## Compléments sur les groupes.

L'ensemble $\mathfrak{G}(E)$ des permutations d'un ensemble $E$ muni de la loi $\circ$ (composition des applications) est un groupe ; appelé groupe symétrique de $E$. Si $n \geq 1$ est un entier, $E = [\![1, n]\!]$, ce groupe est noté $\mathfrak{S}_n$.

Démo : Id est l'élément neutre, $\forall s \in \mathfrak{S}_n$ possède un symétrique pour $\circ$, la bijection réciproque de $s$, soit $s^{-1}$

Prop : Soient $G$ un groupe multiplicatif et $a \in G$
L'application $t_a : x \mapsto ax$ de $G$ dans $G$ est appelée translation à gauche définie par $a$. C'est une permutation de $G$

## Sous-groupes et morphismes

Déf : Soit $(G, T)$ un groupe et $H$ partie de $G$. C'est 1 sous-groupe de $G$ si elle vérifie les conditions suivantes :

- $H$ n'est pas vide
- $H$ est stable par $T$
- $\forall x \in H$, le symétrique de $x$ appartient aussi à $H$

On utilise plus souvent la propriété avec les conditions
1) l'élément neutre de $G$ appartient à $H$
2) $\forall x, y \in H \quad x T y' \in H$.

Ex : Soit $(G, \times)$ un groupe. Montrer que $Z(G)$ des $a \in G$ commutant avec tout élément de $G$ est un sous-groupe de $G$, appelé centre de $G$

Démo $1 \in Z(G)$ donc non vide

$a, b \in Z(G)$ . $\forall x \in G$

$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$

donc $ab \in Z(G)$

. De même $ax = xa$

$a^{-1}axa^{-1} = a^{-1}xaa^{-1}$

$xa^{-1} = a^{-1}x$ , d'où $a^{-1} \in Z(G)$

Théorème Lagrange

Soit $G$ un groupe fini, $H$ sous-groupe de $G$.

L'ordre de $H$ divise l'ordre de $G$.

Déf Soit $G$ un groupe et $S$ une partie de $G$. On appelle sous-groupe de $G$ engendré par $S$ l'intersection de tous les sous-groupes de $G$ contenant $S$ ($G$ est lui-même un tel sous-groupe) et ce sous-groupe est noté $\langle S \rangle$. Si $\langle S \rangle = G$ on dit que $S$ engendre $G$ ou est une partie génératrice de $G$.

Par exemple, $\langle \emptyset \rangle = \{e\}$

Prop : Soit $S$ une partie de $G$, $G$ sous-groupe $\langle S \rangle$ est, pour l'inclusion, le plus petit sous-groupe de $G$ contenant $S$ : c'est un sous-groupe de $G$ contenant $S$ et il contient tout sous-groupe de $G$ contenant $S$.

Prop = Soient $G$ un groupe multiplicatif et $x \in G$. Alors $\langle x \rangle$ est formé des puissances $x^n$ de $x$, $n \in \mathbb{Z}$.

idem pour un groupe additif avec $nx$, $n \in \mathbb{Z}$

Déf : Un groupe $G$ est dit monogène s'il existe $x \in G$ tel que $\langle x \rangle = G$ (on dit que $x$ est générateur). Un groupe monogène fini est dit cyclique.

Tout groupe fini $G$ d'ordre $p$ premier est cyclique.

Soit en effet, $x \in G$ distinct du neutre, alors $\langle x \rangle$ est 1 sous-groupe non trivial de $G$, son ordre est $n > 1$ et 1 diviseur de $p$.

Or $p$ premier, donc $n = p$ d'où $\langle x \rangle = G$

**Déf** Soient $G$ et $G'$, deux groupes multiplicatifs. On appelle morphisme de $G$ dans $G'$ toute application $f : G \to G'$ vérifiant

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

**Prop.** Soit $f : G \to G'$ un morphisme de groupes multiplicatifs

$\forall x \in G \ \forall n \in \mathbb{Z}$, $f(x^n) = f(x)^n$

En particulier $f(x^{-1}) = f(x)^{-1}$

Si $e$ (resp $e'$) est l'élément neutre de $G$ (resp $G'$) $f(e) = e'$

**Théorème.** Soit $f : G \to G'$ morphisme.

1) L'image $f(H)$ d'un sous-groupe $H$ de $G$ est 1 sous-groupe de $G'$

Alors $f(G)$ est 1 sous-groupe de $G'$ noté $\mathrm{Im}(f)$

2) Soit $H'$ sous-groupe de $G'$, son image réciproque $f^{-1}(H')$ est 1 sous-groupe de $G$

$$f^{-1}(H') := \{ x \in G \mid f(x) \in H' \}$$

3) En particulier, notons $e'$ l'élément neutre de $G'$. Alors $f^{-1}(e')$ est 1 sous-groupe de $G$, appelé noyau $\mathrm{Ker}(f)$.

**Théorème.** Soit $f : G \to G'$ morphisme.

1) Pour que $f$ soit injectif, il faut et il suffit que son noyau soit trivial

2) Si $f$ est bijectif, la bijection réciproque $f^{-1}$ est aussi un morphisme

3) Supposons $G$ fini, alors $\mathrm{Im}(f)$ est finie et l'on a

$$\text{ordre}(G) = \text{ordre}(\mathrm{Ker} f) \times \text{ordre}(\mathrm{Im} f)$$

**Théorème :** Soit $G$ un groupe multiplicatif, $x \in G$.

1) Il existe un unique morphisme $f$ de $(\mathbb{Z}, +)$ dans $G$ tel que

$$f(1) = x$$

De plus $f(n) = x^n \quad \forall n \in \mathbb{Z}$ et l'image de $f$ est $\langle x \rangle$

2) Si $f$ est injectif, c'est l'isomorphisme de $(\mathbb{Z}, +)$ sur $\langle x \rangle$ en particulier, $\langle x \rangle$ est infini et l'on dit que $x$ est d'ordre infini

3) Si $f$ n'est pas injectif, $\exists! n \in \mathbb{N}^*$ tel que le noyau de $f$ soit égal à $n\mathbb{Z}$. Alors $1, x, x^2, \dots x^{n-1}$ sont deux à deux distincts, $\langle x \rangle = \{1, x, x^2, \dots x^{n-1}\}$ et $\langle x \rangle$ est cyclique d'ordre $n$, $n$ est appelé ordre de $\langle x \rangle$, c'est le plus petit entier $k$ tel que $x^k = 1$

**Théorème : Lagrange**

Soient $G$ un groupe fini et $x \in G$. L'ordre de $x$ divise l'ordre de $G$.

**Groupe symétrique** $E$ un ensemble

Le groupe symétrique de $E$ est l'ensemble $\mathfrak{S}(E)$ des permutations de $E$ muni de la loi $\circ$.

$(\mathfrak{S}(E), \circ)$ est un groupe. Si $E = [\![1, n]\!]$ $n \geq 1$, on le note $\mathfrak{S}_n$.

Points importants :

- Soit $s$ et $t \in \mathfrak{S}(E)$, $x \in E$ $(s \circ t)(x) = s(t(x))$

l'élément neutre est l'application identité, notée 1

Soit $s \in \sigma(E)$, l'inverse de $s$ dans $\sigma(E)$ est la bijection réciproque $s^{-1}$ de $s$ : $s^{-1} \circ s = 1 = s \circ s^{-1}$

Si $E$ est fini, de cardinal $n \geq 1$, l'ordre de $\sigma(E)$ est $n!$

**Déf :** Soit $E$ un ensemble, $n \geq 2$ un entier, $a_1 \dots a_n \in E$ des éléments deux à deux distincts

Considérons la permutation $c$ de $E$ définie par

$$\begin{cases} c(a_1) = a_2 \,,\ c(a_2) = a_3 \,, \dots c(a_n) = a_1 \\ c(x) = x \quad \forall x \in E \text{ distincts de } a_1, \dots a_n \end{cases}$$

$c$ est notée $(a_1\ a_2 \dots a_n)$. Une permutation de ce type est appelé $n$-cycle de $E$. Un 2-cycle est une transposition.

**Prop :** Soit $c := (a_1 \dots a_n)$ un $n$ cycle de $E$.

1) La permutation $c$ est la composition de $n-1$ transpositions

$$(a_1 \dots a_n) = (a_1\ a_2) \circ (a_2\ a_3) \circ \dots \circ (a_{n-1}\ a_n)$$

2) Pour tout $s \in \sigma(E)$, on a la formule de conjugaison

$$s \circ (a_1 \dots a_n) \circ s^{-1} = (s(a_1) \dots s(a_n))$$

**Ex** Soit $E$ un ensemble avec au moins 3 éléments, le centre de $\sigma(E)$ est trivial.

en effet, soit $s \in \sigma(E)$, $s \neq 1$. $\exists a \in E$ tel que $s(a) \neq a$

posons $b := s(a)$

$\forall x \in E \setminus \{a, b\}$

$$s \circ (a\ x) \circ s^{-1} = (s(a)\ s(x))$$
$$= (b\ 1(x)) \neq (a\ x) \text{ car } b \neq a, x$$

Ainsi $s \circ (a\ x) \neq (a\ x) \circ s$

$s$ ne commute pas avec $(a\ x)$

Toute transposition est d'ordre 2

$t \neq 1$ mais $t^2 = t \circ t = 1$ d'où $t^{-1} = t$

**Théorème :**

1). Soit $n$ entier $\geq 2$. Chacune des parties suivantes engendre $\sigma_n$

$S = \{(1\,2), (2\,3), \dots (n-1\ n)\}$

$T = \{(1\,2), (1\,3) \dots (1\ n)\}$

$U = \{(1\,2), (1\,2 \dots n)\}$

2) Toute permutation d'un ensemble fini $E$ s'écrit comme composée de transpositions. L'ensemble des transpositions engendre donc $\sigma(E)$

Lemme : Soient $n \geq 0$ un entier et $s_1, \dots s_n$ des transpositions d'un ensemble $E$ telles que $s_1 \circ \dots \circ s_n = 1$

Alors $n$ est pair.

**Théorème** 1) Si $n \geq 2$, il existe un unique morphisme $\varepsilon$ non trivial de $\sigma(E)$ dans le groupe multiplicatif $\{-1, 1\}$

si $n = 1$, on note $\varepsilon : \sigma(E) \to \{-1, 1\}$ le morphisme trivial. Si $s \in \sigma(E)$, $\varepsilon(s)$ est appelé signature de $s$ ; si $s$ est dite paire si $\varepsilon(s) = 1$, impaire sinon

2) Soit $s \in \sigma(E)$. Il existe un entier $k \geq 0$ et des transpositions $s_1, \dots s_k$ telles que $s = s_1 \circ \dots \circ s_k$

alors $\varepsilon(s) = (-1)^k$

3) Si $c$ est un cycle de longueur $m \geq 2$

$$\varepsilon(c) = (-1)^{m-1}$$

En particulier, la signature d'une transposition est $-1$

Le noyau de $\varepsilon$ est appelé groupe alterné de $\bar{E}$, on le note $\mathcal{A}(\bar{E})$

**Prop** Soient $n \geq 2$ un entier et $s \in \mathfrak{S}_n$. Appelons inversion de $s$ tout couple d'entiers $(i,j)$ tel que $1 \leq i < j \leq n$ et $s(i) > s(j)$. Notons $N(s)$ le nombre d'inversions de $s$.
Alors $\varepsilon(s) = (-1)^{N(s)}$

## Groupe additif des entiers modulo $n$

**Prop** : Soit $n \geq 1$ un entier, muni de l'addition, $\mathbb{Z}/n\mathbb{Z}$ est un groupe
Ce groupe est cyclique d'ordre $n$ et $\bar{1}$ est générateur

**Preuve** : Associativité de l'addition de $\mathbb{Z}/n\mathbb{Z}$ provient de celle de $\mathbb{Z}$
$\bar{0}$ étant neutre $x \in \mathbb{Z}$, $-\bar{x}$ est l'opposé de $\bar{x}$
donc $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe
et $\bar{k} = k.\bar{1}$ par récurrence, passage à l'opposé $\bar{k} = k.\bar{1}$ $k \in \mathbb{Z}$
donc $\bar{1}$ engendre $\mathbb{Z}/n\mathbb{Z}$

L'application $\pi : k \longmapsto \bar{k}$ est un morphisme de groupe
$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

appelé morphisme canonique. Il est surjectif et $\mathrm{Ker}(\pi) = n\mathbb{Z}$

**Théorème** : Un groupe monogène est isomorphe soit à $\mathbb{Z}$ s'il est infini,
soit à $\mathbb{Z}/n\mathbb{Z}$ s'il est fini (donc cyclique) d'ordre $n \geq 1$