Groupes finis. Exemples et applications.

Motivation : Les groupes sont des structures algébriques élémentaires qui apparaissent dans de très nombreux champs en mathématiques. On retrouve en particulier des groupes finis en théorie de Galois et en géométrie (par exemple les groupes d'isométries d'un polyèdre).

I] Définitions et propriétés clefs

On suppose connues les notions de groupe, groupe abélien, de sous-groupe et de morphisme de groupes.
Le théorème suivant permet, au moins d'un point de vue théorique de ramener l'étude des groupes finis à l'étude des groupes symétriques :

Théorème de Cayley :
Si G est fini de cardinal n, G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Corollaire : Pour tout corps k, il existe un plongement de G dans $GL_n(k)$.

exemple : $\mathfrak{S}_n \hookrightarrow GL_n(\mathbb{F}_2)$.
$\sigma \longrightarrow P_\sigma := (\delta_{i,\sigma(j)})_{1\leq i,j\leq n}$

définition : L'ordre d'un élément $g \in G$ est le plus petit $n \geq 1$ tel que $g^n = 1$. Le PPCM des ordres des éléments du groupe G s'appelle l'exposant du groupe.

remarque : Il ne faut pas confondre l'exposant d'un groupe avec son ordre. Par exemple $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ est d'ordre infini mais d'exposant fini égal à 2. Cependant, tout groupe fini est d'exposant fini.

On a une réciproque dans le cas des sous-groupes de $GL_n(\mathbb{C})$.

Théorème de Burnside : Tout sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini est fini.

Si H est un sous-groupe de G, on peut définir l'ensemble G/H des classes à gauche de G relativement à H qui sont les sous-ensembles $aH = \{g \in G \mid g = ah,\ h \in H\}$ lorsque a parcourt G. Le cardinal de G/H est appelé l'indice de H dans G.

Théorème de Lagrange : Avec les notations précédentes, $|G| = |H| \times |G/H|$. En particulier l'ordre d'un élément $g \in G$ divise l'ordre de G.

exemples :
- Tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ sont d'ordre p (sauf le neutre qui est d'ordre 1).
- $\mathbb{F}_q^*$ admet un élément d'ordre $q-1$.
- Si G est un sous-groupe fini de $GL_2(\mathbb{Z})$, alors $|G|$ est un diviseur strict de 48.

proposition : Si G contient un élément d'ordre $|G|$, alors G est cyclique.

exemples : $\mathbb{F}_q^\times$, $\mathbb{Z}/n\mathbb{Z}$, U_n.

définition : On dit que H est distingué dans G s'il est invariant par automorphisme intérieur i.e. si on a : $\forall a \in G, \forall h \in H, aha^{-1} \in H$. On note alors $H \triangleleft G$.

Application : Si on a $H \triangleleft G$, le quotient G/H est naturellement muni d'une structure de groupe et on a un morphisme surjectif $p : G \longrightarrow G/H$ de noyau H.

exemple : pour $n \geq 5$, les sous groupes distingués de $\mathfrak{S}_n$ sont $\{1\}$, A_n et $\mathfrak{S}_n$.

- si G est abélien, tout sous-groupe de G est distingué dans G.
- le groupe dérivé $D(G) = \langle xyx^{-1}y^{-1} ; x, y \in G \rangle$ et le centre $Z(G) = \{a \in G \mid \forall g \in G, ag = ga\}$ sont toujours distingués dans G. Ainsi $Z(\mathbb{H}_8) = \{\pm 1\}$ est distingué dans le groupe des quaternions $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

De même, $D(\mathfrak{S}_3) = \{1, \sigma, \sigma^2\}$ est distingué dans $\mathfrak{S}_3$.

définition : Un groupe $G \neq \{1\}$ est dit **simple** si ses seuls sous-groupes distingués sont $\{1\}$ et G.

exemples :
- $\mathbb{Z}/p\mathbb{Z}$ est simple pour p premier
- A_n est simple pour $n \geq 5$
- $PSL_n(\mathbb{F}_q)$ est simple pour $q \geq 3$, $n \geq 1$.
- les groupes Monstre et Bébé Monstre sont simples.

II] Opération d'un groupe sur un ensemble

définition : Soit G un groupe, X un ensemble, on dit que G opère sur X s'il existe une application : $G \times X \longrightarrow X$, $(g, x) \longrightarrow g.x$ qui vérifient :
1) $\forall g, g' \in G, \forall x \in X, g.(g'.x) = (gg').x$
2) $\forall x \in X, 1.x = x$.

exemples :
- G agit sur lui-même par conjugaison.
- $GL_n(\mathbb{F}_q)$ opère sur $\mathbb{F}_q^n$

définition : $\forall x \in X$, on pose $H_x := \{g \in G \mid g.x = x\}$ le stabilisateur de x dans G.

$\forall x \in X$, on pose $\omega(x) = \{g.x, g \in G\}$ l'orbite de x sous G.

proposition : $\forall x \in X$, $|\omega(x)| = |G|/|H_x|$.

formule des classes : $|X| = \sum_{i=1}^{k} [G : H_{x_i}]$ où les H_{x_i} sont les G-orbites qui partitionnent G.

Applications : i) Toute permutation $\sigma \in \mathfrak{S}_n$ se décompose en un produit commutatif de cycles à supports disjoints.

ii) **lemme de Cauchy :** Si p est premier et divise l'ordre de G, alors G admet un élément d'ordre p.

Cette théorie des opérations de groupe est un outil très puissant qui va vous permettre de classifier les groupes, de faire du dénombrement et d'étudier les groupes en situation géométrique.

III] Classification des groupes finis

En fixe $n \in \mathbb{N}^*$, on souhaite connaître tous les groupes d'ordre n à isomorphisme près. Les opérations de groupe sont un premier outil, nous allons en définir deux autres :

Théorèmes de Sylow :

Soit G un groupe de cardinal $|G| = p^k m$ avec $p \nmid m$.
i) G contient au moins un sous-groupe de cardinal p^k (appelé p-sous-groupe de Sylow).
ii) Si H est un p-groupe de G, alors il existe un p-Sylow S, avec $H \subset S$.
iii) Les p-Sylows sont tous conjugués et leur nombre k divise m.
iv) On a $k \equiv 1 [p]$ et donc $k \mid m$.

exemple : L'ensemble des matrices unitriangulaires supérieures est un p-sous-groupe de Sylow de $GL_n(\mathbb{F}_p)$.

Corollaire : Si S est un p-Sylow de G, on a :
$S \lhd G \Leftrightarrow S$ est l'unique p-Sylow de $G \Leftrightarrow k = 1$.

Application : Un groupe d'ordre 63 ou 255 n'est pas simple.

• produit semi-direct : Soit G un groupe, N un sous-groupe distingué de G, on a donc une suite exacte :
$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$$
On souhaiterait exprimer G sous la forme "$G = N \times G/N$".

définition : Soient N, H deux groupes de G, $\varphi : H \to \mathrm{Aut}\, N$, on définit sur l'ensemble produit $N \times H$ une loi par : $(n, h)(n', h') := (n\,\varphi(h)(n'), hh')$, le groupe ainsi construit est appelé produit semi-direct de N par H et noté $N \rtimes H$.
On a alors une suite exacte : $1 \to N \xrightarrow{i} N \rtimes H \xrightarrow{p} H \to 1$
où s est une section de p.
Et la réciproque est vraie.

exemples : le groupe diédral $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$
le groupe symétrique $\mathfrak{S}_n \simeq A_n \rtimes \mathbb{Z}/2\mathbb{Z}$

Application : Si l'on connaît tous les groupes simples dans un groupe G, on va chercher à écrire G comme un produit de ces groupes ; on parle de démontage de groupes. La principale difficulté réside alors dans la détermination des groupes d'automorphismes de ces groupes simples.

exemples • les groupes d'ordre 12 sont :
$\mathbb{Z}/12\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$; $V_4 \rtimes \mathbb{Z}/3\mathbb{Z}$; $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$; $\mathbb{Z}/3\mathbb{Z} \rtimes V_4$
• les groupes d'ordre 8 sont :
$\mathbb{Z}/8\mathbb{Z}$; $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z})^3$; D_4 ; H_8

Théorème : Structure des groupes abéliens finis
Soit A un groupe abélien, alors $\exists\, r \geq 0$ et des entiers $d_1, \dots, d_r \geq 2$ avec $d_1 | d_2 | \dots | d_r$ tels que : $A \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$.

remarque : Il existe des groupes non simples et qui ne sont pas décomposables en produit de groupes simples, par exemple H_8.

III. Les groupes finis en situation géométrique

Théorème de Maschke : Si G est un groupe fini, $\exists\, n \geq 1$ et φ un produit scalaire sur $\mathbb{R}^n$ tel que $G \hookrightarrow O_n(\varphi)$.

conséquence : On a un théorème de semi-simplicité des représentations linéaires des groupes finis en caractéristique 0.

Les groupes finis sont naturellement présents en géométrie, par exemple comme groupes de transformations laissant une structure géométrique invariante.

Théorème : $SO_3(\mathbb{R})$ admet exactement 5 types de sous-groupes finis, les 3 groupes A_4, $\mathfrak{S}_4$ et A_5, et les deux séries infinies $\mathbb{Z}/n\mathbb{Z}$ et D_n pour $n \geq 1$.

autres exemples • les sous-groupes finis de $SL_2(\mathbb{Z})$ sont des groupes cycliques.
• le groupe des points rationnels d'une cubique est naturellement muni d'une structure de groupe abélien.

Et à l'inverse, il peut être utile de mettre un groupe en situation géométrique pour mieux comprendre sa structure.

exemples : • $\mathfrak{S}_n$ peut se réaliser comme un groupe de réflexion dans $\mathbb{R}^n$
• le groupe diédral D_n se réalise naturellement comme le groupe des isométries du plan euclidien qui conservent un polygone régulier à n côtés.

Enfin, les groupes de réflexion apparaissent naturellement en théorie de Lie, en théorie des représentations des groupes algébriques, dans l'étude des réseaux, ...

Réf :
- Perrin
- Ortiz
- Francinou (Gaux x ENS + Agreg)
- Lang, Algebre
- Hneimmé Testard