108 EXEMPLES DE PARTIES GÉNÉRATRICES D'UN GROUPE. APPLICATIONS.

Sous-groupe engendré par une partie (c'est l'intersection des sous-groupes la contenant), partie génératrice
Exemple du groupe dérivé

I. Cas des groupes abéliens

I. A. Groupes monogènes et cycliques Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$

[Rom17, §1.4-5/1.9/10.1, p13–19/27/277] [Per96, §1.1/1.7, p10/24]

Groupe monogène, cyclique, monogène/cyclique implique abélien

EXEMPLE 1. $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe cyclique à n éléments engendré par $\overline{1}$.

APPLICATION 2. Tout groupe cyclique à n éléments est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

EXEMPLE 3. $\mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$: considérer $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{U}_n, \overline{k} \longmapsto e^{2ik\pi/n}$.
Si G est un groupe, $\langle a\rangle$ où $a \in G$ est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$ pour un $n \in \mathbb{N}^*$.

PROPOSITION 4. *L'ordre de $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est $\frac{n}{k\wedge n}$.*

COROLLAIRE 5. *$(\mathbb{Z}/n\mathbb{Z},+)$ est engendré par les $\overline{k}$ tels que $k \wedge n = 1$.*

EXEMPLE 6. $\mathbb{Z}/8\mathbb{Z}$ est engendré par $\overline{1}, \overline{3}, \overline{5}$ et $\overline{7}$.

APPLICATION 7.
- Les sous-groupes d'un groupe cyclique sont cycliques.
- Si $|G| = p$, G est cyclique.

DÉFINITION 8. [INDICATRICE D'EULER]
Pour $n \geq 2$, on définit $\varphi(n)$ le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z},+)$.

EXEMPLE 9. Pour $p \in \mathcal{P}$ et $\alpha \in \mathbb{N}^*$, on a $\varphi(p^\alpha) = p^\alpha(p-1)$.

PROPOSITION 10. [SOUS-GROUPES DE $\mathbb{Z}/n\mathbb{Z}$]
Pour $d \mid n$, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, engendré par $\overline{\frac{n}{d}}$ et formé des éléments dont l'ordre divise d.

PROPOSITION 11. *Si $d \mid n$, $\mathbb{Z}/n\mathbb{Z}$ contient $\varphi(d)$ éléments d'ordre d.*

APPLICATION 12. $n = \sum_{d|n} \varphi(d)$

I. B. Groupes abéliens finis

[Ulm12, Ch12, p103]

Groupe abélien de type fini, exemple des groupes abéliens finis

THÉORÈME 13. [STRUCTURE DES GROUPES ABÉLIENS DE TYPE FINI]
Soit G un groupe abélien de type fini. Alors il existe $\ell, r \in \mathbb{N}$ uniques et une unique suite $d_1 \geq d_2 \geq \cdots \geq d_\ell$ d'entiers supérieurs à 2 tels que $d_{i+1} \mid d_i$ pour tout $i \leq \ell-1$ et $G \simeq \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z} \times \mathbb{Z}^r$.

COROLLAIRE 14. [STRUCTURE DES GROUPES ABÉLIENS FINIS]
Soit G un groupe abélien fini. Il existe un unique entier ℓ et une unique suite $d_1 \geq d_2 \geq \cdots \geq d_\ell$ d'entiers supérieurs à 2 tels que d_1 est l'exposant de G, $d_{i+1} \mid d_i$ pour tout $i \leq \ell-1$ et $G \simeq \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$.

EXEMPLE 15. Les groupes abéliens d'ordre 24 sont isomorphes à $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $(\mathbb{Z}/6\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

REMARQUE 16. Dans le cas d'un groupe fini, on peut trouver des générateurs du groupe en trouvant un élément d'ordre l'exposant du groupe, puisque l'on montre que d_1 est l'exposant de G. Une fois ce premier élément trouvé, on peut se restreindre à un sous-groupe de G et réitérer l'opération, via la théorie des caractères.

II. Groupe symétrique

[Rom17, Ch2, p39]

On note $\mathfrak{S}_n$ le groupe des permutations de n éléments.

II. A. Générateurs

Les cycles engendre $\mathfrak{S}_n$. Application : décomposition en produit de cycles à support disjoints (unique à l'ordre près !)

PROPOSITION 17. *Toute permutation de $\mathfrak{S}_n$ se décompose en un produit de (au plus $n-1$) transpositions.*

EXEMPLE 18. $(4\,3\,1) = (4\,3)(3\,1) = (3\,1)(1\,4)$.

APPLICATION 19. La signature d'un élément σ de $\mathfrak{S}_n$ est déterminée par la parité du nombre de transpositions intervenant dans une décomposition de σ.

APPLICATION 20. Les familles suivantes engendrent $\mathfrak{S}_n$:

- les transpositions $(1\,i)_{2\leq i\leq n}$,
- les transpositions $(i\,i+1)_{1\leq i\leq n-1}$,
- la transposition $(1\,2)$ et le cycle $(1\,2\ \ldots\ n)$.

Utilité : petites familles de générateurs : deux éléments suffisent à engendrer le groupe

II. B. Groupe alterné

Proposition 21. *Il existe deux morphismes de $\mathfrak{S}_n$ dans $\mathbb{C}^*$: l'identité et le morphisme $\mathcal{E}$ qui envoie toute transposition sur -1.*

Définition 22. On définit le groupe alterné $\mathfrak{A}_n$ comme étant le noyau de la signature.

Proposition 23.
- *$\mathcal{E}$ est à valeurs dans $\{-1,1\}$,*
- *La signature d'un ℓ-cycle vaut $(-1)^{\ell+1}$,*
- *Pour $\sigma\in\mathfrak{S}_n$, on a $\mathcal{E}(\sigma)=\prod_{1\leq i<j\leq n}\frac{\sigma(i)-\sigma(j)}{i-j}=(-1)^{i(\sigma)}$ où $i(\sigma)$ est le nombre d'inversions de σ.*

Proposition 24. *$\mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$. Il est de cardinal $n!/2$.*

Lemme 25. *$\mathfrak{A}_n$ est le sous-groupe engendré par les trois cycles.*

Proposition 26. *Pour $n\geq 5$, $\mathfrak{A}_n$ est simple.*

Corollaire 27. *Pour $n\geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Application 28. [groupe dérivé]
- $D(\mathfrak{S}_n)=\mathfrak{A}_n$
- $D(\mathfrak{A}_n)=\mathfrak{A}_n$ pour $n\geq 5$.

III. Groupes linéaires/spéciaux

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n, où $\mathbb{K}$ est un corps commutatif
Définition du groupe linéaire, de $\mathrm{SL}(E)$. Exemple des homothéties
On se ramène à l'étude de $\mathcal{GL}_n(\mathbb{K})$ via un isomorphisme, et $\mathcal{GL}_n(\mathbb{K})\simeq\mathcal{GL}_n(\mathbb{K})$
Proposition : $u\in\mathrm{GL}(E)\iff\ker u=\{0\}\iff\mathrm{Im}(u)=E\iff\det(u)\neq 0$

III. A. Générateurs de $\mathcal{GL}_n(\mathbb{K})$ [Per96, ChIV, p95]

Homothéties, déterminant, u homothétie si et seulement si u stabilise toutes les droites $\to$ stabilisateur de l'action de $\mathrm{GL}(E)$ sur les droites
Dilatations, propriétés des dilatations de rapport $\notin\{0,1\}$
Deux dilatations de même rapport sont conjuguées
Transvections, définitions équivalentes
Les transvections sont conjuguées (dans $\mathcal{SL}_n(\mathbb{K})$ lorsque $n\geq 3$)
Formule de conjugaison
$\mathcal{SL}_n(\mathbb{K})$ est engendré par les transvections, $\mathcal{GL}_n(\mathbb{K})$ est engendré par les transvections et les dilatations
Approche matricielle, pivot de Gauss
$\mathcal{SL}_n(\mathbb{K})$ est connexe par arcs
$Z(\mathcal{GL}_n(\mathbb{K}))$ est l'ensemble des homothéties, $Z(\mathcal{SL}_n(\mathbb{K}))$ est l'ensemble des homothéties de déterminant 1.
Groupes dérivés

III. B. Groupe orthogonal/unitaire [Per96, ChVI, p142] [CG13, §VII.3, p232]

Groupe orthogonal, engendré par les réflexions orthogonales. Groupe spécial orthogonal engendré par les renversements
Déplacement engendré par un nombre pair de réflexions
Groupes dérivés
Application : groupe des quaternions sous forme matricielle, conjugué, norme d'un quaternion, produit scalaire associé, base $(1,\mathrm{i},\mathrm{j},\mathrm{k})$ orthonormée, $\mathbb{H}=\mathbb{I}\oplus^{\perp}\mathbb{R}$, $\mathbb{R}$-espace vectoriel de dimension 4. On définit $\mathrm{SU}_2(\mathbb{C})=\{h\in\mathbb{H}\,|\,N(h)=1\}$.

Théorème 29. *On a $\mathrm{SU}_2(\mathbb{C})/\{\pm I_2\}\simeq\mathrm{SO}_3(\mathbb{R})$.*

III. C. Groupe diédral [Aud06, ChIII/V, p360] [Rom17, §3.4.3/6.1, p87/180]

Sous-groupe D_{2n} de $\mathcal{O}_2(\mathbb{R})$ des isométries préservant un polygone régulier à n sommets.
D_{2n} est engendré par la symétrie et la rotation d'angle $\frac{2\pi}{n}$, d'ordres 2 et 4, ce qui donne la liste des éléments de D_{2n}.

Application 30. D_{2n} s'injecte naturellement dans $\mathcal{GL}_2(\mathbb{C})$, envoyant la rotation d'angle $2\pi/n$ et la symétrie sur

$$R=\begin{pmatrix}\cos(2\pi/n) & -\sin(2\pi/n)\\ \sin(2\pi/n) & \cos(2\pi/n)\end{pmatrix}\quad\text{et}\quad S=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

Énumérations des isométries positives, des isométries négatives

ANNEXE

Transvections, dilatations
Groupe diédral

SPEECH

L'intérêt des parties génératrices est de réduire l'étude d'un groupe à ses générateurs, ce qui permet d'obtenir des propriétés de celui-ci, comme par exemple montrer la surjectivité d'un morphisme ou la simplicité d'un groupe.

QUESTIONS

Q Que peut-on dire du groupe $G = \langle (i\ j), (1\ 2\ \ldots\ n) \rangle$?

R Regardons l'action de G sur $[\![1, n]\!]$. Posons $\ell = (j-i) \wedge n$.
Pour $\sigma \in \mathfrak{S}_n$, on note $P(\sigma)$ la propriété $\forall u, v \in [\![1, n]\!], u \equiv v \mod \ell \implies \sigma(u) \equiv \sigma(v) \mod \ell$.
Les éléments de G vont vérifier cette propriété. En effet $P((1\ 2))$ et $P((1\ 2\ \ \ldots\ n))$ sont vraies, et si $P(\sigma)$ et $P(\sigma')$ sont vraies, alors $P(\sigma^{-1})$ et $P(\sigma\sigma')$ le sont aussi.
Ainsi $P(\sigma)$ est vraie pour $\sigma \in G$. Or pour $n \geq 3$, $P((1\ 2))$ n'est vraie que si $\ell = 1$. Ainsi si $\ell > 1, G \neq \mathfrak{S}_n$.
Réciproquement si $\ell = 1$, on vérifie que $G = \mathfrak{S}_n$.

BIBLIOGRAPHIE

[Aud06] M. Audin : *Géométrie*. EDP Sciences, 2006.

[CG13] P. Caldero et J. Germoni : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Ulm12] F. Ulmer : *Théorie des groupes*. Ellipses, 2012.