# Groupes

1. Révisions de première année.
2. Intersection de sous-groupes. Sous-groupe engendré par une partie, par un élément. Partie génératrice d'un groupe.
3. Sous-groupes de $(\mathbb{Z}, +)$.
4. Groupe $\mathbb{Z}/n\mathbb{Z}$ et générateurs de $\mathbb{Z}/n\mathbb{Z}$.
5. Groupe monogène, groupe cyclique. À quel groupe est isomorphe un groupe monogène infini ? À quel groupe est isomorphe un groupe monogène fini ?
6. Ordre d'un élément dans un groupe, et correspondance avec le cardinal du sous-groupe engendré par cet élément. On a $a^k = e$ si et seulement si l'ordre de $a$ divise $k$.
7. Théorème de Lagrange concernant l'ordre d'un élément dans un groupe fini.

---

## 1 Révisions de première année

### 1.1 généralités sur les groupes et morphismes de groupes

**Définition 1**

Soit $G$ un ensemble muni d'une loi de composition interne $\star$. On dit que $(G, \star)$ est un *groupe* lorsque

- $\star$ est associative
- $\star$ admet un élément neutre
- tout élément de $G$ est symétrisable (inversible).

L'élement neutre du groupe $G$ est noté $e$, ou encore $1_G$ si la loi est notée multiplicativement et $0_G$ si la loi est notée additivement.

Le groupe $(G, \star)$ est dit *commutatif* (ou *abélien*) lorsque la loi $\star$ est commutative.

Exercice 1 : Donner des exemples usuels de groupes additifs et de groupes multiplicatifs rencontrés dans les cours de première année.

Si $(G, \star)$ est un groupe et $a, b \in G$, alors

$$\forall x \in G, \quad a \star x = b \quad \text{si et seulement si} \quad x = a^{-1} \star b$$

De même

$$\forall x \in G, \quad x \star a = b \quad \text{si et seulement si} \quad x = b \star a^{-1}$$

On peut ainsi résoudre facilement de nombreuses équations dans un groupe $G$ !

### 1.2 sous-groupe

**Définition 2**

Soit $(G, \star)$ un groupe et $H$ une partie de $G$. On dit que $H$ est un *sous-groupe* de $(G, \star)$ lorsque $H$ est stable par $\star$ et que $(H, \star)$ est un groupe.

La notion de sous-groupe est importante car en pratique, pour montrer que $(H, \star)$ est un groupe, on le fait presque toujours apparaître comme sous-groupe d'un groupe connu.

**Propriété 1**

Soit $(G, \star)$ un groupe et $H$ une partie de $G$.

$$H \text{ est un sous-groupe de } G \Leftrightarrow \begin{cases} 1_G \in H \\ H \text{ est stable par produit : } \forall h, h' \in H, \quad h \star h' \in H \\ H \text{ est stable par inversion : } \forall h \in H, \quad h^{-1} \in H \end{cases}$$

$$\Leftrightarrow \begin{cases} 1_G \in H \\ H \text{ est stable par produit-inversion : } \forall h, h' \in H, \quad h^{-1} \star h' \in H \end{cases}$$

En notation additive,

$$H \text{ est un sous-groupe de } G \Leftrightarrow \begin{cases} 0_G \in H \\ \forall h, h' \in H, \quad h' - h \in H \end{cases}$$

**Propriété 2 – groupe produit**

Soient $(G_1, \square)$ et $(G_2, \diamond)$ deux groupes. On définit une loi de composition interne sur $G_1 \times G_2$ en posant, pour $x = (x_1, x_2)$ et $y = (y_1, y_2)$ dans $G_1 \times G_2$ :

$$x \star y = (x_1 \square y_1, x_2 \diamond y_2)$$

Muni de cette loi, $G_1 \times G_2$ est un groupe, appelé *groupe produit*, d'élément neutre $(1_{G_1}, 1_{G_2})$.

**Définition 3**

Soit $(G, \square)$ et $(G', \diamond)$ deux groupes. On dit qu'une application $f$ de $G$ dans $G'$ est un *morphisme de groupe* lorsque

$$\forall x, y \in G, \quad f(x \square y) = f(x) \diamond f(y)$$

On dit que $f$ est :

- un *endomorphisme* lorsque $(G, \square) = (G', \diamond)$.
- un *isomorphisme* lorsque $f$ est bijective.
- un *automorphisme* lorsque $f$ est un endomorphisme et un isomorphisme.

Exemples :

- L'exponentielle complexe est un morphisme de groupe de $\mathbb{C}$ dans $\mathbb{C}^*$ car

- L'application $f$ de $\mathbb{R}$ dans $\mathbb{U}$ qui à $\theta$ associe $e^{i\theta}$ est un morphisme du groupe $(\mathbb{R}, +)$ dans le groupe $(\mathbb{U}, \times)$ car

- La fonction module est un endomorphisme de groupes de $\mathbb{C}^*$ car

- Trace est un morphisme de groupes de dans car

**Propriété 3**

Soit $f$ un morphisme du groupe de $(G, \square)$ dans $(G', \diamond)$. Alors

$$\begin{aligned} & f(1_G) = 1_{G'} \\ \forall x \in G, \quad & f\left(x^{-1}\right) = [f(x)]^{-1} \end{aligned}$$

**Propriété 4**

Soit $f$ un morphisme de $(G, \square)$ dans $(G', \diamond)$. Alors
- l'image réciproque d'un sous-groupe de $G'$ est un sous-groupe de $G$.
- l'image directe d'un sous-groupe de $G$ est un sous-groupe de $G'$.

Image et noyau :
$\operatorname{Im} f = \{f(x),\ x \in G\} = f(G)$ est un sous-groupe de $G'$. $f$ est surjectif si et seulement si $\operatorname{Im} f = G'$.
Et $\ker f = \{x \in G \mid f(x) = 1_{G'}\}$ est un sous-groupe de $G$. $f$ est injectif si et seulement si $\ker f = \{1_G\}$.

Enfin,
- La composée de deux morphismes de groupes est un morphisme de groupe.
- La bijection réciproque d'un isomorphisme de groupe est un isomorphisme de groupe.

### 1.3 le groupe symétrique

Soit $E$ un ensemble de cardinal $n \in \mathbb{N}^*$. Une permutation de $E$ est une bijection de $E$ dans $E$. L'ensemble des permutations de $E$ est noté $\mathcal{S}_E$. L'ensemble $E$ étant de cardinal $n$, il est en bijection avec $[\![1, n]\!]$ donc il est équivalent d'étudier l'ensemble $\mathcal{S}_n$ des permutations de $[\![1, n]\!]$ . On représente usuellement une permutation par la liste des éléments de $[\![1, n]\!]$ en-dessous de laquelle on indique l'image de chaque élément.
La notation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 4 & 5 \end{pmatrix}$$

désigne l'application $\sigma$ telle que $\sigma(1) = 3$, $\sigma(2) = 2$, $\sigma(3) = 1$, $\sigma(4) = 6$, $\sigma(5) = 4$ et $\sigma(6) = 5$.

L'ensemble $\mathcal{S}_n$ est un groupe pour la composition, non commutatif pour $n \geqslant 3$. L'ordre de la permutation $\sigma$ est le plus petit entier naturel $k$ non nul tel que $\sigma^k = \mathrm{Id}$.

**Support**
On appelle support d'une permutation $\sigma$ l'ensemble des éléments $x$ de $[\![1,n]\!]$ tels que $\sigma(x) \neq x$. Dans l'exemple ci-dessus, le support de $\sigma$ est $\{1,3,4,5,6\}$. Deux permutations à supports disjoints commutent.

**Cycles**
Soit $p \in [\![2,n]\!]$. On appelle *p-cycle*, toute permutation $\sigma$ de $[\![1,n]\!]$ pour laquelle il existe des éléments distincts $x_1,\dots,x_p$ de $[\![1,n]\!]$ pour lesquels :

$$\sigma(x_1)=x_2,\ \sigma(x_2)=x_3,\dots\sigma(x_{p-1})=x_p \text{ et } \sigma(x_p)=x_1, \quad \text{ et } \sigma(x)=x \text{ si } x \notin \{x_1,\dots,x_p\}$$

Un tel $p$-cycle est noté $(x_1\ x_2 \dots x_p)$.
On remarque qu'une transposition est un 2-cycle.
Toute permutation de $[\![1,n]\!]$ peut être décomposée d'une et une seule manière, à l'ordre des facteurs près, comme un produit de cycles disjoints.

**Transpositions**
Supposons $n \geqslant 2$. On appelle *transposition* une permutation qui échange deux éléments distincts et qui laisse les autres invariants. On la note usuellement $(i\ j)$. Une transposition est d'ordre 2, elle est son propre inverse : c'est une involution.
Toute permutation de $[\![1,n]\!]$ est un produit de transpositions. Il n'y a pas unicité de la décomposition en produit de transpositions.

**Signature**
Il existe un et un seul morphisme de groupes $\varepsilon$ de $\mathcal{S}_n$ dans $\{-1,1\}$, appelée *signature*, qui donne à toute transposition la valeur $-1$ et pour lequel pour tous $\sigma,\sigma' \in \mathcal{S}_n$ :

$$\varepsilon(\sigma\circ\sigma')=\varepsilon(\sigma)\varepsilon(\sigma')$$

La signature d'une transposition est $-1$ ; la signature d'un $p$-cycle est $(-1)^{p-1}$.

Exercice 2 : Savoir-faire : les étudiants doivent savoir décomposer une permutation.
On reprend l'exemple de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 4 & 5 \end{pmatrix}$.

1. Donner la décomposition de $\sigma$ en produit de cycles à supports disjoints.
2. Donner une décomposition de $\sigma$ en produit de transpositions.
3. Donner la signature de $\sigma$.

## 2 Les sous-groupes de $(\mathbb{Z},+)$

**Propriété 5**

Les sous-groupes de $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$, pour $n \in \mathbb{N}$.

## 3 Groupes engendrés par une partie

Dans toute cette partie, $G$ est un groupe.

**Propriété 6**

L'intersection de sous-groupes du groupe $G$ est un sous-groupe de $G$.

**Définition - propriété 1**

Soit $A$ une partie de $G$. L'intersection de tous les sous-groupes de $G$ contenant $A$ est un sous-groupe de $G$, et c'est le plus petit sous-groupe de $G$ contenant $A$. On l'appelle *groupe engendré* par $A$.

MÉTHODE

Pour montrer que $A$ est le plus petit ensemble (au sens de l'inclusion) vérifiant la propriété $\mathcal{P}$, on montre :

- $A$ vérifie la propriété $\mathcal{P}$,
- si $B$ est un ensemble qui vérifie la propriété $\mathcal{P}$, alors $A \subset B$.

**Définition 4**

On dit que la partie $A$ engendre $G$ (ou encore que $A$ est une partie génératrice de $G$) si le sous-groupe engendré par $A$ est égal à $G$.

Exemples :

- Puisque toute permutation de $\mathcal{S}_n$ se décompose en produits de cycles (à support disjoints), l'ensemble des cycles est une partie génératrice de $\mathcal{S}_n$.
- Puisque toute permutation de $\mathcal{S}_n$ se décompose en produits de transpositions, l'ensemble des transpositions est une partie génératrice de $\mathcal{S}_n$.

**Propriété 7**

En notation multiplicative, le sous-groupe engendré par l'élément $a$ de $G$ est $\{a^n,\ n \in \mathbb{Z}\}$.
En notation additive, le sous-groupe engendré par l'élément $a$ de $G$ est $\{na,\ n \in \mathbb{Z}\}$.

Exemples : le groupe engendré par 2 dans $(\mathbb{R}^*, \times)$ est

Le groupe engendré par $\sigma = (1\ 2\ 3\ 4)$ dans $\mathcal{S}_4$ est

Le groupe engendré par $\omega^2$ dans $\mathcal{U}_5$ est

Exercice 3 : pour $A$ partie de $G$, on considère

$$H = \{x_1 x_2 \dots x_n \mid n \in \mathbb{N} \text{ et } \forall i \in [\![1, n]\!],\ (x_i \in A) \text{ ou } (x_i^{-1} \in A)\}$$

$H$ est l'ensemble des produits d'éléments de $A$ et d'inverses d'éléments de $A$. Par convention, lorsque $n = 0$, $x_1 \dots x_n = e$.
Montrer que $H$ est le sous-groupe engendré par $A$.

Exercice 4 : Pour $i \in [\![1, n]\!]$, $t_i = (1, i)$. Montrer que $(t_2, \dots, t_n)$ engendre $\mathcal{S}_n$.

**Définition 5**

Un groupe est *monogène* s'il est engendré par un de ses éléments. Un tel élément est appelé *générateur* de $G$.
Un groupe est *cyclique* s'il est monogène et fini.

Un groupe monogène est nécessairement commutatif.

Exemples :

- Pour $n \geqslant 3$, $\mathcal{S}_n$ n'est pas un groupe monogène.
- Le groupe $3\mathbb{Z}$ est monogène. Il a deux générateurs : 3 et $-3$.
- Plus généralement, les sous-groupes de $(\mathbb{Z}, +)$ sont monogènes, d'après la propriété 5. Si l'on excepte $\{0\}$, ce sont des groupes monogènes infinis.
- Le groupe $\mathbb{U}_4 = \{1, \mathrm{i}, -1, -\mathrm{i}\}$ est monogène. Il a deux générateurs : i et $-\mathrm{i}$.
- Plus généralement, les sous-groupes de $\mathbb{U}$ constitués des racines $n$-ième de l'unité, autrement dit les sous-groupes

  $\mathbb{U}_n \quad =$

  sont des groupes monogènes et finis, autrement dits cycliques.

Nous reviendrons un peu plus loin sur la structure des groupes monogènes. Avant cela, il faut étudier plus en détail le groupe $\mathbb{Z}/n\mathbb{Z}$ ...

## 4 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Soit $n$ un entier naturel. En première année, il a été rencontré la relation de congruence modulo $n$ définie par :

$$x \equiv y \ [n] \quad \Leftrightarrow \quad x - y \in n\mathbb{Z}$$

Il s'agit d'une relation d'équivalence sur $\mathbb{Z}$ qui est compatible avec les opérations $+$, $-$ et $\times$ de $\mathbb{Z}$, c'est-à-dire :

$$\forall (x, y, x', y') \in \mathbb{Z}^4, \quad \begin{cases} x \equiv x' & [n] \\ y \equiv y' & [n] \end{cases} \quad \Rightarrow \quad \begin{cases} x + y & \equiv x' + y' & [n] \\ x - y & \equiv x' - y' & [n] \\ x \times y & \equiv x' \times y' & [n] \end{cases}$$

**Définition 6**

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour la relation de congruence modulo $n$. La classe d'un élément $k$ de $\mathbb{Z}$ est notée $\overline{k}$.

Ensembles $\mathbb{Z}/n\mathbb{Z}$ pour les premières valeurs de $n$ (0, 1, 2, 3) :

- La relation de congruence modulo 0 est la relation d'égalité, donc $\mathbb{Z}/0\mathbb{Z} = \{\{k\}, k \in \mathbb{Z}\}$ et il y a une infinité de classes d'équivalence modulo 0. Dans toute la suite, on se préoccupera de $\mathbb{Z}/n\mathbb{Z}$ pour $n \neq 0$.
- Deux entiers sont toujours congrus modulo 1 donc il n'y a qu'une seule classe d'équivalence modulo 1, et $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$.
- Pour la relation de congruence modulo 2, tous les entiers $n$ pairs sont congrus à 0, et tous les impairs sont congrus à 1. Il n'y a donc que 2 classes d'équivalence.

  $$\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$$

- Dans $\mathbb{Z}/3\mathbb{Z}$, il y a 3 classes d'équivalence :

  $$\overline{0} = \{3k, \ k \in \mathbb{Z}\} \quad \overline{1} = \{1 + 3k, \ k \in \mathbb{Z}\} \quad \overline{2} = \{2 + 3k, \ k \in \mathbb{Z}\}$$

Et plus généralement, en considérant le reste de la division euclidienne d'un entier par $n$, un entier est toujours congru modulo $n$ à un entier compris entre 0 et $n-1$. La classe de $x$ est égale à $\overline{r}$ où $r$ est le reste dans la division euclidienne de $x$ par $n$.

Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{37} =$
Dans $\mathbb{Z}/5\mathbb{Z}$, $\overline{29} =$

On visualise :

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| classe de $x$ dans $\mathbb{Z}/4\mathbb{Z}$ | | | | | | | | | | | | | | |

**Propriété 8**

Pour $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ a $n$ éléments : $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.

**Propriété 9 – groupe $\mathbb{Z}/n\mathbb{Z}$**

Dans $\mathbb{Z}/n\mathbb{Z}$, on définit l'addition suivante :

$$\overline{k} + \overline{\ell} = \overline{k+\ell}$$

Muni de cette addition, $\mathbb{Z}/n\mathbb{Z}$ est un groupe commutatif, d'élément neutre $\overline{0}$.

On a $-\overline{k} = \overline{-k}$.

Exercice 5 : dans $\mathbb{Z}/6\mathbb{Z}$, donner l'inverse (le symétrique) de $\overline{21}$ et l'inverse (le symétrique) de $\overline{8}$.

**Lemme 1**

Pour $k$ et $p$ entiers, $p\overline{k} = \overline{pk}$.

**Propriété 10 – générateurs de $\mathbb{Z}/n\mathbb{Z}$**

Pour $k \in \mathbb{Z}$, $\overline{k}$ est générateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.

Exercice 6 : Donner les générateurs de $\mathbb{Z}/6\mathbb{Z}$. Donner les générateurs de $\mathbb{Z}/12\mathbb{Z}$. Donner les générateurs de $\mathbb{Z}/11\mathbb{Z}$.

**Définition 7**

On appelle *indicatrice d'Euler* de $n \in \mathbb{N}^*$, et on note $\varphi(n)$, le cardinal de l'ensemble :

$$\{k \in [\![1, n]\!] \mid k \wedge n = 1\}$$

On a $\varphi(1) = 1$, et pour $n \geqslant 2$, $\varphi(n)$ est le nombre d'entiers de $[\![1, n-1]\!]$ premiers avec $n$.
On vient de voir qu'il y avait $\varphi(n)$ générateurs de $\mathbb{Z}/n\mathbb{Z}$.

## 5 Structure des groupes monogènes

**Théorème 1**

- Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.
- Tout groupe monogène fini de cardinal $n \in \mathbb{N}^*$ (autrement dit tout groupe cyclique de cardinal $n \in \mathbb{N}^*$) est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Conséquence : pour $n \in \mathbb{N}^*$, le groupe $\mathbb{U}_n$ des racines $n$-ième de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exercice 7 : Montrer que l'application $\psi : \begin{pmatrix} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{U}_n \\ \overline{k} & \mapsto & e^{\frac{2ik\pi}{n}} \end{pmatrix}$ est bien définie et que c'est un isomorphisme de groupes.

## 6 Ordre d'un élément dans un groupe

**Définition 8**

En notation multiplicative, un élément $a$ de $G$ est *d'ordre fini* s'il existe un entier $n$ non nul tel que $a^n = e$. *L'ordre* de $a$ est le plus petit entier naturel $n$ non nul tel que $a^n = e$.

Si $a$ n'est pas d'ordre fini, on dit que $a$ est d'ordre infini.
Par exemple, les transpositions dans $\mathcal{S}_n$ sont d'ordre 2, et un $p$-cycle est d'ordre $p$.

**Propriété 11**

- L'ordre de $a$ dans $G$ est le cardinal du sous-groupe de $G$ engendré par $a$.
- Pour $k \in \mathbb{Z}$, $a^k = e$ si et seulement si l'ordre de $a$ divise $k$.

**Théorème 2 – théorème de Lagrange**

Dans un groupe fini, tous les éléments sont d'ordre fini et leur ordre divise le cardinal du groupe.

Exercice 8 : Donner l'ordre de chacun des éléments de $\mathbb{Z}/6\mathbb{Z}$ et vérifier sur cet exemple la propriété précédente.

Exercice 9 : Montrer qu'un groupe fini de cardinal $p$ premier est cyclique.

Exercice 10 : Soit $G$ un groupe fini. Montrer que pour tout élément $x$ de $G$, $x^{|G|} = e$.

# 7 Annexe : quelques éléments de démonstrations

## Propriété 1

Démonstration en notation multiplicative.
$(i) \Rightarrow (ii)$ Comme $1_H$ et $1_G$ sont des éléments neutres, on a $1_H \star 1_G = 1_H = 1_H \star 1_H$, et en multipliant à gauche par ${1_H}^{-1}$, on trouve $1_G = 1_H$.
Soit $h \in H$. On note $h'$ son inverse dans $H$ et, comme d'habitude, $h^{-1}$ son inverse dans $G$.
On a $h \star h' = 1_H = 1_G = h * h^{-1}$. On multiplie à gauche par $h^{-1}$ : $1_G \star h' = 1_G \star h^{-1}$, et donc $h' = h^{-1} \in G$.

$(ii) \Rightarrow (iii)$ est facile puisque $\star$ est une loi de composition interne.
$(iii) \Rightarrow (i)$ Supposons que $H$ contient $1_G$ et est stable par produit-inversion.
Commençons par montrer que $\star$ est une loi interne à $H$. Soient $x$ et $y$ dans $H$.
$x \star y = x \star (y^{-1})^{-1}$. Or $y^{-1} = y^{-1} \star 1_G \in H$. Donc $x \star y \in H$.

$\star$ est bien associative (pour tous $x, y, z$ de $H \subset G$, $x \star (y \star z) = (x \star y) \star z$).
$1_G \in H$ est élément neutre.
Tout $h$ de $H$ a son inverse $h^{-1} = h^{-1} \star 1_G \in H$.

## Propriété 3

$(i)$ $f(1_G) = f(1_G \square 1_G) = f(1_G) \diamond f(1_G)$ donc $1_{G'} \diamond f(1_G) = f(1_G) \diamond f(1_G)$ et comme $f(1_G)$ est inversible, $1_{G'} = f(1_G)$.

$(ii)$ On a $f(x) \diamond f(x^{-1}) = f(x \square x^{-1}) = f(1_G) = 1_{G'}$ et aussi $f(x^{-1}) \diamond f(x) = f(x^{-1} \square x) = f(1_G) = 1_{G'}$.

## Propriété 6

Soit $H = \bigcap_{i \in I} G_i$ où les $G_i$ sont des sous-groupes de $G$.
$1_G$ appartient à tous les sous-groupes de $G$, donc $1_G \in \bigcap_{i \in I} G_i$.
Soit $h$ et $g$ dans $H$. Pour $i \in I$, $h$ et $g$ sont dans $G_i$, et $G_i$ est stable par produit inversion, donc $hg^{-1} \in G_i$.
Donc $hg^{-1} \in \bigcap_{i \in I} G_i$.

## Propriété 5

On précise que $n\mathbb{Z} = \{nk,\ k \in \mathbb{Z}\}$.
• $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, car $0 = n.0 \in n\mathbb{Z}$ et si $nk$ et $nk'$ sont dans $n\mathbb{Z}$, alors $nk + nk' = n(k + k') \in n\mathbb{Z}$ (« stable par produit » : stable par addition, donc), et $-(nk) = n(-k) \in n\mathbb{Z}$ (« stable par inversion » : stable par passage à l'opposé, donc).

• Soit $H$ un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$, on a $H = 0\mathbb{Z}$. Et si $H \neq \{0\}$, $H \cap \mathbb{N}^*$ est une partie non vide (puisque si $h \in H$, $-h \in H$) de $\mathbb{N}$. Cette partie admet un plus petit élément $n_0$.
Soit $h \in H \cap \mathbb{N}^*$. On effectue la division euclidienne de $h$ par $n_0$. Il existe $q, r$ entiers tel que

$$h = qn_0 + r \text{ et } 0 \leqslant r < n_0$$

Comme $r = h - qn_0$, $r \in H$. Et comme $r < n_0$ et $r \geqslant 0$, $r = 0$ par définition de $n_0$. Donc $h = qn_0 \in n_0\mathbb{Z}$.
Soit $h \in H \cap \mathbb{Z}^-$. Alors $-h \in H \cap \mathbb{Z}$, et soit $h = 0 \in n_0\mathbb{Z}$, soit $h \neq 0$ et $-h \in n_0\mathbb{Z}$ par le premier cas. Dans tous les cas, $h \in n_0\mathbb{Z}$.

## Propriété 7

Démonstration en notation additive. Tout groupe contenant $a$ doit contenir $0_G = 0.a$ (c'est la définition de $0.a$, comme avait été défini, en notation multiplicative, $x^0 = E = 1_G$), et ses itérés : $a+a$, $a+a+a$,..., soit tous les $n.a$ pour $n \in \mathbb{N}$, et l'inverse de $a$, $-a$, ainsi que ses itérés : $-a-a$, etc. Donc tout groupe contenant $a$ contient $H = \{na,\ n \in \mathbb{Z}\}$.
Et par ailleurs, $H$ contient $a = 1.a$ (définition) et vérifions que $H = \{na,\ n \in \mathbb{Z}\}$ est un groupe.
$0.a = 0_G \in H$ et si $na$ et $ma$ sont dans $H$, alors $na - ma \underset{(*)}{=} (n-m)a \in H$ ($(*)$ est une règle de calcul vue en première année).
$H$ est bien le plus petit sous-groupe contenant $a$.

## Propriété 9

L'effort principal est de vérifier que la loi d'addition ainsi présentée est bien définie, c'est-à-dire qu'elle ne dépend pas du choix des représentants des classes, ou encore : si $\overline{k} = \overline{k'}$ et si $\overline{\ell} = \overline{\ell'}$, alors on a bien

$$\overline{k + \ell} = \overline{k' + \ell'}$$

Partant de $\overline{k} = \overline{k'}$ et si $\overline{\ell} = \overline{\ell'}$, on a l'existence de $p$ et $p'$ tels que $k' = k + np$, $\ell' = \ell + np'$, et donc

$$k' + \ell' = k + \ell + n(p + p') \text{ et } \overline{k + \ell} = \overline{k' + \ell'}$$

Montrons maintenant que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe. On ne peut pas le situer comme sous-groupe d'un groupe connu. Donc on passe par la définition.

• Associativité :

$$\begin{aligned}\overline{k}+(\overline{\ell}+\overline{r}) &= \overline{k}+\overline{\ell+r}=\overline{k+(\ell+r)}\\ &= \overline{k+\ell+r}(\text{on est dans } \mathbb{Z})\\ &= \overline{k+\ell}+\overline{r}=(\overline{k}+\overline{\ell})+\overline{r}\end{aligned}$$

• Élément neutre :
$\overline{k}+\overline{0}=\overline{k+0}=\overline{k}$ et de même, $\overline{0}+\overline{k}=\overline{0+k}=\overline{k}$.

• Opposé pour chaque élément :
$\overline{k}+\overline{-k}=\overline{k+(-k)}=\overline{0}=\overline{-k+k}=\overline{-k}+\overline{k}$. Donc l'opposé de $\overline{k}$ est $\overline{-k}$.
Par ces 3 points, $\mathbb{Z}/n\mathbb{Z}$ est un groupe.

• Enfin, $\overline{k}+\overline{\ell}=\overline{k+\ell}=\overline{\ell+k}=\overline{\ell}+\overline{k}$, donc ce groupe est commutatif.

### Lemme 1
• Pour $m=0$, par définition d'un itéré dans un groupe additif, $0\overline{k}=0_G=\overline{0}$.
• Pour $m\in\mathbb{N}^*$, toujours par définition d'un itéré dans un groupe additif,

$$m\overline{k}=\underbrace{\overline{k}+\overline{k}+\cdots+\overline{k}}_{m \text{ termes}}=\overline{k+k+\cdots+k}=\overline{mk}$$

• Comme $\overline{k}+\overline{-k}=\overline{k-k}=\overline{0}$, l'opposé de $\overline{k}$ est $\overline{-k}$.
Pour $m\in Z^-$, on a donc $m\overline{k}=-(-m)\overline{k}=-\overline{(-m)k}$ par le premier point. Et par la remarque sur l'opposé, $-\overline{(-m)k}=\overline{-(-m)k}=\overline{mk}$.

### Propriété 10
• Soit $\overline{k}$ un générateur de $\mathbb{Z}/n\mathbb{Z}$. En particulier, $\overline{1}$ est dans le groupe engendré par $\overline{k}$, et il existe donc $p\in\mathbb{Z}$ tel que :

$$\overline{1}=p\overline{k}=\overline{pk} \text{ (on utilise là le lemme précédent)}$$

Donc il existe $r$ entier tel que $1=pk+rn$. Par le théorème de Bézout, $k\wedge n=1$.
• Réciproquement, si $k\wedge n=1$, on trouve une égalité de Bézout de la forme $pk+rn=1$, puis $\overline{1}=\overline{pk}=p\overline{k}$.
Et alors, pour $\ell$ entier, $\overline{\ell}=\ell\overline{1}=\ell p\overline{k}$, et $\overline{\ell}$ est dans le groupe engendré par $\overline{k}$.

### Théorème 1
Soit $G$ un groupe monogène et $a$ un générateur de $G$. L'application :

$$\varphi:\left(\begin{array}{ccc}\mathbb{Z} & \mapsto & G\\ k & \mapsto & a^k\end{array}\right)$$

est surjective. C'est aussi un morphisme de groupes puisque :

$$\varphi(k+\ell)=a^{k+\ell}=a^k a^\ell=\varphi(k)\varphi(\ell) \quad \text{(règle sur les itérés)}$$

Son noyau est un sous-groupe de $(\mathbb{Z},+)$, donc il existe $n\in\mathbb{N}$ tel que $\ker\varphi=n\mathbb{Z}$.

— Premier cas : $\ker\varphi=\{0\}$.
$\varphi$ est injective, et alors bijective. $G$ est isomorphe à $\mathbb{Z}$ (et par conséquent, $G$ est infini).

— Deuxième cas : il existe $n\in\mathbb{N}^*$ tel que $\ker\varphi=n\mathbb{Z}$. On considère alors

$$\psi:\left(\begin{array}{ccc}\mathbb{Z}/n\mathbb{Z} & \mapsto & G\\ \overline{k} & \mapsto & a^k\end{array}\right)$$

On pourrait vérifier que $\psi$ est bien définie, que $\psi$ est un morphisme de groupes, que $\psi$ est surjective (puisque $a$ engendre $G$), et que $\psi$ est injective (ce qui vient de $\ker\varphi=n\mathbb{Z}$).

Il en résulte que $\mathbb{Z}/n\mathbb{Z}$ et $G$ sont isomorphes. De plus,

$$\begin{aligned}G &= \{\psi(\overline{0}),\psi(\overline{1}),\ldots,\psi(\overline{n-1})\}\\ &= \{1_G,a,\ldots,a^{n-1}\}\end{aligned}$$

Enfin, pour $k\in\mathbb{Z}$, on a

$$a^k=1_G \Leftrightarrow \overline{k}=\overline{0} \Leftrightarrow n\mid k$$

### Propriété 11
$(i)$ Considérons $a$ un élément d'ordre fini $n$. $n$ est le plus petit entier naturel non nul tel que $a^n=e$. Le groupe engendré par $a$ est $\{e,a,a^2,\ldots,a^{n-1}\}$. Raisonnons par l'absurde en supposant qu'il y a une répétition dans ces éléments : il existe

$0 \leqslant i < j \leqslant n-1$ tel que $a^i = a^j$. Mais alors en multipliant par $(a^{-1})^i$, $e = a^{j-i}$ avec $1 \leqslant j-i < n$, ce qui contredit la définition de l'ordre de $a$. Donc le cardinal du groupe engendré par $a$ est $n$.

(*ii*) Notons $n$ l'ordre de $a$.
Si $n \mid k$, il existe $\ell \in \mathbb{Z}$ tel que $k = n\ell$, et $a^k = (a^n)^\ell = e^\ell = e$.
Et si $a^k = e$, effectuons la division euclidienne de $k$ par $n$. Il existe $q, r$ entiers tels que $k = nq + r$ avec $0 \leqslant r < n$.

$$e = a^k = a^{nq+r} = (a^n)^q a^r = ea^r = a^r$$

et comme $n$ est le plus petit entier non nul tel que $a^n = e$, on a $r = 0$, et $n$ divise $k$.

## Théorème 2

Conformément au programme, la démonstration n'est à faire que dans le cadre d'un groupe commutatif. Soit donc $G$ un groupe fini, de cardinal $n$, commutatif, et $a$ un élément de $G$.
On introduit $P$, produit (fini) des éléments de $G$ ($P$ est bien défini par cette seule phrase puisque $G$ est commutatif, donc l'ordre des termes du produit n'a aucune importance).
L'application $f : G \to G$, $x \mapsto ag$ est bijective (sa bijection réciproque est $g \mapsto a^{-1}g$) et autorise le changement d'indice dans $P$, et nous donne :

$$P = \prod_{h \in G} h = \prod_{g \in G} (ag) = a^{\mathrm{Card}(G)} \prod_{g \in G} g = a^{\mathrm{Card}(G)} P$$

En multipliant par $P^{-1}$, on obtient $a^{\mathrm{Card}(G)} = e$. Donc $a$ est d'ordre fini. Et par la propriété précédente, l'ordre de $a$ divise $\mathrm{Card}(G)$.