

# Théorie des groupes

Bcp de monde...

September 2024

# Table des matières

# Exemples en tout genres

## 0.1 Section1

### Définition :

distance mdr a definition d'une distance

### 0.1.1 Sous-section1

#### Preuve :

exemple de preuve

□

### 0.1.2 Comment faire un lemme

#### Lemme :

avec la box noire sans nom

#### Lemme : nom

sasn la box mais avec le nom

# Chapitre 1

## Notion de groupe, morphisme, produit direct

### 1.1 Groupes, sous-groupes, exemples

#### 1.1.1 Définitions

**Définition :**

Groupe Un groupe est un ensemble non vide  $G$  munis d'une loi  $*$  telle que :

- (i)  $*$  est associative
- (ii)  $*$  possède un neutre  $e \in G$
- (iii) Tout élément possède un inverse pour  $*$

**Définition :** Groupe abélien

Un groupe  $G$  est dit abélien si :  $\forall (x, y) \in G, xy = yx$

#### 1.1.2 Sous-groupes

**Définition :** Sous-groupe

Un sous-ensemble  $H$  de  $G$  est appelé sous-groupe si :

- $e \in H$
- $\forall x, y \in H, xy^{-1} \in H$

**Définition :** Groupe fini

$G$  est dit fini si il est cardinal fini, on note alors  $o(G) = |G|$ , appelé ordre de  $G$ .

#### 1.1.3 Sous-groupe engendré

**Définition :** Sous-groupe engendré par une partie

Soient  $G$  un groupe et  $S \subset G$

Soit  $G_S$  l'ensemble des sous groupes de  $G$  qui contiennent  $S$ .

On appelle sous groupe engendré par  $S$  l'ensemble :  $\langle S \rangle := \bigcap_{H \in G_S} H$

Si de plus  $\langle S \rangle = G$  on dit que  $S$  est une partie génératrice de  $G$  ou que  $S$  engendre  $G$

**Définition :** Groupe de type fini

Si  $G$  est engendré par un singleton, on dit que  $G$  est monogène.

Un groupe monogène fini est dit cyclique.

Si il existe une partie finie  $S \subseteq G$  qui engendre  $G$ , on dit que  $G$  est de type fini.

**Définition :** Ordre d'un élément

- Si  $\langle x \rangle$  est infini, on dit que  $x$  est d'ordre infini.
- Si  $\langle x \rangle$  est fini, on dit que  $x$  est d'ordre  $|\langle x \rangle|$

Si  $x^n = e$  alors  $o(x) | n$

## 1.2 morphismes de groupes

**Définition :** Morphisme de groupe

Soit  $(G, *)$ ,  $(H, \cdot)$  deux groupes. Un morphisme de groupes de  $G$  dans  $H$  est une application  $f: G \longrightarrow H$  tel que  $\forall x, y \in G, f(x * y) = f(x) \cdot f(y)$

**Exercice :**

1.  $f(e_G) = e_H$
2.  $f^{-1}(x) = f(x^{-1})$
3.  $\forall n \in \mathbb{N}, f^n(x) = f(x^n)$
4. Si  $K < G$ , alors  $f(K) < H$
5. Si  $K < H$ , alors  $f^{-1}(K) < G$

**Exemple :**

1.  $\epsilon: \mathcal{S}_n \longrightarrow \{-1, 1\}$
2.  $\det: \text{GL}_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$
3.  $\exp: \mathbb{C} \longrightarrow \mathbb{C}^*$
4. Mais  $\exp: \mathcal{M}_2(\mathbb{R}) \longrightarrow (\text{GL}_2(\mathbb{R}), \times)$

### 1.2.1 Isomorphismes

**Définition :** Isomorphisme

1. Un isomorphisme de  $G$  dans  $H$  est un morphisme de groupes bijectif.
2.  $G$  et  $H$  sont isomorphe ssi il existe un isomorphisme entre les deux.

**Exercice :**

Si  $f$  est un isomorphisme alors  $f^{-1}$  aussi

**Exercice :**

1.  $\mathbb{Z}/4\mathbb{Z}$  et  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  ne sont pas isomorphe
2.  $\mathbb{Z}/6\mathbb{Z}$  et  $\mathbb{S}_n$  ne sont pas isomorphe (car l'un est abélien et l'autre non).
3.  $\mathbb{Z}/mn\mathbb{Z}$  et  $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  sont isomorphe ssi  $m \wedge n = 1$

**Définition : Automorphisme**

Un automorphisme est un isomorphisme d'un groupe  $G$  dans lui-même. L'ensemble des automorphismes de  $G$  se note  $Aut(G)$ .

**Exercice :**

Montrer que  $Aut(G) < \mathbb{S}_G$ , où  $\mathbb{S}_G$  désigne l'ensemble des bijections de  $G$  dans lui-même

**Exercice :**

$\forall g \in G$ , on note  $\sigma_g : \begin{cases} G & \longrightarrow & G \\ x & \longmapsto & gxg^{-1} \end{cases}$  (automorphisme intérieur associé à  $g$ ), montrer que  $\sigma_g \in Aut(G)$

**Exercice :**

On note  $Int(G)$  l'ensemble des automorphismes intérieurs de  $G$ , montrer que  $Int(G) < Aut(G)$

**Théorème : Théorème de Cayley**

Tout groupe  $G$  est isomorphe à un sous-groupe de  $\mathbb{S}_G$ . En particulier, si  $|G| = n$ , alors  $G$  est isomorphe à un sous-groupe de  $\mathcal{S}_n$ .

**Preuve :**

Pour tout  $g \in G$ , on pose  $\tau_g : \begin{cases} G & \longrightarrow & G \\ x & \longmapsto & gx \end{cases}$   $\tau_g$  est une bijection de  $G$  dans  $G$ . Notons  $T_G := \{\tau_g, g \in G\} \subseteq \mathbb{S}_G$ .

Vérifions que :

1.  $T_G < \mathbb{S}_G$
2.  $G$  est isomorphe à  $T_G$

Preuve de 1 :

- $Id_G = \tau_e \in T_G (T_G \neq \emptyset)$
- $\forall g_1, g_2 \in G, \forall x \in G, \tau_{g_1 g_2}(x) = g_1 g_2 x = g_1(g_2 x) = \tau_{g_1}(\tau_{g_2}(x))$ , donc on a bien  $\tau_{g_1 g_2} = \tau_{g_1} \tau_{g_2}$
- $\forall g \in G, \tau_{g^{-1}} \circ \tau_g = \tau_g \circ \tau_{g^{-1}} = Id_G$  Donc  $(\tau_g)^{-1} = \tau_{g^{-1}} \in T_G$

Preuve de 2 :

Notons  $\phi : \begin{cases} G & \longrightarrow & T_G \\ g & \longmapsto & \tau_g \end{cases}$  Alors  $\phi$  est un morphisme (d'après la preuve de 1)  $\phi$  est immédiatement surjectif, mais il est également injectif :

Soit  $g \in G$  tel que  $\tau_g = Id_G$ . Alors  $\forall x \in G, gx = x$ . Si on prend  $x = e_G$ , on obtient  $g = e_G$ . Donc  $Ker(\phi) = e_G$ , et donc  $\phi$  est injectif.

□

## 1.3 Produits directs

**Définition : Produit direct**

Le groupe "produit direct" de deux groupes  $G_1, G_2$  est l'ensemble  $G_1 \times G_2$  muni de la loi :

$$\cdot : \begin{cases} (G_1 \times G_2) \times (G_1 \times G_2) & \longrightarrow & G_1 \times G_2 \\ ((x_1, x_2), (y_1, y_2)) & \longmapsto & (x_1 y_1, x_2 y_2) \end{cases}$$

**Exercice :**

vérifier que  $G_1 \times G_2$  muni de cette loi est bien un groupe.

**Définition :** Projections et injections canoniques

1. Projections canoniques  $p_i : \begin{array}{c|c} G_1 \times G_2 & \longrightarrow G_i \\ (x_1, x_2) & \longmapsto x_i \end{array}$
2. Injections canoniques :  $q_1 : \begin{array}{c|c} G_1 & \longrightarrow G_1 \times G_2 \\ x_1 & \longmapsto (x_1, e_2) \end{array}$  et  $q_2 : \begin{array}{c|c} G_2 & \longrightarrow G_1 \times G_2 \\ x_2 & \longmapsto (e_1, x_2) \end{array}$

**Remarque :**

$\text{Im}(q_i)$  est isomorphe à  $G_i$ . Ainsi  $G_1 \times G_2$  contient un sous-groupe isomorphe à  $G_1$ , de même pour  $G_2$ .

**Remarque :**

$\forall x = (x_1, x_2) \in G_1 \times G_2$ , on a :

$$x = (p_1(x), p_2(x)) = (x_1, x_2) = (x_1, e_2)(e_1, x_2) = (e_1, x_2)(x_1, e_2) = q_1(x_1)q_2(x_2) = q_2(x_2)q_1(x_1)$$

**Théorème :**

Un groupe  $G$  est isomorphe au produit direct  $G_1 \times G_2$  ssi  $G$  contient deux sous-groupes  $H_1, H_2$  tel que :

1.  $H_i$  est isomorphe à  $G_i (i = 1, 2)$
2.  $h_1 h_2 = h_2 h_1, \forall h_1 \in H_1, \forall h_2 \in H_2$
3.  $G = H_1 H_2$
4.  $H_1 \cap H_2 = \{e_G\}$

**Preuve :**

$\Rightarrow$  Supposons qu'il existe  $\phi : G_1 \times G_2 \longrightarrow G$  isomorphe.

1. On a que  $G_1 \simeq \{G_1, e_2\} \simeq \phi(\{G_1, e_2\}) := H_1$  il suffit alors de remarquer que  $H_1$  est un sous groupe de  $G$ . On construit de même  $H_2$
2.  $\forall (h_1, h_2) \in H_1 \times H_2$ , on note  $h'_1 = (h_1, e_2)$  idem pour  $h'_2$ , on a alors :

$$h_1 h_2 = \phi(h'_1 h'_2) = \phi(h'_2 h'_1) = h_2 h_1$$

3.  $\forall x \in G, \exists ! x' = (h_1, h_2) \in G_1 \times G_2$  tel que  $\phi(x') = x$ . On a alors :

$$x = \phi(x') = \phi(h'_1 h'_2) = h_1 h_2$$

4. Immédiat

$\Leftarrow$  Construisons un isomorphisme de  $G$  dans  $G_1 \times G_2$

Fait :  $\forall g \in G, \exists ! (h_1, h_2) \in H_1 \times H_2$  tel que  $g = h_1 h_2$

En effet : l'existence vient de 3), l'unicité vient de 4) :  $g = h_1 h_2 = k_1 k_2$  alors  $(k_1)^{-1} h_1 = k_2 (h_2)^{-1}$ .

Comme  $H_1 \cap H_2 = \{e\}$  on obtient  $(k_1)^{-1} h_1 = k_2 (h_2)^{-1} = e_G \Rightarrow h_1 = k_1$  et  $h_2 = k_2$

Notons  $\phi_1 : H_1 \longrightarrow G_1$  et  $\phi_2 : H_2 \longrightarrow G_2$  les isomorphismes données par 1).

Posons  $\phi : \begin{array}{c|c} G & \longrightarrow G_1 \times G_2 \\ h_1 h_2 & \longmapsto (\phi_1(h_1), \phi_2(h_2)) \end{array}$

Mq  $\phi$  est un morphisme ( $\alpha$ ), injectif ( $\beta$ ), surjectif  $\gamma$

( $\alpha$ ) :  $\phi(h_1 h_2 h'_1 h'_2) = \phi(h_1 h'_1 h_2 h'_2) = (\phi_1(h_1 h'_1), \phi_2(h_2 h'_2)) = (\phi_1(h_1), \phi_1(h'_1), \phi_2(h_2) \phi_2(h'_2)) = (\phi_1(h_1), \phi_2(h_2))(\phi_1(h'_1), \phi_2(h'_2)) = \phi(g) \phi(g')$

( $\beta$ ) : Soit  $x = h_1 h_2$  tel que  $\phi(x) = (\phi_1(h_1), \phi_2(h_2)) = (e_1, e_2)$

Alors  $\phi_1(h_1) = e_1$  et  $\phi_2(h_2) = e_2 \Rightarrow h_1 = h_2 = e_G$

( $\gamma$ ) : Soit  $x = (x_1, x_2) \in G_1 \times G_2$ , soit  $(h_1, h_2)$  tel que  $\phi_i(h_i) = x_i$ , alors  $x = (\phi_1(h_1), \phi_2(h_2)) = \phi(h_1, h_2)$ , cela montre la surjectivité de  $\phi$ .

□

**Exemple :**

$(\mathbb{Z}/2^\alpha\mathbb{Z}, +, \times)$  est anneau. On note  $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$  l'ensemble des éléments inversibles de l'anneau (pour la loi  $\times$ ). Si  $\alpha \geq 3$ ,  $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$  est isomorphe à  $(\mathbb{Z}/2^{\alpha-2}\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$



## Chapitre 2

# Classes modulo un sous-groupe, sous-groupes distingués

### 2.1 Classes à droite, classes à gauche

Soit  $H < G$ . On définit  $x\mathcal{R}_Hy \iff xy^{-1} \in H$  et  $x_H\mathcal{R}y \iff x^{-1}y \in H$

**Exemple :**

1.  $\mathcal{R}_H$  et  $_H\mathcal{R}$  définissent deux relations d'équivalences
2. La classe d'équivalence de  $x$  pour  $\mathcal{R}_H$  est  $Hx$  appelée classe à droite de  $x$  modulo  $H$ , idem pour  $_H\mathcal{R}$

**Exemple :**

On se place dans  $\mathcal{S}_3$ , on pose  $\sigma = (1, 2, 3)$  et  $\tau = (1, 2)$ , on a alors  $\mathbb{S}_3 = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \sigma\tau\}$ .

Pour  $H = \{e, \tau\}$ , on a :

$$H\sigma = \{\sigma, \tau\sigma\}, H\sigma^2 = \{\sigma^2, \tau\sigma^2 (= \sigma\tau)\}$$

$$\sigma H = \{\sigma, \sigma\tau\}, \sigma^2 H = \{\sigma^2, \sigma^2\tau (= \tau\sigma)\}$$

donc  $\sigma H \neq H\sigma$ .

**Exemple :**

Si  $G$  est abélien, on a  $xH = Hx, \forall x \in G$ .

**Remarque :**

$\forall g \in G, \tau_g : \begin{cases} G & \longrightarrow G \\ x & \longmapsto gx \end{cases}$  est une bijection. En particulier,  $\tau_g|_H$  est une bijection de  $H$  sur  $gH$ . De même,  $\rho_g : \begin{cases} G & \longrightarrow G \\ x & \longmapsto xg \end{cases}$ , alors  $\rho_g|_H$  est une bijection de  $H$  sur  $Hg$ .

**Remarque :**

Soit  $\{e\} \cup \{x_i, i \in I\}$  un système de représentants des classes à gauche modulo  $H$ . On a alors  $G = H \sqcup \bigsqcup_{i \in I} x_i H$  (union disjointe).

**Remarque :**

L'application  $: x_i H \longrightarrow H(x_i)^{-1}$  est une bijection de l'ensemble des classes à gauche sur l'ensemble des classes à droite.

**Définition :** Indice de  $H$  dans  $G$ 

L'indice de  $H$  dans  $G$  est le cardinal (fini ou infini) de l'ensemble des classes à gauche (= cardinal de l'ensemble des classes à droite), il est noté  $[G : H]$

On en déduit le théorème de Lagrange :

**Théorème :** Théorème de Lagrange

Soit  $G$  un groupe fini et  $H < G$ . Alors :

1.  $|G| = |H|[G : H]$
2.  $\forall x \in G, o(x) \mid |G|$

## 2.2 Sous-groupes distingués

**Définition :**

Soit  $G$  un groupe fini,  $H < G$  est dit distingué (ou normal) dans  $G$  ssi  $\forall x \in G, xH = Hx$ .  
Le cas échéant on note :  $H \triangleleft G$

**Définition :**

Un groupe  $G$  est dit simple ssi ses seuls sous-groupes distingués sont  $\{e\}$  et  $G$ .

**Remarque :**

Si  $G$  est abélien, tout  $H < G$  est distingué.

**Exemple :**

Soit  $H < G$ . Alors  $H \triangleleft G \iff \forall g \in G, gHg^{-1} = H$

**Propriété :**

Soit  $H \backslash G$  l'ensemble des classes à gauche modulo  $H$ .

L'application :  $(xH, yH) \longrightarrow xyH$  est bien définie ssi  $H \triangleleft G$ .

Idem pour les classes à droites  $G/H$ .

**Preuve :**

$\Rightarrow$ : Soit  $h \in H, y \in G$ , l'application est bien définie, donc  $egH = hgH$  donc  $yH = hgH$  donc  $H = y^{-1}hyH$ , donc  $y^{-1}hy \in H$ .

$\Leftarrow$ : Si  $x, x' \in G$  tel que  $xH = x'H$ , et si  $y, y' \in G$  tel que  $yH = y'H$ , alors on a  $h, h' \in H$  vérifiant :  $x' = xh$  et  $y' = yh'$ . Donc  $x'y' = xy y^{-1} h y h'$ , avec  $y^{-1} h y h' \in H$  car  $H \triangleleft G$ . Donc  $x'y'H \subseteq xyH$ , par symétrie on a  $\supseteq$

□

**Théorème :** Groupe quotient

Soit  $G$  un groupe,  $H \triangleleft G$ . On note  $\bar{x}$  la classe de  $x$  modulo  $H$ ,  $\frac{G}{H}$  l'ensemble des classes modulo  $H$ . Alors :

1. L'application  $*$  :  $\left( \frac{G}{H} \right) \times \left( \frac{G}{H} \right) \longrightarrow \frac{G}{H}$   
 $(\bar{x}, \bar{y}) \longmapsto \bar{x} * \bar{y} := \overline{xy}$  munit  $\frac{G}{H}$  d'une structure de groupe tel que  $\bar{e} = H$  est l'élément neutre.

2. En particulier, l'application  $\pi : G \longrightarrow \frac{G}{H}$  est un morphisme de groupes de noyau  $H$ .

### 2.2.1 Sous-groupes distinguées et noyaux

**Propriété :**

Si  $\phi : G \longrightarrow G'$  un morphisme, alors  $\text{Ker}(\phi) \triangleleft G$ .

**Preuve :**

Si  $h \in \text{Ker}(\phi), g \in G, \phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_{G'}$ , donc  $ghg^{-1} \in \text{Ker}(\phi)$ .

□

**Théorème :** Groupes distingués et morphismes

Soit  $G$  un groupe. Alors  $H \triangleleft G$  ssi  $\exists G'$  groupe,  $\exists \phi : G \longrightarrow G'$  morphisme tel que  $H = \text{Ker}(\phi)$

**Exemple :**

1.  $\varepsilon : \mathbb{S}_n \longrightarrow \{-1, 1\}$  (*signature*), alors  $A_n := \text{Ker}(\varepsilon) \triangleleft \mathbb{S}_n$
2.  $\det : \text{GL}_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$ , alors  $\text{SL}_n(\mathbb{R}) := \text{Ker}(\det) \triangleleft \text{GL}_n(\mathbb{R})$

**Théorème :** Premier théorème d'isomorphisme

Soit  $\phi : G \longrightarrow G'$  un morphisme de groupe. Alors,  $G/\text{Ker}(\phi)$  est isomorphe à  $\text{Im}(\phi)$ .

## Chapitre 3

# Étude de $\mathbb{Z}/n\mathbb{Z}$ , de $\mathcal{S}_n$ , de $\mathbb{D}_n$

### 3.1 J'ai pas le nom...

#### 3.1.1 Autres exemples de sous groupes normaux

- j'ai pas le premier...
- Le centre d'un groupe  $Z(G) = \{g \in G, gx = gx \forall x \in G\}$  est un sous groupe normal de  $G$ . (preuve en exercice (feuille 3)).  $Z(G)$  est en fait caractéristique c'est à dire qu'il est invariant par tout automorphisme intérieur
- Le groupe dérivé de  $G$  est le sous-groupe (noté  $D(G)$ ) qui est engendré par les commutateurs de  $G$  c'est à dire les éléments de la forme  $[a, b] = aba^{-1}b^{-1}$  est aussi un sous-groupe normal.

##### Exemple :

1. Si  $G$  est abélien alors  $Z(G) = G$
2. Si  $n \leq 3$  alors  $Z(S_n) = \{e\}$

##### Preuve :

Preuve du deuxième point :

Soit  $\sigma \in \mathcal{S}_n$  avec  $\sigma \neq e$ .

Soit alors  $i \in \llbracket 1, n \rrbracket$  tel que l'on ait  $\sigma(i) := j \neq i$

Soit enfin  $k \in \llbracket 1, n \rrbracket \setminus \{i, j\}$ , on pose  $\tau = (j, k)$ .

On a bien  $\sigma\tau \neq \tau\sigma$ , car  $\sigma\tau(i) = j \neq \tau\sigma(j) = k$

□

##### Exercice :

- $D(G) \triangleleft G$  et  $G/D(G)$  est abélien
- Soit  $H \triangleleft$  alors  $G/H$  est abélien  $\Leftrightarrow D(G) < H$
- $D(G)$  est un sous groupe caractéristique de  $G$
- $\forall n \leq 3$   $D(S_n) = A_n$  ou  $A_n$  est le groupe alterné, désigne les permutations de signature paire

##### Définition : Normalisateur d'un sous-groupe

Soit  $H < G$ , on note  $N_G(H) = \{g \in G, gH = Hg\}$ , on l'appelle le normalisateur de  $H$  dans  $G$

**Exercice :**

Mq  $H \triangleleft N_g(H)$  et que  $N_g(H) < G$

**Exemple :**

Dans  $A_4$

Soit  $H = \{e, (1, 2), (3, 4)\} < A_4$ ,  $|H| = 2$ .

O a  $H < D(A_4)$  et  $H \triangleleft D(A_4)$  car  $\frac{|D(A_4)|}{|H|} = 2$ .

Verifier que  $N_{A_4}(H) = D(A_4)$  :

Soit  $N = N_{A_4}(H)$  pour simplifier. On sait que  $D(A_4) < N$  donc  $|D(A_4)| = 4$  divise  $|N|$  donc  $|N| \in \{4, 8, 12\}$ , mais vu  $N < A_4$ ,  $|N|$  divise 12, donc  $|N| = 4$  où  $|N| = 12$ . Mais  $N \neq A_4$  car  $(1, 2, 3)H(1, 2, 3) \neq H$

## 3.2 Groupes Monogènes, cycliques, symétriques, diédraux

### 3.2.1 Groupes Monogènes

**Définition :** Groupe monogène

Un groupe  $G$  est dit monogène si il est engendré par une unique élément

**Théorème :**

Soit  $G$  un groupe monogène alors :

- Ou bien  $G$  est isomorphe à  $\mathbb{Z}$
- Ou bien  $G$  est isomorphe à  $\mathbb{Z}/n\mathbb{Z}$  pour un certain  $n \in \mathbb{N}$

**Preuve :**

Soit  $G = \langle x \rangle$  et soit  $\psi : \begin{cases} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & x^k \end{cases}$ .  $\psi$  est un morphisme de groupe, il est surjectif.

Si il est injectif on à bien  $G \simeq \mathbb{Z}$ .

Sinon, il existe  $n \in \mathbb{N}$  tq  $\ker \psi = n\mathbb{Z}$

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\psi} & G \\ \pi \downarrow & \nearrow \tilde{\psi} & \\ \mathbb{Z}/n\mathbb{Z} & & \end{array}$$

Et d'après le premier théorème d'isomorphisme, il existe un isomorphisme de groupe  $\tilde{\psi} : \mathbb{Z}/n\mathbb{Z} \longrightarrow \text{Im}(\psi) = G$  tel que le diagramme ci-dessus commute.

□

**Propriété :**

Tout groupe fini d'ordre  $p$  avec  $p$  premier est cyclique

**Preuve :**

utiliser lagrange

□

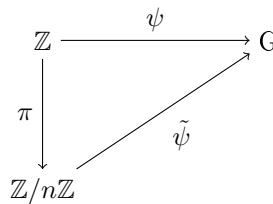
### 3.2.2 Sous-groupes d'un groupe monogène

**Propriété :**

1. Tout sous-groupe non trivial d'un groupe monogène infini est infini
2. Tout sous-groupe d'un groupe cyclique est monogène et cyclique

**Preuve :**

1. Ici  $G \simeq \mathbb{Z}$ , donc tout  $H < G$  est isomorphe à un sous-groupe de  $\mathbb{Z}$  ie. un groupe de la forme  $n\mathbb{Z}$  pour  $n \neq 0$ , donc  $H$  est infini
2. On reprend le diagramme :



Soit  $K < G = \mathbb{Z}/n\mathbb{Z}$  on a  $K = \pi(\pi^{-1}(K))$  car  $\pi$  est surjective. Comme  $\pi^{-1}(K)$  est un sous-groupe de  $\mathbb{Z}$  il existe  $k > 0$  tq  $\pi^{-1}(K) = k\mathbb{Z}$ .

Alors  $K = \pi(k\mathbb{Z})$  est le sous-groupe de  $\mathbb{Z}/n\mathbb{Z}$  engendré par  $\pi(k)$ ,  $K$  est donc monogène et fini

□

**Remarque :**

Si on reprend la preuve précédente on a  $\pi^{-1}(0) = n\mathbb{Z} \subset \pi^{-1}(K) = k\mathbb{Z}$ .

Ainsi,  $n\mathbb{Z} \subset k\mathbb{Z}$  et donc  $k|n$ . Par conséquent, pour tout sous-groupe  $K$  de  $\mathbb{Z}/n\mathbb{Z}$ , il existe un diviseur  $k$  de  $n$  tel que  $\pi(k)$  engendre  $K$ , l'ordre de  $\pi(k)$  étant  $\frac{n}{k}$ , on a  $|K| = \frac{n}{k}$  en particulier ce diviseur est unique on a donc le théorème suivant.

**Théorème :**

Soit  $G = \langle x \rangle$  un groupe cyclique d'ordre  $n$  alors :

Pour tout diviseur  $d$  de  $n$ , il existe un unique sous-groupe d'ordre  $d$  de  $G$  et ce sous-groupe est engendré par  $x^{n/d}$

**Propriété :**

Soit  $G$  un groupe non trivial alors :

$G$  n'a pas de d'autres sous-groupes que  $G$  et  $\{e\} \iff G$  est cyclique d'ordre  $p$  premier

**Preuve :**

⊆ évident par Lagrange

⊇ Soit  $x \in G \setminus \{e\}$  alors  $\langle x \rangle = G$  par hypothèse. Si  $G$  était infini, il posséderait des sous-groupes non triviaux de type  $n\mathbb{Z}$ , donc  $G$  est fini. Comme il n'a pas d'autres sous-groupes que  $\{e\}$  et  $G$  on a forcément  $|G| = p$  premier par le théorème précédent.

□

**Théorème :**

Soit  $G$  un groupe monogène :  $G = \langle x \rangle$

1. Si  $G$  est infini, alors les seuls générateurs de  $G$  sont  $x$  et  $x^{-1}$
2. Si  $G$  est fini (il est cyclique d'ordre  $n$ ) alors l'ensemble de ses générateurs est donné par  $\{x^k : k \in \mathbb{Z}, k \wedge n = 1\}$

**Preuve :**

1. Soit  $\psi : k \in \mathbb{Z} \rightarrow x^k \in G$  (vue précédemment) qui est un isomorphisme de groupes. En particulier,  $\psi$  échange les générateurs. Comme les seuls générateurs de  $\mathbb{Z}$  sont 1 et  $-1$ , on conclut.
2. Soit  $k \in \mathbb{Z}$ , alors :

$$\begin{aligned}
 G = \langle x \rangle &\iff \exists m \in \mathbb{Z}, x^{km} = x \\
 &\iff \exists m \in \mathbb{Z}, n \mid km - 1 \\
 &\iff \exists (m, q) \in \mathbb{Z}, km - nq = 1 \\
 &\iff \text{pgcd}(k, n) = 1
 \end{aligned}$$

□

**Exercice :**

L'ensemble des générateurs de  $G \simeq \mathbb{Z}/n\mathbb{Z}$  est aussi égal à  $\{\bar{k} \in \mathbb{Z}/n\mathbb{Z} : 0 \leq k \leq n-1, k \wedge n = 1\}$

**Définition :** Fonction d'Euler

La fonction d'Euler est la fonction  $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$  telle que :

- $\varphi(1) = 1$
- $\varphi(n) = |\{k \in \mathbb{N} : 1 \leq k \leq n, k \wedge n = 1\}|$

### 3.3 Anneau $\mathbb{Z}/n\mathbb{Z}$

On rappelle que les opérations d'addition et de multiplication sont bien définies sur  $\mathbb{Z}/n\mathbb{Z}$  (pas de dépendance des représentants) et que cet anneau est unitaire.

**Définition :** Inverse modulo  $n$ 

On dit que  $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$  est inversible s'il existe  $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$  tel que  $\bar{k}\bar{m} = \bar{1}$

**Propriété :**

Soit  $n \geq 2$ . Les éléments inversibles de  $\mathbb{Z}/n\mathbb{Z}$  sont exactement les générateurs de  $(\mathbb{Z}/n\mathbb{Z}, +)$ . L'ensemble des éléments inversibles est alors un groupe abélien fini d'ordre  $\varphi(n)$ .

**Preuve :**

Utiliser la caractérisation précédente avec Bézout.

□

### 3.4 Produits directs de groupes cycliques, calcul de $\varphi(n)$

On considère le morphisme d'anneaux unitaires :

$$f : k \in \mathbb{Z} \rightarrow (\bar{k}, \bar{k}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

**Théorème :**

Le morphisme d'anneaux unitaires  $f$  induit par passage au quotient par son noyau un isomorphisme d'anneaux unitaires  $\bar{f} : \mathbb{Z}/nm\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  si et seulement si  $m \wedge n = 1$

**Preuve :**

Il faut vérifier  $\bar{f}$  est bijective ssi  $m \wedge n = 1$  :

$$\begin{aligned}
 f \text{ est surjective} &\iff |Im(f)| = mn \\
 &\iff |\mathbb{Z}/ker(f)| = mn \text{ (grâce au théorème d'isomorphisme)} \\
 &\iff ker(f) = mn\mathbb{Z} \\
 &\iff m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z} \\
 &\iff m \wedge n = 1
 \end{aligned}$$

□

**Propriété :**

Si  $m \wedge n = 1$ , alors  $\varphi(nm) = \varphi(n)\varphi(m)$

**Théorème :**

Soit  $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ , décomposé en facteur premiers. Alors :

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \times \cdots \times \left(1 - \frac{1}{p_k}\right)$$

**Preuve :**

Il nous suffit de calculer  $\varphi(p^\alpha)$  pour  $p$  premier et  $\alpha \geq 1$ . On a :

$$\begin{aligned}
 \varphi(p^\alpha) &= |\{k \in \{1, \dots, p^\alpha\} : k \wedge p^\alpha = 1\}| \\
 &= |\{1, \dots, p^\alpha\} \setminus \{p, 2p, \dots, p^{\alpha-1}p\}| \\
 &= p^\alpha - p^{\alpha-1}
 \end{aligned}$$

□

### 3.5 Structure des groupes abéliens finis (admis)

Référence : Livre de F. Ulmer "Théorie des groupes" chap 12

Soit  $G$  un groupe fini abélien d'ordre  $N$ . Il existe une décomposition unique  $N = d_1 \cdots d_n$  avec  $d_n \geq 2$  et  $d_{i+1} | d_i$  telle que :

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$$

**Exemple :**

On peut lister, à isomorphisme près, tous les groupes abéliens d'ordre  $72 = 3^2 \times 2^3$  avec les séquences suivantes :  $(3^2 \times 2^2, 2), (3 \times 2, 3 \times 2, 2), (3 \times 2^3, 3), (2^2 \times 3, 2 \times 3), (3^2 \times 2, 2, 2)$

### 3.6 Groupes symétriques

On note  $\mathcal{S}_n$  l'ensemble des permutations de  $\{1, 2, \dots, n\}$  que l'on munit de la loi de composition : c'est un groupe d'ordre  $n!$



### 3.6.1 Support et Orbite

**Définition : Support**

Le support de  $\sigma \in \mathcal{S}_n$  est l'ensemble  $\{i \in \{1, \dots, n\} ; \sigma(i) \neq i\}$

**Exercice :**

Soit  $\sigma \in \mathcal{S}_n$ . Montrer que

- $\sigma$  et  $\sigma^{-1}$  ont le même support
- si  $k \in \mathbb{Z}$ ,  $\sigma$  et  $\sigma^k$  ont le même support
- deux permutations dont les supports sont disjoints commutent

**Définition : Orbite**

Soit  $\sigma \in \mathcal{S}_n$ . On définit la relation d'équivalence sur  $\{1, \dots, n\}$  :

$$i \mathcal{R} j \iff \exists r \in \mathbb{Z} \mid \sigma^r(i) = j.$$

La classe de  $i$  est notée  $\Omega(i) = \{\sigma^r(i), r \in \mathbb{Z}\}$  et est appelée  $\sigma$ -orbite de  $i$ .

### 3.6.2 Notion de cycle

**Définition : r-cycle**

$\sigma \in \mathcal{S}_n$  est un  $r$ -cycle si il existe  $j_1, \dots, j_r$  dans  $\{1, \dots, n\}$  tq  $\sigma(j_1) = j_2, \dots, \sigma(j_{r-1}) = j_r, \sigma(j_r) = j_1$ , et si pour  $k \notin \{j_1, \dots, j_r\}, \sigma(k) = k$ .

Alors le support de  $\sigma$  est  $\{j_1, \dots, j_r\}$ . On notera  $\sigma = (j_1, \dots, j_r)$

**Définition : Transposition et permutation circulaire**

1. Un 2-cycle est appelé transposition
2. le  $n$ -cycle  $(1, \dots, n)$  est appelé permutation circulaire

**Exemple :**

Si  $\sigma_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 5 & 4 \end{pmatrix} \leftarrow \begin{matrix} i \\ \sigma_0(i) \end{matrix}$   
alors  $\sigma_0 = (1, 3, 2)(4, 6)$ .

**Théorème :**

Toute permutation  $\sigma \in \mathcal{S}_n \setminus \{e\}$  se décompose sous la forme  $\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_s$  où  $s \in \mathbb{N}^*$ , et où les  $\gamma_i$  sont des cycles différents de  $e$  dont les supports sont disjoints deux à deux. Cette décomposition est unique à l'ordre près des facteurs.

**Exercice :**

1. Montrer que l'ordre de  $\sigma$  est égal au ppcm des longueurs des cycles  $\gamma_1, \dots, \gamma_s$ .
2. Calculer  $\sigma_0^{1000}$ .

### 3.6.3 Formules importantes

**Propriété :**

Pour tout  $\tau \in \mathcal{S}_n$ ,  $\tau(j_1, \dots, j_r)\tau^{-1} = (\tau(j_1), \dots, \tau(j_r))$ .

**Propriété :**

On a :  $(j_1, \dots, j_r) = (j_1, j_2)(j_2, j_3) \dots (j_{r-1}, j_r)$

**Cas particulier :**  $(a, b, c) = (a, b)(b, c)$

**Applications de ces deux propriétés :**

1. Deux  $r$ -cycles de  $\mathcal{S}_n$  sont conjugués dans  $\mathcal{S}_n$
2.  $(1, i)(1, j)(1, i) = (1, i)(1, j)(1, i)^{-1} = (i, j)$
3.  $\mathcal{S}_n$  est engendré par les transpositions du type  $(j, j+1)$  où  $j \in \{1, \dots, n-1\}$   
 preuve : laissée en exercice au lecteur, l'idée est de montrer que  $(i, j)$  est un produit de transpositions du type  $(k, k+1)$  par récurrence sur  $j-1$  en utilisant  $(i, j) = (j-1, j)(i, j-1)(j-1, j)$
4.  $\mathcal{S}_n$  est engendré par  $(1, 2)$  et  $\eta = (1, 2, \dots, n)$   
 preuve :  $\eta^i(1, 2)\eta^{-i} = (i+1, i+2)$

**3.6.4 Générateurs**

Soit  $n \geq 2$ .

**Théorème :**

1.  $\mathcal{S}_n$  est engendré par les transpositions
2.  $\mathcal{S}_n$  est engendré par les transpositions du type  $(1, j)$  où  $j \in \{2, \dots, n\}$

**3.6.5 Centre****Théorème :**

$Z(\mathcal{S}_n) = \{e\}$  pour  $n = 1$  et  $n \geq 3$ .

**3.6.6 Signature****Définition :** Signature

Soit  $\sigma \in \mathcal{S}_n$ . On pose  $\epsilon(\sigma) = (-1)^{n-t}$  où  $t$  est le nombre de  $\sigma$ -orbites différentes.

**Exemple :**

- $\sigma = e$  : on a  $\sigma(i) = i$  pour tout  $i \in \{1, \dots, n\}$ , chaque point est une orbite donc  $t = n$  et  $\epsilon(\sigma) = 1$
- $\sigma = (1, 2)$  : ici il y a  $n-2$  éléments fixés qui donnent chacun une orbite, et  $\{1, 2\}$  est une autre orbite donc  $\epsilon(\sigma) = -1$ .
- $\sigma = (1, \dots, r)$  :  $\epsilon(\sigma) = (-1)^{r-1}$

**Propriété :**

Soit  $\sigma \in \mathcal{S}_n$  où  $n \geq 2$ . Alors  $\epsilon(\sigma \circ \tau) = (-1) \times \epsilon(\sigma)$  pour toute transposition  $\tau \in \mathcal{S}_n$ .  
 En particulier, si  $\sigma$  est un produit de  $k$  transpositions, on a  $\epsilon(\sigma) = (-1)^k$ .

**Remarque :**

Ainsi, la parité du nombre de transpositions nécessaires pour décomposer  $\sigma$  ne dépend que de  $\sigma$ .

**Théorème :**

Si  $n \geq 2$ ,  $\epsilon : \mathcal{S}_n \longrightarrow \{1, -1\}$  est un morphisme de groupes surjectif.

**Preuve :**

Soient  $\sigma, \sigma' \in \mathcal{S}_n$ . On décompose  $\sigma = \tau_1 \circ \dots \circ \tau_k$  et  $\sigma' = \tau'_1 \circ \dots \circ \tau'_{k'}$  en produits de transpositions. Alors  $\epsilon(\sigma \circ \sigma') = (-1)^{k+k'} = \epsilon(\sigma) \times \epsilon(\sigma')$ .

□

**Définition : Groupe alterné**

Soit  $n \geq 2$ .  $\mathcal{A}_n$  est le noyau de  $\epsilon$ , on le nomme groupe alterné.

**Remarque :**

C'est un sous groupe distingué de  $\mathcal{S}_n$  d'indice 2, car le noyau d'un morphisme

**Remarque :**

Si  $\tau$  est une transposition,  $(\tau \mathcal{A}_n) \cap \mathcal{A}_n = \emptyset$ , d'où  $\mathcal{S}_n = (\tau \mathcal{A}_n) \sqcup \mathcal{A}_n$ .

**Théorème :**

1. Si  $n \geq 3$ ,  $\mathcal{A}_n$  est engendré par les 3-cycles.
2. Si  $n \geq 5$ , deux 3-cycles sont conjugués dans  $\mathcal{A}_n$
3. Si  $n \geq 2$ , alors  $D(\mathcal{S}_n) = \mathcal{A}_n$ , si  $n \geq 5$  alors  $D(\mathcal{A}_n) = \mathcal{A}_n$ .

**Preuve :**

1. Soit  $\sigma \in \mathcal{A}_n$ ,  $\sigma$  est un produit d'un nombre pair de transpositions, or  $(i, j)(j, k) = (i, j, k)$  et  $(i, j)(k, l) = (i, j, k)(j, k, l)$ .
2. Soient  $(i, j, k), (i', j', k')$  deux 3-cycles. Il existe  $\sigma \in \mathcal{S}_n$  tel que  $\sigma(i) = i', \sigma(j) = j', \sigma(k) = k'$ . Alors  $\sigma(i, j, k)\sigma^{-1} = (i', j', k')$ . Sans perte de généralité, on peut supposer que  $\sigma \in \mathcal{A}_n$ , en effet  $n \geq 5$ , donc il existe une transposition  $\tau = (r, s)$  avec  $r, s \notin \{i, j, k\}$ , et on peut remplacer  $\sigma$  par  $\sigma\tau$ .
3.  $D(\mathcal{A}_n) \subset D(\mathcal{S}_n) \subset \mathcal{A}_n$  car si  $a, b \in \mathcal{S}_n$ , alors  $\epsilon([a, b]) = 1$ .  
Montrons que si  $n \geq 5$ , les 3-cycles, qui engendrent  $\mathcal{A}_n$ , sont des commutateurs (de  $\mathcal{A}_n$ ).  
Soit  $\sigma = (i, j, k)$  un 3-cycle.  $\sigma^2$  est aussi un 3-cycle donc d'après 2. les deux sont conjugués : il existe  $\eta \in \mathcal{A}_n$  tel que  $\sigma^2 = \eta\sigma\eta^{-1}$  i.e.  $\sigma = [\eta, \sigma]$ .

□

**Cas particuliers :**

1.  $D(\mathcal{A}_3) = \{e\}$
2.  $D(\mathcal{A}_4) = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$

**Preuve :**

1.  $\mathcal{A}_3 = \langle (1, 2, 3) \rangle$  donc  $\mathcal{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$  est abélien
2. On note  $V = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ , c'est un sous groupe distingué de  $\mathcal{A}_4$ . Alors le groupe quotient  $\mathcal{A}_4/V$  est d'ordre 3 donc isomorphe à  $\mathbb{Z}/3\mathbb{Z}$  qui est abélien. Ainsi  $D(\mathcal{A}_4)$  est un sous-groupe de  $V$ . Par le théorème de Lagrange,  $D(\mathcal{A}_4)$  est de cardinal 1, 2, ou 4.  $\mathcal{A}_4$  n'est pas abélien donc ce n'est pas 1. Si c'était 2,  $D(\mathcal{A}_4)$  serait de la forme  $\{e, (i, j)(k, l)\}$  qui n'est pas distingué.

□