Leçon 104 Groupes finis. Exemples et applications

→ Rapport du jury:

- [x] Ordre d'un grpe, élément + Thm Lagrange
- [x] Parler de $\mathbb{Z}/n\mathbb{Z}$ et $\mathfrak{S}_n$: savoir proposer un générateur / une famille de gén.
- [x] ~~Calculs sur~~ Savoir faire des calculs avec les éléments de $\mathfrak{S}_n$
- [ ] Thm de structure des groupes abéliens finis
  - ↳ savoir l'appliquer
- [ ] Connaître groupes d'ordre 1er et grpe d'ordre ≤ 7
- [ ] Bcp d'exemple
- [ ] Étude des groupes d'isométries laissant fixe un polygone
- [ ] Groupes d'automorphismes
- [ ] Représentat° de groupes
- [ ] Étudier $\mathfrak{S}_4$, $\mathfrak{A}_4$, $\mathfrak{D}_{2S}$ + relier géom↔alg
- [ ] Dualité d'un grpe abélien fini
- [ ] Cyclicité de $K^\times$, K corps
- [ ] T. F discrète ...

Dév	Réf
CNS cycl. $(\mathbb{Z}/n\mathbb{Z})^\times$	Zémor + Perrin
fct simple ?	Rom + Per ? + Ulmer ?

Aller voir :
- [ROM], [PER],
- [ULMER] "Théorie des groupes"
- [COMBES] - Algèbre et géométrie

(peut-être [CAL] ou Berhuy)

$24 = 2\times2\times2\times3 = 2^3 3$

Idée plan:

I) Outils pour l'étude des groupes finis

A) Ordre et thm de Lagrange — [ROM] + [PER] (+ [ULM] + [COM])

B) Action de groupes — éq aux classes, Burnside. — [PER] ou [ULM]

C) Application aux p-groupes : — [PER]

II) Cas des groupes abéliens.

A) Groupes cycliques — [ROM] + [PER] + [ZEN] ou [ULM] ou [COM]?

Dév 1 CNS $(\mathbb{Z}/n\mathbb{Z})^\times$ cyclique

B) Structure des groupes abéliens finis — [COM] ou [ULM]

III) Exemples remarquables :

A) Groupe symétrique - alterné — [ROM] + [COM] ou [ULM]

Dév 2 (fct simple) ← ? ← Ulmer ou Per ou Rom?

- déf, générateurs, signature

B) Groupes diédraux — [TERCIER] ou [CAL] ou [ULM] + [PER]

déf + dessin ?

je sais pas trop si quoi sert cette partie

IV) Représentations de groupes

(surtout KR et tables de KR) — [ROM] ou [ULM] ([BER])

Aller voir ce que font des gens sur internet

Plan détaillé [104] Groupes finis

I) Outils pour l'étude des groupes finis

A) Ordre et thm de Lagrange :

G groupe fini
$H < G$ sous-groupe de G

[BER] p. 128

Déf 1 : ordre de $G \rightsquigarrow |G|$

Rmq 2 : $aH = \{ah \mid h \in H\}$, Ha, on a 2 relations d'éq : $x \sim_g y \Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH$
$x \sim_d y \Leftrightarrow yx^{-1} \in H \Leftrightarrow y \in Hx$

Déf 3 : classe à gauche/droite modulo H
+ $[G : H] = |G/H| = |H\backslash G|$

Rmq 4 : les classes à g/d mod H forment une partit° de G.

[BER] p. 144 - 150

THM 5 : Thm de Lagrange : $|G| = [G : H]\,|H|$.

Déf 6 : ordre de $x \in G$, noté $o(x)$ $(= |\langle x \rangle|)$

THM 7 : ~~G fini, $x \in G$~~ $o(x) < +\infty \Leftrightarrow \exists m > 0$ tq $x^m = 1_G$
ds ce cas $o(x) = \min\{m \geq 1 \mid x^m = 1_G\}$. + $x^m = 1_G \Leftrightarrow o(x) \mid m$.
+ $o(x) \mid |G|$ si G fini ← thm de Lag sur $|\langle x \rangle|$

exemples : $\mathbb{Z}/3\mathbb{Z}$, $H = \bar{3}\mathbb{Z}/3\mathbb{Z}$, $[G : H] = 3$
$o(\bar{3}) = |\langle \bar{0}, \bar{3}, \bar{6} \rangle| = 3$, $o(\bar{2}) = 9$
• Dans S_n $(|S_n| = n!)$ un p-cycle est d'ordre p.

Cor 9 : $|G| = n \geq 1$, $\forall x \in G$, $x^n = 1_G$

Prop 10 : $x \in G$ d'ordre fini. $\forall d \geq 1$, $o(x^d) = \dfrac{o(x)}{\text{pgcd}(d, o(x))}$
Si $d \wedge o(x) = 1$, $o(x^d) = o(x)$

Prop 11 : $x, y \in G$ tq $o(x), o(y)$ fini, $xy = yx$. Alors xy d'ordre fini
→ Si $o(x) \wedge o(y) = 1$, $o(xy) = o(x)o(y)$.

B) Actions de groupes :

[BER] p. 169 - 177

Déf 12 : action de groupe + équivalence avec morphisme de grpe de $G \to \mathfrak{S}(X)$

Ex 13 : • translat° à gauche
• conjugaison sur $H \lhd G$
• $S_n \times [\![1;n]\!]$ via $\sigma \cdot k = \sigma(k)$

Déf 14 : Stab(x) + Fix(g)
$\mathcal{O}(x)$

Prop 15 : $\Psi_x : \left| \begin{array}{ccc} G/\text{Stab}(x) & \xrightarrow{\sim} & \mathcal{O}(x) \\ \bar{g} & \longmapsto & g \cdot x \end{array} \right.$ est un isomorphisme

Cor 16 : éq. aux classes : X fini $|X| = \sum_{\omega \in \Omega} |\omega| = \sum_{x \in S} \dfrac{|G|}{\text{Stab}(x)}$
$\Omega = \{\mathcal{O}(x), x \in X\}$
S système de représentant des orbites

Rem 17 : formule utile lorsqu'on a besoin de dénombrer des ens. ex : preuve de la loi de récip. quad.

Prop 17 : Formule de Burnside

Appli 18 : Thm de Cayley : $|G| = n$, $G \simeq$ ss-grpe de S_n.

C) Application à l'étude de p-groupes : p 1er

[ULM] p. 72 - 74

Déf 19 : p-groupe

Ex 20 : $G = \{e\}$, Q_8, D_4,

Prop 21 : G un p-groupe opérant sur X ens. fini. On note
$X^G = \{x \in X \mid \forall g \in G, g \cdot x = x\} = \bigcap_{g \in G} \text{Fix}(g)$
↳ $|X^G| \equiv |X| \bmod p$.

THM 22 : Cauchy : G grpe fini tq $p \mid |G|$, $\exists g \in G$ tq $o(g) = p$.

Cor 23 : autre déf d'un p-grpe ← groupe d'ordre p^α.

THM 24 : $Z(G)$ non trivial, G p-grpe

Cor 25 : un grpe d'ordre p^2 est abélien.

[BER] p. 151

[ULM] p. 83

À ne pas mettre mais à connaître : Thm de Sylow
↳ • p-Sylow = p-grpe d'ordre max dans G ↝ $G = p^\alpha p_1 \cdots p_n$. p_1-Sylow = grpe d'ordre p^α (↳ ou encore grpe maximal pour la qualité de p-grpe)
• $N \subseteq G$ P-p-grpe : $N \lhd G \Rightarrow N \subset \bigcap_{P \in \text{Syl}_p(G)} P$
• Un P-Sylow est distingué ⟺ c'est l'unique p-Sylow de G

Thm : $|G| = p^\alpha m$, $p \nmid m$ (normalisateur de P)
1) p-Sylow de G sont les ss-grpes d'ordre p^α
2) p-Sylow tous conjugués : Si P p-Syl(G), le nbre de p-Sylow(G) est $[G : N_G(P)]$
3) $n_p = |\text{Syl}_p(G)|$. $\boxed{n_p \mid m \text{ et } n_p \equiv 1 \ [p]}$

[BER]

Plan détaillé [104] suite

II) Cas des groupes abéliens :

A) Groupes cycliques : G groupe abélien

Déf26 : grpe monogène + cyclique
Rem27 : Un tel groupe est forcément abélien, $\langle g\rangle = \{g^n, n\in\mathbb{Z}\}$
Ex28 $(\mathbb{Z},+)$, $(\mathbb{Z}/n\mathbb{Z},+)$, $(\mathbb{U}_n,\times)$

THM28 : G monogène, $\begin{cases}\text{infini} \longrightarrow \simeq (\mathbb{Z},+)\\ \text{fini} \longrightarrow \simeq (\mathbb{Z}/n\mathbb{Z},+),\ n=|G|\end{cases}$

Rq29 : 2 grpes cycliques sont $\simeq$ $\Leftrightarrow$ ils ont même cardinal][BER]
Ex30 $U_4 \simeq \mathbb{Z}/4\mathbb{Z}$
Déf30 : $G=\langle g\rangle$ cyclique d'ordre n. Ses générateurs sont les g^k, $k\wedge n = 1$

THM31 : • $|G|=p$, premier $\Rightarrow$ G cyclique
• $|G|=pq$, p q 2 nbres 1er $\neq$, G cyclique

THM32 : sous-groupes des groupes ~~cyc~~ cycliques
Déf33 : déf $\varphi(n)$ ind. euler
Rem34 : $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

[ROM] p. 13 - 15
[BER] P 155 - 156

→ Exemples de groupes cycliques "non évidents"

THM35 : K corps, tout sous-groupe fini de K^* est cyclique

[ROM] p 25

THM36 : CNS de cyclicité de $(\mathbb{Z}/n\mathbb{Z})^\times$ (Dév 1)

[RER] (+[ZÉM])

B) Structure des groupes abéliens finis G gpe ab. fini

Déf37 : $e(G) = \max_{g\in G}(o(g))$.
Rq38 : $e(G) = \text{ppcm}(o(g), g\in G)$
Déf39 : caractère de G = morphisme de $G \to \mathbb{C}^*$

Lemme40 : $H \lhd G$, $\forall \varphi : H \to \mathbb{C}^*$ caract. on peut le prolonger en $\tilde{\varphi} : G \to \mathbb{C}^*$ caract

THM41 : $|G|=n\geq 2$, $\exists!\,(n_k)_{1\leq k\leq r}$ d'entiers tq $n_1\geq 2$, $n_1 | n_2 | \dots | n_r$ tq
$G \simeq \prod_{k=1}^{r} U_{n_k} \simeq \prod_{k=1}^{r} (\mathbb{Z}/n_k\mathbb{Z})$

[ROM] p. 26 - 28

Ex42 : À isom. près les grpes abéliens d'ordre 24 sont : $\{\mathbb{Z}/24\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}\}$,

[BER] p. 364

Ex24 : $G = \mathbb{Z}/4\mathbb{Z}^\times \times (\mathbb{Z}/2\mathbb{Z})^4 \times \mathbb{Z}/9\mathbb{Z}^\times \times \mathbb{Z}/3\mathbb{Z}^\times \times \mathbb{Z}/5\mathbb{Z}^\times \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/180\mathbb{Z}$

III) Exemples remarquables :

A) Groupe symétrique - alterné : $n\in\mathbb{N}^*$

→ S_n : ⚠ = essentiel

Prop25 : $|S_n| = n!$
Déf26 : $\text{supp}(\sigma) = \{x\in[\![1,n]\!] \mid \sigma(x)\neq x\}$
Ex27 : $\sigma = (1\,2\,3)(4\,5\,1)(1\,2)$. $\text{supp}(\sigma) = \{1,2,3,4,5\}$
Prop28 : propriété sur $\text{supp}(\sigma)$, σ'...
Prop29 : 2 permutat° à supp disjoint commutent
THM30 : Toute permutat° se décompose de manière unique (à l'ordre) en produit de cycles à support disjoints
↳ Donc S_n est engendré par les cycles. + ex30 : $\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&4&7&5&6\end{pmatrix} = (1\,2\,3)(5\,7\,6)$
Cor31 : S_n est engendré par les transpositions.
Prop32 : • Un p-cycle est d'ordre p
• L'ordre d'une permutat° est le ppcm des long. des cycles à supp disj qui la composent
Prop33 : • $\sigma\in S_n$, $(a_1,\dots,a_p)$ p-cycles, $\sigma(a_1,\dots,a_p)\sigma^{-1} = (\sigma(a_1)\dots\sigma(a_p))$
• Les p-cycles sont tous conjugués dans S_n.

[BER] P 200 - 209

→ $\mathcal{A}_n$

[ULM] p.62 - 66

Déf34 : signature (celle que je connais) + ex
Prop35 : ε morphisme (unique ?) ← je sais pas si on le met parce que c'est unique... et $\varepsilon(\sigma) = (-1)^s$, s = un nbre de transpo dans déc
Prop-déf36 : $\mathcal{A}_n$, $|\mathcal{A}_n| = \frac{n!}{2}$, $\mathcal{A}_n \lhd S_n$
Ex37 : $\mathcal{A}_4 = \dots$
Lemme38 : $\mathcal{A}_n$ engendré par les 3-cycles
Lemme39 : S_n et $\mathcal{A}_n$ agissent par conjugaison sur eux même. Pour $\sigma\in\mathcal{A}_n$
On note $\mathcal{O}_{\mathcal{A}_n}(\sigma)$, $\mathcal{O}_{S_n}(\sigma)$ les orbites de σ sur $\mathcal{A}_n$ et S_n, et $\text{Stab}_{\mathcal{A}_n}(\sigma)$, $\text{Stab}_{S_n}(\sigma)$ les stab.
↳ soit $\text{Stab}_{S_n}(\sigma) = \text{Stab}_{\mathcal{A}_n}(\sigma) \subseteq \mathcal{A}_n$ et alors $|\mathcal{O}_{S_n}(\sigma)| = |\mathcal{O}_{\mathcal{A}_n}(\sigma)| \times 2$
soit $\exists x\in S_n\setminus\mathcal{A}_n$, $x\sigma x^{-1} = \sigma$ et dc $|\mathcal{O}_{\mathcal{A}_n}(\sigma)| = |\mathcal{O}_{S_n}(\sigma)|$

(Dév 2) je sais plus la réf ? [PER] ?

THM40 : $\forall n\geq 5$, $\mathcal{A}_n$ simple

→ Peut-être en dire moins... ?

B) Groupe diédraux : $n \geq 1$

D_{41} : déf $D_n \rightsquigarrow D_n = \langle s, r \rangle \subseteq \mathcal{O}_2(\mathbb{R})$

P_{42} : $|D_n| = 2n$, $\begin{cases} r^n = id = s^2 \\ srs = r^{-1} \end{cases}$ ces relations déterminent entièrement $D_n = \langle r, s \rangle$] cf Annexe (table de D_3)

D_{43} $D_n = \langle \alpha, \beta \rangle$ où $\alpha = rs$, $\beta = s$ d'ordre 2

P_{43} : D_2 abélien non cyclique, $\forall n \geq 3$, D_n non abélien

m_{44} : D_n agit sur l'espace affine $E = (\mathbb{R}^2, 0)$, par exemple D_4 représente transformations conservant un carré (cf dessin annexe)

(à savoir : Perrin $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ $\langle r \rangle \simeq \mathbb{Z}/n\mathbb{Z}$, $D_3 \simeq \mathfrak{S}_3$)

HM_{45} : Le groupe des isométries conservant les sommet d'un polygone régulier à n côtés est $\simeq D_n$ ← à mettre

[ULM] p. 8 à 9

[ULM] p. 33

[RON] p 84

IV) Représentations de groupes : ← si marque de place tps cette partie saute ?

D_{45} : représentat° + degré

$_{46}$: $g \mapsto 1$, ~~$S_n \to GL_n$~~ rep régulière

D_{46} : sous-rep + rep irréductible

HM_{47} : Maschke

D_{48} : caractère d'une rep. + caractère irréductible

peut-être Thm 16.17 ULM

P_{49} : G fini, G simple $\forall$ caract. irréd $\neq$ non trivial, $\{g \mid \chi(g) = \chi(e)\} = \{e\}$

$_{50}$: Table de S_4

[ULM] p. 144 - 155

159

155

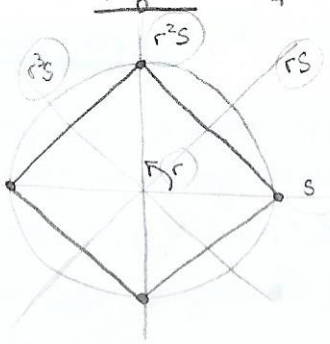
j'aime pas cette partie

Annexe

Fig 1 : Table de $D_3 = \{e, r, r^2, s, rs, r^2s\}$

. . . . .

Fig 2 : D_4



Réf : [BER] - Berhuy le grand combat

[ULM] - Ulmer - Théorie des groupes

[ROM] - Rombaldi - Algèbre

([PER] + [ZEM]) : 2 dév