104 Groupes Finis. Exemples et Applications

I. Généralités

1) Quotient et produit

<u>Définition 1</u> G groupe de cardinal $|G|$ fini. H sous groupe. On note $[G:H] := |G|/|H|$ l'indice de H dans G.

<u>Théorème 2 (Lagrange)</u> : $\left[[G:H] \text{ est un entier} \right]$

Si H est <u>distingué</u>, l'ensemble quotient G/H a une structure de groupe.

<u>Théorème 3</u> : $\left[\varphi : G \to G', \text{ alors } G/_{\mathrm{Ker}\varphi} \cong \mathrm{Im}\varphi. \right]$

<u>Définition 4</u> : On dit que G est une extension de H et K si on a une suite exacte :

$$1 \longrightarrow H \longrightarrow G \xrightarrow{\varphi} K \longrightarrow 1.$$

→ On a $H \triangleleft G$ et $K \cong G/H$.

→ Si il existe $K' \subset G$ tel que $K' \xrightarrow{\varphi} K$, on dit que G est produit semi-direct, noté $G = H \rtimes K$.

→ Si on a : $K' \triangleleft G$, on parle de produit direct.

<u>Exemple 5</u> : Bien distinguer $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, D_n et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

- On a $\mathfrak{S}_n = \mathcal{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$

2) <u>Exemples fondamentaux</u>

- Le groupe $\mathfrak{S}_n$ des permutation de $[\![1, n]\!]$.

<u>Proposition 6</u> : $\mathfrak{S}_n$ est engendré par les transpositions. $\mathcal{A}_n$ est engendré par les 3-cycles

- Les groupes linéaires sur les corps finis

<u>Proposition 7</u> : $GL_n(\mathbb{F}_q)$ est d'ordre $(q^n-1)\cdots(q^n-q^{n-1})$.

- Les groupes $\langle S, R \rangle := S^* / \langle\langle R \rangle\rangle$ définis par générateurs et relation

<u>Proposition 8</u> : Tout groupe fini est défini par générateurs et relations.

<u>Exemple 9</u> : $\mathbb{Z}/n\mathbb{Z} = \langle a, a^n \rangle$, $D_n = \langle \{r, s\}, \{r^n, s^2, (sr)^2\} \rangle$

3) <u>Sous-groupes particulier</u>

- Centre : $Z(G) := \{ g \in G ;\ \forall h \in G,\ gh = hg \}$
- Groupe dérivé : $D(G) := \langle \{ g h g^{-1} h^{-1},\ g, h \in G \} \rangle$

Ce sont des sous groupes distingués.

<u>Proposition 10</u> : $Z(G) = G \iff D(G) = 1$

<u>Définition 11</u> : Un tel groupe est dit commutatif ou abélien.

Alors G/H Abélien $\iff D(G) \subset H$

<u>Exemple 12</u> : $Z(\mathfrak{S}_n) = 1$ pour $n \geq 3$

$D(\mathfrak{S}_3) = \langle (123) \rangle$

<u>Définition 13</u> : On dit que G est résoluble si : $\exists k \in \mathbb{N},\ D^k(G) = 1$

II - Actions de Groupe

1) Sur un ensemble fini X

On a morphisme : $G \to \mathfrak{S}_{|X|}$

Définition 14 :

Orbite : $\mathcal{O}_x := \{g.x, g \in G\} \subset X$

Stabilisateur : $H_x := \{g \in G, g.x = x\} \subset G$

Proposition 15 : On a : $|G| = |\mathcal{O}_x| . |H_x|$ pour tout $x \in X$.

Applications : • Théorème de Cayley : $[G \hookrightarrow \mathfrak{S}_{|G|}]$

• Calcul de $\binom{n}{k} = \dfrac{|\mathfrak{S}_n|}{|\mathfrak{S}_k| . |\mathfrak{S}_{n-k}|}$

• Théorème de Cauchy : si p premier divise $|G|$, alors G possède un élément d'ordre p

• Soit $p | |G|$ minimal et $H \subset G$ d'indice p, alors $H \lhd G$

• Théorème de Wedderburn : Si on autorise les corps non commutatifs, tous les corps finis sont encore commutatifs

• Pour $n \geq 5$, le groupe $\mathcal{A}_n$ est simple. [DEV]

2) Théorèmes de Sylow

Définition 16 : On appelle p-groupe un groupe d'ordre p^α pour p premier.

Un p-sous-groupe de Sylow de G est un p-sous-groupe d'ordre maximal dans G.

Théorème 17 :

Pour tout p premier divisant $|G|$, il existe un p-Sylow dans G (notation : S_p)

Théorème 18 : Tout p-sous-groupe de G est inclus dans un p-Sylow.

• Les p-Sylow sont conjugués, leur nombre divise $|G|$

• Le nombre de p-Sylow est congru à 1 modulo p et divise $|G|/|S_p|$

→ Permet de décrire les groupes de petits cardinaux.

Exemple 19 : Groupes d'ordre 12 [DEV].

A isomorphisme près, il existe 2 groupes abéliens d'ordre 12 et 3 non abéliens.

3) Sur un espace vectoriel E de dimension finie

Définition 20 : On appelle représentation la donnée d'un morphisme $G \to GL(E)$.

Exemple 21 : On représente $\mathfrak{S}_n$ par son action sur k^n définie par : $\sigma . e_i := e_{\sigma(i)}$

Théorème 22 : Les sous groupes finis de $SO_3(\mathbb{R})$ sont isomorphes à $\mathbb{Z}/n\mathbb{Z}$, D_n, $\mathcal{A}_4$, $\mathfrak{S}_4$, $\mathcal{A}_5$.

[DEV] : Représentation de $\mathfrak{S}_4$ comme le groupe des isométries directes du cube.

III - Groupes Abéliens finis

1) Groupe cyclique

Théorème 23 [Lemme Chinois] : $(n \wedge m = 1)$

$\Longleftrightarrow$ (On a un isomorphisme d'anneaux : $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$)

Proposition 24 : Soit $s, n \in \mathbb{Z}$, sont équivalents :

- $s \wedge n = 1$ • $\bar{s}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$
- $\bar{s}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$
- Il existe un automorphisme φ de $\mathbb{Z}/n\mathbb{Z}$ vérifiant $\varphi(\bar{1}) = \bar{s}$.

Définition 25 : On note $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$. C'est le nombre d'éléments de $[\![1, n]\!]$ premiers à n.

Applications :

- Petit Théorème de Fermat : $\forall a \in \mathbb{Z}, \forall n \geq 2$, on a :
$$a^{\varphi(n)} \equiv 1 [n]$$
- Classification des groupes d'ordre pq, p, q premiers.

2) Etude générale

Comme en réduction, par exemple, on a deux décompositions. Soit $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et $S_{p_1}, \dots S_{p_r}$ des sous-groupes de Sylow de G pour $p_1 \dots p_r$. alors on a :

- $G \cong S_{p_1} \times \cdots \times S_{p_r}$

- [Théorème de Structure] :
Il existe des entiers $d_1 | \dots | d_k$ tels que
$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}.$$

Références :

[Perrin] : Pour Sylow, les groupes abéliens, $\mathcal{A}_n$ simple

[Combes] : Pour l'arithmétique et les groupes d'ordre 12

[Rauch] : Les groupes finis et leurs représentations

Pour le reste du plan, notamment sa structure, ainsi que le joli calcul de $\binom{n}{k}$.

Voir aussi les isométries du tétraèdre et du cube, p40.