

Chapitre 1 : Groupes

I Loi de composition interne

Définition : Soit E un ensemble. Une **loi de composition interne** sur E est une application $*$: $E \times E \rightarrow E$ qui à tout couple $(x, y) \in E \times E$ associe un élément $x * y \in E$.

Propriété : Associativité

$*$ est associative si $\forall x, y, z \in E, (x * y) * z = x * (y * z)$.

Propriété : Élément neutre

On dit que $e \in E$ est un élément neutre si $\forall x \in E, e * x = x * e = x$.

Remarque : L'élément neutre est unique. La démonstration découle du fait que si on prend deux éléments neutres e et e' , on a $e * e' = e$ et $e * e' = e'$, donc $e = e'$.

Propriété : Symétrique

Soient $a, b \in E$. On dit que b est symétrique (ou inverse, ou opposé) de a si $a * b = b * a = e$, où e est l'élément neutre.

Propriété : Commutativité

$*$ est commutative si $\forall x, y \in E, x * y = y * x$.

Vocabulaire : Notations typiques pour les lois de composition interne : $+$, \times , \cdot , \circ , etc.

II Notions de groupe

A Généralités

Définition : Soit G un ensemble muni d'une loi de composition interne $*$. On dit que $(G, *)$ est un **groupe** si les trois propriétés suivantes sont vérifiées :

- $*$ est associative.
- Il existe un élément neutre $e \in G$.
- Tout élément de G possède un symétrique dans G .

Si $*$ est en plus commutative, on dit que $(G, *)$ est un **groupe abélien**.

Exemple : Exemples de groupes :

- $(\mathbb{Z}, +)$: l'ensemble des entiers avec l'addition.
- (\mathbb{R}^*, \times) , (\mathbb{Q}^*, \times) , (\mathbb{C}^*, \times) : l'ensemble des réels, rationnels et complexes non nuls avec la multiplication.
- $(\{\text{bijections } X \rightarrow X \mid X \text{ est un ensemble}\}, \circ)$: l'ensemble des bijections d'un ensemble X dans lui-même avec la composition.

Contre-exemples de groupes :

- $(\mathbb{N}, +)$: l'ensemble des entiers naturels avec l'addition (pas d'élément neutre dans \mathbb{N}).

🗨 Vocabulaire : Systèmes de notations pour les groupes :

- Système additif : on note le groupe $(G, +)$, l'élément neutre est noté 0 et le symétrique de x est noté $-x$.
- Système multiplicatif : on note le groupe (G, \times) ou (G, \cdot) , l'élément neutre est noté 1 et le symétrique de x est noté x^{-1} .

Propriété : Produit de lois (admise)

Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. On définit une loi de composition interne sur $G_1 \times G_2$ par $*$:

$$(g_1, g_2) * (h_1, h_2) \mapsto (g_1 *_1 h_1, g_2 *_2 h_2)$$

pour tout $(x_1, y_1), (x_2, y_2) \in G_1 \times G_2$. Alors $(G_1 \times G_2, *)$ est un groupe.

Proposition : Produit cartésien

Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. On définit une loi de composition interne sur $G_1 \times G_2$ par $*$ comme susdit. Alors l'ensemble $(G_1 \times G_2, *)$ est un groupe, appelé le **groupe produit** de $(G_1, *_1)$ et $(G_2, *_2)$.

Preuve:

- **Associativité** : Soient $(g_1, g_2), (h_1, h_2), (k_1, k_2) \in G_1 \times G_2$.

$$\begin{aligned} ((g_1, g_2) * (h_1, h_2)) * (k_1, k_2) &= (g_1 *_1 h_1, g_2 *_2 h_2) * (k_1, k_2) \\ &= ((g_1 *_1 h_1) *_1 k_1, (g_2 *_2 h_2) *_2 k_2) \\ &= (g_1 *_1 (h_1 *_1 k_1), g_2 *_2 (h_2 *_2 k_2)) \quad (\text{par associativité dans } G_1 \text{ et } G_2) \\ &= (g_1, g_2) * (h_1 *_1 k_1, h_2 *_2 k_2) \\ &= (g_1, g_2) * ((h_1, h_2) * (k_1, k_2)) \end{aligned}$$

- **Élément neutre** : Soient e_1 et e_2 les éléments neutres de G_1 et G_2 respectivement. Alors (e_1, e_2) est l'élément neutre de $G_1 \times G_2$ car pour tout $(g_1, g_2) \in G_1 \times G_2$, $(e_1, e_2) * (g_1, g_2) = (e_1 *_1 g_1, e_2 *_2 g_2) = (g_1, g_2)$ et $(g_1, g_2) * (e_1, e_2) = (g_1 *_1 e_1, g_2 *_2 e_2) = (g_1, g_2)$.
- **Symétrique** : Soit $(g_1, g_2) \in G_1 \times G_2$. Comme G_1 et G_2 sont des groupes, il existe $g_1^{-1} \in G_1$ et $g_2^{-1} \in G_2$ tels que $g_1 *_1 g_1^{-1} = e_1$ et $g_2 *_2 g_2^{-1} = e_2$. Alors le symétrique de (g_1, g_2) dans $G_1 \times G_2$ est (g_1^{-1}, g_2^{-1}) car :

Propriété : Produit cartésien et commutativité (admise)

Si $(G_1, *_1)$ et $(G_2, *_2)$ sont des groupes abéliens, alors leur produit cartésien $(G_1 \times G_2, *)$ est aussi un groupe abélien.

📌 **Remarque** : On pourrait prendre plus de deux groupes et faire le produit cartésien de plusieurs groupes.

B Sous-groupes

Définition : Soit (G, \cdot) un groupe (on utilise la notation multiplicative, mais cela fonctionne aussi en notation additive). Un **sous-groupe** de G est un sous-ensemble $H \subseteq G$ tel que (H, \cdot) est lui-même un groupe.

Propriété : Lien entre sous-groupe et groupe (admise)

Un sous-groupe est lui-même un groupe pour la même loi de composition interne que le groupe dont il est issu.

💡 **Exemple** : $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.

Proposition : Sous-groupe

Soit (H, \cdot) un sous-groupe de $(G, \cdot) \Leftrightarrow$

- $H \neq \emptyset : 1$
- $\forall h, h' \in H, h \cdot h' \in H$ (stabilité par la loi) : 2
- $\forall h \in H, \exists h^{-1} \in H$ (stabilité par l'inverse) : 3

Preuve:

- \Rightarrow : Si H est un sous-groupe de G , alors par définition de groupe, H satisfait 1, 2 et 3.
- \Leftarrow : Supposons que H vérifie les trois conditions. Nous devons montrer que (H, \cdot) est un groupe.
 - *Associativité* : La loi de composition interne sur H est la même que celle sur G , donc elle est associative.
 - *Élément neutre* : Soit e l'élément neutre de G . Comme H est non vide, $\exists h_0 \in H$ et par la condition 3, $h_0^{-1} \in H$. Par la définition de l'élément neutre dans G , on a $h_0 \cdot h_0^{-1} = e$. Donc $e \in H$.
 - *Symétrique* : Par la condition 3, pour tout $h \in H$, son inverse h^{-1} appartient à H .

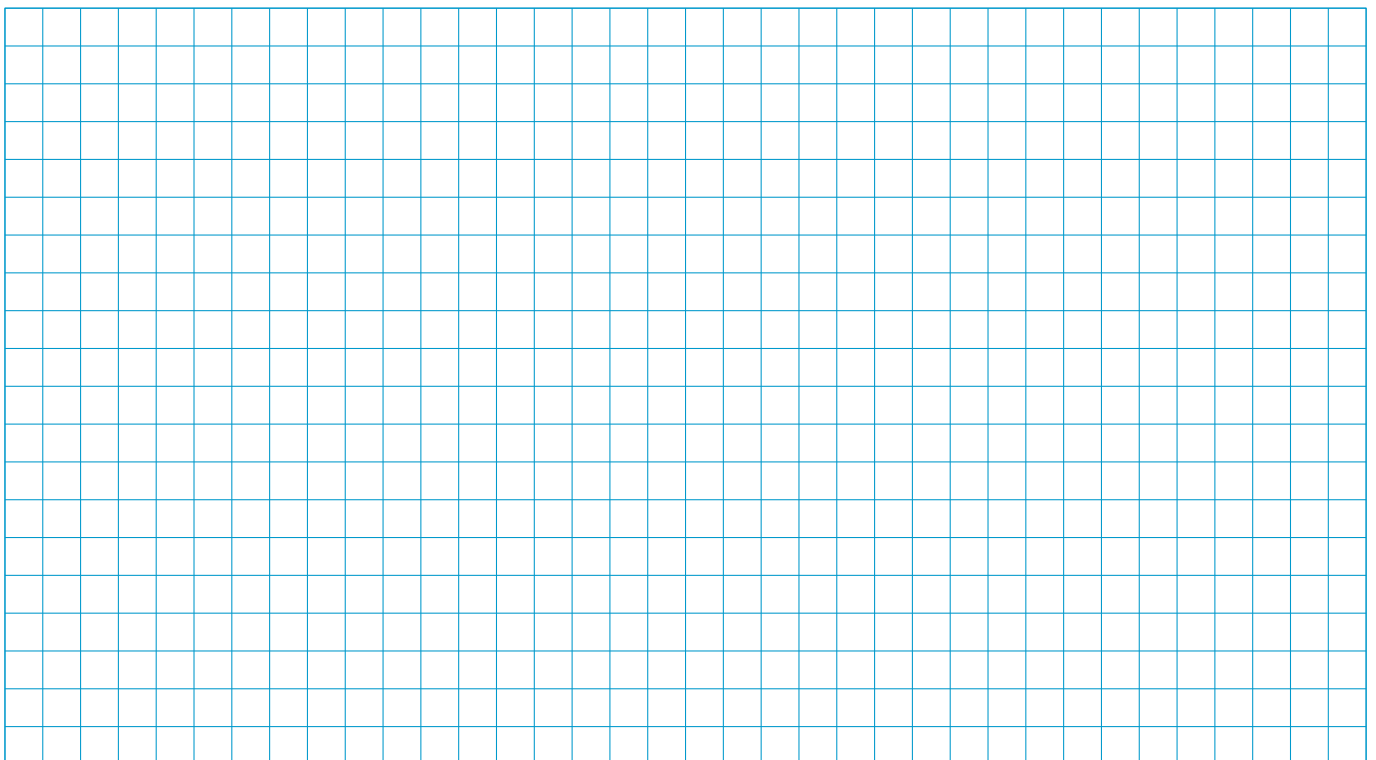
Ainsi, toutes les propriétés d'un groupe sont satisfaites pour H , donc H est un sous-groupe de G .

Exemple :

- (G, \cdot) est un sous-groupe de lui-même.
- $\{1\}$ est un sous-groupe de G .
- $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.

Proposition : Intersection

Soit $(H_i)_{i \in I}$ une famille de sous-groupes de (G, \cdot) . Alors l'intersection $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G .

Preuve:

Corollaire : Sous-groupe engendré

Soit $X \subseteq G$. Considérons $H = \bigcap_{i \in I} H_i$. C'est un **sous-groupe de G engendré par X** .

Définition : Soit $g \in G$.

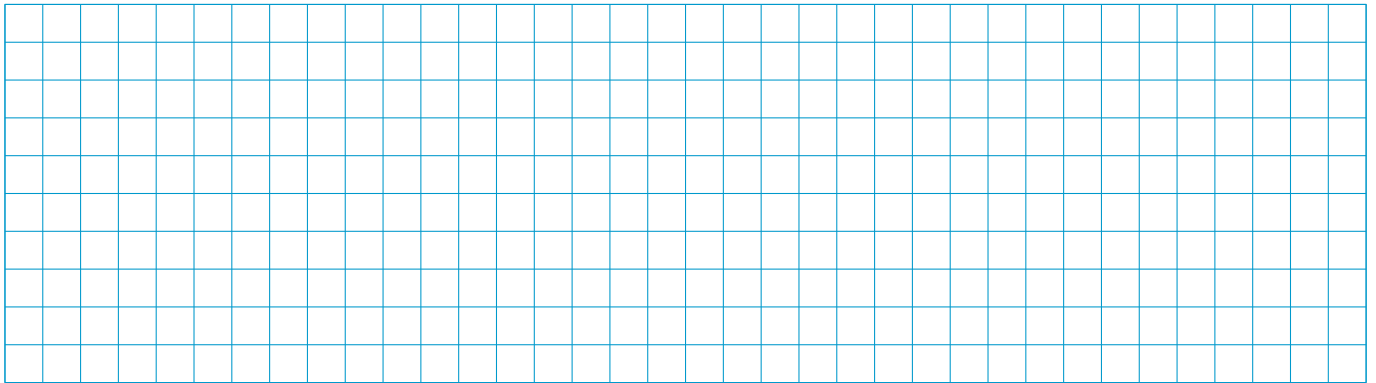
On a posé pour $n \in \mathbb{Z}$, $g^n = \underbrace{g \cdot g \cdot \dots \cdot g}_{n \text{ fois}}$ si $n > 0$, $g^0 = e$ (élément neutre) et $g^n = \underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{-n \text{ fois}}$ si $n < 0$.

On pose $g^{\mathbb{Z}} = \{g^n \mid n \in \mathbb{Z}\}$: c'est l'**ensemble des itérés** de g .

Proposition : Sous-groupe engendré

On a que $g^{\mathbb{Z}}$ est un sous-groupe de G engendré par g .

Preuve:



Remarque : En notation additive, l'ensemble des itérés de g est noté $\mathbb{Z}g = \{ng \mid n \in \mathbb{Z}\}$.

Définition : Si $G = g^{\mathbb{Z}}$, on dit que G est monogène et que g est un générateur de G .

Exemple : \mathbb{Z} est monogène et engendré par 1.

Vocabulaire : Un groupe est cyclique s'il est fini et monogène.

Définition : Si le sous-groupe engendré par X est G , on dit que X est un système de générateurs de G .

C Sous-groupes de $(\mathbb{Z}, +)$

Proposition : (admis)

Soit $k \in \mathbb{Z}$. On pose $k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\}$. On a que $k\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ engendré par k .

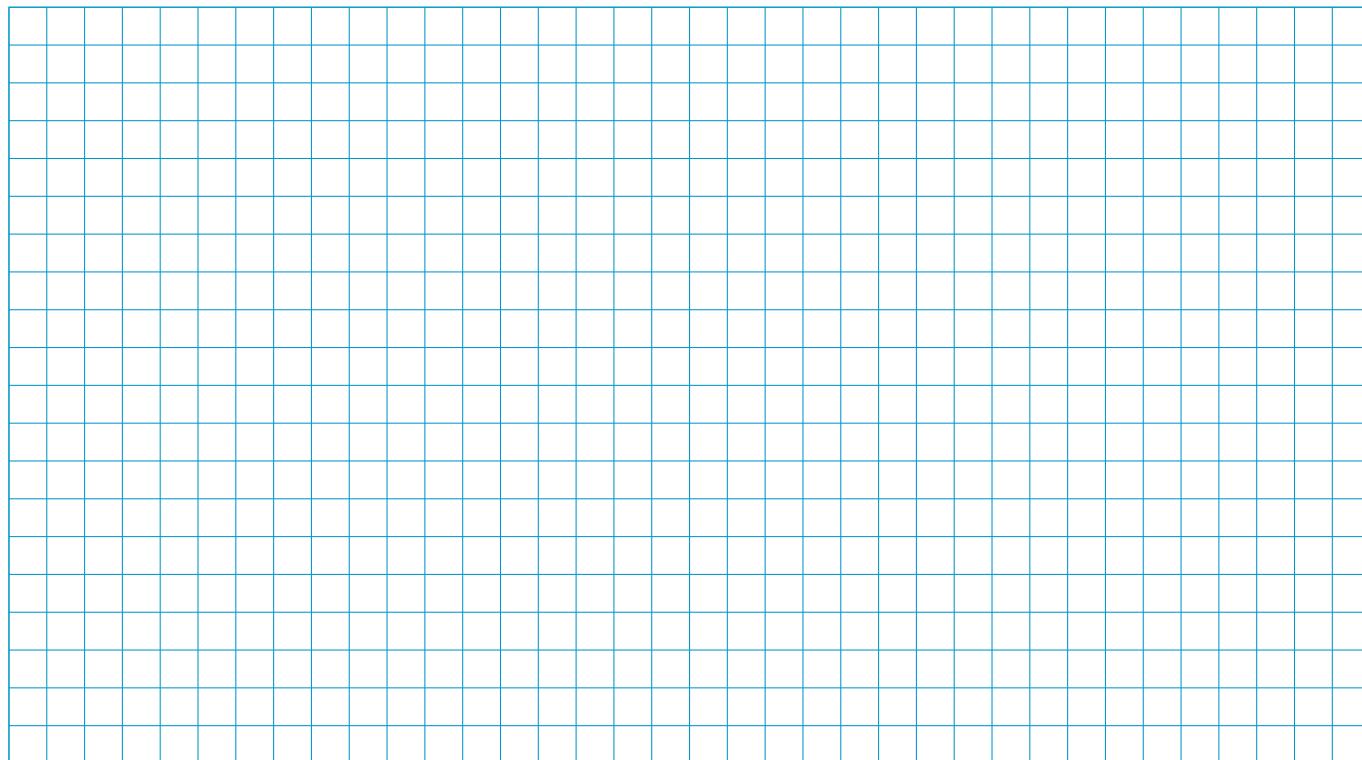
Remarque : $k\mathbb{Z} = \langle k \rangle$ pour la loi +.

Théorème :

Soit $(H, +)$ un sous-groupe de $(\mathbb{Z}, +)$. Alors $\exists! k \in \mathbb{N}$ tel que $H = k\mathbb{Z}$.

Remarque : Cela veut dire que tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $k\mathbb{Z}$ pour un certain $k \in \mathbb{N}$.

Preuve:



III Relations d'équivalence et classes d'équivalence

Définition : Soit E un ensemble. Soit R (un sous-ensemble de $E \times E$) une relation. On pose $xRy \Leftrightarrow (x, y) \in R$ et on dit que x est en relation avec y par R .

Propriété : Relation d'équivalence (*admise*)

Soit R une relation sur E . On dit que R est une **relation d'équivalence** si :

- R est réflexive : $\forall x \in E, xRx$.
- R est symétrique : $\forall x, y \in E, xRy \Rightarrow yRx$.
- R est transitive : $\forall x, y, z \in E, (xRy \wedge yRz) \Rightarrow xRz$.

Définition : Soit R une relation d'équivalence sur E . Pour $x \in E$, on appelle **classe d'équivalence** de x et on note \bar{x} (ou $[x]_R$ ou $x + k\mathbb{Z}$) l'ensemble $\{y \in E \mid xRy\}$.

Proposition : (*admis*)

Si deux classes d'équivalence ont un élément en commun, alors elles sont égales.

Définition : Soit $(F_i)_{i \in I}$ une famille de parties de E . On dit que cette famille est une **partition** de E si :

- $E = \bigcup_{i \in I} F_i$ (la réunion des F_i est E).
- $\forall i, j \in I, i \neq j \Rightarrow F_i \cap F_j = \emptyset$ (les F_i sont deux à deux disjointes).

Illustration : On peut reprendre l'idée intuitive d'un univers en probabilités :

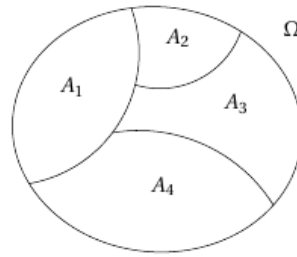


Figure 1: Partition de Ω en A_1, A_2, A_3, A_4

Proposition :

Les classes d'équivalence d'une relation d'équivalence R forment une partition de E .

Preuve:

- Les classes sont non vides.
- Deux classes différentes sont disjointes (elles n'ont pas d'élément en commun).
- L'union des classes est E . \square

Proposition :

Soit $(F_i)_{i \in I}$ une partition de E . On peut définir une relation d'équivalence R sur E par : $xRy \Leftrightarrow \exists i \in I : x, y \in F_i$. Alors R est d'équivalence.

Preuve:

- **Réflexivité :** Soit $x \in E$. Par définition de partition, $\exists i \in I$ tel que $x \in F_i$. Donc xRx .
- **Symétrie :** Soient $x, y \in E$ tels que xRy . Par définition de R , $\exists i \in I$ tel que $x, y \in F_i$. Donc $y, x \in F_i$ et ainsi yRx .
- **Transitivité :** Soient $x, y, z \in E$ tels que xRy et yRz . Par définition de R , $\exists i, j \in I$ tels que $x, y \in F_i$ et $y, z \in F_j$. Comme $y \in F_i$ et $y \in F_j$, on a $F_i \cap F_j \neq \emptyset$. Par définition de partition, on en déduit que $i = j$. Donc $x, z \in F_i$ et ainsi xRz . \square

Définition : Soit R une relation d'équivalence sur E .

On appelle **ensemble quotient** de E par R et on note E/R l'ensemble des classes d'équivalence de R .
i.e. $E/R = \{\bar{x} \mid x \in E\}$.

Définition : Soit $f : E \rightarrow F$ une application.

On dit que f **passe au quotient** si $\forall x, y \in E$ avec $xRy \Rightarrow f(x) = f(y)$.

Définition : Soit $S \subseteq E$. On dit que S est un **système de représentants** pour R si pour toute classe C de R , il existe un unique élément dans $S \cap C$.

IV Congruences

A Rappels et généralités

Définition : Soit $k \in \mathbb{Z}$. On pose la relation \equiv_k sur \mathbb{Z} définie par : $x \equiv_k y \Leftrightarrow y - x \in k\mathbb{Z}$ (i.e. k divise $y - x$). On écrit aussi $x \equiv y[k]$. i.e. $\exists n \in \mathbb{Z}, y - x = kn$.

💬 **Vocabulaire :** \equiv_k est appelée **congruence modulo k** .

Proposition : Equivalence

\equiv_k est une relation d'équivalence sur \mathbb{Z} .

Preuve:

[illegible]

Proposition : $\mathbb{Z}/k\mathbb{Z}$

On a que $\mathbb{Z}/\equiv_k = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{k-1}\}$ noté $\mathbb{Z}/k\mathbb{Z}$.

En particulier, $\{0, 1, 2, \dots, k-1\}$ est un système de représentants pour \equiv_k .

Preuve:

Soit $x \in \mathbb{Z}$.

Par la division euclidienne, $\exists!(q, r) \in \mathbb{Z} \times \{0, 1, 2, \dots, k-1\}$ tel que $x = kq + r$. Donc $x - r = kq \in k\mathbb{Z}$ et ainsi $x \equiv_k r$.

Il reste à voir que $\bar{i} \neq \bar{j}$ si $i \neq j$ avec $i, j \in \{0, 1, 2, \dots, k-1\}$.

En effet, $i - j \in \{1 - k, 2 - k, \dots, -1, 1, 2, \dots, k - 1\}$ et $i - j \neq 0$.

Donc $i - j \notin k\mathbb{Z}$ et ainsi $i \not\equiv_k j$ donc $\bar{i} \neq \bar{j}$. \square

Lemme :

Soient $x, y \in \mathbb{Z}$.

Considérons $\overline{x+y} \in \mathbb{Z}/k\mathbb{Z}$. Alors $\overline{x+y}$ ne dépend que de \overline{x} et \overline{y} .

Autrement dit : $\mathbb{Z} \rightarrow \mathbb{Z}/k\mathbb{Z}, x \mapsto \overline{x+y}$ et $y \mapsto \overline{x+y}$ passent au quotient.

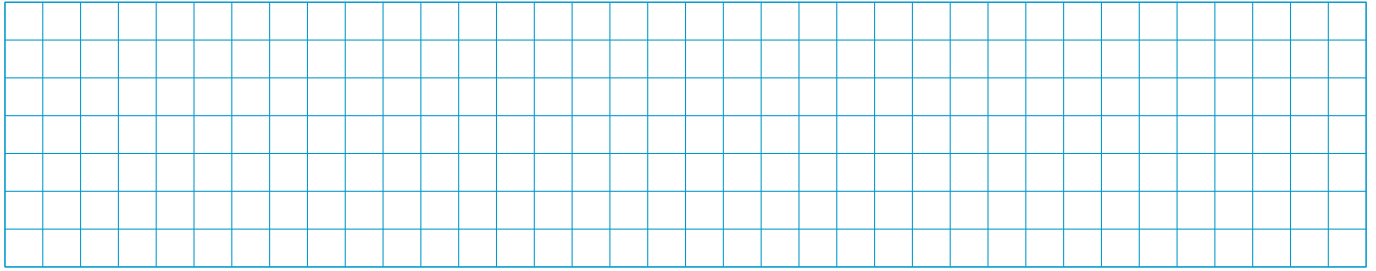
Preuve:

[illegible]

Théorème : $\mathbb{Z}/k\mathbb{Z}$

On a que $(\mathbb{Z}/k\mathbb{Z}, +)$ est un groupe abélien.

Preuve:



Proposition : $\mathbb{Z}/k\mathbb{Z}$

Le groupe $(\mathbb{Z}/k\mathbb{Z}, +)$ est le groupe des entiers modulo k .

Proposition : $\mathbb{Z}/k\mathbb{Z}$

Le groupe $(\mathbb{Z}/k\mathbb{Z}, +)$ est cyclique et engendré par $\bar{1}$.

Preuve:

Le sous-groupe engendré par $\bar{1}$ est $\{\bar{n} \mid n \in \mathbb{Z}\} = \{\overline{n \cdot 1} \mid n \in \mathbb{Z}\} = \mathbb{Z}/k\mathbb{Z}$. \square