Groupes

1. Révisions de première année.
2. Intersection de sous-groupes. Sous-groupe engendré par une partie, par un élément. Partie génératrice d'un groupe.
3. Sous-groupes de $(\mathbb{Z}, +)$.
4. Groupe $\mathbb{Z}/n\mathbb{Z}$ et générateurs de $\mathbb{Z}/n\mathbb{Z}$.
5. Groupe monogène, groupe cyclique. À quel groupe est isomorphe un groupe monogène infini ? À quel groupe est isomorphe un groupe monogène fini ?
6. Ordre d'un élément dans un groupe, et correspondance avec le cardinal du sous-groupe engendré par cet élément. On a $a^k = e$ si et seulement si l'ordre de a divise k.
7. Théorème de Lagrange concernant l'ordre d'un élément dans un groupe fini.

---

1 Révisions de MPSI

1.1 généralités sur les groupes et morphismes de groupes

Définition 1

Soit G un ensemble muni d'une loi de composition interne $\star$. On dit que $(G, \star)$ est un *groupe* lorsque

- $\star$ est associative
- $\star$ admet un élément neutre
- tout élément de G est inversible.

L'élement neutre du groupe G est noté e, ou encore 1_G si la loi est notée multiplicativement et 0_G si la loi est notée additivement.

Le groupe $(G, \star)$ est dit *commutatif* (ou *abélien*) lorsque la loi $\star$ est commutative.

Exercice 1 : Donner des exemples usuels de groupes additifs et de groupes multiplicatifs rencontrés dans les cours de première année.

Si $(G, \star)$ est un groupe et $a, b \in G$, alors

$$\forall x \in G, \quad a \star x = b \quad \text{ssi} \quad x = a^{-1} \star b$$

De même

$$\forall x \in G, \quad x \star a = b \quad \text{ssi} \quad x = b \star a^{-1}$$

On peut ainsi résoudre facilement de nombreuses équations dans un groupe G !

1.2 sous-groupe

Définition 2

Soit $(G, \star)$ un groupe et H une partie de G. On dit que H est un *sous-groupe* de $(G, \star)$ lorsque H est stable par $\star$ et que $(H, \star)$ est un groupe.

La notion de sous-groupe est importante car en pratique, pour montrer que $(H, \star)$ est un groupe, on le fera presque toujours apparaître comme sous-groupe d'un groupe connu.

Propriété 1

Soit $(G, \star)$ un groupe et H une partie de G.

$$H \text{ est un sous-groupe de } G \quad \Leftrightarrow \quad \begin{cases} 1_G \in H \\ H \text{ est stable par produit : } \forall h, h' \in H, \quad h \star h' \in H \\ H \text{ est stable par inversion : } \forall h \in H, \quad h^{-1} \in H \end{cases}$$
$$\Leftrightarrow \quad \begin{cases} 1_G \in H \\ H \text{ est stable par produit-inversion : } \forall h, h' \in H, \quad h^{-1} \star h' \in H \end{cases}$$

En notation additive,

$$H \text{ est un sous-groupe de } G \Leftrightarrow \begin{cases} 0_G \in H \\ \forall h, h' \in H, \quad h' - h \in H \end{cases}$$

Propriété 2 – groupe produit

Soient $(G_1, \square)$ et $(G_2, \diamond)$ deux groupes. On définit une loi de composition interne sur $G_1 \times G_2$ en posant, pour $x = (x_1, x_2)$ et $y = (y_1, y_2)$ dans $G_1 \times G_2$:

$$x \star y = (x_1 \square y_1, x_2 \diamond y_2)$$

Muni de cette loi, $G_1 \times G_2$ est un groupe, appelé *groupe produit*, d'élément neutre $(1_{G_1}, 1_{G_2})$.

Définition 3

Soit $(G, \square)$ et $(G', \diamond)$ deux groupes. On dit qu'une application f de G dans G' est un *morphisme de groupe* lorsque

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

On dit que f est :

— un *endomorphisme* lorsque $(G, \square) = (G', \diamond)$.

— un *isomorphisme* lorsque f est bijective.

— un *automorphisme* lorsque f est un endomorphisme et un isomorphisme.

Exemples :

- L'exponentielle complexe est un morphisme de groupe de $\mathbb{C}$ dans $\mathbb{C}^*$ car

- L'application f de $\mathbb{R}$ dans $\mathbb{U}$ qui à θ associe $e^{i\theta}$ est un morphisme du groupe $(\mathbb{R}, +)$ dans le groupe $(\mathbb{U}, \times)$ car

- La fonction module est un endomorphisme de groupes de $\mathbb{C}^*$ car

- Trace est un morphisme de groupes de dans car

Propriété 3

Soit f un morphisme du groupe de $(G, \square)$ dans $(G', \diamond)$. Alors

$$\begin{aligned} & f(1_G) = 1_{G'} \\ \forall x \in G, \quad & f\left(x^{-1}\right) = [f(x)]^{-1} \end{aligned}$$

Propriété 4

Soit f un morphisme de $(G, \square)$ dans $(G', \diamond)$. Alors
- l'image réciproque d'un sous-groupe de G' est un sous-groupe de G.
- l'image directe d'un sous-groupe de G est un sous-groupe de G'.

Image et noyau :
$\operatorname{Im} f = \{f(x),\ x \in G\} = f(G)$ est un sous-groupe de G'. f est surjectif si et seulement si $\operatorname{Im} f = G'$.
Et $\ker f = \{x \in G \mid f(x) = 1_{G'}\}$ est un sous-groupe de G. f est injectif si et seulement si $\ker f = \{1_G\}$.

Enfin,
- La composée de deux morphismes de groupes est un morphisme de groupe.
- La bijection réciproque d'un isomorphisme de groupe est un isomorphisme de groupe.

1.3 le groupe symétrique

Soit E un ensemble de cardinal $n \in \mathbb{N}^*$. Une permutation de E est une bijection de E dans E. L'ensemble des permutations de E est noté $\mathcal{S}_E$. L'ensemble E étant de cardinal n, il est en bijection avec $[\![1, n]\!]$ donc il est équivalent d'étudier l'ensemble $\mathcal{S}_n$ des permutations de $[\![1, n]\!]$. On représente usuellement une permutation par la liste des éléments de $[\![1, n]\!]$ en-dessous de laquelle on indique l'image de chaque élément.
La notation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 4 & 5 \end{pmatrix}$$

désigne l'application σ telle que $\sigma(1) = 3$, $\sigma(2) = 2$, $\sigma(3) = 1$, $\sigma(4) = 6$, $\sigma(5) = 4$ et $\sigma(6) = 5$.

L'ensemble $\mathcal{S}_n$ est un groupe pour la composition, non commutatif pour $n \geqslant 3$. L'ordre de la permutation σ est le plus petit entier naturel k non nul tel que $\sigma^k = \mathrm{Id}$.

Support
On appelle support d'une permutation σ l'ensemble des éléments x de $[\![1, n]\!]$ tels que $\sigma(x) \neq x$. Dans l'exemple

ci-dessus, le support de σ est $\{1,3,4,5,6\}$. Deux permutations à supports disjoints commutent.

Cycles
Soit $p \in [\![2,n]\!]$. On appelle *p-cycle*, toute permutation σ de $[\![1,n]\!]$ pour laquelle il existe des éléments distincts $x_1,\dots,x_p$ de $[\![1,n]\!]$ pour lesquels :

$$\sigma(x_1)=x_2,\ \sigma(x_2)=x_3,\dots\sigma(x_{p-1})=x_p \text{ et } \sigma(x_p)=x_1, \quad \text{ et } \sigma(x)=x \text{ si } x\notin\{x_1,\dots,x_p\}$$

Un tel p-cycle est noté $(x_1\ x_2\dots x_p)$.
On remarque qu'une transposition est un 2-cycle.
Toute permutation de $[\![1,n]\!]$ peut être décomposée d'une et une seule manière, à l'ordre des facteurs près, comme un produit de cycles disjoints.

Transpositions
Supposons $n \geqslant 2$. On appelle *transposition* une permutation qui échange deux éléments distincts et qui laisse les autres invariants. On la note usuellement $(i\ j)$. Une transposition est d'ordre 2, elle est son propre inverse : c'est une involution.
Toute permutation de $[\![1,n]\!]$ est un produit de transpositions. Il n'y a pas unicité de la décomposition en produit de transpositions.

Signature
Il existe un et un seul morphisme de groupes ε de $\mathcal{S}_n$ dans $\{-1,1\}$, appelée *signature*, qui donne à toute transposition la valeur -1 et pour lequel pour tous $\sigma,\sigma'\in\mathcal{S}_n$:

$$\varepsilon(\sigma\circ\sigma')=\varepsilon(\sigma)\varepsilon(\sigma')$$

La signature d'une transposition est -1 ; la signature d'un p-cycle est $(-1)^{p-1}$.

Exercice 2 : Savoir-faire : les étudiants doivent savoir décomposer une permutation.
On reprend l'exemple de $\sigma=\begin{pmatrix}1&2&3&4&5&6\\3&2&1&6&4&5\end{pmatrix}$.

1. Donner la décomposition de σ en produit de cycles à supports disjoints.
2. Donner une décomposition de σ en produit de transpositions.
3. Donner la signature de σ.

2 Programme de MP

Voir votre cours écrit en classe.