104

Groupes abéliens et non abéliens finis. Exemples et applications.

Cadre : Tous les groupes considérés sont finis. E un ensemble.

I) Outils pour l'étude des groupes

1) Ordre d'un élément d'un groupe fini

<u>def 1</u> : l'ordre d'un élément $g \in G$ est l'élément $O(g) \in \mathbb{N}^*$ défini par $O(g) = \text{card}(\langle g \rangle)$ où $\langle g \rangle$ est le sous-groupe de G engendré par g.

<u>Rq 2</u> : Comme G est fini, $O(g) \in \mathbb{N}^*$ et g est d'ordre fini.

<u>Thm 3</u> : Si $\varphi : G \to G'$ est un isomorphisme de groupes, on a alors $O(\varphi(g)) = O(g)$, pour tout $g \in G$.

<u>Rq 4</u> : Pour $g \in G$, on a $\langle g \rangle = \text{Im}(\varphi_g)$ avec $\varphi_g : \begin{array}{l} \mathbb{Z} \to G \\ k \mapsto g^k \end{array}$

<u>Thm 5</u> : Pour $g \in G$, on a $\text{Ker}(\varphi_g) = O(g)\mathbb{Z}$.

<u>Thm 6</u> (Lagrange) Soient G un groupe fini d'ordre $n \geq 2$ et H un sous-groupe de G. Pour tout $g \in G$, on a :

$\text{card}(gH) = \text{card}(H)$ et $\text{card}(G) = [G : H]\,\text{card}(H)$.

<u>Rq 7</u> : Dans le cas où $H = \langle g \rangle$, on en déduit que $O(g) \mid \text{Card}(G)$

<u>Thm 8</u> : Soient g, h dans G d'ordre fini et $k \in \mathbb{Z}^*$.

(i) $O(g^k) = \dfrac{O(g)}{\text{pgcd}(O(g), k)}$ (et en particulier $O(g^{-1}) = O(g)$)

(ii) Si $gh = hg$ alors hg est d'ordre fini divisant $\text{ppcm}(O(g), O(h))$. Dans le cas où $\langle g \rangle \cap \langle h \rangle = \{1\}$, on a $O(gh) = \text{ppcm}(O(g), O(h))$. Si $O(g) \wedge O(h) = 1$, alors $\langle g \rangle \cap \langle h \rangle = \{1\}$ et $O(gh) = O(g)O(h)$

<u>C-ex 9</u> : Si g et h ne commutent pas (ii) est faux. Dans le groupe symétrique S_3 d'ordre 6, $g = (1\,2)$ est d'ordre 2, $h = (1\,2\,3)$ est d'ordre 3, mais gh ne peut pas être d'ordre 6, sans quoi S_3 serait cyclique. ($gh = (3\,2)$, d'ordre 2)

<u>Thm 10</u> : Si G est un groupe commutatif, $n \geq 2$ un entier, et $g_1, \dots, g_n$ des éléments 2 à 2 distincts de G, d'ordres respectifs $m_1, \dots, m_n$. Alors il existe dans G un élément g_0 d'ordre <u>égal</u> au ppcm de $m_1, \dots, m_n$.

<u>Appli 11</u> : On appelle exposant d'un groupe fini G, l'entier $\max\limits_{g \in G} O(g)$. Dans le cas d'un groupe commutatif on a $\max\limits_{g \in G} O(g) = \text{ppcm}\{O(g) / g \in G\}$

<u>Thm 12</u> (Cauchy) Soit G un groupe commutatif fini d'ordre $n \geq 2$. Pour tout diviseur premier p de n, il existe dans G un élément d'ordre p.

2) Actions de groupes et applications

<u>def 13</u> : On dit que le groupe G opère à gauche sur l'ensemble E, si on a une application : $\begin{array}{l} G \times E \to E \\ (g, x) \mapsto g \cdot x \end{array}$

telle que $\begin{cases} \forall x \in E, \ 1 \cdot x = x \\ \forall (g, g', x) \in G^2 \times E, \ g \cdot (g' \cdot x) = (gg') \cdot x \end{cases}$

<u>Ex 14</u> : G agit sur lui-même par conjugaison. $\begin{array}{l} G \times G \to G \\ (g, h) \mapsto ghg^{-1} \end{array}$

Le morphisme de groupes correspondant de $(G, \cdot)$ dans $(S(G), \circ)$ est noté

$\text{Int}(g) : \begin{array}{l} G \to G \\ h \mapsto ghg^{-1} \end{array}$

Son image est $\text{Int}(G)$ le groupe des automorphismes intérieurs de G

<u>Ex 15</u> : G agit sur tout sous-groupe distingué H par conjugaison :

$\begin{array}{l} G \times H \to H \\ (g, h) \mapsto ghg^{-1} \end{array}$

<u>def 16</u> : Soit G un groupe opérant sur E. Pour tout $x \in E$, $G \cdot x = \{g \cdot x \,/\, g \in G\}$ est un sous-ensemble de E, appelé orbite de x sous l'action de G

<u>def 17</u> : On dit que l'action de G sur E est transitive (resp. simplement transitive) si :

$\forall (x, y) \in E^2, \ \exists g \in G \,/\, g \cdot x = y$

(resp. $\forall (x, y) \in E^2, \ \exists!\, g \in G \,/\, g \cdot x = y$)

<u>Rq 18</u> : Dans le cas d'une action transitive il n'y a qu'une seule orbite.

<u>def 19</u> : On dit que l'action est fidèle si le morphisme de groupes :

$\varphi : \begin{array}{l} G \to S(E) \\ g \mapsto (\varphi(g) : x \mapsto g \cdot x) \end{array}$ est injectif

ie : $(g \in G \text{ et } \forall x \in E, \ g \cdot x = x) \iff (g = 1)$

<u>Thm 20</u> : (Cayley) L'action de G sur lui-même par translation à gauche est fidèle, et G isomorphe à un sous-groupe de $S(G)$.

def 21 : $\forall x \in E$, le sous-groupe $G_x = \{g \in G \,/\, g\cdot x = x\}$ de G est le stabilisateur de x sous l'action de G

Thm 22 : Dans le cas où G est fini, on a $\forall x \in E$.
$\mathrm{Card}(G) = \mathrm{card}(G_x)\,\mathrm{card}(G\cdot x)$

Thm 23 (Equation aux classes) : En notant $G\cdot x_1, \dots, G\cdot x_n$ toutes les orbites, deux à deux distinctes, on a : $\mathrm{Card}(E) = \sum_{i=1}^{n} \mathrm{Card}(G\cdot x_i) = \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|}$

Thm 24 (formule de Burnside) : le nombre d'orbites de l'action de G sur E est $k = \frac{1}{|G|} \sum_{g\in G} |Fix(g)|$ où $Fix(g) = \{x \in E \,/\, g\cdot x = x\}$

Appli 25 : Il y a 3 coloriages du cube à trois faces blanches, deux faces rouges et une face noire.

def 26 : on note $E^G = \{x \in E \,/\, G\cdot x = \{x\}\}$. C'est l'ensemble des éléments de E dont l'orbite est réduite à un point

def 27 : Si $p \geq 2$ est un nombre premier, on appelle p-groupe tout groupe de cardinal p^α où $\alpha \in \mathbb{N}^*$.

Thm 28 : Tout groupe d'ordre p^2 avec p premier est abélien

3) Sous-groupes remarquables d'un groupe fini

def 29 : on dit qu'un sous-groupe H de G est distingué si on a $gH = Hg$ pour tout $g \in G$

Ex 30 : les sous-groupes $\{1\}$ et G sont distingués dans G.

Ex 31 : Si G est abélien, tous ses sous-groupes sont distingués.

Thm 32 : Si G, G' sont deux groupes et φ un morphisme de groupes de G dans G', alors $\mathrm{Ker}(\varphi)$ est un sous-groupe distingué de G.

prop 33 : Le centre $Z(G)$ de G est un sous-groupe distingué de G.

Rq 34 : Si H est distingué dans G alors G/H est un sous-groupe de G. et on a la suite exacte : $\{1\} \to H \to G \to G/H \to \{1\}$

def 35 : On dit que G est un groupe simple s'il n'a pas d'autres sous-groupes distingués que les sous-groupes triviaux

Ex 36 : Les seuls groupes abéliens simples sont les groupes isomorphes à $\mathbb{Z}/p\mathbb{Z}$ avec p premier

def 37 : Soient $x, y \in G$, on appelle commutateur de x et y l'élément $[x,y] = xyx^{-1}y^{-1}$. Le sous-groupe $D(G)$ engendré par l'ensemble des commutateurs est appelé groupe dérivé de G

prop 38 . Le groupe dérivé de G est distingué dans G.

def 39 : Le quotient de G par son sous-groupe dérivé est appelé abélianisé de G

Rq 40 : L'abélianisé de G est un groupe abélien

Ex 41 : Pour $n \geq 3$, on a $D(SL_n(\mathbb{F}_q)) = D(GL_n(\mathbb{F}_q)) = SL_n(\mathbb{F}_q)$ $(q \neq 2)$.

def 42 : Si $n = |G| = p^k q$ et si l'ordre de H est exactement p^k, on dit que H est un p-sous-groupe de Sylow de G.

Thm 42 (Sylow) : G un groupe fini, d'ordre n et $n = p^k q$ sa décomposition en facteurs premiers

(i) Il existe dans G un p-sous-groupe de Sylow

(ii) Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow de G

(iii) les p-sous-groupes de Sylow de G sont conjugués

(iv) le nombre n_p de p-SS-groupes de Sylow de G divise q et $n_p \equiv 1 \pmod p$

II) Classification des groupes abéliens finis

1) Groupes Cycliques

def 43 : On dit qu'un groupe G est cyclique lorsqu'il est monogène et fini. Un élément $a \in G$ tel que $\langle a \rangle = G$ est appelé un générateur de G.

Ex 44 : Le groupe additif $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}$ est engendré par $\bar{1}$. C'est donc un groupe cyclique d'ordre n

prop 45 . Si G est un groupe cyclique d'ordre n, alors il y a $\varphi(n)$ générateurs dans G, où $\varphi(n) = \#\{k \in [\![1,n]\!] \,/\, k \wedge n = 1\}$.

prop 46 : Deux groupes cycliques G et G' sont isomorphes si et seulement si ils ont le même ordre.

prop 47 : Soit G un groupe cyclique d'ordre n. Alors $\mathrm{Aut}(G)$ 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 48 : Soient G un groupe cyclique d'ordre n et 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.
En posant $\delta = n/d$, on a $H_d = \langle a^\delta \rangle$

Appli 49 : les éléments d'ordre 6 dans U_{30} sont ξ^5 et ξ^{25} où $\xi = \exp(\frac{2i\pi}{30})$.

prop 50 : G est d'ordre premier $\iff$ G est cyclique et simple.

2) Produits de groupes cycliques

prop 51 : Le produit $G_1 \times G_2$ de deux groupes est cyclique $\iff$ G_1 et G_2 sont cycliques d'ordres m et n premiers entre eux.

Ex 52 : le groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ est cyclique isomorphe à $\mathbb{Z}/12\mathbb{Z}$

Coro 53 : Le produit $G = G_1 \times \dots \times G_k$ de k groupes cycliques est cyclique $\iff$ les ordres $n_1, \dots, n_k$ de ces groupes sont 2 à 2 premiers entre eux.

3) Décomposition cyclique d'un groupe abélien fini.

Thm 54 (de Structure) : Soit G un groupe abélien fini d'ordre $n \geq 2$. Il existe des entiers $q_1, \dots, q_k$ avec $q_1 \geq 2$ et $\forall i \in [\![2, k]\!]$ q_i est multiple de q_{i-1}, uniques, et tels que G est isomorphe à :
$$(\mathbb{Z}/q_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/q_k\mathbb{Z}).$$

Coro 55 : Si G est un groupe abélien d'ordre p^m avec p premier, alors il existe une unique suite $r_1 \leq \dots \leq r_k$ dans $\mathbb{N}^*$ telle que :
$$G \simeq (\mathbb{Z}/p^{r_1}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p^{r_k}\mathbb{Z}).$$

Appli 56 : Il y a 6 structures possibles pour un groupe abélien d'ordre 600

III) Quelques groupes non abéliens finis.

1) Groupe Symétrique.

def 57 : $S_n(E)$ est le groupe des bijections de E dans E. S_n est appelé groupe des permutations de E.

prop 57 : $|S_n(E)| = n!$

Thm 58 : S_n est engendré par :
- les transpositions
- les $n-1$ transpositions $(1, k)$ avec $k \in [\![2, n]\!]$
- les $n-1$ transpositions $(k, k+1)$ avec $k \in [\![1, n-1]\!]$

def 59 : La signature d'une permutation $\sigma \in S_n$ est l'élément de $\{-1, 1\}$ défini par $\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)}$ où $\mu(\sigma)$ est le nombre d'orbites de σ.

def 60 : On dit qu'une permutation $\sigma \in S_n$ est paire si $\varepsilon(\sigma) = 1$

def 61 : Le groupe alterné est le sous-ensemble de S_n formé des permutations paires. On le note $A_n(E)$.

prop 62 : pour $n \geq 3$, A_n est engendré par les 3-cycles

Thm 63 : Pour $n = 3$ ou $n \geq 5$, A_n est simple. Dev

Thm 64 : pour $n \geq 5$, $D(S_n) = A_n$, $D(A_n) = A_n$, $D(A_3) = \{e\}$, et $D(A_4) = V$ où V est le groupe de Klein.

Rq 65 : Pour $n \geq 5$, on dit que A_n est un groupe parfait.

2) Groupes d'isométries laissant invariant une figure.

def 66 : On appelle groupe diédral d'ordre n le groupe des isométries du plan euclidien qui conservent un polygone régulier convexe à n côtés.

Thm 67 : Le groupe diédral est d'ordre $2n$. Engendré par la rotation d'angle $\frac{2\pi}{n}$ et la symétrie par rapport à l'axe horizontal

Rq 68 : Le groupe diédral est donc constitué de n rotations et n réflexions.

Thm 69 : En dimension 3, si C_6 est le cube et T_4 le tétraèdre régulier, on a :
$$\begin{cases} Is(T_4) \simeq S_4 \text{ et } Is^+(T_4) \simeq A_4 \\ Is(C_6) \simeq \mathbb{Z}/2\mathbb{Z} \times S_4 \text{ et } Is^+(C_6) \simeq S_4 \end{cases}$$
Dev

où $Is(\mathcal{C}) = \{f \in O_3(\mathbb{R}) \,/\, f(\mathcal{C}) = \mathcal{C}\}$ est le groupe des isométries affines de $\mathcal{C}$.
Et $Is^+(\mathcal{C}) = Is(\mathcal{C}) \cap SL_3(\mathbb{R})$, le groupe des déplacements de $\mathcal{C}$

Références :
- François Combes, Algèbre et Géométrie
- Jean Delcourt, Théorie des groupes.
- Rombaldi, Algèbre et géométrie.
- Rotman, Introduction to the theory of groups