

Structures algébriques usuelles

B. Seddoug. Médiane Sup, Oujda

I Structure de groupe

I.1 Définition-Exemples

Définition 1 (groupe) On appelle groupe tout monoïde dans lequel tout élément est symétrisable. i.e: (G, \cdot) est un groupe si:

- La loi est associative: $\forall (x, y, z) \in G^3, x(yz) = (xy)z$.
- La loi admet un élément neutre $e : \forall x \in G, xe = ex = x$.
- Tout élément est symétrisable: $\forall x \in G, \exists x' \in G \mid xx' = x'x = e$.

On dit alors que (G, \cdot) est un groupe. Si en plus la loi est commutative on dit que G est un groupe abélien.

Remarque 1 Dans le cas de groupe abélien, on utilise par fois une notation additive et note le neutre par 0, le symétrique de x est noté $-x$. Dans le cas général, on utilise une loi sans symbole et le symétrique de x est noté x^{-1} .

Exemple 1

1. $(\mathbb{N}, +)$ n'est pas un groupe.
2. $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$ et (\mathbb{R}_+^*, \times) sont des groupes abéliens.
3. L'ensemble des permutations (bijections) d'un ensemble E est un groupe pour la composition des application on le note S_E et on l'appelle le groupe symétrique de E .

P I.1 Dans un groupe tout élément est régulier.

i.e: $\forall x \in G : \forall (y, z) \in G^2, xy = xz \implies y = z$.
 $\forall (y, z) \in G^2, yx = zx \implies y = z$.

Exemple 2 (Groupe à deux éléments) Soit $G = \{e; a\}$ une loi de groupe sur G est représentée par la table suivante, on remarque qu'il est abélien:

.	e	a
e	e	a
a	a	e

table de groupe à deux éléments.

Exemple 3 (Groupe à trois éléments) Soit $G = \{e; a; b\}$ une loi de groupe sur G est représentée par la table suivante, on remarque qu'il est abélien:

.	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

table de groupe à trois éléments.

Exercice 1 Donner les tables possibles d'un groupe à 4 éléments.

I.2 Sous groupe

Définition 2 (Sous groupe) On appelle sous groupe d'un groupe (G, \cdot) toute partie H de G stable pour la loi et telle que (H, \cdot) soit un groupe.

Propriétés

P I.2 Si H est un sous groupe de G alors $e_H = e_G$, (même élément neutre). Et pour élément $x \in H$, son symétrique dans H est celui dans G .

P I.3 Propriété caractéristique

Soit $H \subset G$, H est un sous groupe de G si et seulement si

- (i) $H \neq \emptyset$.
- (ii) $\forall (x, y) \in H : xy \in H$.
- (iii) $\forall x \in H : x^{-1} \in H$.

Les conditions (ii) et (iii) peuvent être remplacées par l'unique condition

- (iv) $\forall (x, y) \in H : xy^{-1} \in H$.

P I.4 Intersection de sous groupes

Toute intersection de sous groupes de G est un sous groupe de G .

Remarque 2 L'union de sous groupe n'est pas toujours un sous groupe.

Exemple 4

1. $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ sont deux sous groupes de $(\mathbb{R}, +)$.
2. G et $\{e_G\}$ sont deux sous groupe de G .
3. Centre d'un groupe
Soit G un groupe, on note $C = \{g \in G \mid \forall x \in G : gx = xg\}$. C est un sous groupe de G appelé le centre de G .
4. **Sous groupes additifs de \mathbb{R}**
Soit $G \neq \{0\}$ un sous groupe de $(\mathbb{R}, +)$. On note $a = \inf G \cap \mathbb{R}_+^*$.
 - Si $a > 0$ on montre que $G = a\mathbb{Z}$, on dit que G est discret.
 - Si $a = 0$ on montre que G est dense dans \mathbb{R} .

En effet: 1^{er} cas: D'abord $G \cap \mathbb{R}_+^* \neq \emptyset$ et a existe.

Si $a > 0$ alors $a \in G$, si non $\exists x, y \in G$ tel que $a < x < y < 2a$ et par suite $y - x \in G$ ce qui absurde car $0 < y - x < a$.

Donc $a \in G$ et par suite $a\mathbb{Z} \subset G$.

Réciproquement soit $x \in G, \exists (n, r) \in \mathbb{Z} \times [0, a[$ | $x = na + r$ donc $r = x - na \in G$ et par suite $r = 0$ et donc $x \in a\mathbb{Z}$.

2^{ème} cas: si $a = 0$ alors $\forall x < y \in \mathbb{R}, \exists z \in G$ | $0 < z < y - x$. La division de y par z donne n et $r \in [0, z[$ tels que $y = nz + r$.

Donc $0 \leq r = y - nz < z < y - x$ c.à.d $x - y < nz - y \leq 0$ ou $x < nz \leq y$. cqfd .

I.3 Morphisme de groupe

Définition 3 (homomorphisme) Soient G et G' deux groupes. Une application $f : G \rightarrow G'$ est appelé *homomorphisme* de groupes si

$$\forall (x, y) \in G^2 : f(xy) = f(x)f(y).$$

Si en plus f est bijective, on dit que f est un *isomorphisme*.

Si $G = G'$ on dit que f est *endomorphisme* et *automorphisme* dans le cas f bijective.

Exemple 5

1. Id_G est un automorphisme de G .

2. $(\mathbb{R}, +) \xrightarrow{\exp} (\mathbb{R}_+^*, \times), x \mapsto \exp x$ est un isomorphisme. Sa bijection réciproque: $(\mathbb{R}_+^*, \times) \xrightarrow{\ln} (\mathbb{R}, +), x \mapsto \ln x$ est aussi un isomorphisme.

Propriétés

P I.5 La composée de deux morphismes est un morphisme.

P I.6 Si f est un isomorphisme, f^{-1} est aussi un isomorphisme.

P I.7 Si $f : G \rightarrow G'$ est un morphisme alors

- $f(e_G) = e_{G'}$.
- $\forall x \in G : f(x^{-1}) = [f(x)]^{-1}$.

Théorème I.1 Soit $f : G \rightarrow G'$ un morphisme de groupes.

- Pour tout sous groupe H de G , $f(H)$ est un sous groupe de G' .
- Pour tout sous groupe H' de G' , $f^{-1}(H')$ est un sous groupe de G .

En particulier $\text{Im } f$ est un sous groupe de G' et $f^{-1}\{e_{G'}\}$ est un sous groupe de G .

Définition 4 (Noyau) Le sous groupe $f^{-1}\{e_{G'}\}$ de G est appelé le *noyau* de f . On le note $\ker f$.

Théorème I.2 Soit $f : G \rightarrow G'$ un morphisme de groupes.

- f est injective si et seulement si $\ker f = \{e_G\}$.
- f est surjective si et seulement si $\text{Im } f = G'$.

I.4 Le groupe $(\mathbb{Z}, +)$ des entiers relatifs

$(\mathbb{Z}, +)$ est un groupe abélien d'élément neutre 0.

Si G est un groupe noté multiplicativement, pour tout $x \in G$ et pour tout $m \in \mathbb{N}^*$, le produit $\prod_{i=1}^m x$ est noté x^m .

On pose $x^0 = e_G$ et si $m \in \mathbb{Z}_-^*$, on pose $x^m = (x^{-1})^{-m}$.

Si G est un groupe noté additivement, pour tout $x \in G$ et pour tout $m \in \mathbb{N}^*$, la somme $\sum_{k=1}^m x$ est noté mx .

On pose $0x = 0_G$ et si $m \in \mathbb{Z}_-^*$, on pose $mx = (-m)(-x)$.

Théorème I.3 Soit G un groupe noté multiplicativement, pour tout $a \in G$, l'application

$$\begin{aligned} \varphi_a : \mathbb{Z} &\rightarrow G \\ m &\mapsto a^m \end{aligned}$$

est un morphisme de groupes. Et pour tout morphisme $\varphi : \mathbb{Z} \rightarrow G$, il existe $a \in G$ tel que $\varphi = \varphi_a$.

Preuve: On montre que φ_a est morphisme en distinguant les cas.

Réciproquement si $\varphi : \mathbb{Z} \rightarrow G$ est un morphisme, $a = \varphi(1)$ répond à la question.

En effet $\forall m \in \mathbb{Z}_+^* : \varphi(m) = \varphi(\underbrace{1 + \dots + 1}_{m \text{ fois}}) = \underbrace{\varphi(1) \dots \varphi(1)}_{m \text{ fois}} = \varphi(1)^m = \varphi_a(m)$.

L'égalité s'étend sans difficulté à \mathbb{Z} tout entier .

II Anneaux et Corps

II.1 Définitions-Exemples

Définition 5 (Anneau) Soit A un ensemble muni de deux lois de composition interne notées $+$ et \times (ou sans symbole) on dit $(A, +, \times)$ est un *anneau* si:

(A1) $(A, +)$ est un groupe abélien (on note 0_A son élément neutre).

(A2) \times est associative, admet un neutre (noté 1_A) et distributive par rapport à $+$.
Si en plus la loi \times est commutative l'anneau est dit commutatif.

Définition 6 Si $(A, +, \times)$ est un anneau commutatif, on dit que A est un corps si en plus

- $0_A \neq 1_A$.
- Tout élément non nul (i.e: $\neq 0_A$) est inversible pour la loi \times . On note alors l'inverse de x par x^{-1} ou $\frac{1}{x}$.

Exemple 6

1. $(\mathbb{Z}, +, \times), (\mathbb{R}^N, +, \times)$ sont des anneaux commutatifs.
2. $(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$ sont des corps.

Remarque 3 Si A est un singleton $\{a\}$, on peut définir une structure d'anneau en posant: $a + a = a \times a = a$ et donc $0_A = 1_A = a$. Cet anneau est appelé *l'anneau nul*. Un corps peut être réduit à la paire $\{0; 1\}$.

Définition 7 (Sous anneau) Soit A un anneau et B une partie de A . On dit que B est un sous anneau de A si

- $(B, +)$ est un sous groupe de $(A, +)$.
- B est stable par la loi \times : $\forall x, y \in B, x \times y \in B$.
- $1_A \in B$.

Dans ce cas les lois de A induisent une structure d'anneau sur B .

Proposition 1 (Propriété caractéristique d'un sous anneau) Soit A un anneau et B une partie de A . B est un sous anneau de A si et seulement si

- $1_A \in B$.
- $\forall (x, y) \in B : x \times y \in B$ et $x - y \in B$.

P II.1 (Intersection de sous anneaux) Toute intersection de sous anneaux de A est un sous anneau de A .

Définition 8 (Sous corps) Soit K un corps et L une partie de K . On dit que L est un sous corps de K si

- $(L, +, \times)$ est un sous anneau de $(K, +, \times)$.
- $\forall x \in L \setminus \{0_K\} : x^{-1} \in L$.

Proposition 2 (Propriété caractéristique d'un sous corps) Soit K un corps et L une partie de K . L est un sous corps de K si et seulement si

- $1_K \in L$.
- $\forall (x, y) \in L : x \times y \in L$ et $x - y \in L$.
- $\forall x \in L \setminus \{0_K\} : x^{-1} \in L$.

P II.2 (Intersection de sous corps) Toute intersection de sous corps de K est un sous corps de K .

Définition 9 (Morphisme d'anneaux) Soient deux anneaux A et A' . On dit qu'une application $f : A \rightarrow A'$ est morphisme d'anneaux si

- $\forall x, y \in A : f(x + y) = f(x) + f(y)$ et $f(x \times y) = f(x) \times f(y)$.
- $f(1_A) = 1_{A'}$.

Si A et A' sont des corps, le morphisme est dit morphisme de corps.

Exercice 2 Déterminer tous les morphismes de l'anneau \mathbb{Z} vers un anneau A .

II.2 Règles de calcul dans un anneau

On considère un anneau $(A, +, \times)$. On a les règles de calcul suivantes:

$$\text{P II.3 } \forall x \in A : 0_A \times x = x \times 0_A = 0_A.$$

$$\text{P II.4 } \forall x \in A : -x = (-1_A) \times x = x \times (-1_A).$$

$$\text{P II.5 } \forall x, y \in A : (-x) \times y = x \times (-y) = -x \times y \text{ et } (-x) \times (-y) = x \times y.$$

Notations

Pour tout $n \in \mathbb{N}$, et pour tout $x \in A$, on note

$$\bullet nx = \begin{cases} \underbrace{x + x + \dots + x}_{n \text{ fois}} & \text{si } n \neq 0 \\ 0 & \text{si } n = 0. \end{cases};$$

$$\bullet (-n)x = n(-x).$$

$$\bullet x^n = \begin{cases} \underbrace{x \times x \times \dots \times x}_{n \text{ fois}} & \text{si } n \neq 0 \\ 1_A & \text{si } n = 0. \end{cases};$$

$$\bullet x^{-n} \text{ n'a de sens que si } x \text{ est inversible.}$$

P II.6 (Binôme de Newton) Si $(x, y) \in A^2$ tel que $x \times y = y \times x$, alors pour tout $n \in \mathbb{N}$, on a

$$(x + y)^n = \sum_{k=0}^n C_n^k x^k y^{n-k}$$

Et pour tout $n \in \mathbb{N}^*$, on a:

$$x^n - y^n = (x - y) \left(x^{n-1} + x^{n-2}y + \dots + xy^{n-2} + y^{n-1} \right) = (x - y) \sum_{k=0}^{n-1} x^{n-1-k} y^k.$$

Preuve: Par récurrence sur n et à l'aide des formules de Pascal.

Pour la formule de factorisation, on raisonne par récurrence en remarquant que

$$\begin{aligned} x^{n+1} - y^{n+1} &= xx^n - xy^n + xy^n - yy^n \\ &= x(x^n - y^n) + (x - y)y^n \end{aligned}$$

$$\text{Donc } x^{n+1} - y^{n+1} = (x - y) \left(\sum_{k=0}^{n-1} x^{n-k} y^k + y^n \right) = (x - y) \left(\sum_{k=0}^n x^{n-k} y^k \right). \text{ cqfd.}$$

Conséquence La somme des n premiers termes d'une suite géométrique

Pour tout $x \in A$, si $1_A - x$ est inversible alors pour tout $n \in \mathbb{N}$, on a

$$1 + x + x^2 + \dots + x^n = \frac{1 - x^{n+1}}{1 - x}.$$

Définition 10 (éléments nilpotents dans un anneau) Un élément $a \neq 0_A$ d'un anneau A est dit nilpotent s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0_A$. Le plus petit entier n vérifiant $a^n = 0$ s'appelle l'indice de nilpotence de l'élément a .

Proposition 3 Si a est nilpotent d'indice n alors $1_A - x$ est inversible et on a

$$(1 - x)^{-1} = 1 + x + x^2 + \dots + x^{n-1}.$$

II.3 Groupe $\mathcal{U}(\mathbf{A})$ des éléments inversibles

Théorème II.1 Soit un anneau $(\mathbf{A}, +, \times)$. On note $\mathcal{U}(\mathbf{A})$ l'ensemble des éléments inversibles pour la loi \times :

$$\mathcal{U}(\mathbf{A}) = \{a \in \mathbf{A} \mid \exists a' \in \mathbf{A} : aa' = a'a = 1_{\mathbf{A}}\}$$

Alors muni de la seconde loi de l'anneau, l'ensemble $(\mathcal{U}(\mathbf{A}), \times)$ a une structure de groupe: c'est le groupe des unités de l'anneau \mathbf{A} .

Exemple 7 $\mathcal{U}(\mathbb{Z}) = \{-1; 1\}$, dans un anneau \mathbf{A} quelconque on a $\{-1_{\mathbf{A}}; 1_{\mathbf{A}}\} \subset \mathcal{U}(\mathbf{A})$. Si \mathbf{A} est un corps alors $\mathcal{U}(\mathbf{A}) = \mathbf{A} \setminus \{0_{\mathbf{A}}\}$.

II.4 Anneau intègre

Définition 11 (Diviseur de zéro) Soit un anneau $(\mathbf{A}, +, \times)$ non nul. Un élément $a \neq 0$ de \mathbf{A} est appelé diviseur de zéro s'il existe $b \neq 0$ tel que $a \times b = 0_{\mathbf{A}}$ ou $b \times a = 0_{\mathbf{A}}$.

Exemple 8 Dans $\mathbf{A} = \mathbb{R}^{\mathbb{R}}$ on considère $f, g : \mathbb{R} \rightarrow \mathbb{R}$ telles que:

$$\begin{cases} f(x) = 1 \text{ si } x > 0, \\ f(x) = 0 \text{ si non} \end{cases} \quad \text{et} \quad \begin{cases} g(x) = 0 \text{ si } x > 0, \\ g(x) = 1 \text{ si non.} \end{cases}$$

On a $fg = gf = 0$ mais $f \neq 0_{\mathbf{A}}$ et $g \neq 0_{\mathbf{A}}$...

Définition 12 (Anneau intègre) On dit qu'un anneau $(\mathbf{A}, +, \times)$ non nul est intègre s'il commutatif et sans diviseurs de zéro:

1. La loi \times est commutative;
2. $\forall x, y \in \mathbf{A} : x \times y = 0_{\mathbf{A}} \implies x = 0_{\mathbf{A}}$ ou $y = 0_{\mathbf{A}}$.

Remarque 4 Dans un anneau intègre, on peut (simplifier) à gauche et à droite:

$$\forall a, x, y \in \mathbf{A} : ax = ay \implies x = y \text{ et } xa = ya \implies x = y.$$

Cette propriété est fautive dans un anneau non intègre. On dit alors que tout élément est régulier.

Exemple 9

1. Tout corps est intègre et tout sous anneau d'un corps est intègre.
2. Les anneaux $\mathbb{R}^{\mathbb{N}}$ et $\mathbb{R}^{\mathbb{R}}$ ne sont pas intègres...

Corps des fractions d'un anneau intègre

Théorème II.2 (admis) Soit un anneau $(\mathbf{A}, +, \times)$ intègre. Il existe un corps \mathbf{K} unique, à isomorphisme près, tel que \mathbf{A} soit un sous anneau de \mathbf{K} et tout élément de \mathbf{K} s'écrit sous la forme $\frac{a}{b}$ avec $a, b \in \mathbf{A}$ et $b \neq 0_{\mathbf{A}}$. à isomorphisme près: si \mathbf{K}' est un corps vérifiant les mêmes propriétés alors il existe un isomorphisme de corps entre \mathbf{K} et \mathbf{K}' . \mathbf{K} est alors appelé le corps des fractions de \mathbf{A} .

Exemple 10 \mathbb{Q} est le corps des fractions de \mathbb{Z} .

II.5 L'anneau \mathbb{Z} des entiers relatifs

II.5.1 Divisibilité dans \mathbb{Z}

Définition 13 Soient a et b deux entiers relatifs. On dit que b divise a s'il existe $q \in \mathbb{Z}$ tel que $a = qb$. On note alors b/a . Si b divise a , on dit que a est un multiple de b .

Remarque 5 Ces définitions s'étendent à un anneau quelconque.

Exemple 11

- $\forall n \in \mathbb{Z} : n/0$.
- $\forall n \in \mathbb{Z} : 0/n \iff n = 0$.

Proposition 4 Soient a, b dans \mathbb{Z} , on a les équivalences suivantes:

$$\begin{aligned} a/b &\iff b \in a\mathbb{Z} \iff b\mathbb{Z} \subset a\mathbb{Z} \\ (a/b \text{ et } b/a) &\iff b\mathbb{Z} = a\mathbb{Z} \iff a = b \text{ ou } a = -b. \end{aligned}$$

Théorème II.3 (Division euclidienne) $\forall (a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}, \exists!(q, r) \in \mathbb{Z} \times \mathbb{Z} \mid a = bq + r$ et $0 \leq r < |b|$.
 q est appelé quotient et r le reste dans la division euclidienne de a par b .

Preuve: 1^{er} cas: $a, b \in \mathbb{N}$, déjà démontré.

2^{ème} cas: En général $|a| = |b|q' + r'$, donc $a = b \cdot \text{signe}(ab) \cdot q' + \text{signe}(a) \cdot r'$.

Alors si $a \geq 0$, on pose $r = r'$ et $q = \text{signe}(ab) \cdot q'$, et si $a < 0$, on pose $r = \text{signe}(a) \cdot r' + |b|$ et $q = \text{signe}(ab) \cdot q' - \text{signe}(b)$.

Pour l'unicité c'est le même raisonnement que dans le cas de \mathbb{N} . •

Algorithme de la division euclidienne

On suppose a et b deux entiers naturels $b > 0$.

1. Initialisation: $q \leftarrow 0$;
2. Tant que $a \geq b$
Faire
 $q \leftarrow q + 1; a \leftarrow a - b$;
Fin Faire
3. $r \leftarrow a$;
4. Résultat: $q; r$.

Exemple 12 $a = 17; b = 3$

$$\begin{array}{cccccc} a & 17 & 14 & 11 & 8 & 5 & 2 \\ q & 0 & 1 & 2 & 3 & 4 & 5 \end{array} \quad \text{donc } r = 2 \text{ et } q = 5, \text{ soit } 17 = 5 \times 3 + 2.$$

Théorème II.4 (Sous groupe de $(\mathbb{Z}, +)$) Les sous groupes de \mathbb{Z} sont les ensembles de la forme

$$a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$$

où $a \in \mathbb{Z}$.

Preuve: Soit $\mathbf{G} \neq \{0\}$ un sous groupe de \mathbb{Z} . On considère $a = \min \mathbf{G} \cap \mathbb{N}^*$, et on montre que $\mathbf{G} = a\mathbb{Z}$.

On a $a \in \mathbf{G}$ donc $a\mathbb{Z} \subset \mathbf{G}$. Et réciproquement si $m \in \mathbf{G}$ la Division Euclidienne de m par a donne $m = qa + r$ donc $r = m - qa \in \mathbf{G} \cap \llbracket 1, a \rrbracket$, donc $r = 0$. •

II.5.2 Ordre d'un élément dans un groupe

Soit G un groupe et $a \in G$. On considère le morphisme de groupes

$$\begin{aligned} \varphi_a : \mathbb{Z} &\longrightarrow G \\ n &\longmapsto a^n \quad (na \text{ si } G \text{ est noté additivement}). \end{aligned}$$

Son noyau $\ker \varphi_a$ est un sous groupe de $(\mathbb{Z}, +)$, donc il existe un unique $n \in \mathbb{N}$ tel que $\ker \varphi_a = n\mathbb{Z}$. Si φ_a n'est pas injective $n \in \mathbb{N}^*$.

Définition 14 (Ordre d'un élément) Si φ_a n'est pas injective, l'unique entier n tel que $\ker \varphi_a = n\mathbb{Z}$ est appelé l'ordre de a .

Si φ_a est injective alors $\forall n \in \mathbb{N}^* : a^n \neq e_G$. On dit que a est d'ordre infini.

Remarque 6 Par définition si $\text{ordre}(a) = n \in \mathbb{N}^*$, alors n est le plus petit entier naturel non nul vérifiant $a^n = e_G$ (ou $na = 0_G$ dans le cas additif):

$$\text{ordre}(a) = \min \{m \in \mathbb{N}^* \mid a^m = e_G\}.$$

Proposition 5 (Caractérisation de l'ordre d'un élément) Soit G un groupe et $a \in G$, alors on a l'équivalence suivante

$$\text{ordre}(a) = n \iff \begin{cases} a^n = e_G; \\ \forall k \in \mathbb{N} : [a^k = e_G \implies n/k]. \end{cases}$$

Exemple 13

1. $\text{ordre}(e_G) = 1$.
2. $G = \{-1; 1\}$ muni de la multiplication $\text{ordre}(-1) = 2$.
3. Dans (\mathbb{C}^*, \times) , $\text{ordre}(i) = 4$; $\text{ordre}(j = e^{i\frac{2\pi}{3}}) = 3$; en général $\text{ordre}(e^{i\frac{2\pi}{n}}) = n$.

Définition 15 (Sous groupe engendré par un élément) Soit G un groupe et $a \in G$. Le sous groupe $\text{Im } \varphi_a = \{a^n \mid n \in \mathbb{Z}\}$ de G est appelé sous groupe engendré par a . On le notera $\langle a \rangle$.

Théorème II.5 (Description de $\langle a \rangle$) Soit G un groupe et $a \in G$ d'ordre fini $n \in \mathbb{N}^*$. Le groupe engendré par a est fini de cardinal n et l'application

$$\begin{aligned} \llbracket 0, n-1 \rrbracket &\longrightarrow \langle a \rangle \\ k &\longmapsto a^k \end{aligned}$$

est bijective. i.e: $\langle a \rangle = \{e_G = a^0; a; a^2; \dots; a^{n-1}\}$.

Remarque 7 Dans la cas additif remplacer a^k par ka et e_G par 0_G .

Preuve: D'abord $\forall k, k' \in \llbracket 0, n-1 \rrbracket$:

$$a^k = a^{k'} \iff \varphi_a(k) = \varphi_a(k') \iff k - k' \in \ker \varphi_a \iff k - k' = 0.$$

D'autre part $\forall k \in \mathbb{Z}$, la D.E de k par n donne $k = aq + r$ et $a^k = a^r$ avec $r \in \llbracket 0, n-1 \rrbracket$.

Remarque 8 Si a est d'ordre infini $\langle a \rangle$ est isomorphe à \mathbb{Z} .

Définition 16 (Groupe monogène, groupe cyclique) Un groupe G est dit *monogène* s'il existe $a \in G$ tel que $G = \langle a \rangle$. Si en plus a est d'ordre fini G est dit *cyclique*, dans ce cas $G = \{e_G = a^0; a; a^2; \dots; a^{n-1}\}$, l'ordre de a est aussi appelé l'ordre de G .

Exemple 14 Tout groupe à deux éléments ou à trois éléments est cyclique.

Exercice 3 Donner un groupe cyclique à 4 éléments; à n éléments $n \geq 1$.

Proposition 6 Tout groupe monogène est abélien.

Remarque 9 Si G est un groupe et A une partie non vide de G . On définit le sous groupe de G engendré par A comme étant l'intersection de tous les sous groupes contenant A .