SYNTHESE : Les Groupes

I] Les Groupes et sous-groupes

Groupes de référence :

- Nombres : $(\mathbb{Z},\ +)$, $(\mathbb{Q},\ +)$, $(\mathbb{R},\ +)$ et $(\mathbb{C},\ +)$, $(\mathbb{Q}^*,\ \times)$, $(\mathbb{R}^*,\ \times)$ et $(\mathbb{C}^*,\ \times)$.
- Ensembles : $(\mathbb{Z}/n\mathbb{Z},\ +)$
- Fonctions : $(\mathcal{F}(A,\mathbb{K}),\ +)$, $(\mathrm{GL}(\mathbb{E}),\ \circ)$, $(\mathrm{O}(E),\ \circ)$, $(\mathrm{SO}(E),\ \circ)$, $(S_n,\ \circ)$.
- Matrices : $(\mathfrak{M}_n(\mathbb{R}),+)$, $(\mathrm{GL}_n(\mathbb{R}),\times)$, $(\mathrm{O}_n(\mathbb{R}),\times)$, $(\mathrm{SO}_n(\mathbb{R}),\times)$.

Pour tous ces groupes de référence, on oublie souvent de préciser la lci.
On parle ainsi du Groupe Symétrique S_n, du Groupe $\mathbb{Z}/n\mathbb{Z}$ ou du Groupe $\mathrm{GL}_n(\mathbb{K})$.

Notation : un groupe quelconque est souvent simplement noté G et la composition de a et b : ab.

Pour montrer que $(G,\ \star)$ est un groupe

- Avec la définition :

  → $\star$ est une lci,
  → $\star$ est associative
  → Existence d'un élément neutre dans G pour $\star$
  → Existence d'un symétrique pour tout élément de G

- ♡ Avec les sous-groupes : On montre que $(G,\ \star)$ est un sous-groupe d'un groupe $(H,\ \star)$ connu

  → $G \subset H$
  → H non vide
  → Stabilité par $\star$: $\quad x, y \in G \Rightarrow x \star y \in G$
  → Stabilité par symétrisation : $\quad x \in G \Rightarrow x^{-1} \in G$

  Cette méthode ne peut s'appliquer que si $\star$ est la lci d'un groupe connu. Pour l'appliquer, il faut donc connaître parfaitement les groupes de référence.

Notations :

- Lorsque la lci est notée $+$: $\quad 0_G,\ -x,\ nx$
- Sinon on utilise les notations : $\quad 1_G,\ x^{-1},\ x^n$

Les sous-groupes usuels :

- Nombres :
  - $\to$ $\mathbb{U}$, et $\mathbb{U}_n$ sont des sous-groupes usuels de $(\mathbb{C}^*,\ \times)$.
  - $\to$ $n\mathbb{Z}$ sont les sous-groupes de $(\mathbb{Z},\ +)$
- Fonctions :
  - $\to$ $(\mathrm{O}(E),\ \circ)$ et $(\mathrm{SO}(E),\ \circ)$ sont des sous-groupes usuels de $(\mathrm{GL}(\mathbb{E}),\ \circ)$,
  - $\to$ $\mathcal{A}_n$ (ensemble des permutations de signature 1) est un sous-groupe de $(S_n,\ \circ)$.
- Matrices : $(\mathrm{O}_n(\mathbb{R}), \times)$, $(\mathrm{SO}_n(\mathbb{R}), \times)$ et $(SL_n(\mathbb{R}),\ \times)$ sont des sous-groupes usuels de $(\mathrm{GL}_n(\mathbb{R}), \times)$
- Opérations : Pour un groupe G
  - $\to$ L'intersection de sous-groupes de G est un sous-groupe de G
  - $\to$ La somme de sous-groupes d'un groupe additif G est un sous-groupe de G
  - $\to$ L'ensemble $\mathrm{Vect}(A)$ des éléments engendrés par les éléments de $A \subset G$ est un sous-groupe de G

II] Le groupe $\mathbb{Z}/n\mathbb{Z}$

Définition :

- $\mathbb{Z}/n\mathbb{Z} = \{\bar{0},\ \bar{1},\ \ldots,\ \overline{n-1}\}$ où $\bar{k}$ est une notation qui désigne l'ensemble des entiers congrus à k modulo n.
- On définit sur $\mathbb{Z}/n\mathbb{Z}$ les lci $\left\{ \begin{array}{c} + \\ \times \end{array} \right.$ par : $\left\{ \begin{array}{l} \bar{x} + \bar{y} = \overline{x+y} \\ \bar{x} \times \bar{y} = \overline{x \times y} \end{array} \right.$.
- $(\mathbb{Z}/n\mathbb{Z},\ +)$ est un groupe commutatif fini
  - $\to$ de cardinal n,
  - $\to$ d'élément neutre $\bar{0}$,
  - $\to$ engendré par $\bar{1}$ et tous les éléments $\bar{k}$ tels que $k \wedge n = 1$

A savoir :

- Lien avec l'arithmétique : $x \equiv y\ [n] \iff \bar{x} = \bar{y}$ (Dans $\mathbb{Z}/n\mathbb{Z}$)
- Les générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$ sont les éléments $\bar{k}$ tels que $k \wedge n = 1$.

III] Le groupe $\mathcal{S}_n$

$(\mathcal{S}_n,\ \circ)$ est un groupe de cardinal $n!$ appelé le *groupe des permutations* de $[\![1, n]\!]$.

A savoir :

Pour une permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ x_1 & x_2 & x_3 & \cdots & x_n \end{pmatrix} \in S_n$, vous devez être capable de déterminer

- sa représentation orbitale (et donc ses orbites)
- son support
- sa décomposition (unique et commutative) en produit de cycles de supports disjoints
- sa décomposition (non unique et non commutative) en produits de transpositions
- sa signature
- son ordre : le ppcm des cardinaux des différentes orbites
- ses inversions

Les différents types de permutations de S_n

- les cycles : $c = (x_1\ x_2\ \ldots\ x_p)$ (ordre p)
- les transpositions : $\tau = (x_1\ x_2)$ (ordre 2)
- les permutations circulaires : $c = (x_1\ x_2\ \ldots\ x_n)$ (ordre n)

IV] Les morphismes de groupes

Exemples usuels : $\exp : \mathbb{R} \to \mathbb{R}^*$, $\varepsilon : \mathcal{S}_n \to \{-1,\ 1\}$

Pour montrer que $\varphi : H \to G$ est un morphisme de groupe

On montre que :

- $(H,\ \star)$ et $(G,\ \circ)$ sont deux groupes
- On pose $x,\ y \in H$ et on prouve que $\varphi(x \star y) = \varphi(x) \circ \varphi(y)$

Vocabulaire :

- On dit que le morphisme φ est un $\begin{cases} \text{Endomorphisme :} & \text{lorsque } \varphi : G \to G \\ \text{Isomorphisme :} & \text{lorsque } \varphi \text{ est bijectif} \\ \text{Automorphisme :} & \text{lorsque } \varphi : G \to G \text{ et est bijectif} \end{cases}$
- Lorsqu'il existe un isomorphisme $\varphi : H \to G$, on dit que G et H sont isomorphes.

Isomorphes ou pas ?

- Pour montrer que 2 groupes H et G sont isomorphes.

  On procède par intuition :

  $\to$ On propose une application $\varphi : H \to G$

→ On montre que φ est un isomorphisme

- Pour montrer que $(G,+)$ et $(H,\star)$ ne sont pas isomorphes

  → On suppose qu'il existe un isomorphisme de l'un vers l'autre.

  → On considère 2 équations, équivalentes via cet isomophisme : en général $\begin{cases} 2x=0 \text{ dans } (G,\ +) \\ x^2=0 \text{ dans } (H,\ \star) \end{cases}$.

  → On montre que ces 2 équations n'ont pas le même nombre de solutions.

A savoir :

- Effectuer des calculs avec un morphisme : $\varphi(e_G)$, $\varphi(a^n)$, $\varphi(a^{-1})$...
- La composée de 2 morphismes est un morphisme
- Les noyaux et les images d'un morphisme sont des sous-groupes
- La bijection réciproque d'un isomorphisme est un isomorphisme
- Les images directe et réciproque d'un sous-groupe par un morphisme est un sous-groupe.
- Caractérisation de l'injectivité et de la surjectivité d'un morphisme à l'aide de l'image et du noyau

Méthode : Recherche du noyau et de l'image de $\varphi : G \to H$

- $\ker\varphi$: On recherche les antécédents de e_H par φ.

  Pour cela, on résout l'équation $\varphi(x) = e_H$ dans G

- $\mathrm{Im}\,\varphi$: On recherche l'ensemble des images.

  Pour cela, on procède par analyse/synthèse...

  → Analyse : Soit $y = \varphi(x) \in \mathrm{Im}\,\varphi$, alors ... et donc $y \in \Delta$

  → Synthèse : Soit $y \in \Delta$, vérifions s'il existe $x \in G$ tel que $y = \varphi(x)$...

  ... ou par intuition puis validation par double inclusion !

V] Les groupes monogènes

Il s'agit des sous-groupes $< a >= \{a^k \mid k \in \mathbb{Z}\}$ engendrés par un élément a d'un groupe G.

On distingue :

- Les groupes monogènes finis (de cardinal n) : $\mathbb{Z}/n\mathbb{Z} =< \bar{1} >$, $\mathbb{U}_n =< e^{\frac{2i\pi}{n}} >$...

  Ils sont isomorphes à $\mathbb{Z}/n\mathbb{Z}$ via l'isomorphisme $\varphi_n : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & < a > \\ \bar{k} & \mapsto & a^k \end{array}$

  Les groupes monogènes finis sont appelés des groupes cycliques.

- Les groupes monogènes infinis : $\mathbb{Z} =< 1 >$, $n\mathbb{Z} =< n >$...

  Ils sont isomorphes à $\mathbb{Z}$ via l'isomorphisme $\varphi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & < a > \\ k & \mapsto & a^k \end{array}$

Exemples usuels de groupes monogènes :

- $\mathbb{Z} =< 1 >$
- $\mathbb{U}_n =< e^{i2\pi/n} >$
- $\mathbb{Z}/n\mathbb{Z} =< \bar{1} >$

A savoir :

- Les groupes monogènes sont commutatifs
- Deux groupes cycliques (monogènes finis) de même cardinal sont isomorphes
- Les éléments générateurs d'un groupe monogène $< a >$ de cardinal n sont les a^k avec $k \wedge n = 1$
- Les éléments générateurs d'un groupe monogène $< a >$ infini sont a et a^{-1}

Monogène ou pas monogène ?

- Prouver qu'un groupe H est monogène :
  On recherche un élément $h \in H$ tel que $H =< h >$

- Prouver qu'un groupe H n'est pas monogène :
  Souvent, on montre qu'il n'est pas commutatif

L'indicatrice d'Euler φ :

Pour tout $n \in \mathbb{N}^*$:

- $\varphi(n)$ est le nombre d'entiers de $[\![1, n]\!]$ premiers avec n.
- $\varphi(n)$ est le nombre de générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$
- $\varphi(n)$ est le nombre de générateurs de tout groupe monogène fini de cardinal n
- $\varphi(n)$ est le nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z},\ +,\ \times)$ (voir le cours sur les anneaux)

Une expression de $\varphi(n)$ sera vue dans le cours sur les anneaux.

VI] L'ordre d'un élément

Lorsqu'il existe, l'ordre d'un élément $a \in G$ est le plus petit entier $p \in \mathbb{N}^*$ tel que $a^p = e_G$.

Exemples :

- L'élément neutre est le seul élément d'ordre 1.
- i est d'ordre 4 et j est d'ordre 3 dans $\mathbb{U}$.
- 2 n'est pas d'ordre fini dans les groupes $(\mathbb{R}^*, \times)$ et $(\mathbb{R}, +)$.
- Les p-cycles sont d'ordre p et donc les transpositions sont d'ordre 2.
- Les permutations sont d'ordre le PPCM des cardinaux des différentes orbites de la permutation.
- Dans un groupe cyclique de cardinal n, un générateur est d'ordre n.

A savoir :

- Lorsque a est d'ordre p, on a $< a >= \{e_G,\ a,\ \ldots,\ a^{p-1}\}$ et $< a >$ est de cardinal p.
- Lorsque $a^m = e_G$, l'ordre de a divise m.
- Dans un groupe fini G de cardinal n :
  - $\rightarrow$ les éléments de G sont d'ordre fini
  - $\rightarrow$ leur ordre divise n
  - $\rightarrow$ $a^n = e_G$.

Méthode : Pour déterminer l'ordre d'un élément $a \in G$

- Si c'est possible, on calcule a^2, a^3 ... etc ...jusqu'à obtenir $a^p = e_G$
- Plus généralement, on procède par Analyse/Synthèse :
  - $\rightarrow$ Analyse : Soit r l'ordre de a, alors ...
    On trouve finalement un $p \in \mathbb{N}^*$ qui divise r et qui vérifie donc $p \leq r$
  - $\rightarrow$ Synthèse : On vérifie alors que $a^p = e_G$ et donc $r \leq p$.
    On en déduit finalement que $r = p$.

Démonstration à savoir :

Pourquoi tout groupe fini de cardinal p premier est-il cyclique ?

D/ Soit G un groupe de cardinal p premier :

- Les ordres des éléments de G divisent p donc valent 1 ou p.
- e_G étant le seul élément d'ordre 1, il existe donc un élément a d'ordre p
- nous avons alors $< a > \subset G$ avec $< A >$ et G de même cardinal.
- Par conséquent, $G =< a >$ et donc G est un groupe monogène fini, cad un groupe cyclique.