104 Groupes finis. Exemples et applications

I- Définitions et premières propriétés

1) Groupe fini et ordre

Def 1 : L'ordre d'un groupe G, noté $|G|$, est le cardinal de G. On dit que G est un groupe fini si $|G|$ est fini. [ULM] p2

Ex 2 : $\mathbb{Z}/n\mathbb{Z}$ est un groupe fini de cardinal n [ULM] p4

Def 3 : On appelle ordre d'un élément $g \in G$, l'ordre du sous-groupe $\langle g \rangle$ engendré par g. [ULM] p6

Ex 4 : $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL(2,2)$ est d'ordre 2 [ULM] p7

Def 5 : On appelle exposant de G, le ppcm des ordres des éléments de G si celui-ci est défini. [FGN] p171

Ex 6 : Un groupe fini d'exposant 2 est abélien. [FGN] p172

Thm 7 : (Burnside) Tout sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini est fini. (DEV) [FGN] p171

C-ex 8 : $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ est d'exposant fini égal à 2 mais est infini. [ULM] p24

2) Théorème de Lagrange

Def 9 : Soit G un groupe, H un sous-groupe de G. On appelle indice de H dans G, et on note $(G:H)$, le cardinal de l'ensemble quotient G/H [ULM] p25

Ex 10 : $(\mathbb{Z} : 2\mathbb{Z}) = 2$ [ULM] p25

Thm 11 : Soit H sous-groupe de G alors $|G| = |H|\,(G:H)$ [ULM] p25

Thm 12 : (Lagrange) : Soit G un groupe fini et $H \leq G$ alors l'ordre de H divise l'ordre de G. En particulier l'ordre d'un élément de G divise toujours l'ordre de G. [ULM] p25

Appli 13 : K, M deux sous-groupes de G d'ordres k et m. Si $k \wedge m = 1$ alors $K \cap M = \{e\}$ [GOU] p22

3) Théorème de factorisation de morphismes

Prop 14 : Soit G un groupe et $H \trianglelefteq G$. Soit j le morphisme canonique de G sur G/H. Soit $f : G \to G'$ un morphisme de groupes. Si $H \subset \ker(f)$, il existe un unique morphisme $\bar{f} : G/H \to G'$ tel que $\bar{f} \circ j = f$. De plus $\ker(\bar{f}) = j(\ker(f))$ et $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$. [GOU] p24

Coro 15 : Soit G, G' deux groupes, $f : G \to G'$ un morphisme de groupes. Alors $G/\ker(f)$ et $f(G)$ sont isomorphes. Si G et G' sont finis, l'ordre de $f(G)$ divise $|G|$ et $|G'|$. [GOU] p24

Ex 16 : $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{U}_n$ [ULM] p27-28

4) Action de groupe

Def 17 : Une action de G sur X est une application $\begin{array}{ccc} G \times X & \to & X \\ (g,x) & \mapsto & g.x \end{array}$ où $g.(h.x) = (gh).x$, $\forall g,h \in G, \forall x \in X$ et $e.x = x$, $\forall x \in X$. À une action d'un groupe G sur un ensemble X correspond le morphisme $\begin{array}{ccc} G & \to & \mathcal{S}(X) \\ g & \mapsto & \sigma_g \end{array}$ où $\sigma_g(x) = g.x$ [ULM] p29

Def 18 : L'orbite de x sous G est $G.x = \{g.x \mid g \in G\} \subset X$. Le stabilisateur de x dans G est $G_x = \{g \in G \mid g.x = x\} \subset G$ [ULM] p61

Rmq 19 : $|G| = |G_x|\,|G.x|$ [ULM] p61

Coro 20 : G un groupe fini, $G \curvearrowright X$. Si $X = \bigsqcup_{i=1}^{r} X_i$ (partition de X en orbites sous l'action de G) et si $x_i \in X_i$ alors

$$|X| = \sum_{i=1}^{r} |X_i| = \sum_{i=1}^{r} (G : G_{x_i}) = \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}$$ (Formule des classes) [ULM] p68

Coro 21 (Formule de Burnside) : Soit $g \in G$, on note $X^g = \{x \in X \mid g.x = x\}$. Le nombre r des orbites de X sous l'action de G est

$$r = \frac{1}{|G|} \sum_{g \in G} |X^g|$$ [ULM] p68

Prop 22 : Soit p nombre premier, G un p-groupe et $G \curvearrowright X$ avec $|X|$ fini. Alors $|X^G| \equiv |X| \ [p]$ [ULM] p65

Appli 23 : Théorème de Cauchy : Soit G un groupe fini et p un nombre premier tel que $p \mid |G|$ alors il existe dans G au moins un élément d'ordre p. [ULM] p65

[Con] p45

Coro 24 : Soit G un groupe fini et p un nombre premier.
$|G|$ est une puissance de p ssi l'ordre de tout élément de G est une puissance de p.

[ULM] p12

Ex 25 Soit G un groupe fini non trivial et p le plus petit nombre premier divisant $|G|$ alors tout sous-groupe H de G d'indice p est distingué.

II - Cas des groupes finis abéliens

1) Groupes cycliques

[Con] p59

Def 26 : On dit qu'un groupe G est cyclique lorsqu'il est monogène et fini. Tout élément a de G tel que $\langle a \rangle = G$ est appelé un générateur de G.

[Con] p59

Ex 27 : $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n et engendré par $\overline{1}$
U_n est cyclique d'ordre n et engendré par $e^{\frac{2i\pi}{n}}$

[Con] p59

Prop 28 : Soit G un groupe cyclique d'ordre n et a un générateur de G alors pour $k \in \mathbb{Z}$, l'ordre de a^k est $\frac{n}{n \wedge k}$.
a^k est un générateur de G ssi $n \wedge k = 1$.
Il existe donc $\varphi(n)$ générateurs distincts dans G.

[Con] p60

Ex 29 : Les générateurs de $\mathbb{Z}/12\mathbb{Z}$ sont $\overline{1}, \overline{5}, \overline{7}, \overline{11}$
Les générateurs de U_{18} sont $\zeta, \zeta^5, \zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{17}$ avec $\zeta = e^{\frac{2i\pi}{18}}$

[Con] p61

Coro 30 : Deux groupes cycliques G et G' sont isomorphes ssi ils ont le même ordre

[Con] p61

Coro 31 : Soit G cyclique d'ordre n. Le groupe $Aut(G)$ est d'ordre $\varphi(n)$ et ses éléments sont les applications $\alpha_k : x \mapsto x^k$, $k \in [\![0, n-1]\!]$, $k \wedge n = 1$

[Con] p62

Prop 32 : Soit G cyclique d'ordre n, a un 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.

[Con] p62

Ex 33 : Sous-groupes de $\mathbb{Z}/20\mathbb{Z}$
· Eléments d'ordre 6 dans U_{30}

[Con] p64

Def 34 : G est simple si $\{e\}$ et G sont les seuls sous-groupes distingués de G

[Con] p64

Prop 35 : G est d'ordre premier ssi G est cyclique et simple.

[Con] p65

Coro 36 : Si G est d'ordre p^2 alors G est abélien

[ULM] p64

Coro 37 : Un groupe cyclique G d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

[Con] p63

Prop 38 : G_1 et G_2 sont cycliques d'ordres premiers entre eux ssi $G_1 \times G_2$ est cyclique. Dans ce cas, (a, b) est un générateur de $G_1 \times G_2$ ssi a et b sont des générateurs de G_1 et de G_2

2) Décomposition en facteurs invariants

[Con] p66

Prop 39 : Soit G un groupe abélien fini d'ordre $n \geq 2$. Il existe des entiers $q_1, q_2, \dots, q_k$ tels que $q_1 \geq 2$ et $q_1 | q_2 | q_3 \dots | q_k$ uniques tels que G soit isomorphe à $\mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_k\mathbb{Z}$

[Con] p67

Def 40 : Cette suite $q_1, \dots, q_k$ est appelée la suite des invariants de G

[Con] p67

Coro 41 : Soit G un groupe abélien d'ordre p^m. Il existe une unique suite $r_1 \leq \dots \leq r_k$ dans $\mathbb{N}^*$ telle que $G \simeq (\mathbb{Z}/p^{r_1}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p^{r_k}\mathbb{Z})$

[Con] p67

Coro 42 : Soit G un groupe abélien et $|G| = n = p_1^{k_1} \dots p_r^{k_r}$. Pour tout diviseur d de l'ordre n de G, il existe un sous-groupe de G d'ordre d.

[Con] p68

Ex 43 : Décomposition de $G = (\mathbb{Z}/60\mathbb{Z}) \times (\mathbb{Z}/72\mathbb{Z})$ en $(\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/360\mathbb{Z})$
· Structure d'un groupe abélien d'ordre 600

III - Groupes finis non-abéliens

1) Théorème de Sylow, un outil pour l'étude

[ULM] p85

Def 44 : Soit p un nombre premier et G un groupe fini. Un p-sous-groupe de G qui est maximal par rapport à l'inclusion des p-sous-groupes de G est appelé un p-Sylow de G.

[ULM] p87

Thm 45 : Soit p un nombre premier et G un groupe fini, $|G| = p^e m$ avec $p \nmid m$ alors
· Les p-Sylows de G sont les sous-groupes d'ordre p^e de G
· Il existe un p-Sylow de G
· Les p-Sylows sont conjugués et leur nombre n_p divise $|G|$
· $n_p | m$ et $n_p \equiv 1 [p]$

DEV

[ULM] p86 [ULM] p88 [Cam] p93 [ULM] p27 [ULM] p31 [ULM] p43 [ULM] p43 [ULM] p49 [ULM] p49 [ULM] p52 [ULM] p50 [ULM] p52 [ULM] p53 [ULM] p8

Prop 46 : Un p-Sylow de G est distingué ssi $n_p = 1$

Appli 47 : Un groupe d'ordre 15 est cyclique, isomorphe à $\mathbb{Z}/15\mathbb{Z}$

Appli 48 : Structure d'un groupe fini d'ordre 153

2) Groupe symétrique

Def 49 Soit X un ensemble. Alors l'ensemble $\mathfrak{S}(X)$ des bijections de X dans X, muni de la composition des applications est un groupe appelé groupe symétrique de X d'ordre $|X|!$

Thm 50 : Tout groupe fini G d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$. (Cayley)

Def 51 Soient $1 \leq p \in \mathbb{N}$ et $i_1, \dots, i_p$ des éléments de $[\![1, n]\!]$. La permutation $\gamma \in \mathfrak{S}_n$ définie par $\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \dots, i_p\} \\ i_{k+1} & \text{si } j = i_k, k < p \\ i_1 & \text{si } j = i_p \end{cases}$ et notée $(i_1, \dots, i_p)$ est appelée cycle de longueur p. Un cycle de longueur deux est appelé une transposition.

Thm 52 : Tout $\sigma \in \mathfrak{S}_n$ s'écrit comme produit de cycles de longueur ≥ 2 à supports disjoints avec unicité de la décomposition à ordre près.

Def 53 Soit $\sigma \in \mathfrak{S}_n$. On appelle signature de $\sigma \in \mathfrak{S}_n$ et on note $\varepsilon(\sigma)$ le nombre $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$

Prop 54 : $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est un morphisme de groupe et si $\#(\sigma)$ désigne un nombre de transpositions qui apparait dans une décomposition de $\sigma \in \mathfrak{S}_n$ alors $\varepsilon(\sigma) = (-1)^{\#(\sigma)}$

Prop 55 : $\mathfrak{S}_n$ est engendré par $\{(1, i) \text{ avec } i \in [\![2, n]\!]\}$.

Def 56 : Le noyau de $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est un sous-groupe distingué de $\mathfrak{S}_n$, noté A_n et appelé groupe alterné.

Prop 57 : A_n est engendré par les cycles $(1, i, j)$ avec i, j distincts dans $[\![2, n]\!]$. En particulier, A_n est engendré par les 3-cycles de $\mathfrak{S}_n$.

Prop 58 : A_n est simple pour $n \geq 5$ (DEV)

3) Groupe diédral

Def 59 : Soit $n \in \mathbb{N}$, $n \geq 3$. Dans le plan complexe $\mathbb{C}$ identifié à $\mathbb{R}^2$ on considère P_n le polygône régulier à n sommets formés par les racines $n$ièmes de l'unité $\omega_k = e^{\frac{2ik\pi}{n}}$ $(k \in [\![0, n-1]\!])$. Le groupe diédral D_n est le sous-groupe des isométries du plan affine qui laisse P_n invariant.

Prop 60 : Pour un entier $n \geq 3$, le groupe diédral D_n est d'ordre $2n$ et il est engendré par la symétrie axiale s et la rotation r d'angle $\theta = \frac{2\pi}{n}$ définies par $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $r = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

Ces générateurs satisfont aux relations $r^n = e$, $s^2 = e$, $srs = r^{-1}$, et $D_n = \{e, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\}$. Le sous-groupe $\langle r \rangle \subset D_n$ est un sous-groupe distingué de D_n d'ordre n.

IV - Applications

1) Géométrie

[ULM] p9 [ALE] p59 [ALE] p63 [ALE] p64

Def 61 : E un $\mathbb{R}$-espace affine euclidien de dimension 3. X une partie non vide de E : $\mathrm{Isom}(X) := \{f \in \mathcal{O}(E) \mid f(X) = X\}$ et $\mathrm{Isom}^+(X) = \{f \in \mathcal{O}^+(E) \mid f(X) = X\} = \{f \in \mathrm{Isom}(X) \mid \det(f) = 1\}$

Prop 62 : Si on note Δ_4 le tétraèdre régulier, $\mathrm{Isom}(\Delta_4) \simeq \mathfrak{S}_4$ et $\mathrm{Isom}^+(\Delta_4) \simeq A_4$ (voir annexe)

Prop 63 : Si on note C_6 le cube en dimension 3, $\mathrm{Isom}(C_6) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{Isom}^+(C_6) \simeq \mathfrak{S}_4$ (voir annexe)

2) Représentations de groupes

[ULM] p144 [ULM] p150 [ULM] p151 [ULM] p159

Def 64 : Soit V un $\mathbb{C}$-ev de dim finie. On appelle représentation linéaire sur $\mathbb{C}$ du groupe G tout morphisme $\rho : G \to GL(V)$. ρ est le morphisme structurel de l'action de G sur V.

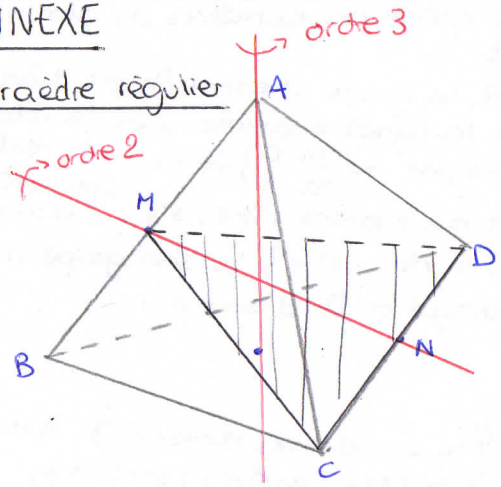
Def 65 Soit $\rho : G \to GL(V)$ une représentation linéaire. Le caractère de ρ est la fonction $\chi : \begin{matrix} G \to \mathbb{C} \\ g \mapsto \mathrm{tr}(\rho(g)) \end{matrix}$. Le degré du caractère $\deg(\chi) = \chi(e)$ est la dimension de V

Appli 66 : Table de $\mathfrak{S}_4$ (voir annexe)

Coro 67 : Un groupe fini G est simple ssi tout caractère irréductible non trivial de G a un noyau trivial : ie $\{g \in G \mid \chi(g) = \chi(e)\} = e$

ANNEXE

Tétraèdre régulier



Cube

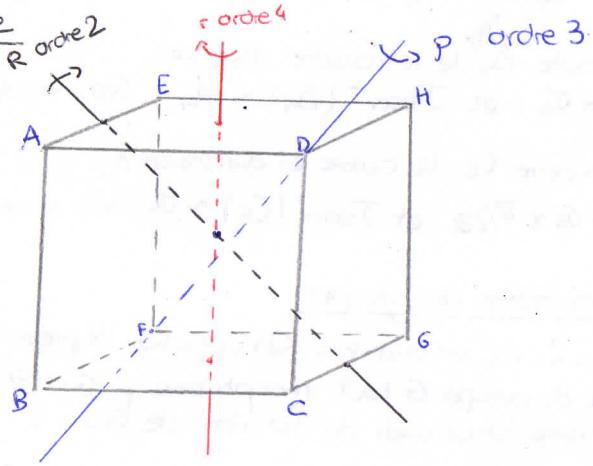


Table de $\mathfrak{S}_4$

	id	(12)(34)	(12)	(123)	(1234)
χ_1	1	1	1	1	1
χ_ε	1	1	-1	1	-1
χ_2	2	2	0	-1	0
χ_3	3	-1	1	0	-1
χ_4	3	-1	-1	0	1

REFERENCES :

- Felix ULMER , "Théorie des groupes"
- Michel ALESSANDRI , "Thèmes de Géométrie", Groupes en situation géométrique
- Français COMBES : "Algèbre et géométrie"
- Francinou, Gianella, Nicolas "Oraux X-ENS Alg 2"