⊕ Isométries
⊕ + de représentations

104 - GROUPES FINIS. EXEMPLES ET APPLICATIONS

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

1 - GÉNÉRALITÉS

1.1 - Définitions [CALAIS, ch 1]

→ Un groupe G est dit fini s'il n'a qu'un nombre fini d'éléments. Dans ce cas, le cardinal de G s'appelle l'ordre du groupe ; il est noté $|G|$.

ex : $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, .., \overline{n-1}\}$ est fini d'ordre n.
S_n est un groupe fini d'ordre $n!$.

→ Soit x un élément de G. Si le sous-groupe de G engendré par x est de cardinal infini, on dit que x est d'ordre infini dans G. Si le sous-groupe de G engendré par x est fini, on dit que x est d'ordre fini dans G et le cardinal du sous groupe $\langle x \rangle$ s'appelle l'ordre de x dans G, noté $o(x)$.

ex : Dans tout groupe G, l'élément neutre est le seul élément d'ordre 1.
Dans S_3, les transpositions sont d'ordre 2, les 3-cycles d'ordre 3.

1.2 - Théorème de Lagrange et indice [COMBES, ch 1]

DEF Le cardinal commun aux ensembles G/H et $G\backslash H$ s'appelle l'indice de H dans G. On le note $[G:H]$. Si $H = \{e\}$, alors $[G:H] = |G|$ est l'ordre de G.

THM DE LAGRANGE. Soit G un groupe fini, K et H deux sous-groupes de G tels que $K \subset H$. On a : $[G:K] = [G:H][H:K]$. En particulier, pour tout sous-groupe H de G, on a : $|G| = [G:H].|H|$.

COR G fini. L'ordre $o(a)$ de tout élément a de G divise $|G|$.

APPLICATIONS
→ Soit $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$. Alors $U_n \cap U_k = U_d$ où $d = pgcd(k,n)$
→ Dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$, $pgcd(X^k - 1, X^{n-1} - 1) = X^d - 1$ où $d = pgcd(k,n)$

2. ACTIONS DE GROUPE ET CONSÉQUENCES [COMBES, ch 2]

DEF On appelle action à gauche du groupe G sur un ensemble X, un homomorphisme t de G dans le groupe S_X des bijections de X sur X, càd une application t de G dans S_X telle que $t(gg') = t(g) \circ t(g')$ pour tout $g \in G$ et pour tout $g' \in G$.

- On appelle orbite de x sous l'action de G la classe d'équivalence $\{g.x \mid g \in G\}$ de $x \in X$

- Le sous-groupe G_x de G, formé des éléments de G qui laissent fixe $x \in X$, s'appelle le stabilisateur de x

PROPOSITION. G groupe fini, on considère une action de G sur un ensemble fini X, les orbites $O_1, .., O_k$ pour cette action. Pour $i = 1, .., k$, soit $x_i \in O_i$. Pour tout G notons $fix(g) = \{x \in X \mid g.x = x\}$ l'ens des éléments fixes par g.
(1) $card(E) = \sum_{i=1}^{k} card(O_i)$ et $card(O_i) = \frac{|G|}{|G_{x_i}|}$ (éq. des classes)
(2) Le nb d'orbites est $k = \frac{1}{|G|} \sum_{g \in G} card(Fix(g))$ (Formule de Burnside)

APPLICATIONS
→ Soit G un groupe d'ordre $|G| = p^m$, avec p premier, agissant sur un ens. fini X. Le nb de points fixes de X fixés pour l'action est congru à $card(X)$ mod p. ex : $\mathbb{Z}/p\mathbb{Z}$
→ Combien de colliers différents peut-on faire avec un fil circulaire, 4 perles bleues, 3 perles blanches et 2 perles oranges ?
→ THM DE CAUCHY : G groupe fini d'ordre n et p facteur premier de n. Alors il existe dans G des éléments d'ordre p.
→ COR : G fini, $p \in \mathbb{N}$ premier. Pour que l'ordre de G soit une puissance de p, il faut et il suffit que l'ordre de tout élément de G soit une puissance de p.
→ THM DE CAYLEY : Tout groupe G est isomorphe à un sous-groupe de $(S(G), \circ)$ [NOURDIN]
→ G fini de cardinal n. Si p est le plus petit nombre premier divisant n et si H est un sous-groupe d'indice p, alors H est distingué dans G.
→ Soit p premier. Le centre d'un p-groupe non trivial est non trivial

3. PROPRIÉTÉS DES GROUPES FINIS

3.1 - Théorème d'isomorphisme [COMBES, ch 1]

THM. Soit $H \lhd G$ et j l'homomorphisme canonique de G sur G/H. Soit $f : G \to G'$ un homomorphisme de groupes. Si $H \subset Ker(f)$, il existe un unique homomorphisme $\bar{f} : G/H \to G'$ tel que $\bar{f} \circ j = f$. Le noyau de $\bar{f}$ est $j(Ker(f))$ et l'image de $\bar{f}$ est égale à celle de f. De plus, les groupes $G/Ker(f)$ et $f(G)$ sont isomorphes.

APPLICATIONS
→ Les sous-groupes $\mathbb{R}/\mathbb{Z}$ et $U = \{z \in \mathbb{C} \mid |z| = 1\}$ sont isomorphes
→ Soient q une puissance non triviale d'un nb premier, K un corps à q éléments et $x \in K^*$. Alors x est un carré $\Leftrightarrow x^{\frac{q-1}{2}} = 1$. [NOURDIN]

3.2. Théorème de Sylow [COMBES, ch 5]

THM. Soit G groupe fini, p facteur premier de $n = |G|$ et soit $n = p^k p_2^{k_2} \dots p_s^{k_s} = p^k q$ la décomposition en facteurs premiers de n.

(1) Il existe dans G un p-sous-groupe de Sylow
(2) Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow de G.
(3) Les p-sous-groupes de Sylow de G sont conjugués
(4) Le nb n_p de p-sous-groupes de Sylow de G divise q et $n_p \equiv 1 \pmod p$.

APPLICATIONS

→ Structure d'un groupe d'ordre 153. DVPT
→ A_n est simple pour $n \geq 5$
→ Dans S_5, il n'y a aucun sous-groupe d'ordre 15.
→ Structure des groupes d'ordre 8.
→ Un groupe d'ordre 56 n'est pas simple.
→ À isomorphisme près, il existe 5 groupes d'ordre 12 DVPT
→ Si G est d'ordre pq, où p et q sont premiers, alors G n'est pas simple. Si de plus $p \not\equiv 1 \pmod q$ et $q \not\equiv 1 \pmod p$, alors tout groupe d'ordre pq est cyclique. [CALAIS, ch 6]
→ Soit p premier impair. Si G est d'ordre $2p$, alors $G \simeq C_{2p}$ (Groupe cyclique) ou $G \simeq D_p$ (Groupe diédral)

3.3. Autres propriétés [COMBES, ch 3]

→ G est d'ordre premier ssi il est cyclique et simple
→ Soit G fini s'il existe H sous-groupe de $Z(G)$ tel que G/H soit cyclique, alors G est abélien.
→ Si G est d'ordre p^2, avec p premier, alors G est abélien

4. GROUPES ABÉLIENS FINIS [COMBES, ch 3]

4.1. Groupes cycliques.

DEF. G est cyclique s'il est engendré par un élément et s'il est fini.
- Pour $n \geq 2$, on note $\varphi(n)$ le cardinal de l'ensemble des entiers k tels que $0 \leq k \leq n-1$ et $k \wedge n = 1$. On convient que $\varphi(1) = 1$. La fonction φ de $\mathbb{N}_*$ dans $\mathbb{N}_*$ ainsi définie est appelée fonction d'Euler

LEMME. G cyclique d'ordre n et a générateur de G. L'homomorphisme $k \mapsto a^k$ de $\mathbb{Z}$ sur G se factorise et définit un isomorphisme $\alpha_a : \bar{k} \mapsto a^k$, où $0 \leq k < n$, du groupe $\mathbb{Z}/n\mathbb{Z}$ sur G.

COR. Deux groupes cycliques G et G' sont isomorphes ssi ils ont le même ordre.
- G cyclique d'ordre n. Le groupe $\mathrm{Aut}(G)$ est d'ordre $\varphi(n)$ et ses éléments sont les applications $\alpha_k : x \mapsto x^k$ où $k \in [0, n-1]$ est premier avec n

PROP. G cyclique d'ordre n, a générateur de G. Tout sous-groupe de G est cyclique et pour tout diviseur d de n, il existe un unique sous-groupe H_d de G d'ordre d. En posant $s = n/d$, ce sous-groupe est caractérisé par :

$$H_d = \{x \in G \mid x^d = e\} = \{x \in G \mid \exists y \in G \ y^s = x\} = \langle a^s \rangle.$$

APPLICATIONS

→ détermination des sous-groupes de $\mathbb{Z}/20\mathbb{Z}$
→ détermination des éléments d'ordre 6 dans U_{30}.

ex : Tout groupe fini d'ordre un nb premier est cyclique [NOURDIN]
Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est fini ☺
Les sous-groupes finis de $SO_2(\mathbb{R})$ sont cycliques

4.2. Décomposition d'un groupe abélien fini.

PROPOSITION. Soit G groupe abélien fini d'ordre $n \geq 2$. Il existe des entiers $q_1 \geq 2$, q_2 multiple de $q_1, \dots, q_k$ multiple de q_{k-1}, uniques, tels que G soit isomorphe à $(\mathbb{Z}/q_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/q_k\mathbb{Z})$

DEF. Cette suite $q_1, \dots, q_k$ qui caractérise G à isomorphisme près, est appelée la suite des invariants de G

COR. Soit G abélien fini. Il existe un élément a de G dont l'ordre est le ppcm des ordres des éléments de G

APPLICATIONS

→ décomposition canonique de $G = (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})$

5. AUTRES GROUPES FINIS

5.1. Le groupe symétrique [NOURDIN]

DEF. Soit E un ensemble fini. Une bijection de E sur lui-même est appelée une permutation de E. L'ensemble des permutations de E est un groupe, appelé groupe symétrique de E noté S_E

DEF Si $g \in S_E$ s'écrit $\tau_1 \dots \tau_r$ où τ_i sont des transpositions, on pose $\varepsilon(g) = (-1)^r$. On l'appelle la signature de g

PROP l'application ε est un homomorphisme non trivial entre les groupes S_E et $\{\pm 1\}$. C'est la seule à avoir cette propriété.

PROP Le sous-groupe A_E de S_E défini par $A_E = \ker(\varepsilon)$ est le seul sous-groupe d'indice 2 de S_E.

APPLICATION : EN GÉOMÉTRIE [COMBES, ch 8]

→ Soit G sous-groupe fini d'ordre $n \geq 2$ du groupe I^+ des déplacements de l'espace affine euclidien $\mathcal{E}$. Alors G est isomorphe à U_n ou à $D_{n/2}$ (n pair) ou bien à l'un des trois groupes des déplacements qui conservent l'un des cinq polyèdres réguliers, cad isomorphe à A_4, S_4 ou A_5.

5.2. Le groupe diédral [CALAIS, ch 3]

Pour $n \geq 2$, on note P_n un polygone régulier à n sommets dans le plan $\mathcal{P}$. Soit D_n l'ens. des isométries du plan qui conservent P_n.
D_n est un sous-groupe de $I(2)$, le groupe des isométries du plan

DEF Pour tout $n \geq 2$, le groupe D_n est appelé groupe diédral d'ordre $2n$.

PROP Pour tout $n \geq 2$, le groupe diédral D_n est fini, d'ordre $2n$
- D_n est non abélien pour $n \geq 3$.
- Tout groupe engendré par 2 éléments a et b tels que $o(a) = n$ $(n \geq 2)$, $o(b) = 2$ et $o(ab) = 2$ est isomorphe au groupe diédral D_n.

5.3. Le groupe des quaternions [L3]

$\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ est le groupe des quaternions, où la multiplication est définie par : $i^2 = j^2 = k^2 = -1$; $ij = -ji = k$; $jk = -kj = i$, $ki = -ik = j$

PROP $Z(\mathbb{H}_8) = \{\pm 1\}$
- Les sous-groupes de $\mathbb{H}_8$ sont $H_1 = \{1\}$, $H_2 = \{\pm 1\}$, $H_3 = \{\pm 1, \pm i\}$, $H_4 = \{\pm 1, \pm j\}$, $H_5 = \{\pm 1, \pm k\}$ et $H_6 = \mathbb{H}_8$.
H_1, H_2 et H_6 sont distingués

6. REPRÉSENTATIONS LINÉAIRES DES GROUPES FINIS [RAUCK]

DEF - On appelle représentation linéaire d'un groupe G la donnée d'un espace vectoriel V et d'un morphisme de groupes
$\rho : G \longrightarrow GL(V)$
- On appelle caractère de la représentation $\rho : G \to GL(V)$ la fonction $\chi_\rho : G \to \mathbb{C}$ définie par $\chi_\rho(g) = \text{Trace}(\rho(g))$, $g \in G$

PROP Les caractères du groupe symétrique sont à valeurs dans les entiers relatifs
- Tout caractère irréductible d'un groupe fini, de degré strictement supérieur à 1, s'annule au moins une fois.

ex - Table des caractères de S_4 [SERRE]

	1	(ab)	(ab)(cd)	(abc)	(abcd)
χ_0	1	1	1	1	1
ε	1	-1	1	1	-1
θ	2	0	2	-1	0
ψ	3	1	-1	0	-1
$\varepsilon\psi$	3	-1	-1	0	1

Références -
[L3] Mathématiques L3 algèbre [Escofier]
[CALAIS] Théorie des groupes
[COMBES] Algèbre et Géométrie
[NOUROW] Épreuve orale
[RAUCK] les groupes finis et leurs représentations
[SERRE] Représentations linéaires des groupes finis