad h = g^{-1}. \end{aligned}$$

Vérifions que $(b,h) = (a^{-1}f(g,g^{-1})^{-1}, g^{-1})$ est bel et bien un inverse.

$$\begin{aligned} (a^{-1}f(g,g^{-1})^{-1}, g^{-1}) *_f (a,g) &= (aa^{-1}f(g,g^{-1})^{-1}f(g^{-1},g), g^{-1}g) \\ &= (f(g,g^{-1})^{-1}f(g^{-1},g), 1_G). \end{aligned}$$

Or, en utilisant la condition d'un cocycle avec les éléments (g,g^{-1},g) on obtient $f(g^{-1},g)f(g,g^{-1}g) = f(g,g^{-1})f(gg^{-1},g)$ d'où $f(g^{-1},g) = f(g,g^{-1})$.

On a donc effectivement que $(a,g)^{-1} = (a^{-1}f(g^{-1},g), g^{-1})$.

On peut donc conclure que $(A \times G, *_f)$ est un groupe. \square

On remarque ainsi que chaque cocycle f mène à une extension $(A \times G, *_f)$.

Proposition 5.8. *Soit $f : G \times G \rightarrow A$ un cocycle normalisé. Le groupe $A \times G$ muni de l'opération $*_f$ a la structure d'une extension centrale.*

Démonstration. Considérons les fonctions suivantes

$$1 \longrightarrow A \xrightarrow{i} A \times G \xrightarrow{\pi} G \longrightarrow 1.$$

avec

$$\begin{aligned} i : A &\rightarrow A \times G & \pi : A \times G &\rightarrow G \\ a &\mapsto (a, 1_G) & (a, g) &\mapsto g. \end{aligned}$$

Il faut donc démontrer que i et π sont des homomorphismes, que i est injective, que π est surjective, que $\text{Ker}(\pi) = \text{Im}(i)$ et que $i(A) \subseteq Z(A \times G, *_f)$.

Commençons par montrer que i et π sont des homomorphismes. On a que $i(a_1) *_f i(a_2) = (a_1, 1_G) *_f (a_2, 1_G) = (a_1a_2f(1_G, 1_G), 1_G1_G) = (a_1a_2, 1_G) = i(a_1a_2)$. On peut donc conclure que i est un homomorphisme. Regardons maintenant la fonction π . On a que $\pi((a_1, g_1) *_f (a_2, g_2)) = \pi(a_1a_2f(g_1, g_2), g_1g_2) = g_1g_2 = \pi(a_1, g_1)\pi(a_2, g_2)$. Il en suit que π est également un homomorphisme.

De plus, il est trivial par la définition de i que cette fonction est injective. Il est également trivial par la définition de π que cette fonction est surjective. On a en plus que $\text{Ker}(\pi) = \{(a, 1_G) | a \in A\} = \text{Im}(i)$.

Finalement, il faut vérifier que $i(A) \subseteq Z(A \times G, *_f)$. Prenons $(a, 1_G) \in i(A)$ et $(b, g) \in A \times G$. On a $(a, 1_G) *_f (b, g) = (abf(1_G, g), 1_Gg) = (ab, g)$ et $(b, g) *_f (a, 1_G) = (baf(g, 1_G), g1_G) = (ba, g) = (ab, g)$.

On peut donc finalement conclure que le groupe $A \times G$ muni de l'opération $*_f$ a la structure d'une extension centrale. \square

Note 5.9. La discussion ci-dessus nous donne comme résultat qu'avec une extension E donnée et une fonction s choisie, on obtient un cocycle f . On peut ainsi conclure que chaque extension donne un cocycle f . De même, chaque cocycle donne une extension. On aimerait maintenant savoir quand deux telles extensions sont isomorphes.

Proposition 5.10. *Soit $f_1, f_2 : G \times G \rightarrow A$ des cocycles normalisés menant aux groupes $(A \times G, *_f_i), i = 1, 2$. Supposons qu'on a un isomorphisme des extensions centrales.*

$$\begin{array}{ccccccc} 1 & \longrightarrow & A & \xrightarrow{i_1} & (A \times G, *_f_1) & \xrightarrow{\pi_1} & G \longrightarrow 1 \\ & & \parallel & & \downarrow \tilde{\phi} & & \parallel \\ 1 & \longrightarrow & A & \xrightarrow{i_2} & (A \times G, *_f_2) & \xrightarrow{\pi_2} & G \longrightarrow 1. \end{array}$$

Il suit que $\tilde{\phi}$ est de la forme $\tilde{\phi}(a, g) = (a\phi(g), g)$, où $\phi : G \rightarrow A$ est tel que $\frac{f_2(g, h)}{f_1(g, h)} = \frac{\phi(g)\phi(h)}{\phi(gh)}$. Par contre, chaque fonction $\phi : G \rightarrow A$ satisfaisant $\frac{f_2(g, h)}{f_1(g, h)} = \frac{\phi(g)\phi(h)}{\phi(gh)}$ nous donne un isomorphisme $\tilde{\phi}$ d'extensions.

Démonstration. Notons $\tilde{\phi}(a, g) = (\tilde{\phi}_A(a, g), \tilde{\phi}_G(a, g))$. On sait par la commutativité du diagramme que $\pi_2 \circ \tilde{\phi} = \pi_1$. On doit donc avoir que

$$\pi_2(\tilde{\phi}(a, g)) = \tilde{\phi}_G(a, g) = \pi_1(a, g) = g.$$

On conclut donc que $\tilde{\phi}_G(a, g) = g$, et ce, pour tout $(a, g) \in A \times G$.

De plus, on sait que $\tilde{\phi} \circ i_1 = i_2$. On doit donc avoir

$$\tilde{\phi}(i_1(a)) = \tilde{\phi}(a, 1_G) = (\tilde{\phi}_A(a, 1_G), 1_G) = i_2(a) = (a, 1_G).$$

On a ainsi que $\tilde{\phi}_A(a, 1_G) = a$ et ce, pour tout $a \in A$.

En sachant que $\tilde{\phi}$ est un homomorphisme de groupes, on doit avoir

$$\tilde{\phi}((a_1, g_1) *_f_1 (a_2, g_2)) = \tilde{\phi}(a_1, g_1) *_f_2 \tilde{\phi}(a_2, g_2).$$

En particulier, il faut

$$\tilde{\phi}((a, 1_G) *_f_1 (1_A, g)) = \tilde{\phi}(a1_Af_1(1_G, g), 1_Gg) = \tilde{\phi}(a, g) = (\tilde{\phi}_A(a, g), g).$$

Cependant,

$$\begin{aligned} \tilde{\phi}(a, 1_G) *_f_2 \tilde{\phi}(1_A, g) &= (\tilde{\phi}_A(a, 1_G), 1_G) *_f_2 (\tilde{\phi}_A(1_A, g), g) \\ &= (a, 1_G) *_f_2 (\tilde{\phi}_A(1_A, g), g) \\ &= (a\tilde{\phi}_A(1_A, g)f_2(1_G, g), 1_Gg) \\ &= (a\tilde{\phi}_A(1_A, g), g). \end{aligned}$$

On conclut donc que $\tilde{\phi}_A(a,g) = a\tilde{\phi}_A(1_A,g)$ et ce, pour tout $g \in G$ et $a \in A$.
Donc en posant

$$\begin{aligned}\phi : G &\rightarrow A \\ g &\mapsto \tilde{\phi}_A(1_A,g),\end{aligned}$$

on a $\tilde{\phi}(a,g) = (a\phi(g),g)$ et ce, pour tout $(a,g) \in A \times G$.

Finalement, on doit avoir que $\tilde{\phi}_A((1_A,g) *_{f_1} (1_A,h)) = \tilde{\phi}_A(1_A,g) *_{f_2} \tilde{\phi}_A(1_A,h)$.
D'un côté on obtient

$$\tilde{\phi}_A((1_A,g) *_{f_1} (1_A,h)) = \tilde{\phi}_A(f_1(g,h),gh) = (f_1(g,h)\phi(gh),gh).$$

Et de l'autre côté on obtient

$$\tilde{\phi}_A(1_A,g) *_{f_2} \tilde{\phi}_A(1_A,h) = (\phi(g),g) *_{f_2} (\phi(h),h) = (\phi(g)\phi(h)f_2(g,h),gh).$$

On obtient ainsi $f_1(g,h)\phi(gh) = \phi(g)\phi(h)f_2(g,h)$, c'est à dire que

$$\frac{f_1(g,h)}{f_2(g,h)} = \frac{\phi(g)\phi(h)}{\phi(gh)}. \quad (8)$$

À l'opposé, si nous avons une fonction $\phi : G \rightarrow A$ satisfaisant la relation (8), alors on pose

$$\begin{aligned}\tilde{\phi} : A \times G &\rightarrow A \times G \\ (a,g) &\mapsto (a\phi(g),g).\end{aligned}$$

Il restera donc à vérifier les conditions suivantes

1. $\tilde{\phi} \circ i_1 = i_2$
2. $\pi_2 \circ \tilde{\phi} = \pi_1$
3. $\tilde{\phi}((a_1,g_1) *_{f_1} (a_2,g_2)) = \tilde{\phi}(a_1,g_1) *_{f_2} \tilde{\phi}(a_2,g_2)$

afin de s'assurer que la fonction $\tilde{\phi}$ définie nous donne un isomorphisme d'extensions. \square

Remarque 5.11. On peut donc en tirer la conclusion que deux cocycles f_1 et f_2 donnent des extensions isomorphes si et seulement si $\frac{f_1}{f_2} = d\phi$ avec $d\phi$ le cobord défini à la proposition 2.4. Dans un groupe additif on écrira donc que $f_1 - f_2 = d\phi$.

Remarque 5.12. On obtient alors une bijection entre l'ensemble des classes d'isomorphismes des extensions et l'ensemble $H^2(G,A)$. En effet, on sait du théorème 5.3 et du lemme 5.5 qu'à partir d'une extension centrale E il est possible d'obtenir un cocycle noté f_E . À partir de ce cocycle on obtient l'extension centrale $A \times G$ munie de l'opération $*_{f_E}$ comme démontré à la proposition 5.8. Il ne reste qu'à vérifier que celle-ci est isomorphe à E . La définition 5.1 nous affirme qu'il

est toujours possible de définir une fonction $s : G \rightarrow E$ telle que $\pi \circ s = id_G$. Il faudra donc montrer que cette fonction s est un homomorphisme. Or on a que la fonction σ définie à la proposition 5.2 est un homomorphisme. En effet,

$$\sigma((a, g) *_{f_E} (b, h)) = (abf_E(g, h), gh) = i(abf_E(g, h))s(gh).$$

Or, i est un homomorphisme, on obtient donc

$$\sigma((a, g) *_{f_E} (b, h)) = i(a)i(b)i(f_E(g, h))s(gh).$$

Suite au théorème 5.3, on sait que $s(g)s(h) = i(f_E(g, h))s(gh)$. Ainsi on a

$$\sigma((a, g) *_{f_E} (b, h)) = i(a)i(b)s(g)s(h) = i(a)s(g)i(b)s(h) = \sigma(a, g)\sigma(b, h)$$

car on sait que $i(A) \subset Z(E)$. Ainsi on peut conclure que σ est un homomorphisme et par la proposition 5.2.2 il en suit que s est un homomorphisme. Nous pouvons ainsi appliquer le théorème 5.3 et conclure que l'extension centrale E est isomorphe à l'extension $A \times G$ munie de l'opération $*_{f_E}$.

En fait, il y a une structure de groupe sur les classes d'extensions qui fait que cette bijection est un isomorphisme de groupes, mais les détails vont au delà des notions abordées dans cet article.

6 La cohomologie des groupes cycliques

Dans cette section, pour la simplicité, on travaille avec les groupes $A = \mathbb{Z}_m$ et $G = \mathbb{Z}_n$. Nous travaillerons donc avec des suites exactes courtes de la forme suivante :

$$0 \longrightarrow \mathbb{Z}_m \xrightarrow{i} E \xrightarrow{\pi} \mathbb{Z}_n \longrightarrow 0.$$

Proposition 6.1. *Soit τ le plus grand commun diviseur de m et n . Il existe τ choix d'homomorphismes $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$.*

Démonstration. Notons par \bar{k} la classe de $k \in \mathbb{Z}$ dans \mathbb{Z}_n . Comme $\bar{1}$ est le générateur de \mathbb{Z}_n , le choix de $\phi(\bar{1}) = a \in \mathbb{Z}_m$ détermine toutes les valeurs de ϕ . Considérons a comme entier entre 0 et $m-1$, et voyons quels choix de a donnent des homomorphismes ϕ .

Comme $\phi(0) = \phi(n \times \bar{1}) = n \times a$, on a que $na \equiv 0 \pmod{m}$. Il suit qu'il existe $b \in \mathbb{N}$ tel que $na = mb$, et donc $\frac{n}{\tau}a = \frac{m}{\tau}b$. Comme $\frac{n}{\tau}$ et $\frac{m}{\tau}$ sont copremiers, on voit que $\frac{m}{\tau}$ divise a et donc qu'il existe un $j \in \{0, 1, \dots, \tau-1\}$ tel que $a = j\frac{m}{\tau}$. Il y a donc τ possibilités de choix pour a . \square

Proposition 6.2. *Soit τ le plus grand commun diviseur de m et n . Alors la cardinalité de $B^2(\mathbb{Z}_n, \mathbb{Z}_m)$ est donnée par*

$$|B^2(\mathbb{Z}_n, \mathbb{Z}_m)| = \frac{m^{n-1}}{\tau}.$$

Démonstration. Soit $\delta : C^1(\mathbb{Z}_n, \mathbb{Z}_m) \rightarrow B^2(\mathbb{Z}_n, \mathbb{Z}_m)$ l'homomorphisme $\delta(\phi) = d\phi$. Cette fonction est surjective par définition de $B^2(\mathbb{Z}_n, \mathbb{Z}_m)$. Selon le premier théorème d'isomorphisme on a que $B^2(\mathbb{Z}_n, \mathbb{Z}_m) \cong C^1(\mathbb{Z}_n, \mathbb{Z}_m)/\ker(\delta)$. On a donc que $|B^2(\mathbb{Z}_n, \mathbb{Z}_m)| = |C^1(\mathbb{Z}_n, \mathbb{Z}_m)|/|\ker\delta|$, et il nous reste à compter les éléments de $C^1(\mathbb{Z}_n, \mathbb{Z}_m)$ et de $\ker\delta$.

Premièrement, on voit que $\ker\delta = \{\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m \mid d\phi = 0\} = Z^1(\mathbb{Z}_n, \mathbb{Z}_m)$. La proposition 6.1 nous permet de conclure que $|Z^1(\mathbb{Z}_n, \mathbb{Z}_m)| = \tau$.

Finalement, les éléments de $C^1(\mathbb{Z}_n, \mathbb{Z}_m)$ sont des fonctions $\phi : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$ avec $\phi(0) = 0$. Pour chacun des $n - 1$ éléments non nuls de \mathbb{Z}_n , on a un choix pour son image sous ϕ dans \mathbb{Z}_m . Il suit que $|C^1(\mathbb{Z}_n, \mathbb{Z}_m)| = m^{n-1}$. \square

Objectif. Notre but est de construire explicitement chaque extension, à isomorphisme près. On voit qu'il suffit de donner un représentant $f \in Z^2(\mathbb{Z}_n, \mathbb{Z}_m)$ de chaque élément de $Z^2(\mathbb{Z}_n, \mathbb{Z}_m)/B^2(\mathbb{Z}_n, \mathbb{Z}_m)$; l'extension correspondante serait $(A \times G, *_f)$.

Lemme 6.3. *Soit $f : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_m$, un cocycle normalisé, alors $f(i, 1) = f(1, i)$ pour tout $i \in \mathbb{Z}_n$.*

Remarque . Parce qu'on utilise la notation additive, la condition de normalisation nous donne que $f(i, 0) = 0_{\mathbb{Z}_m}$, mais nous dit rien au sujet de $f(i, 1)$.

Démonstration. Pour $i = 1$ on a bien sûr que $f(1, 1) = f(1, 1)$. Supposons que l'égalité est vraie pour un $i \geq 1$ et montrons qu'elle est également vraie pour $i + 1$. En prenant le triplet $(1, i, 1)$ la définition du cocycle nous donne l'égalité $f(i, 1) + f(1, i + 1) = f(i + 1, 1) + f(1, i)$. Or, comme $f(i, 1) = f(1, i)$, il en suit que $f(i + 1, 1) = f(1, i + 1)$. On peut donc conclure que $f(i, 1) = f(1, i)$ pour tout $i \in \mathbb{Z}_n$. \square

Proposition 6.4. *Chaque cocycle normalisé f est déterminé par ses valeurs $f(1, k) \in \mathbb{Z}_m, 0 \leq k \leq n$. Plus précisément, pour $i, j \in \{0, \dots, n - 1\}$ on a*

$$f(i, j) = \sum_{k=i}^{i+j-1} f(1, k) - \sum_{k=1}^{j-1} f(1, k). \quad (9)$$

Démonstration. Démontrons cette proposition par une double récurrence.

Commençons avec le cas $i = 1$. On a $f(1, j) = \sum_{k=1}^j f(1, k) - \sum_{k=1}^{j-1} f(1, k)$ par définition, pour chaque $j \in \mathbb{Z}_n$.

Supposons que le résultat est vrai pour $i \geq 1$ et pour chaque $j \geq 1$. On veut démontrer que c'est aussi vrai pour $i + 1$ et pour chaque j . On fera donc une récurrence sur j .

Si $j = 1$, le côté droit de (8) devient $\sum_{k=i+1}^{i+1} f(1, k) = f(1, i + 1)$. On sait que $f(1, i + 1) = f(i + 1, 1)$ selon le lemme 6.3. On voit donc que la formule est vraie pour $(i + 1, 1)$. Supposons que c'est vrai pour $(i + 1, j)$; on va le montrer pour $(i + 1, j + 1)$.

En vérifiant la condition pour être un cocycle avec les éléments $(i + 1, j, 1)$, on obtient $f(j,1) + f(i + 1, j + 1) = f(i + j + 1, 1) + f(i + 1, j)$. En utilisant nos hypothèses on obtient

$$\begin{aligned}
f(i + 1, j + 1) &= f(i + 1, j) + f(i + j + 1, 1) - f(j, 1) \\
&= \left(\sum_{k=i+1}^{i+j} f(1, k) - \sum_{k=1}^{j-1} f(1, k) \right) + \left(\sum_{k=i+j+1}^{i+j+1} f(1, k) - \sum_{k=1}^0 f(1, k) \right) \\
&\quad - \left(\sum_{k=j}^j f(1, k) - \sum_{k=1}^0 f(1, k) \right) \\
&= \sum_{k=i+1}^{i+j} f(1, k) - \sum_{k=1}^{j-1} f(1, k) + \sum_{k=i+j+1}^{i+j+1} f(1, k) - \sum_{k=j}^j f(1, k) \\
&= \sum_{k=i+1}^{i+j+1} f(1, k) - \sum_{k=1}^j f(1, k).
\end{aligned}$$

On peut conclure que $f(i, j) = \sum_{k=i}^{i+j-1} f(1, k) - \sum_{k=1}^{j-1} f(1, k)$. \square

Lemme 6.5. Si $i + j \geq n$, on obtient $f(i, j) = \sum_{k=i}^{n-1} f(1, k) - \sum_{k=i+j-n}^{j-1} f(1, k)$.

Démonstration. On obtient

$$\begin{aligned}
f(i, j) &= \sum_{k=i}^{i+j-1} f(1, k) - \sum_{k=1}^{j-1} f(1, k) \\
&= \sum_{k=i}^{n-1} f(1, k) + \sum_{k=n}^{i+j-1} f(1, k) - \sum_{k=1}^{j-1} f(1, k) \\
&= \sum_{k=i}^{n-1} f(1, k) + \sum_{k=1}^{i+j-n-1} f(1, k) - \sum_{k=1}^{j-1} f(1, k) \\
&= \sum_{k=i}^{n-1} f(1, k) - \sum_{k=i+j-n}^{j-1} f(1, k).
\end{aligned}$$

\square

Voici une réciproque de la proposition 6.4.

Proposition 6.6. Étant donnée une liste de valeurs $f(1, k), k \geq 1$, la formule (8) définit toujours un cocycle normalisé.

Démonstration. Avant de commencer, définissons une notation qui sera utilisée lors de la démonstration. Soient $g + n\mathbb{Z}, h + n\mathbb{Z} \in \mathbb{Z}_n$ avec $g, h \in \{0, \dots, n-1\}$; on note

$$\lfloor g + h \rfloor = \begin{cases} g + h & \text{si } g + h < n \\ g + h - n & \text{si } g + h \geq n. \end{cases}$$

On a tout d'abord besoin de démontrer la condition de cocycle pour $g + n\mathbb{Z}, h + n\mathbb{Z}, k + n\mathbb{Z} \in \mathbb{Z}_n$.

D'un côté,

$$\begin{aligned} f(h,k) + f(g,h+k) &= \sum_{l=h}^{[h+k-1]} f(1,l) - \sum_{l=1}^{k-1} f(1,l) + \sum_{l=g}^{[g+h+k-1]} f(1,l) - \sum_{l=1}^{[h+k-1]} f(1,l) \\ &= \sum_{l=g}^{[g+h+k-1]} f(1,l) - \sum_{l=1}^{k-1} f(1,l) - \sum_{l=1}^{h-1} f(1,l). \end{aligned}$$

De l'autre côté ,

$$\begin{aligned} f(g+h,k) + f(g,h) &= \sum_{l=g}^{[g+h-1]} f(1,l) - \sum_{l=1}^{h-1} f(1,l) + \sum_{l=[g+h]}^{[g+h+k-1]} f(1,l) - \sum_{l=1}^{k-1} f(1,l) \\ &= \sum_{l=g}^{[g+h+k-1]} f(1,l) - \sum_{l=1}^{h-1} f(1,l) - \sum_{l=1}^{k-1} f(1,l). \end{aligned}$$

On observe que $f(h,k) + f(g,h+k) = f(g+h,k) + f(g,h)$ comme désiré.

Vérifions maintenant la condition de normalisation.

$$f(0,j) = \sum_{k=0}^{j-1} f(1,k) - \sum_{k=1}^{j-1} f(1,k) = f(1,0) = \sum_{k=1}^0 f(1,k) - \sum_{k=1}^{-1} f(1,k) = 0.$$

On peut donc conclure qu'étant donnée une liste de valeurs $f(1,k), k \geq 1$, la formule (8) définit toujours un cocycle normalisé comme désiré. \square

Proposition 6.7. *La cardinalité du groupe $Z^2(\mathbb{Z}_n, \mathbb{Z}_m)$ est m^{n-1} .*

$$|Z^2(\mathbb{Z}_n, \mathbb{Z}_m)| = m^{n-1}.$$

Démonstration. On a démontré précédemment qu'il est possible d'exprimer tout cocycle en spécifiant les valeurs $f(1,k) \in \mathbb{Z}_m$ pour $k = 1, \dots, n-1$. Le nombre de cocycles différents dépend donc des différentes combinaisons de $f(1,k)$ possibles. Chaque $f(1,k)$ a m valeurs possibles. On a ainsi m^{n-1} cocycles différents. \square

Proposition 6.8. *La cardinalité du groupe $H^2(\mathbb{Z}_n, \mathbb{Z}_m)$ est le plus grand commun diviseur de m et n noté τ .*

$$|H^2(\mathbb{Z}_n, \mathbb{Z}_m)| = \tau.$$

Démonstration. On sait que

$$|H^2(\mathbb{Z}_n, \mathbb{Z}_m)| = |Z^2(\mathbb{Z}_n, \mathbb{Z}_m)| / |B^2(\mathbb{Z}_n, \mathbb{Z}_m)| = \frac{m^{n-1}}{\frac{m^{n-1}}{\tau}} = \tau,$$

par les propositions 6.2 et 6.8. \square

Proposition 6.9. Soit $a \in \mathbb{Z}_m$. Définissons $f_a : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ par

$$f_a(i,j) = \begin{cases} 0 & \text{si } i + j < n \\ a & \text{si } i + j \geq n \end{cases} \quad \text{pour } (i + n\mathbb{Z}, j + n\mathbb{Z}) \text{ avec } i, j \in \{0, \dots, n-1\}.$$

Alors f_a est un cocycle normalisé.

Démonstration. Avant de commencer, définissons une notation qui sera utilisée lors de la démonstration. Soit $g + n\mathbb{Z}, h + n\mathbb{Z} \in \mathbb{Z}_n$, on note $\overline{g+h}$ le résultat de l'addition dans \mathbb{Z}_n . Ainsi, $\overline{g+h} = g + h + n\mathbb{Z}$. Commençons maintenant la démonstration.

On démontre que la condition de cocycle est vérifiée pour chaque triplet (g, h, k) , avec $g, h, k \in \{0, \dots, n-1\}$. On considère quatre cas différents selon les valeurs de $h+k$ et $g+h$.

- **cas 1 : $h+k \geq n$ et $g+h < n$.** On a d'un côté

$$f(h,k) + f(g, \overline{h+k}) = a + 0 = a.$$

En effet, $f(h,k) = a$, car $h+k \geq n$. De plus, comme $g+h < n$ et que $\overline{h+k} < h$ car $h+k > n$, on peut conclure que $g + \overline{h+k} < n$ ce qui nous confirme que $f(g, \overline{h+k}) = 0$.

De l'autre côté,

$$f(\overline{g+h}, k) + f(g, h) = a + 0 = a.$$

En effet, $f(g, h) = 0$, car $g+h < n$. De plus, comme $g+h < n$ alors $\overline{g+h} = g+h$. Ainsi, comme $k \geq 0$ on a que $\overline{g+h+k} = g+h+k \geq h+k \geq n$, ce qui nous confirme que $f(\overline{g+h}, k) = a$.

On a donc $f(h,k) + f(g, \overline{h+k}) = f(\overline{g+h}, k) + f(g, h)$.

- **cas 2 : $h+k < n$ et $g+h \geq n$.** La preuve sera la même que pour le cas 1.

- **cas 3 : $h+k < n$ et $g+h < n$.** On a d'un côté

$$f(h,k) + f(g, \overline{h+k}) = 0 + f(g, \overline{h+k}).$$

De l'autre côté on obtient

$$f(\overline{g+h}, k) + f(g, h) = f(\overline{g+h}, k) + 0.$$

Comme $h+k < n$, $\overline{h+k} = h+k$. Ainsi, $g + \overline{h+k} = g+h+k$. Par le même argument, $\overline{g+h+k} = g+h+k$. On a donc que $f(g, \overline{h+k}) = f(\overline{g+h}, k)$. On obtient donc la confirmation que $f(h,k) + f(g, \overline{h+k}) = f(\overline{g+h}, k) + f(g, h)$.

- **cas 4 : $h + k > n$ et $g + h > n$.** On a d'un côté

$$f(h,k) + f(g, \overline{h+k}) = a + f(g, \overline{h+k}).$$

De l'autre côté on a

$$f(\overline{g+h}, k) + f(g, h) = f(\overline{g+h}, k) + a.$$

Comme $h + k > n$ on a que $g + \overline{h+k} = g + h + k - n$. Par le même argument on a que $\overline{g+h} + k = g + h - n + k = g + h + k - n$ car l'addition est commutative dans \mathbb{Z}_n . Ainsi, on a $f(g, \overline{h+k}) = f(\overline{g+h}, k)$, ce qui nous permet de conclure que $f(h,k) + f(g, \overline{h+k}) = f(\overline{g+h}, k) + f(g, h)$.

On a donc effectivement que f_a est un cocycle et il est clair que celui-ci est normalisé. \square

Remarque 6.10. Soit f_a et $f_b : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ définies comme dans la proposition 6.10. On observe que

$$f_a(i,j) - f_b(i,j) = \begin{cases} 0 & \text{si } i + j < n \\ a - b & \text{si } i + j \geq n \end{cases} = f_{a-b}(i,j).$$

Note. On a donc défini une collection de cocycles $\{f_a\}$ déterminant des extensions centrales de \mathbb{Z}_n par \mathbb{Z}_m . On veut savoir quand deux de ces cocycles déterminent la même extension, à isomorphisme près. C'est-à-dire, on veut savoir quand $f_a - f_b = f_{a-b}$ est un élément de $B^2(\mathbb{Z}_n, \mathbb{Z}_m)$.

Théorème 6.11. *Le cocycle $f_a - f_b = f_{a-b}$ est un cobord si et seulement si $a - b$ est divisible par τ , le plus grand commun diviseur de m et n .*

Démonstration. Supposons que $f_a - f_b$ est un cobord. Alors il existe $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ tel que $f_{a-b} = d\phi$. En particulier, si $i + j < n$, $\phi(i)\phi(j) = \phi(i+j)$.

Supposons que $\phi(1) = \alpha$. On a alors que $\phi(2) = \phi(1) + \phi(1) = \alpha + \alpha = 2\alpha$ (si $n > 2$). On utilise la même logique pour tout les éléments de \mathbb{Z}_n jusqu'à $\phi(n-1) = (n-1)\alpha$.

Maintenant, si $i + j \geq n$, on a que $\phi(i) + \phi(j) - \phi(\overline{i+j}) = \phi(i) + \phi(j) - \phi(i+j-n) = a - b$. Il faut donc que $i\alpha + j\alpha - (i+j-n)\alpha = a - b$. En simplifiant cette équation, on obtient $n\alpha = a - b \pmod{m}$.

Cela implique qu'il existe un $k \in \mathbb{N}$ tel que $n\alpha = a - b + mk$ et donc que $a - b = n\alpha + ml$ où $l = -k$. Or, comme τ est le $\text{pgcd}(n, m)$, on a que $a - b = \tau \frac{n}{\tau} \alpha + \tau \frac{m}{\tau} k = \tau (\frac{n}{\tau} \alpha + \frac{m}{\tau} k)$. On peut ainsi conclure que $a - b$ est divisible par τ .

Maintenant supposons que $a - b$ est divisible par τ . Il existe donc un $k \in \mathbb{N}$ tel que $\tau k = a - b$. On peut donc réécrire la fonction $f_a - f_b$ comme

$$f_a(i,j) - f_b(i,j) = \begin{cases} 0 & \text{si } i + j < n \\ \tau k & \text{si } i + j \geq n. \end{cases}$$

Comme $\tau = \text{pgcd}(n, m)$, il existe $\alpha, c \in \mathbb{N}$ tel que $n\alpha + cm = \tau k$. On cherche donc un ϕ tel que si $i + j < n$ alors $\phi(i) + \phi(j) = \phi(i + j)$.

Supposons que $\phi(1) = \alpha$. On pose $\phi(2) = \phi(1) + \phi(1) = \alpha + \alpha = 2\alpha$ et ainsi de suite jusqu'à obtenir $\phi(n - 1) = (n - 1)\alpha$. Pour $i + j \geq n$ on pose $\phi(i) + \phi(j) - \phi(\overline{i + j}) = \phi(i) + \phi(j) - \phi(i + j - n) = n\alpha$. On obtiendra donc que $\phi(i) + \phi(j) - \phi(i + j - n) = n\alpha = n\alpha + cm = \tau k = f_a(i, j) - f_b(i, j)$.

Il en suit que, pour ce ϕ , on a $f_a - f_b = d\phi$. On peut donc conclure comme désiré que le cocycle $f_a - f_b = f_{a-b}$ est un cobord. \square

Note. On sait maintenant que la collection $\{f_0, \dots, f_{\tau-1}\}$ donne lieu à τ extensions non-isomorphes de \mathbb{Z}_n par \mathbb{Z}_m . On prétend que chaque extension est isomorphe à une de ces extensions. Il suffit de démontrer que chaque cocycle f est équivalent à un f_a pour $a \in \{0, \dots, \tau - 1\}$.

Proposition 6.12. *Chaque cocycle $f : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ est équivalent à un f_a défini à la proposition 6.10, pour une unique valeur de $a \in \{0, \dots, \tau - 1\}$, où τ est le plus grand commun diviseur de m et n .*

Démonstration. On cherche $a \in \mathbb{Z}_m$ et $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ tel que $f - f_a = d\phi$.
On aura

$$f(i, j) - f_a(i, j) = \begin{cases} f(i, j) & \text{si } i + j < n \\ f(i, j) - a & \text{si } i + j \geq n. \end{cases}$$

On sait qu'il existe $a \in \{0, \dots, n-1\}$ et qu'il existe $\beta \in \mathbb{Z}$ tels que $\sum_{k=1}^{n-1} f(1, k) = n\beta + a$. On obtient donc que $a = \sum_{k=1}^{n-1} f(1, k) - n\beta$.

Posons que $\phi(1) = \beta$. Pour que $\phi(1) + \phi(1) - \phi(2) = f(1, 1)$ on pose $\phi(2) = 2\beta - f(1, 1)$.

On utilise la même logique pour tout les éléments de \mathbb{Z}_n jusqu'à $\phi(n - 1) = (n - 1)\beta - \sum_{k=1}^{n-2} f(1, k)$.

Si $i + j < n$, on obtient

$$\begin{aligned} \phi(i) + \phi(j) - \phi(i + j) &= i\beta - \sum_{k=1}^{i-1} f(1, k) + j\beta - \sum_{k=1}^{j-1} f(1, k) - i\beta - j\beta + \sum_{k=1}^{i+j-1} f(1, k) \\ &= - \sum_{k=1}^{i-1} f(1, k) - \sum_{k=1}^{j-1} f(1, k) + \sum_{k=1}^{i+j-1} f(1, k) = \sum_{k=i}^{i+j-1} f(1, k) - \sum_{k=1}^{j-1} f(1, k) = f(i, j). \end{aligned}$$

Si $i + j \geq n$, on a

$$\begin{aligned}
\phi(i) + \phi(j) - \phi(i + j - n) &= i\beta - \sum_{k=1}^{i-1} f(1,k) + j\beta - \sum_{k=1}^{j-1} f(1,k) - i\beta - j\beta + n\beta \\
&\quad + \sum_{k=1}^{i+j-n-1} f(1,k) \\
&= n\beta - \sum_{k=i+j-n}^{j-1} f(1,k) - \sum_{k=1}^{i-1} f(1,k) \\
&= \sum_{k=i}^{n-1} f(1,k) - \sum_{k=i+j-n}^{j-1} f(1,k) - \sum_{k=1}^{n-1} f(1,k) + n\beta \\
&= \sum_{k=i}^{i+j-1} f(1,k) - \sum_{k=1}^{j-1} f(1,k) - \sum_{k=1}^{n-1} f(1,k) + n\beta \\
&= f(i,j) - a.
\end{aligned}$$

On vient ainsi de démontrer que $d\phi = f - f_a$. Ici on a prit $a \in \{0, \dots, n-1\}$, mais selon le théorème 6.11 on peut remplacer cette valeur de a par $a' \in \{0, \dots, \tau-1\}$ tel que $a - a'$ est divisible par τ . \square

7 Conclusion

On a donc réussi à démontrer que $H^2(\mathbb{Z}_n, \mathbb{Z}_m) \simeq \mathbb{Z}_\tau$ où τ est le plus grand commun diviseur de m et n . Ainsi, avec la suite exacte courte suivante :

$$0 \longrightarrow \mathbb{Z}_m \xrightarrow{i} E \xrightarrow{\pi} \mathbb{Z}_n \longrightarrow 0$$

on peut conclure que si m et n sont copremiers $H^2(\mathbb{Z}_n, \mathbb{Z}_m)$ ne contient qu'un seul élément soit l'extension triviale $\mathbb{Z}_n \times \mathbb{Z}_m$.

Il pourrait être intéressant dans le futur d'appliquer les différents concepts abordés dans cet article afin de définir la cohomologie de groupes non cycliques. Il serait aussi possible par la suite de définir ce que représente $H^3(G, A)$ et de l'étudier en utilisant les principes définis dans cet article en plus de présenter de nouveaux sujets pour en faciliter la compréhension.

Références

[Cor] David CORFIELD : cohomology in mathematics. <https://ncatlab.org/davidcorfield/show/cohomology+in+mathematics1>. 2012.

CLOÉ ALLARD
DÉPARTEMENT DE MATHÉMATIQUES, UNIVERSITÉ DE SHERBROOKE
Courriel: cloe.allard@USherbrooke.ca