

Leçon 104 – Groupes finis. Exemples et applications.

Cadre : G désigne un groupe fini noté multiplicativement, de neutre 1 et de cardinal (ou d'ordre) $|G|$.

But de la leçon : dans un premier temps, obtenir la classification des petits groupes finis à isomorphismes près ; dans un second temps, faire de la géométrie et notamment étudier les groupes d'isométries de certaines figures.

1 Cardinal, ordre, générateur

Déf 1.1. Soit H un sous-groupe de G . On définit l'ensemble fini $G/H = \{gH, g \in G\}$ des classes à gauche modulo H . On note $(G : H)$ son cardinal, on l'appelle l'indice de H dans G .

Thm 1.2 (Lagrange). L'ordre de H divise celui de G . Précisément : $|G| = |H| (G : H)$.

Appl 1.3. Si $|H| > |G|/2$, alors $H = G$.

Déf 1.4. Pour $A \subseteq G$ une partie de G , on note $\langle A \rangle$ le plus petit sous-groupe de G contenant A . On dit que A génère G lorsque $\langle A \rangle = G$.

Rmq 1.5. Si H est un sous-groupe de $G = \langle A \rangle$, alors $H = G \iff A \subset H$.

Ex 1.6. — pour $n \geq 1$, $(\mathbf{Z}/n\mathbf{Z}, +) = \langle 1 \bmod n \rangle$,
— pour $n \geq 2$, le groupe symétrique est engendré par les transpositions.

Prop 1.7. Soit $g \in G$, il existe un plus petit entier $n \geq 1$ tel que $g^n = 1$, appelé ordre de g . C'est le générateur strictement positif du noyau du morphisme $k \in \mathbf{Z} \mapsto g^k \in G$. On a alors $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\} \simeq \mathbf{Z}/n\mathbf{Z}$.

Prop 1.8. On a : $\text{ord}(g) = |\langle g \rangle|$ divise $|G|$, avec égalité si, et seulement si, $G = \langle g \rangle$. On dit alors que G est cyclique engendré par g , il est en particulier abélien.

Prop 1.9. $\text{ord}(g^k) = \text{ord}(g) / \text{pgcd}(k, \text{ord}(g))$ divise $\text{ord}(g)$.

Ex 1.10. — U_6 est engendré par $e^{i\pi/3}$ et $e^{5i\pi/3}$,
— le groupe de Klein $(\mathbf{Z}/2\mathbf{Z})^2$ n'est pas cyclique car ses éléments non triviaux sont d'ordre 2,
— le groupe $S_3 = \{\text{Id}, (12), (13), (23), (123), (132)\}$ est l'unique groupe d'ordre 6 non abélien, à isomorphisme près,
— soient $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\mathbf{I} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\mathbf{J} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ et $\mathbf{K} = \mathbf{IJ} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$,
alors le groupe quaternionique $H_8 = \{\pm \mathbf{1}, \pm \mathbf{I}, \pm \mathbf{J}, \pm \mathbf{K}\} \subset \text{SL}_2(\mathbf{C})$ possède un élément d'ordre 2 ($-\mathbf{1}$) et six d'ordre 4 (faire la table en annexe).

Prop 1.11. Un groupe de cardinal p premier est cyclique, isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

2 Groupes abéliens finis

2.1 Théorèmes de structure

Prop 2.1 (Structure des groupes cycliques). Soit $G = \langle g \rangle$ cyclique d'ordre n . Alors pour tout $d|n$, G possède un unique sous-groupe d'ordre d , c'est $\langle g^{n/d} \rangle$, il est cyclique. Les générateurs de G sont les g^k avec $\text{pgcd}(k, n) = 1$, il y en a $\varphi(n)$ par définition.

Cor 2.2. Pour tout $n \geq 1$, $n = \sum_{d|n} \varphi(d)$.

Appl 2.3. Pour q puissance d'un nombre premier, le groupe multiplicatif $\mathbf{F}_q^*$ est cyclique.

Prop 2.4 (Exposant). Soit G un groupe abélien fini. Soit $a = \max \{ \text{ord}(g), g \in G \}$ appelé exposant de G . Alors pour tout g dans G , l'ordre de g divise a . On a donc $a = \text{ppcm}(\text{ord}(g), g \in G)$.

Thm 2.5 (Structure des groupes abéliens finis). Soit G un groupe abélien fini. Alors il existe des entiers $r \geq 1$ et $2 \leq a_r | \dots | a_1$ tels que : $G \simeq \mathbf{Z}/a_1\mathbf{Z} \times \dots \times \mathbf{Z}/a_r\mathbf{Z}$.

Rmq 2.6. Les entiers $2 \leq a_r | \dots | a_1$ sont uniquement déterminés par G , ils sont appelés les facteurs invariants de G . En particulier a_1 est l'exposant de G .

Rmq 2.7. À l'aide du théorème de structure on peut retrouver le fait que $\mathbf{F}_q^*$ est cyclique.

2.2 Étude des $((\mathbf{Z}/n\mathbf{Z})^\times, \times)$

Déf 2.8. Pour $n \geq 1$ entier, on note $(\mathbf{Z}/n\mathbf{Z})^\times = \{k \bmod n, \text{pgcd}(k, n) = 1\}$ le groupe abélien (multiplicatif) des éléments inversibles de l'anneau $(\mathbf{Z}/n\mathbf{Z}, +, \times)$. C'est aussi l'ensemble des générateurs du groupe $(\mathbf{Z}/n\mathbf{Z}, +)$. Il est de cardinal $\varphi(n)$.

Prop 2.9. $\text{Aut}(\mathbf{Z}/n\mathbf{Z}, +) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$.

Thm 2.10 (Chinois). Pour $m, n \geq 1$, $\text{pgcd}(m, n) = 1 \iff \mathbf{Z}/mn\mathbf{Z} \simeq \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ (isomorphisme d'anneaux et donc de groupes additifs).

Cor 2.11. Si la décomposition de n en produit de nombres premiers deux à deux distincts est $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, alors on a l'isomorphisme de groupes multiplicatifs $(\mathbf{Z}/n\mathbf{Z})^\times \simeq (\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z})^\times \times \dots \times (\mathbf{Z}/p_r^{\alpha_r}\mathbf{Z})^\times$.

Thm 2.12 (Condition de cyclicité). Le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique si et seulement si $n = 1, 2, 4, p^\alpha, 2p^\alpha$ avec $p \geq 3$ premier et $\alpha \geq 1$.

Prop 2.13. Pour $\alpha \geq 3$, $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$ non cyclique.

Csq 2.14. À l'aide du théorème chinois on peut déterminer les facteurs invariants des groupes abéliens $(\mathbf{Z}/n\mathbf{Z})^\times$.

Ex 2.15. Pour $n = 5808 = 2^4 \times 3 \times 11^2$ les facteurs invariants du groupe $(\mathbf{Z}/5808\mathbf{Z})^\times$ sont $(2, 2, 2, 220)$.

3 Sous-groupes distingués et quotients

Pour étudier les groupes non abéliens on a besoin de plus d'outils.

Déf 3.1. Un sous-groupe H de G est dit distingué lorsque pour tout $g \in G$, $gHg^{-1} = H$. On note alors $H \triangleleft G$.

Rmq 3.2. Le centre $Z(G)$ de G est toujours distingué dans G .

Ex 3.3. $Z(\mathbf{H}_8) = \{\pm 1\} \triangleleft \mathbf{H}_8$ et $\forall n \geq 3$, $Z(\mathbf{S}_n) = \{\text{Id}\}$.

Prop 3.4. Soit H sous-groupe de G . Alors : G/H est un groupe fessant de la projection canonique $G \rightarrow G/H$ un morphisme de groupe si, et seulement si, $H \triangleleft G$.

Prop 3.5. Si $f : G \rightarrow G'$ est un morphisme de groupes et $H' \triangleleft G'$, alors $f^{-1}(H') \triangleleft G$. En particulier $\text{Ker}(f) \triangleleft G$.

Ex 3.6. Le morphisme signature $\epsilon : \mathbf{S}_n \rightarrow \{\pm 1\}$ est l'unique morphisme de groupe (non trivial) de $\mathbf{S}_n$ dans $\mathbf{C}^*$. Son noyau est par définition le groupe alterné $\mathbf{A}_n \triangleleft \mathbf{S}_n$.

Déf 3.7. Un groupe non trivial G est dit simple lorsque ses seuls sous-groupes distingués sont $\{1\}$ et G .

Rmq 3.8. Si G est abélien (non nécessairement fini), alors : G est simple $\iff G$ est cyclique d'ordre premier.

Cex 3.9. On définit $\mathbf{V}_4 = \{\text{Id}, (12)(34), (13)(24), (14)(23)\} \simeq (\mathbf{Z}/2\mathbf{Z})^2$ sous-groupe de $\mathbf{A}_4$ distingué dans $\mathbf{A}_4$ (et même dans $\mathbf{S}_4$). Donc $\mathbf{A}_4$ n'est pas simple.

Prop 3.10. Pour $n \geq 3$ les 3-cycles engendrent $\mathbf{A}_n$ et pour $n \geq 5$ ils sont deux à deux conjugués dans $\mathbf{A}_n$.

Thm 3.11. Pour tout $n \geq 5$, $\mathbf{A}_n$ est simple.

Cor 3.12. Pour $n \geq 5$, $\{\text{Id}\}$, $\mathbf{A}_n$ et $\mathbf{S}_n$ sont les seuls sous-groupes distingués de $\mathbf{S}_n$.

Déf 3.13. Pour x et y dans G le commutateur associé est $[x, y] = xyx^{-1}y^{-1}$. On note $D(G)$ le sous-groupe de G engendré par les commutateurs de G . On le nomme groupe dérivé de G . Il est distingué dans G .

Rmq 3.14. G est abélien $\iff D(G)$ est trivial.

Prop 3.15. $D(G)$ est le plus petit sous-groupe H de G pour l'inclusion tel que G/H soit abélien. En quotientant par $D(G)$ on est ainsi ramené à un groupe abélien.

Ex 3.16. $D(\mathbf{H}_8) = \{\pm 1\}$ et $\mathbf{H}_8 / D(\mathbf{H}_8) \simeq (\mathbf{Z}/2\mathbf{Z})^2$.

Prop 3.17. Pour $n \geq 1$, $D(\mathbf{S}_n) = \mathbf{A}_n$, pour $n \geq 5$, $D(\mathbf{A}_n) = \mathbf{A}_n$ et $D(\mathbf{A}_4) = \mathbf{V}_4$.

Appl 3.18. $\mathbf{S}_4 / \mathbf{V}_4 \simeq \mathbf{S}_3$.

4 Utilisation des actions de groupes

4.1 Premiers exemples

En faisant agir G par translation à gauche sur lui-même, on obtient :

Thm 4.1 (Caley). G est isomorphe à un sous-groupe de $\mathbf{S}_n$, où $n = |G|$.

Soit p premier divisant $|G|$. En faisant agir $\mathbf{Z}/p\mathbf{Z}$ sur G^p via $(k \bmod p) \cdot (g_1, \dots, g_p) = (g_{1+k \bmod p}, \dots, g_{p+k \bmod p})$, on obtient via l'équation aux classes :

Thm 4.2 (Cauchy). G possède un élément d'ordre p .

Soit p le plus petit facteur premier de $|G|$. Pour H sous-groupe de G , en faisant agir H sur G/H par translation à gauche, on obtient :

Thm 4.3 (Frobenius). Si $(G : H) = p$ alors $H \triangleleft G$.

Ex 4.4. Un sous-groupe d'indice 2 est distingué. Cela permet de montrer que $\mathbf{A}_4$ est un groupe d'ordre 12 sans sous-groupe d'ordre 6.

4.2 Action par conjugaison

On fait agir G sur lui-même par conjugaison. Les orbites obtenues sont appelées classes de conjugaison de G . Leur cardinal divise celui de G . On regarde $G = \mathbf{S}_n$.

Prop 4.5. Dans $\mathbf{S}_n$, $\sigma(a_1 \dots a_r)\sigma^{-1} = (\sigma(a_1) \dots \sigma(a_r))$ r -cycle.

Prop 4.6. Pour $2 \leq r \leq n$, les r -cycles forment une classe de conjugaison dans $\mathbf{S}_n$.

Soit $\sigma \neq \text{Id}$ dans $\mathbf{S}_n$ fixé. En faisant agir $\langle \sigma \rangle$ sur $\{1, \dots, n\}$, on obtient :

Prop 4.7. Il existe un unique $r \geq 1$, des uniques cycles $c_1, \dots, c_r$ à supports deux à deux disjoints tels que $\sigma = c_1 \dots c_r$. Notons $l_1 \leq \dots \leq l_r$ les longueurs respectives de ces cycles. Alors $(l_1, \dots, l_r)$ est appelé le type de σ .

Prop 4.8. Deux permutations σ et τ sont conjugués dans $\mathbf{S}_n$ si, et seulement si, elles ont même type.

Cor 4.9. Le nombre de classes de conjugaison de $\mathbf{S}_n$ est égal au nombre de partitions de n .

Ex 4.10. Classes de conjugaison de $\mathbf{S}_4$: $\{\text{Id}\}$ ($4 = 1 + 1 + 1 + 1$), $\{6 \text{ transpositions}\}$ ($4 = 2 + 1 + 1$), $\{8 \text{ 3-cycles}\}$ ($4 = 3 + 1$), $\{3 \text{ double-transpositions}\}$ ($4 = 2 + 2$), $\{6 \text{ 4-cycles}\}$ ($4 = 4$).

4.3 p -groupe

Déf 4.11. G est un p -groupe lorsque son ordre est une puissance de p premier : $|G| = p^\alpha$, $\alpha \geq 1$.

En utilisant l'équation aux classes pour l'action par conjugaison, on obtient :

Prop 4.12. Le centre d'un p -groupe n'est pas trivial.

Cor 4.13. Si $|G| = p^2$, alors G est abélien, donc $G \simeq (\mathbf{Z}/p\mathbf{Z})^2$ ou $\mathbf{Z}/p^2\mathbf{Z}$.

Dans la suite $|G| = p^\alpha m$, avec p premier, $\alpha \geq 1$ et p non diviseur de m .

Déf 4.14. Un p -Sylow de G est un sous-groupe de G d'ordre p^α .

Thm 4.15 (Sylow). 1. G possède un p -Sylow,
2. tout p -sous-groupe de G est inclus dans un p -Sylow de G ,
3. les p -Sylow de G sont deux à deux conjugués,
4. leur nombre k vérifie $k \equiv 1 \pmod p$ et $k|m$.

Cor 4.16 (du point 3). Soit S un p -Sylow de G , alors : S est l'unique p -Sylow de G si, et seulement, si $S \triangleleft G$.

Ex 4.17. Un groupe d'ordre 63 n'est pas simple.

Cor 4.18 (du point 1). Pour tout $0 \leq \beta \leq \alpha$, il existe dans G un groupe d'ordre p^β . Avec $\beta = 1$, on retrouve le théorème de Cauchy.

Ex 4.19. Exo du jury : déterminer les p -Sylow de $\mathbf{S}_4$.

5 Groupes et géométrie

Dans cette section, $\mathcal{E}$ est l'espace affine euclidien $\mathbf{R}^2$ ou $\mathbf{R}^3$. $\mathcal{P}$ désignera une partie quelconque de $\mathcal{E}$.

Déf 5.1. Le groupe des isométries de $\mathcal{P}$ est le groupe des isométries de $\mathcal{E}$ fixant $\mathcal{P}$: $\text{Isom}(\mathcal{P}) = \{\varphi \in \text{Isom}(\mathcal{E}), \varphi(\mathcal{P}) = \mathcal{P}\}$. On note aussi $\text{Isom}^+(\mathcal{P}) = \text{Isom}^+(\mathcal{E}) \cap \text{Isom}(\mathcal{P})$ et $\text{Isom}^-(\mathcal{P}) = \text{Isom}(\mathcal{P}) \setminus \text{Isom}^+(\mathcal{P})$.

Prop 5.2. — Pour toute similitude φ de $\mathcal{E}$ on a : $\text{Isom}(\varphi(\mathcal{P})) \simeq \text{Isom}(\mathcal{P})$.
— Si $\mathcal{P}$ est fini et si O est un centre de symétrie de $\mathcal{P}$ alors $\varphi(O) = O$ pour tout $\varphi \in \text{Isom}(\mathcal{P})$. De plus : $\text{Isom}(\mathcal{P}) \simeq \text{Isom}^+(\mathcal{P}) \times \mathbf{Z}/2\mathbf{Z}$.

5.1 Polygones réguliers

On suppose ici $\mathcal{E} = \mathbf{R}^2$.

Prop 5.3. Pour tout $n \geq 3$ il existe un polygone régulier à n côtés. C'est l'enveloppe convexe de $\mathbf{U}_n$ dans $\mathbf{C} \simeq \mathbf{R}^2$ (d'origine O), on le note $\mathcal{P}_n$. Deux polygones réguliers à n côtés sont semblables, donc leurs groupes d'isométries sont isomorphes.

Prop 5.4. Soit ρ est la rotation de centre O et d'angle $2\pi/n$. Soit $\mathcal{D}$ la droite réelle, on note σ la réflexion d'axe $\mathcal{D}$. Alors :

- ρ est d'ordre n , σ est d'ordre 2, $\sigma\rho\sigma = \rho^{-1}$,
- $\text{Isom}^+(\mathcal{P}_n) = \langle \rho \rangle = \{\text{Id}, \rho, \dots, \rho^{n-1}\}$,
- $\text{Isom}(\mathcal{P}_n) = \langle \rho, \sigma \rangle = \{\text{Id}, \rho, \dots, \rho^{n-1}\} \cup \{\sigma, \sigma\rho, \dots, \sigma\rho^{n-1}\}$.

On dit que $\text{Isom}(\mathcal{P}_n)$ est diédrale d'ordre $2n$. On le note $\mathbf{D}_n$.

Rmq 5.5. La notation $\mathbf{D}_n$ a un sens pour $n \geq 1$.

Prop 5.6. Pour tout $n \geq 1$, $\mathbf{Z}(\mathbf{D}_n)$ est trivial si n est impair et vaut $\{\text{Id}, \rho^{n/2}\}$ si n est pair. Et $\mathbf{D}(\mathbf{D}_n) = \langle \rho^2 \rangle$ ($= \langle \rho \rangle$ si n est impair).

5.2 Polyèdres convexes

On se place maintenant dans $\mathcal{E} = \mathbf{R}^3$.

Déf 5.7. On note T « le » tétraèdre régulier (à similitude près) de $\mathcal{E}$, c'est-à-dire l'enveloppe convexe de quatre points équidistants dans l'espace.

Thm 5.8. En faisant agir $\text{Isom}(T)$ sur l'ensemble des sommets de T , on obtient : $\text{Isom}(T) \simeq \mathbf{S}_4$, et donc $\text{Isom}^+(T) \simeq \mathbf{A}_4$.

Faire des dessins en annexe pour illustrer le tableau suivant :

Isométries de T	Permutations de $\mathbf{S}_4$
Id	Id
rotation d'axe sommet-centre de face opposée	3-cycle
rotation d'axe passant par le milieu de 2 arêtes opposées	double-transpositions
symétrie par rapport à un plan médiateur	transposition
composée d'une symétrie et d'une rotation sommet-centre	4-cycle

Déf 5.9. On choisit un repère dans l'espace affine $\mathcal{E} = \mathbf{R}^3$. Soit C « le » cube (à similitude près) de $\mathcal{E}$, c'est-à-dire l'enveloppe convexe de $\mathcal{S} = \{(\pm 1/2, \pm 1/2, \pm 1/2)\}$ (ensemble à huit éléments).

Prop 5.10. $\text{Isom}(C) \simeq \text{Isom}(\mathcal{S})$

On fait agir $\text{Isom}^+(\mathcal{S})$ sur l'ensemble des quatre diagonales du cube pour obtenir :

Thm 5.11. $\text{Isom}^+(\mathcal{S}) \simeq \mathbf{S}_4$, puis $\text{Isom}(\mathcal{S}) \simeq \mathbf{S}_4 \times \mathbf{Z}/2\mathbf{Z}$.

Annexe

Ordre	Groupes à isomorphisme près
1	$\{1\}$
2	$\mathbf{Z}/2\mathbf{Z}$
3	$\mathbf{Z}/3\mathbf{Z}$
4	$\mathbf{Z}/4\mathbf{Z}, (\mathbf{Z}/2\mathbf{Z})^2 \simeq \mathbf{D}_2$
5	$\mathbf{Z}/5\mathbf{Z}$
6	$\mathbf{Z}/6\mathbf{Z}, \mathbf{S}_3 \simeq \mathbf{D}_3$
7	$\mathbf{Z}/7\mathbf{Z}$
8	$\mathbf{Z}/8\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}, (\mathbf{Z}/2\mathbf{Z})^3, \mathbf{D}_4, \mathbf{H}_8$
9	$\mathbf{Z}/9\mathbf{Z}, (\mathbf{Z}/3\mathbf{Z})^2$

Dessiner $\mathbf{U}_6$ sur un cercle avec les ordres des éléments.

Faire une partie de la table de $\mathbf{H}_8$.

Faire des dessins du tétraèdre régulier illustrant le dictionnaire de $\text{Isom}(\mathbf{T})$.

Avertissements

C'est le plan que j'ai réalisé le jour J. Il est là pour vous donner des idées. Faites un plan à votre niveau. Développez d'avantage des parties et rajoutez/supprimez en d'autres à votre guise.

Développements possibles

- Théorème de structure des groupes abéliens finis,
- Condition nécessaire et suffisante sur $n \geq 1$ pour que $(\mathbf{Z}/n\mathbf{Z})^\times$ soit cyclique,
- Simplicité des $\mathbf{A}_n$ pour $n \geq 5$ et sous-groupes distingués des $\mathbf{S}_n$,
- Les théorèmes de Sylow par les actions de groupes (preuve du Perrin),
- Groupe d'isométries du cube,
- Table de caractères de $\mathbf{S}_4$ (si on parle de représentations).

Références

- Nouvelles histoires hédonistes de groupes et de géométrie - Caldero Germoni (Tome 2, pour le théorème de structure et la partie 5)
- Mathématiques pour l'agrégation - Rombaldi (pour la partie 5 et un peu la partie 1)
- Oraux X-ENS Algèbre 1 - Francinou Gianella Nicolas (pour Frobenius et pour faire des exos)
- Cours d'algèbre - Perrin (pour tout le reste)