Fiche de révisions chapitre 2 : Notions de groupes SECS01

I. Notions de base.

- Une **opération binaire** sur un ensemble G est une application $\cdot$ de $G \times G \to G$

- Un **groupe** $(G, *)$ est une structure algébrique consistant en un ensemble G muni d'une opération binaire $*$ satisfaisant les conditions suivantes :
  - $*$ est associative $\to \forall a, b, c \in G,\ a*(b*c) = (a*b)*c$
  - $\exists e \in G\ \forall a \in G\ \ a*e = a = e*a$ et e est l'élément neutre de G
  - $\forall a \in G\ \exists a' \in G$ tq $a*a' = e$ $\to$ tout élément de G possède un inverse.
- Un **groupe commutatif** noté $+$ est dit abélien $\forall a, b \in G\ \ a*b = b*a$
- L'**ordre** d'un groupe G est le nombre d'éléments de ce groupe et noté $|G|$.
- Un sous ensemble H d'un groupe $(G, *)$ est un **sous groupe** de G si et seulement si $\Leftrightarrow$
  - H est non vide
  - H est interne pour $*$
  - $\forall x, y \in H\ \ x \cdot y^{-1} \in H$.
  - e neutre de G et $e \in H$

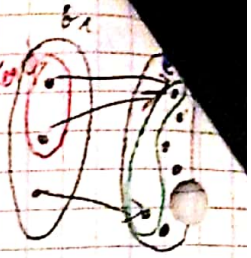
↳ **Preuve** : $\Rightarrow$ $H \neq \emptyset$. Pour $y \in H$ $y^{-1} \in H$ donc Pour $x \in H$ $x \cdot y^{-1} \in H$.
$\Leftarrow$ On suppose $\forall x, y \in H$ $x \cdot y^{-1} \in H$ et si $x = y$ alors $x \cdot x^{-1} = e$
Donc $e \in H$

- Considérons deux groupes $(G_1, *_1)$ et $(G_2, *_2)$
  Un **homomorphisme** du groupe G_1 vers G_2 est une application $\phi : G_1 \to G_2$ tq $\phi(x *_1 y) = \phi(x) *_2 \phi(y)$
- Un homomorphisme bijectif est un isomorphisme et on note $G_1 \cong G_2$

- **Propriété** : Soient G_1 et G_2 deux groupes. Soit $\phi : G_1 \to G_2$ un homomorphisme.
  Alors $\phi(e_1) = e_2$ et $\phi(x^{-1}) = \phi(x)^{-1}$

↳ $e_2 = \phi(e_1) *_2 \phi(e_1)^{-1}$ or $\phi(e_1) = \phi(e_1 *_1 e_1) = \phi(e_1) *_2 \phi(e_1)$
donc $e_2 = \phi(e_1) *_2 \phi(e_1) *_2 \phi(e_1)^{-1} = \phi(e_1)$

↳ $x *_1 x^{-1} = e_1$ donc $\phi(x *_2 x^{-1}) = \phi(x) *_2 \phi(x^{-1})$
Or $\phi(x *_1 x^{-1}) = \phi(e_1) = e_2 = \phi(x) *_2 \phi(x)^{-1}$
Donc $\phi(x) *_2 \phi(x)^{-1} = \phi(x) *_2 \phi(x^{-1}) \Rightarrow \phi(x^{-1}) = \phi(x)^{-1}$



- Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. Soit $\phi : G_1 \to G_2$

$\text{Im}\,\phi = \{\phi(x) \mid x \in G_1\}$: tous les éléments étant une image pour G_1

$\text{Ker}\,\phi = \{x \in G_1 \mid \phi(x) = e_2 \text{ et } e_2 \text{ neutre de } G_2\}$

II. Théorème de Lagrange.

- Théorème: Dans un groupe fini, l'ordre d'un sous groupe divise l'ordre du groupe.

Preuve:
Soit $(G, *)$ un groupe fini et H un sous groupe de G
Soit $a \in G$, observons $\varphi : H \to aH$ est une bijection.
Donc $|H| = |aH| \ \forall a \in G$.
On a formé une partition de G et on a $G = \bigcup_{a \in I} aH$ et $aH \cap bH = \emptyset$ si $a, b \in I$

Donc $|G| = \sum_{a \in I} |aH| = \sum_{a \in I} |H| = |I| \cdot |H|$ et donc $|H| \mid |G|$

III. Construction de groupes.

- Soit $(G_i, *_i)$ $i = 0, \dots, n$ des groupes alors l'ensemble $G_0 \times \dots \times G_n$ muni de l'opération $(x_0, \dots, x_n) \times (y_0, \dots, y_n) = (x_0 *_0 y_0, \dots, x_n *_n y_n)$ est un groupe dont le neutre $(e_0, e_1, \dots, e_n)$ où e_i est le neutre de G_i $(i = 0, \dots, n)$.

- Soit H un sous groupe de G, on dit que H est distingué de G si
$\forall a \in G \quad a.H = H.a$

- Si G est un groupe commutatif alors tout sous groupe de G est distingué.

- Soit G un groupe et H un sous groupe distingué alors $\forall a, b \in G \quad a.H.b.H = (a.b).H$

- Théorème: Soit G un groupe et H un sous groupe distingué de G.
Alors l'ensemble des classes à gauche de H dans G forme un groupe pour l'opération
$a.H.b.H = a.b.H \quad \forall a, b \in G$.
On l'appelle groupe quotient de G par H et est noté G/H
Le neutre est H.

Preuve: → Montrons que H est le neutre
$\forall a \in G \quad a.H.H = (a.e)H = a.H$ car $H = eH$
→ Montrons associativité
$\forall a, b, c \in G \quad (a.H.b.H).c.H = (a.b)H\,c.H = ((a.b).c).H = (a.(b.c))H$
$= aH.(bH.cH)$
→ Montrons tout élem G a un inverse
$\forall a \in G \quad a.H.a^{-1}H = (a.a^{-1})H = eH = H = (a^{-1}a)H = a^{-1}H.aH$
↳ G/H groupe quotient.

- Théorème: $n\mathbb{Z} = \{x.n \mid x \in \mathbb{Z}\}$ forme un sous groupe de $(\mathbb{Z}, +)$, distingué dans $(\mathbb{Z}, +)$

Preuve: $-n\mathbb{Z} \neq \emptyset$
- $+$ est interne à $n\mathbb{Z}$
- $\forall a, b \in \mathbb{Z} \quad [a + n\mathbb{Z}] + [b + n\mathbb{Z}] = [(a+b) + n\mathbb{Z}]$ loi interne à l'addition
- distingué car $(\mathbb{Z}, +)$ commutatif

- Soit G un groupe et P un sous ensemble de G. On appelle <u>sous groupe engendré par P</u> l'intersection de tous les sous groupes de G contenant P.
Si $P = \{x_1, \dots, x_n\}$ on notera $\langle x_1, \dots, x_n \rangle$ le sous groupe engendré par P.
Les éléments x_i sont appelés les générateurs.

- Un groupe est <u>monogène</u> s'il est engendré par un seul élément. <u>ex</u>: $(\mathbb{Z}, +) \to \langle 1 \rangle$ monogène.

- Soit G un groupe et soit x un élément de G. On appelle ordre de x, noté $|x|$, s'il existe le plus petit entier n non nul positif tq $x^n = e$ (où e est neutre de G)

- L'ordre de tout élément d'un groupe fini divise l'ordre du groupe.

↳ <u>Preuve</u>: cf TD2 exo 5 q2.
L'ordre de x est l'ordre du sous groupe de G engendré par x. Ainsi par le théorème de Lagrange, l'ordre d'un élément divise toujours l'ordre du groupe.