
Groupes

EL AMDAOUI Mustapha,

Lycée IBN TIMIYA,
site web: www.elamdaoui.com,
email: elamdaoui@gmail.com

Niveau: MP

Table des matières

I Groupes	2
I.1 Définitions et exemples	2
I.2 Groupe produit	3
I.3 Les itérés d'un élément	3
II Sous-groupes	4
II.1 Sous-groupe	4
II.2 Les sous-groupes de $(\mathbb{Z}, +)$	5
II.3 Sous-groupe engendré par une partie	6
III Morphisme de groupes	7
III.1 Morphisme de groupes	8
III.2 Noyau et image d'un endomorphisme	9
IV Groupes monogènes et cycliques	10
IV.1 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$	10
IV.2 Ordre d'un élément, d'un groupe	11
IV.3 Théorème de Lagrange	13

I Groupes

I.1 Définitions et exemples

Définition 1: Groupe

On appelle groupe un ensemble G muni d'une loi de composition interne $\star$ vérifiant :

- la loi $\star$ est associative :

$$\forall x, y, z \in G : (x \star y) \star z = x \star (y \star z)$$

On notera alors $x \star y \star z$ cette quantité commune

- G possède un élément neutre : $\exists e \in G$ tel que

$$\forall x \in G, \quad x \star e = e \star x = x$$

- Tout élément x de G admet un symétrique, c'est-à-dire $\forall x \in G, \exists x' \in G$ tel que $x \star x' = x' \star x = e$

Si de plus $\forall x, y \in G : x \star y = y \star x$, on dit que la loi $\star$ est commutative, et que le groupe est abélien (ou commutatif).

Exemple

1. Si $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}\}$ alors $(\mathbb{K}, +)$ est un groupe abélien ;
2. Si $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}, \mathbb{Q}\}$ alors $(\mathbb{K}^*, \times)$ est un groupe abélien.
3. $(\text{GL}_n(\mathbb{R}), \times)$ est un groupe d'élément neutre I_n non abélien lorsque $n \geq 2$

Notation :

L'élément symétrique de x dans un groupe multiplicatif (resp additif) se note x^{-1} (resp $-x$) et est appelé inverse (resp opposé) de x

Propriété 1

Soit $(G, \star)$ un groupe.

1. G est non vide ;
2. L'élément neutre dans un groupe est unique ;
3. Le symétrique d'un élément x est unique, noté x^{-1} .

Preuve:

1. G est non vide car il contient un élément neutre ;
2. Soit e et e' deux éléments neutres de G pour $\star$. On a $e \star e' = e'$ car e est neutre et $e \star e' = e$ car e' est neutre, donc $e = e'$
3. Soit x' et x'' deux symétriques de x dans G pour $\star$. Par associativité, on a

$$x'' = x'' \star e = x'' \star (x \star x') = (x'' \star x) \star x' = e \star x' = x'$$

Remarque :

1. En notation additive, l'inverse de x se note $-x$ et est appelé l'opposé de x
2. Pour tout $a \in G$, les applications $x \mapsto a \star x$ et $x \mapsto x \star a$ sont des bijections de G dans G .
3. Pour tous $a, b \in G$, il existe un unique $x \in G$ tel que $a \star x = b$ à savoir $x = a^{-1} \star b$

Propriété 2

Soit $(G, \star)$ un groupe d'élément neutre e , alors

1. $e^{-1} = e$;
2. Pour tout $x \in G : (x^{-1})^{-1} = x$
3. Pour tous $x, y \in G : (x \star y)^{-1} = y^{-1} \star x^{-1}$
4. Pour tous $x_1, \dots, x_n \in G :$

$$(x_1 \star \dots \star x_n)^{-1} = x_n^{-1} \star \dots \star x_1^{-1}$$

Preuve:

1. e est le neutre de G , donc $e \star e = e$, alors par unicité $e^{-1} = e$
2. Par unicité de l'élément inverse
3. A cause de l'associativité de la loi $\star$ on trouve

$$\begin{cases} (x \star y) \star (y^{-1} \star x^{-1}) = e \\ (y^{-1} \star x^{-1}) \star (x \star y) = e \end{cases}$$

Donc, par l'unicité de l'élément symétrique, $(x \star y)^{-1} = y^{-1} \star x^{-1}$

4. Généralisation de l'assertion 3

I.2 Groupe produit

Soient $\star_1, \star_2, \dots, \star_n$ des lois de composition interne sur des ensembles $G_1, G_2, \dots, G_n$.

On appelle loi produit sur $G = \prod_{i=1}^n G_i$ la loi $\star$ définie par

$$(x_1, \dots, x_n) \star (y_1, \dots, y_n) := (x_1 \star_1 y_1, \dots, x_n \star_n y_n)$$

Propriété 3

Soit $(G_1, \star_1), (G_2, \star_2), \dots, (G_n, \star_n)$ des groupes de neutres respectifs $e_1, \dots, e_n$. Alors

$G = \prod_{i=1}^n G_i$ muni de la loi produit $\star$ est un groupe.

- de neutre $e = (e_1, \dots, e_n)$.
- l'inverse d'un élément $(x_1, \dots, x_n) \in G$ est $(x_1^{-1}, \dots, x_n^{-1})$
- Tous les groupes $(G_1, \star_1), (G_2, \star_2), \dots, (G_n, \star_n)$ sont abéliens si, et seulement si, le groupe $(G, \star)$ est abélien

Preuve:

Laisser au lecteur

Exemple

Si $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}\}$ alors, pour $n \geq 2$, $(\mathbb{K}^n, +)$ est un groupe abélien

Exemple

Pour $(\mathbb{R}_+^*, \cdot)$ et $(\mathbb{R}, +)$, la loi produit sur $\mathbb{R}_+^* \times \mathbb{R}$ que nous notons $\star$ est définie par :

$$(r, \theta) \star (r', \theta') := (r \cdot r', \theta + \theta')$$

$(\mathbb{R}_+^* \times \mathbb{R}, \star)$ est alors un groupe abélien de neutre $e = (1, 0)$. De plus $(r, \theta)^{-1} = \left(\frac{1}{r}, -\theta\right)$

I.3 Les itérés d'un élément

Soit $(G, \star)$ un groupe d'élément neutre e .

Définition 2: Les itérés d'un élément

Soit $x \in G$. On définit x^n pour tout $n \in \mathbb{N}$ par récurrence :

- $x^0 = e$
- $\forall n \in \mathbb{N} \quad x^{n+1} = x^n \star x$

Pour $n \in \mathbb{Z}_-$, on définit $x^n = (x^{-1})^{-n}$

Notation :

Lorsque la loi est notée additivement, les itérés de x ne notent $n.x$

Propriété 4

Soit $x \in G$. Alors :

$$\forall p, q \in \mathbb{Z} \quad \begin{cases} x^{p+q} = x^p \star x^q \\ (x^p)^q = x^{pq} \end{cases}$$

Si $x, y \in G$ commutent, c'est-à-dire si $x \star y = y \star x$, on a :

$$\forall p \in \mathbb{Z} \quad (x \star y)^p = x^p \star y^p$$

En particulier pour tout $x \in G : (x^n)^{-1} = (x^{-1})^n = x^{-n}$.

Preuve:

- Commençons par le cas où p et q sont positifs, et raisonnons par récurrence sur $n = p + q$.

Initialisation : Si $n = 0$, $p = q = 0$, et le résultat est immédiat.

Hérédité : Supposons le résultat vrai pour $n \in \mathbb{N}$. Soient p et q dans $\mathbb{Z}$ tels que $p + q = n + 1$. Supposons par exemple $p \neq 0$.

On écrit

$$x^p \star x^q = x \star (x^{p-1} \star x^q) = x \star x^n = x^{n+1}$$

d'où le résultat.

- Le cas où p et q sont négatifs en découle immédiatement.
- Supposons $p > 0$ et $q < 0$. Si par exemple $|p| \geq |q|$, on écrit $p = -q + r$ avec $r \geq 0$. On a alors d'après le cas positif $x^p = x^{-q} \star a^r$. En multipliant par x^q , on obtient : $x^p \star x^q = a^r \star x^{-q} \star x^q$. Or x^{-q} est l'inverse de x^q . D'où $x^p \star x^q = a^r = x^{p+q}$

II Sous-groupes

$(G, \star)$ un groupe d'élément neutre e .

II.1 Sous-groupe**Définition 3**

Soit $(G, \star)$ un groupe. On dit qu'une partie $H \subset G$ est un sous-groupe de G si, et seulement, si :

1. $H \neq \emptyset$;
2. la partie H est stable par la loi $\star : \forall x, y \in H, \quad x \star y \in H$;
3. Pour tout $x \in H, x^{-1} \in H$.

Notation :

En notation additive, la deuxième et la troisième assertions s'écrivent :

2. la partie H est stable par la loi $+$: $\forall x, y \in H, \quad x + y \in H$;
3. Pour tout $x \in H, -x \in H$.

Exemple: Les sous-groupes triviaux

$\{e\}$ et G sont deux sous-groupes de G appelés sous-groupes triviaux de G

Définition 4

Un sous-groupe de G est dit propre s'il est distinct de G et $\{e\}$

Propriété 5: Caractérisation d'un sous-groupe

Soit $(G, \star)$ un groupe. Une partie $H \subset G$ est un sous-groupe de G si et seulement si :

1. $H \neq \emptyset$;
2. Pour tous $x, y \in H : \quad x \star y^{-1} \in H$.

Preuve:

- $\Rightarrow$ Soit H un sous-groupe de $(G, \star)$, alors $H \neq \emptyset$.
 Soit $x, y \in H$. Avec $y \in H$, on a $y^{-1} \in H$, puis $x \star y^{-1} \in H$.
 $\Leftarrow$ On suppose que pour tous $x, y \in H$, $x \star y^{-1} \in H$. Soit $x, y \in H$
- $x \in H$, donc $e = x \star x^{-1} \in H$
 - $e, x \in H$, donc $x^{-1} = e \star x^{-1} \in H$
 - $x, y \in H$, alors $x, y^{-1} \in H$ et $x \star y = x \star (y^{-1})^{-1} \in H$

Propriété 6

Soit H un sous-groupe d'un groupe $(G, \star)$, alors $(H, \star)$ est un groupe de même neutre.

Preuve:

- La stabilité de H par $\star$ montre que la restriction de $\star$ à $H \times H$ est une loi de composition interne
- $\star$ est associative
- $e \in H$, donc e est neutre de H
- Tout élément de H admet un symétrique dans H

Exemple

Soit $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$. Montrer que $(\mathbb{U}, \times)$ est un groupe.

$\mathbb{U}$ est une partie du groupe $(\mathbb{C}^*, \times)$

- $\mathbb{U} \neq \emptyset$, car il contient 1 ;
- Soit $z, z' \in \mathbb{U}$, alors $z' \neq 0$ et $\left| \frac{z}{z'} \right| = \frac{|z|}{|z'|} = 1$, donc $\frac{z}{z'} \in \mathbb{U}$

Donc $\mathbb{U}$ est un sous-groupe de $(\mathbb{C}^*, \times)$, puis $(\mathbb{U}, \times)$ est un groupe

Exemple

Pour $a \in \mathbb{R}$ on note $a\mathbb{Z} = \{ka \mid k \in \mathbb{Z}\}$.

Montrons que $a\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$

On a évidemment $a\mathbb{Z} \subset \mathbb{R}$

- $a\mathbb{Z} \neq \emptyset$ car $0 = a \times 0 \in a\mathbb{Z}$
- Pour $x, y \in a\mathbb{Z}$, on peut écrire $x = ka$ et $y = k'a$ avec $k, k' \in \mathbb{Z}$ et alors $x - y = ka - k'a = (k - k')a$ avec $k - k' \in \mathbb{Z}$ donc $x - y \in a\mathbb{Z}$

II.2 Les sous-groupes de $(\mathbb{Z}, +)$ **Théorème 1: Caractérisation des sous-groupes de $(\mathbb{Z}, +)$**

Soit H un sous groupe de $(\mathbb{Z}, +)$, alors il existe un unique entier $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$

Preuve:

- **Existence** : Si $H = \{0\}$, on écrit $H = 0\mathbb{Z}$.
 Si $H \neq \{0\}$, on pose

$$A = \{x \in H \mid x \geq 1\} = H \cap \mathbb{N}^*$$

Soit x un élément non nul de H , alors ou bien $x \geq 1$, ou bien $-x \geq 1$, donc $A \neq \emptyset$.

Soit $n \geq 1$ le plus petit élément de A , (propriété fondamentale de $\mathbb{N}$), montrons que $H = n\mathbb{Z}$. Comme $n \in H$, il résulte que $n\mathbb{Z} \subset H$.

Réciproquement, soit $m \in H$, effectuons la division euclidienne de m par n

$$m = nq + r, \quad 0 \leq r < n.$$

De $m \in H$ et $n \in H$, il résulte, H étant un sous-groupe de $\mathbb{Z}$, que $r = m - nq \in H$. D'où $r = 0$, sinon r serait un élément de A strictement plus petit que n . On a donc $m = nq \in n\mathbb{Z}$. D'où $H \subset n\mathbb{Z}$. On en déduit $H = n\mathbb{Z}$.

- **Unicité** : Si $n\mathbb{Z} = m\mathbb{Z}$, m est multiple de n , et n est multiple de m , d'où $m = |m| = |n| = n$.

II.3 Sous-groupe engendré par une partie

Lemme 1

Soit $(H_i)_{i \in I}$ une famille de sous-groupes d'un groupe $(G, \star)$ avec $I \neq \emptyset$.

Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de $(G, \star)$

Preuve:

- $\bigcap_{i \in I} H_i$ est une partie non vide de G , car H_i contient e pour tout $i \in I$
- Soit $x, y \in \bigcap_{i \in I} H_i$. Soit $i \in I$, alors $x, y \in H_i$, donc $x \star y^{-1} \in H_i$. Ainsi $x \star y^{-1} \in \bigcap_{i \in I} H_i$

Ce qui montre que $\bigcap_{i \in I} H_i$ est un sous-groupe de $(G, \star)$

Propriété 7

Soit S une partie d'un sous-groupe $(G, \star)$; désignons par $\mathcal{G}\mathbf{r}(S)$ l'intersection de tous les sous-groupes de $(G, \star)$ contenant S . Alors

1. $\mathcal{G}\mathbf{r}(S)$ est un sous-groupe de $(G, \star)$
2. $\mathcal{G}\mathbf{r}(S)$ est le plus petit sous-groupe de $(G, \star)$, au sens de l'inclusion, contenant S

$\mathcal{G}\mathbf{r}(S)$ est appelé le sous-groupe engendré par S est noté aussi $\mathcal{G}\mathbf{r}(S)$

Preuve:

1. L'ensemble $\mathcal{H}_S$ des sous-groupes de $(G, \star)$ contenant S est non vide puisqu'elle contient G . Comme intersection de sous-groupes de G , l'ensemble $\mathcal{G}\mathbf{r}(S) = \bigcap_{H \in \mathcal{H}_S} H$ est un sous-groupe de G
2. Si H un sous-groupe de $(G, \star)$ contenant S , alors $\mathcal{G}\mathbf{r}(S) \subset H$.

Exemple

$$\mathcal{G}\mathbf{r}(\emptyset) = \{e\}$$

Propriété 8: Caractérisation des sous-groupes engendrés

Soit S une partie non vide d'un sous-groupe $(G, \star)$, alors

$$\mathcal{G}\mathbf{r}(S) = \left\{ \prod_{i=1}^n x_i^{\alpha_i}, n \in \mathbb{N}^*, \forall i \in \llbracket 1, n \rrbracket, x_i \in S, \alpha_i \in \{-1, 1\} \right\} \quad (1)$$

Preuve:

Désignons par H le second membre de (1) et démontrons que $H = \mathcal{G}\mathbf{r}(S)$. On remarque que tout $x \in S$ appartient à H , d'où $S \subset H$.

Montrons que H est un sous-groupe de $(G, \star)$

- $H \neq \emptyset$ car $S \subset H$ et $S \neq \emptyset$
- Soit $x, y \in H$, alors il existe $n, m \in \mathbb{N}^*$, $x_1, \dots, x_n, y_1, \dots, y_m \in S$ et $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m \in \{-1, 1\}$ tels que $x = x_1^{\alpha_1} \star x_2^{\alpha_2} \star \dots \star x_n^{\alpha_n}$ et $y = y_1^{\beta_1} \star y_2^{\beta_2} \star \dots \star y_m^{\beta_m}$. Alors

$$xy^{-1} = x_1^{\alpha_1} \star x_2^{\alpha_2} \star \dots \star x_n^{\alpha_n} \star y_m^{-\beta_m} \star \dots \star y_2^{-\beta_2} \star y_1^{-\beta_1} \in H$$

On en déduit que H est élément de $\mathcal{H}_S$, d'où l'inclusion $\mathcal{G}\mathbf{r}(S) \subset H$.

Montrons que H est le plus petit ?

Soit H_0 un sous-groupe de G contenant S et soit $x \in H$, alors il existe $n \in \mathbb{N}^*$, $x_1, \dots, x_n \in S$ et $\alpha_1, \dots, \alpha_n \in \{-1, 1\}$ tels que $x = x_1^{\alpha_1} \star x_2^{\alpha_2} \star \dots \star x_n^{\alpha_n}$.

On a $x_i \in H_0$, donc $x_i^{-1} \in H_0$. Mais $\alpha_i \in \{-1, 1\}$, alors $x_i^{\alpha_i} \in H_0$. Ainsi, par stabilité de H_0 , $x \in H_0$ puis l'inclusion $H \subset H_0$

Notation :

Si la loi de composition du groupe G est notée *additivement*, on note

$$\mathcal{G}\mathbf{r}(S) = \left\{ \sum_{i=1}^n \alpha_i x_i, n \in \mathbb{N}^*, \forall i \in \llbracket 1, n \rrbracket, x_i \in S, \alpha_i \in \{-1, 1\} \right\} \quad (2)$$

Corollaire 1

Pour tout $a \in G$, alors

$$\mathcal{G}\mathbf{r}(a) = \{a^k \mid k \in \mathbb{Z}\}$$

On note aussi $\mathcal{G}\mathbf{r}(a)$

Exemple

Dans $(\mathbb{C}^*, \times)$

$$\begin{aligned} \mathcal{G}\mathbf{r}\left(e^{\frac{2i\pi}{n}}\right) &= \left\{e^{\frac{2i\pi}{n}} \mid k \in \mathbb{Z}\right\} \\ &= \left\{e^{\frac{2i\pi}{n}} \mid 0 \leq k \leq n-1\right\} \\ &= \mathbb{U}_n \end{aligned}$$

Définition 5: Partie génératrice

Si S est une partie non vide de G telle que $\mathcal{G}\mathbf{r}(S) = G$, on dit que S est *partie génératrice* du groupe G , ou que S est un *ensemble de générateur* de G , ou encore que S engendre G

Exemple: Partie génératrice de $\mathfrak{S}_n$

Le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions

Par récurrence

- **Initialisation** : Pour $n = 2$, nous n'avons rien à démontrer car $\mathfrak{S}_2 = \{e, (1,2)\}$ et $e = (1,2)(1,2)$ est le produit de transpositions.
- **Hérédité** : Soit $n \geq 2$. On suppose que toute permutation de $\llbracket 1, n \rrbracket$ peut être décomposée comme un produit de transpositions. Soit $\sigma \in \mathfrak{S}_{n+1}$. Distinguons deux cas :

1. **Premier cas** : $\sigma(n+1) = n+1$.

Alors $\sigma_{\llbracket 1, n \rrbracket}$ est une permutation de $\llbracket 1, n \rrbracket$ que nous notons σ' . Par hypothèse de récurrence, σ' est donc un produit de transpositions dans $\mathfrak{S}_n$: $\sigma' = \tau'_1 \cdots \tau'_p$.

Pour tout $k \in \llbracket 1, p \rrbracket$, notons τ_k la permutation de $\llbracket 1, n+1 \rrbracket$ égale à τ'_k sur $\llbracket 1, n \rrbracket$ et telle que $\tau_k(n+1) = n+1$; clairement, τ_k est une transposition de $\mathfrak{S}_{n+1}$, tout comme τ'_k . La relation $\sigma' = \tau'_1 \cdots \tau'_p$ (dans $\mathfrak{S}_n$) devient alors : $\sigma = \tau_1 \cdots \tau_p$ (dans $\mathfrak{S}_{n+1}$), et donc σ est un produit de transpositions.

2. **Second cas** : $\sigma(n+1) \neq n+1$.

Notons τ_0 la transposition $((n+1)\sigma(n+1))$. Alors $\tau_0\sigma(n+1) = n+1$. On est donc ramené au cas précédent : $\tau_0\sigma$ est un produit de transpositions : $\tau_0\sigma = \tau_1 \cdots \tau_p$. Multiplions par τ_0 à gauche, en remarquant que $\tau_0^2 = \text{Id}$: $\sigma = \tau_0 \cdots \tau_p$. Bref, σ est un produit de transpositions.

Définition 6: Groupe monogène, groupe cyclique

1. S'il existe $x \in G$ tel que $\mathcal{G}\mathbf{r}(x) = G$, le groupe est dit *monogène*.
2. Un *groupe cyclique* est un groupe monogène fini.

Exemple

1. $(\mathbb{Z}, +)$ est monogène car $\mathbb{Z} = \mathcal{G}\mathbf{r}(1)$
2. $(\mathbb{U}_n, \times)$ est cyclique car $\mathbb{U}_n = \mathcal{G}\mathbf{r}\left(e^{\frac{2i\pi}{n}}\right)$
3. $(\mathbb{R}, +)$ n'est pas monogène

Propriété 9

Tout groupe monogène est abélien

III Morphisme de groupes

Soit $(G, \cdot)$ et $(G', \star)$ sont deux groupes de neutres respectifs e et e' .

III.1 Morphisme de groupes

Définition 7

On dit qu'une application $f : G \longrightarrow G'$ est un morphisme de groupes si :

$$\forall x, y \in G, \quad f(x \cdot y) = f(x) \star f(y)$$

On dira aussi que :

1. f est un isomorphisme (de groupes) si f est bijective ;
2. f est un endomorphisme²⁶ du groupe $(G, *)$ si $(G', \cdot) = (G, *)$;
3. f est un automorphisme du groupe $(G, *)$ si f est à la fois un isomorphisme et un endomorphisme, c'est-à-dire si $f : (G, *) \rightarrow (G, *)$ est un morphisme (de groupes) bijectif.

Exemple: Signature

La signature $\varepsilon : \mathfrak{S}_n \longrightarrow \{-1, 1\}$ définie par

$$\forall \sigma \in \mathfrak{S}_n, \quad \varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

est un morphisme du groupe $(\mathfrak{S}_n, \circ)$ vers $(\{-1, 1\}, \times)$

Exemple: Déterminant

$\det : \text{GL}_n(\mathbb{K}) \longrightarrow \mathbb{K}^*$ est un morphisme du groupes surjectif de $(\text{GL}_n(\mathbb{K}), \times)$ vers $(\mathbb{K}^*, \times)$.

Si A appartient à $\text{GL}_n(\mathbb{K})$, elle est inversible, et $\det(A) \neq 0$. De plus, quelles que soient $A, B \in M_n(\mathbb{K})$, $\det(AB) = \det(A)\det(B)$; par suite, $\det$ est un morphisme de groupes. Il est surjectif car si $\lambda \in \mathbb{K}^*$, la matrice diagonale $\text{diag}(\lambda, 1, \dots, 1)$ appartient à $\text{GL}_n(\mathbb{K})$, et son déterminant vaut λ .

Propriété 10

Soit $f : (G, \cdot) \rightarrow (G', \star)$ un morphisme de groupes, alors

1. $f(e) = e'$
2. Pour tout $x \in G : f(x^{-1}) = f(x)^{-1}$
3. Pour tous $x, y \in G : f(x \cdot y^{-1}) = f(x) \star f(y)^{-1}$
4. Pour tout $x \in G$ et $n \in \mathbb{Z} : f(x^n) = f(x)^n$

Preuve:

1. Pour tout $x \in G$ on a $f(x) = f(xe) = f(x) \star f(e)$; or $f(x) \in G'$, donc $f(x) = f(x) \star e'$. La règle de simplification dans G' donne : $f(e) = e'$
2. Soit $x \in G$ on a $f(xx^{-1}) = f(x)f(x^{-1}) = f(e)$ et $f(x^{-1}x) = f(x^{-1}) \star f(x) = f(e)$; or $f(e) = e'$, donc $f(x) \star f(x^{-1}) = f(x^{-1}) \star f(x) = e$. D'où $f(x)^{-1} = f(x^{-1})$
3. Utiliser la définition et l'assertion précédente
4. Par récurrence sur $n \in \mathbb{N}$ puis par symétrie on déduit l'égalité sur $\mathbb{Z}$

Propriété 11

La composée de deux morphismes de groupes est un morphisme de groupes.

Preuve:

Soient $(G, \cdot)$, $(G', \star)$ et $(G'', \top)$ trois groupes et $f : G \longrightarrow G'$ et $g : G' \longrightarrow G''$ des morphismes de groupes. Montrons $g \circ f$ est un morphisme de $(G, \cdot)$ dans $(G'', \top)$.

Soient $x, y \in G$, alors :

$$\begin{aligned} g \circ f(x \cdot y) &= g(f(x \cdot y)) \\ &= g(f(x) \star f(y)) \\ &= g(f(x)) \top g(f(y)) \\ &= [(g \circ f)(x)] \top [(g \circ f)(y)] \end{aligned}$$

Propriété 12

Si f est un isomorphisme de $(G, \cdot)$ sur $(G', \star)$, alors f^{-1} est un isomorphisme de $(G', \star)$ sur $(G, \cdot)$.

Preuve:

Si f est un isomorphisme, alors f est une bijection, donc f^{-1} aussi. Il suffit de montrer que f^{-1} est un morphisme de groupes.

Soient x et y deux éléments quelconques de G' . On a alors :

$$f(f^{-1}(x) \cdot f^{-1}(y)) = f(f^{-1}(x)) \star f(f^{-1}(y)) = x \star y$$

D'où :

$$f^{-1}(x) \star f^{-1}(y) = f^{-1}(x \cdot y)$$

f^{-1} est donc un isomorphisme de groupes de G' sur G .

Conséquence 1

On note $\text{Aut}(G)$ l'ensemble des automorphismes de G . Alors $(\text{Aut}(G), \circ)$ est un groupe.

Exemple: Les automorphismes intérieurs

Soit $(G, \star)$ un groupe, et $a \in G$. Alors $\sigma_a : \begin{cases} G & \longrightarrow G \\ g & \longmapsto a \star g \star a^{-1} \end{cases}$ est un automorphisme. De plus, l'application $(G, \star) \longrightarrow (\text{Aut}(G), \circ), a \longmapsto \sigma_a$ est un morphisme de groupes : Soit $a, b \in G$. Pour tout $g \in G$, on a :

$$(\sigma_a \circ \sigma_b)(g) = \sigma_a(b \star g \star b^{-1}) = a \star b \star g \star b^{-1} \star a^{-1} = \sigma_{a \star b}(g)$$

Donc $\sigma_a \circ \sigma_b = \sigma_{a \star b}$.

III.2 Noyau et image d'un endomorphisme

Soit f un morphisme de groupes de $(G, \cdot)$ dans $(G', \star)$ et S une partie de G

Propriété 13: Images directe et réciproque d'un sous-groupe

1. Si H est un sous-groupe de G , alors $f(H)$ est un sous-groupe de $(G', \star)$.
2. Si H' est un sous-groupe de G' , alors $f^{-1}(H')$ est un sous-groupe de $(G, \cdot)$.

Preuve:

1. $f(H)$ est un sous-ensemble non vide de G' : Il contient $e' = f(e)$.

Soient z et t deux éléments quelconques de $f(H)$; il existe deux éléments x et y de G tels que $z = f(x)$ et $t = f(y)$.

$$zt^{-1} = f(x)f(y)^{-1} = f(xy^{-1}) \in f(H)$$

Puisque $xy^{-1} \in H$, donc $f(H)$ est un sous-groupe de G' .

2. $f^{-1}(H')$ est un sous-ensemble non vide de G (il contient e).

Soient x et y deux éléments de $f^{-1}(H')$, alors $f(x) \in H'$ et $f(y) \in H'$. Puisque

$$f(xy^{-1}) = f(x)f(y)^{-1} \in H'$$

alors $xy^{-1} \in f^{-1}(H')$; donc $f^{-1}(H')$ est un sous-groupe de G .

Propriété 14

1. $f^{-1}(\{e'\})$, le noyau de f , est un sous-groupe de G . On le note $\text{Ker } f$ ou $\text{Ker}(f)$.
2. $f(G)$, l'image de f , est un sous-groupe de G' . On le note $\text{Im } f$ ou $\text{Im}(f)$

Exemple: Groupe spécial linéaire

Le noyau de déterminant s'appelle groupe linéaire spécial et se note $\text{SL}_n(\mathbb{K})$

$$\text{SL}_n(\mathbb{K}) = \{A \in \text{GL}_n(\mathbb{K}) \mid \det(A) = 1\}$$

Propriété 15

1. f est injectif si, et seulement, si $\text{Ker } f = \{e\}$;
2. f est surjectif si, et seulement, si $\text{Im } f = G'$

Preuve:

On montre la première assertion

$\Rightarrow$) Supposons que f est injectif; soit $x \in \text{Ker } f$, alors $f(x) = e' = f(e)$, d'où $x = e$ et par suite $\text{Ker } f = \{e\}$

$\Leftarrow$) Supposons que $\text{Ker } f = \{e\}$; soient $x, y \in G$ tels que $f(x) = f(y)$; on en déduit : $e' = f(x)^{-1}f(y) = f(x^{-1})f(y) = f(x^{-1}y)$, ce qui implique $x^{-1}y \in \text{Ker } f$; mais $\text{Ker } f = \{e\}$, donc $x^{-1}y = e$ et $x = y$

IV Groupes monogènes et cycliques**IV.1 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$** **Définition 8: Congruence dans $\mathbb{Z}$**

Soit $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo n si $n \mid (b - a)$; cette relation entre a et b se note $a \equiv b \pmod{n}$

$$a \equiv b \pmod{n} \iff \exists k \in \mathbb{Z}, \quad a - b = kn$$

Propriété 16

Soit $n \in \mathbb{N}^*$. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors :

$$a + c \equiv b + d \pmod{n} \quad \text{et} \quad ac \equiv bd \pmod{n}$$

La relation $\equiv \pmod{n}$ est une relation d'équivalence compatible avec la somme et le produit.

$\mathbb{Z}/n\mathbb{Z}$ désigne l'ensemble des classes d'équivalence pour $\equiv \pmod{n}$

On note $\bar{x}$ ou $\text{cl}(x)$ la classe d'équivalence de x dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire $\bar{x} = \{x + kn \mid k \in \mathbb{Z}\}$.

Preuve:

- La réflexivité et la symétrie de $\equiv \pmod{n}$ sont immédiates. Montrons seulement la transitivité. Trois entiers $a, b, c \in \mathbb{Z}$ étant donnés, supposons qu'on ait $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$. Alors $n \mid (a - b)$ et $n \mid (b - c)$, donc par somme $n \mid (a - c)$, c'est-à-dire $a \equiv c \pmod{n}$
- Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $n \mid (a - b)$ et $n \mid (c - d)$, donc par somme $n \mid [(a + c) - (b + d)]$, c'est-à-dire $a + c \equiv b + d \pmod{n}$
- Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $n \mid (a - b)$ et $n \mid (c - d)$, donc $n \mid c(a - b)$ et $n \mid b(c - d)$, par somme $n \mid (ac - bd)$, c'est-à-dire $ac \equiv bd \pmod{n}$

Remarque :

D'après la propriété 16, on peut définir dans $\mathbb{Z}/n\mathbb{Z}$ la somme et le produit de deux classes d'équivalence par : $\forall \bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}$

$$\begin{cases} \bar{x} + \bar{y} := \overline{x + y} \\ \bar{x} \times \bar{y} := \overline{x \times y} \end{cases}$$

Propriété 17

1. Pour tout $x \in \mathbb{Z}$, il existe un unique $r \in \bar{x}$ tel que $0 \leq r < n$;
2. $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$;
3. $\text{card}\left(\mathbb{Z}/n\mathbb{Z}\right) = n$;
4. $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ est un groupe abélien ;
5. Soit $k \in \llbracket 0, n-1 \rrbracket$, alors $\bar{k}$ est générateur de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ si, et seulement si, $k \wedge n = 1$

Preuve:

1. On effectue la division euclidienne de x par n : il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $x = qn + r$ et $0 \leq r < n$, donc $r \equiv x \pmod{n} \iff r \in \bar{x}$ et $0 \leq r < n$.
2. Par la propriété précédente, $r \in \bar{x}$ est unique. Donc, par transitivité, tous les éléments congrus à r modulo n le sont aussi à x modulo n , ce qui nous amène à écrire que $\bar{r} = \bar{x}$. Mais $\bar{r} \in \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, d'où le résultat.
3. L'application

$$\pi_n : \begin{cases} \llbracket 0, n-1 \rrbracket & \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto \bar{x} \end{cases}$$

est bijective

4. Facile à vérifier

5. Soit $k \in \llbracket 0, n-1 \rrbracket$. On a $\mathbb{Z}/n\mathbb{Z} = \mathcal{G}_r(\bar{1})$ et $\mathcal{G}_r(\bar{k}) \subset \mathbb{Z}/n\mathbb{Z}$

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} = \mathcal{G}_r(\bar{k}) &\iff \bar{1} \in \mathcal{G}_r(\bar{k}) \iff \exists q \in \mathbb{Z}, \quad \bar{1} = q \cdot \bar{k} = \overline{q \cdot k} \\ &\iff \exists p, q \in \mathbb{Z}, \quad 1 = qk + np \\ &\stackrel{\text{Bezout}}{\iff} k \wedge n = 1 \end{aligned}$$

Exemple

Les générateurs de $\left(\mathbb{Z}/12\mathbb{Z}, +\right)$ sont $\bar{1}, \bar{5}, \bar{7}$ et $\bar{11}$

IV.2 Ordre d'un élément, d'un groupe

Soit $(G, \cdot)$ un groupe et a un élément du groupe G .
L'application

$$\varphi_a : \begin{cases} \mathbb{Z} & \longrightarrow G \\ k & \longmapsto a^k \end{cases}$$

est un morphisme de groupes, il existe donc un unique $n \in \mathbb{N}$ tel que $\text{Ker}(\varphi_a) = n\mathbb{Z}$

Définition 9: Ordre d'un élément

- Si $n = 0$, alors on dit que a est d'ordre infini
- Si $n \in \mathbb{N}^*$, alors on dit que a est d'ordre fini et n est appelé l'ordre de a .
On note alors $\mathcal{O}(a) = n$

Définition 10: Ordre d'un groupe

Si G est fini, alors son cardinal est appelé son ordre

Propriété 18: Caractérisation des éléments d'ordre fini

Les affirmations suivantes sont équivalentes :

1. a est d'ordre fini ;
2. il existe $k \in \mathbb{Z}^*$ tel que $a^k = e$

Si l'une de ces assertions est vérifiée, alors

$$\mathcal{O}(a) = \min\{k \in \mathbb{N}^* \mid a^k = e\}$$

et aussi l'unique entier n de $\mathbb{N}^*$ tel que l'on ait :

$$\forall k \in \mathbb{Z}, \quad a^k = e \iff n \mid k$$

Preuve:

a est d'ordre fini si, et seulement, si l'application $\varphi_a : n \in \mathbb{Z} \mapsto a^n$ n'est pas injective si, et seulement, s'il existe $k \in \mathbb{Z}^*$ tel que $a^k = e$.

Par définition de l'ordre $\text{Ker}(\varphi_a) = \circ(a)\mathbb{Z}$

Propriété 19: Ordre et cardinal

Si a est d'ordre fini $n \in \mathbb{N}^*$, alors

1. $\mathcal{G}\mathbf{r}(a) := \{e, a, \dots, a^{n-1}\}$;
2. Le groupe $\mathcal{G}\mathbf{r}(a)$ est de cardinal n ;
3. $\mathcal{G}\mathbf{r}(a)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$

Preuve:

1. Il est clair que $\{e, a, \dots, a^{n-1}\} \subset \mathcal{G}\mathbf{r}(a)$.
Inversement soit $b \in \mathcal{G}\mathbf{r}(a)$, il existe $k \in \mathbb{Z}$ tel que $b = a^k$. On effectue la division euclidienne de k par n , alors il existe $(q, r) \in \mathbb{Z}^2$ tel que $\begin{cases} k = nq + r \\ 0 \leq r < n \end{cases}$, soit $b = a^k = a^r$. Donc l'inclusion inverse puis l'égalité est achevée
 2. Montrons que $\mathcal{G}\mathbf{r}(a)$ est de cardinal n .
Soit $r, r' \in \llbracket 0, n-1 \rrbracket$ tel que $a^r = a^{r'}$, alors $a^{r'-r} = e$, donc $r - r' \in \text{Ker}(\varphi_a) = n\mathbb{Z}$, ou encore $n \mid (r' - r)$. Mais $|r' - r| < n$, alors $r' - r = 0$.
 3. Nous pouvons maintenant construire l'isomorphisme entre $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathcal{G}\mathbf{r}(a), \star)$. Soit $f : \mathbb{Z}/n\mathbb{Z} \rightarrow G$ l'application définie par $f(\bar{k}) = a^k$.
 - Il faut tout d'abord montrer que f est bien définie car notre définition de f dépend du représentant k et pas de la classe $\bar{k}$: si $\bar{k} = \bar{k}'$ (une même classe définie par deux représentants distincts) alors $k \equiv k' \pmod{n}$ et donc il existe $\ell \in \mathbb{Z}$ tel que $k = k' + \ell n$. Ainsi $f(\bar{k}) = a^k = a^{k' + \ell n} = a^{k'} \star a^{\ell n} = a^{k'} \star (a^n)^\ell = a^{k'} \star e^\ell = a^{k'} = f(\bar{k}')$. Ainsi f est bien définie.
 - f est un morphisme de groupes car $f(\bar{k} + \bar{k}') = f(\overline{k + k'}) = a^{k+k'} = a^k \star a^{k'} = f(\bar{k}) \star f(\bar{k}')$ (pour tout $k, k' \in \mathbb{Z}$).
 - Il est clair que f est surjective car tout élément de G s'écrit a^k .
 - Comme l'ensemble de départ et celui d'arrivée ont le même nombre d'éléments et que f est surjective alors f est bijective.
- Conclusion : f est un isomorphisme entre $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathcal{G}\mathbf{r}(a), \star)$.

Propriété 20: Classification des groupes monogènes

Soit $G = \text{gr}(a)$ un groupe monogène, alors

- Si G est infini, il est isomorphe à $\mathbb{Z}$
- Si G est d'ordre n , il est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$

Preuve:

1. Si G est infini. On considère l'application

$$\varphi : \begin{cases} \mathbb{Z} & \longrightarrow G \\ k & \longmapsto a^k \end{cases}$$

Il est clair que φ est un morphisme de groupes $(\mathbb{Z}, +)$ dans $(G, \cdot)$. Le fait que G est monogène engendré par a , montre que φ est surjectif. Il reste à montrer que φ est injectif.

Par absurde, on suppose que le sous-groupe $\text{Ker}(\varphi)$ de $(\mathbb{Z}, +)$ est différent de $\{0\}$, alors il existe $n \in \mathbb{N}^*$ tel que $n \in \text{Ker}(\varphi)$, c'est-à-dire $a^n = e$.

Soit $k \in \mathbb{Z}$, on effectue la division euclidienne de k par n , alors il existe $(q, r) \in \mathbb{Z}^2$ tel que $k = qn + r$ et $r \in \llbracket 0, n-1 \rrbracket$.

Et on a donc

$$\varphi(k) = a^k = a^{qn+r} = a^r$$

Ainsi $G = \text{Im}(\varphi) \subset \{e, a, \dots, a^{n-1}\}$, ce qui contredit le fait que G est infini.

Conclusion φ est injectif et, par suite, φ est bijectif, puis $(G, \cdot)$ est isomorphe à $(\mathbb{Z}, +)$

2. Si G est fini. Notons n son cardinal, donc $\text{Card}(\mathcal{G}\mathbf{r}(a)) = n$ et, par suite, $(G, \cdot)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$

Exemple

$\mathbb{U}_n = \mathcal{G}_R\left(e^{i\frac{2\pi}{n}}\right)$ est un groupe monogène fini de cardinal n , donc il est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$

IV.3 Théorème de Lagrange**Propriété 21: Théorème faible de Lagrange**

Soit G un groupe fini. Alors :

1. Tout élément de G est d'ordre fini ;
2. l'ordre de tout élément de G divise l'ordre du groupe.

Preuve:

1. Soit $a \in G$, alors $\mathcal{G}_R(a) \subset G$, donc le groupe $\mathcal{G}_R(a)$ est fini. L'application φ_a n'est pas injective

2. Démonstration dans le cas G abélien. Posons $n = \text{Card}(G)$.

L'application

$$\varphi: \begin{cases} G & \longrightarrow G \\ x & \longmapsto ax \end{cases}$$

est une permutation de G , donc

$$a^n \prod_{x \in G} x = \prod_{x \in G} ax = \prod_{x \in G} x$$

Puisque dans un groupe tout élément est régulier, alors $a^n = e$

Exemple: Groupe d'ordre premier

Soit G un groupe fini d'ordre premier p . Alors G est cyclique.

Soit $a \in G \setminus \{e\}$. Alors $\mathcal{G}_R(a)$ est un sous-groupe de G , d'ordre $\circ(a) \geq 2$. Or, $\circ(a)$ divise $\text{Card}(G) = p$, donc $\circ(a) = p$, et comme $\mathcal{G}_R(a) \subset G$, on a $\mathcal{G}_R(a) = G$, c'est-à-dire G est cyclique, engendré par a .

Attention

Il se peut que tous les éléments d'un groupe soient d'ordre fini sans que le groupe soit d'ordre fini

Exemple: Groupe de Prüfer

Soit p un nombre premier. On pose

$$G_p = \left\{ z \in \mathbb{C}; \exists k \in \mathbb{N}, z^{p^k} = 1 \right\}$$

1. Montrer que G_p est un sous-groupe de $(\mathbb{C}^*, \times)$.
2. Montrer que tout élément de G_p est d'ordre fini et que G_p est infini

1. $G_p \subset \mathbb{C}^*$, $1 \in G_p$, pour $z \in G_p$, il existe $k \in \mathbb{N}$ tel que $z^{p^k} = 1$ et alors $\left(\frac{1}{z}\right)^{p^k} = 1$ donc $\frac{1}{z} \in G_p$. Si de plus $z' \in G_p$, il existe $k' \in \mathbb{N}$ vérifiant $z'^{p^{k'}} = 1$ et alors

$$(zz')^{p^{k+k'}} = (z^{p^k})^{p^{k'}} (z'^{p^{k'}})^{p^k} = 1$$

donc $zz' \in G_p$.

2. ► Pour $z \in G_p$, il existe $k \in \mathbb{N}$ tel que $z^{p^k} = 1$, donc z est d'ordre fini.
 ► Soit $k \in \mathbb{N}$, on note $\mathbb{U}_{p^k} = \{z \in \mathbb{C}^* \mid z^{p^k} = 1\}$. L'ensemble $\mathbb{U}_{p^k}$ est de cardinal p^k et $\mathbb{U}_{p^k} \subset G_p$, donc G_p est infini