Leçon 108 - Exemples de parties génératrices d'un groupe. Applications.

Extrait du rapport de jury

La leçon doit être illustrée par des exemples de groupes très variés, dont il est indispensable de donner des parties génératrices. La description ensembliste du groupe engendré par une partie doit être connue et les groupes monogènes et cycliques doivent être évoqués.
Les groupes $\mathbb{Z}/n\mathbb{Z}$ fournissent des exemples naturels tout comme les groupes de permutations, les groupes linéaires ou leurs sous-groupes (par exemple $\mathrm{SL}_n(\mathbb{K})$, $\mathrm{O}_n(\mathbb{R})$ ou $\mathrm{SO}_n(\mathbb{R})$). Ainsi, on peut s'attarder sur l'étude du groupe des permutations avec différents types de parties génératrices en discutant de leur intérêt (ordre, simplicité de $\mathfrak{A}_5$ par exemple). On peut, en utilisant des parties génératrices pertinentes, présenter le pivot de Gauss, le calcul de l'inverse ou du rang d'une matrice, le groupe des isométries d'un triangle équilatéral. Éventuellement, il est possible de discuter des conditions nécessaires et suffisantes pour que $(\mathbb{Z}/p\mathbb{Z})^\times$ soit cyclique ou la détermination de générateurs du groupe diédral.
On illustre comment la connaissance de parties génératrices s'avère très utile dans certaines situations, par exemple pour l'analyse de morphismes de groupes, ou pour montrer la connexité par arcs de certains sous-groupes de $\mathrm{GL}_n(\mathbb{R})$.
Pour aller plus loin,on peut s'intéresser à la présentation de certains groupes par générateurs et relations. Il est également possible de parler du logarithme discret et de ces applications à la cryptographie (algorithme de Diffie-Hellman, cryptosystème de El Gamal).

Présentation de la leçon

Je vais vous présenter la leçon 108 intitulée : "Exemples de parties génératrices d'un groupe. Applications.". L'intérêt des parties génératrices est de réduire l'étude d'un groupe à ses générateurs (de manière analogue à la notion de base en dimension finie), 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. On donnera dans cette leçon des générateurs de groupes classiques ainsi que plusieurs utilisations de la notion de partie génératrice.
Dans une première partie on s'intéresse aux généralités concernant les parties génératrices en commençant par la définition de partie génératrice. On rappelle ainsi la définition du sous-groupe engendré ainsi qu'une description puis on passe à la définition de groupe engendré par une partie et on fait le lien avec l'ordre qui nous sera utile pour la suite. Dans un deuxième point on fait le lien entre partie génératrice et groupe dérivé et centre.
Dans une deuxième partie, on s'intéresse à l'étude des groupes abéliens finis. On parle tout d'abord des groupes cycliques (dont l'intérêt sera donné dans la sous-partie II.3) en commençant par donner la définition d'un groupe monogène et d'un groupe cyclique puis on commence à classifier ces groupes avec le théorème 16, le corollaire 17 et la proposition 18. On montre ensuite que la réciproque du théorème de Lagrange est vraie pour les groupes cycliques et que les groupes simples abéliens finis sont exactement les $\mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier et on conclut cette sous-partie en donnant des générateurs du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ ainsi que le théorème 23. Dans un deuxième point, on s'attarde sur la notion d'exposant d'un groupe en commençant par donner la définition d'un groupe d'exposant fini ainsi qu'un premier résultat . On donne ensuite deux résultats dans le cas particulier des groupes abéliens. Dans un dernier point, on s'intéresse à la structure des groupes abéliens finis avec tout d'abord le théorème de structure des groupes abéliens finis qui justifie que l'on s'intéresse tant aux groupes cycliques $\mathbb{Z}/n\mathbb{Z}$ et qui possède énormément d'applications. En particulier, on tire de cette partie que tous les groupes abéliens finis vérifient la réciproque du théorème de Lagrange. De plus, le théorème de structure des groupes abéliens finis ainsi que l'étude des groupes cycliques $\mathbb{Z}/n\mathbb{Z}$ justifient que l'on connaît très bien n'importe quel groupe abélien fini en termes de structure interne.
Enfin dans une dernière partie, on s'intéresse aux groupes finis non abéliens où les choses ne sont plus si simples malheureusement... Dans un premier point on s'intéresse au groupe symétrique. On commence par rappeler quelques générateurs avant de parler des classes de conjugaison et d'en venir à la définition du groupe alterné. Le résultat fondamental du groupe alterné est le théorème 48 qui montre que les groupes alternés forment une deuxième famille de groupes finis simples après les $\mathbb{Z}/p\mathbb{Z}$. Ce résultat nous permet d'en déduire le centre de $\mathfrak{S}_n$ ainsi que ses sous-groupes distingués. Dans un deuxième point, on s'intéresse au groupe diédral en en donnant une présentation ainsi qu'une interprétation géométrique. On donne également son centre ainsi que son groupe dérivé en fonction de la parité de n. On termine enfin ce point en classifiant les groupes

d'ordre $2p$. Dans un troisième point on s'intéresse au groupe des quaternions pour deux raisons : tout d'abord car il s'agit du premier groupe "spécial" à apparaître dans la classification des petits groupes (au sens où il est moins naturel que ses prédécesseurs) mais également car il possède la propriété remarquable d'avoir tous ses sous-groupes distingués sans être commutatif !
Dans une dernière partie on s'intéresse à l'étude du groupe linéaire en s'intéressant tout d'abord aux transvections et aux dilatations ainsi qu'à quelque-unes de leur caractérisations. On termine cette partie en montrant que les transvections engendrent $\mathrm{SL}_n(\mathbb{K})$ et que les transvections et les dilatations engendrent $\mathrm{GL}_n(\mathbb{K})$ ainsi que quelques résultats topologiques puis les groupes dérivés en fonction de n et du corps de base. On termine cette leçon par un dernier point consacré au groupe orthogonal avec le théorème de Cartan-Dieudonné qui donne une famille génératrice de $\mathrm{O}(E)$ et qui donne en corollaire la classification des isométries vectorielles en dimension 2 et 3 et on termine avec une famille génératrice de $\mathrm{SO}_n(\mathbb{R})$ et la simplicité de $\mathrm{SO}_3(\mathbb{R})$.
On trouvera enfin en annexe une correspondance entre $\mathfrak{S}_4$ et $\mathrm{Isom}(\mathcal{T})$, une illustration géométrique de D_{10} ainsi que la classification des isométries vectorielles en dimension 2 et 3.

Plan général

Cours détaillé

Dans toute cette leçon, on considère un groupe $(G, *)$.

I Généralités

I.1 Partie génératrice d'un groupe

Définition 1 : Sous-groupe engendré [Berhuy, p.141] :
On considère P une partie de G.
On appelle **sous-groupe engendré par** P (noté $< P >$) l'intersection de tous les sous-groupes de G contenant P.

Théorème 2 : [Berhuy, p.143]
Soit P une partie de G.
Si l'on note $P^{-1} = \{x^{-1},\ x \in P\}$, alors on a la relation suivante :

$$< P >= \{x_1...x_n,\ n \in \mathbb{N} \text{ et } x_1, ..., x_n \in P \cup P^{-1}\}$$

Exemple 3 : [Berhuy, p.142]
Si $x \in G$, alors $< x >= \{x^n,\ n \in \mathbb{Z}\}$.

Remarque 4 : [Berhuy, p.144]
Si G est abélien et que $P = \{a_1, ..., a_r\}$, alors :

$$< P >=< a_1, ..., a_r >= \{a_1^{m_1}...a_r^{m_r},\ m_1, ..., m_r \in \mathbb{Z}\}$$

Définition 5 : Groupe engendré par une partie [Berhuy, p.144] :
On considère P une partie de G.
On dit que G **est engendré par** P lorsque $< P >= G$.

Remarque 6 : [Berhuy, p.145]
La notion de partie génératrice est très utile pour simplifier des calculs, montrer des résultats tels que la simplicité ou les propriétés de morphisme.

Définition 7 : Ordre d'un groupe et d'un élément [Berhuy, p.128 + 149] :
On considère $x \in G$.
* On appelle **ordre du groupe** G le cardinal de G.
* On appelle **ordre de** x le cardinal de $< x >$ et on le note $o(x)$.

Théorème 8 : [Berhuy, p.149]
Soit $x \in G$.
L'élément x est d'ordre fini si, et seulement si, il existe $m > 0$ tel que $x^m = e_G$.
Dans ce cas, l'ordre de x est le plus petit entier $n \in \mathbb{N}^*$ tel que $x^n = e_G$ et on a $< x >= \{x^n,\ n \in [\![0; o(x) - 1]\!]\}$.

I.2 Premières propriétés

Définition 9 : Groupe dérivé [Perrin, p.13] :
On appelle **groupe dérivé de** G (noté $D(G)$) le sous-groupe engendré par les commutateurs (c'est-à-dire les éléments de la forme $xyx^{-1}y^{-1}$).

Exemple 10 : [Perrin, p.13]
* Si G est abélien, alors $D(G) = \{e_G\}$.
* Si $G = \mathfrak{S}_3$, alors $D(G) = \{\mathrm{Id}, \sigma, \sigma^2\}$.

Proposition 11 : [Perrin, p.13]
Si X est une partie génératrice de G, alors $D(G)$ est le plus petit groupe distingué engendré par les commutateurs $[g, h] \in G$ avec $(g, h) \in X^2$.

Définition 12 : Centre [Perrin, p.12] :
On appelle **centre de** G (noté $Z(G)$) le sous-groupe de G formé des éléments qui commutent avec tous les autres.

Proposition 13 :
Si X est une partie génératrice de G, alors $Z(G)$ est composé des éléments commutant avec chaque élément de X.

II Le cas des groupes abéliens

II.1 Groupes monogènes et groupes cycliques

Définition 14 : Groupe monogène/cyclique [Berhuy, p.154] :
On dit que le groupe G est :
* **monogène** lorsqu'il est engendré par un unique élément.
* **cyclique** lorsqu'il est monogène et fini.

Exemple 15 : [Berhuy, p.154]
* Le groupe $\mathbb{Z}$ est monogène mais non cyclique.
* Pour tout entier naturel $n \geq 1$, le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n.

Théorème 16 : [Berhuy, p.154]
* Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.
* Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. En particulier, deux groupes cycliques sont isomorphes si, et seulement si, ils ont le même ordre.

Corollaire 17 : [Berhuy, p.155]
Soit p un nombre premier.
Si G est d'ordre p, alors G est cyclique et $G \cong \mathbb{Z}/p\mathbb{Z}$.

Proposition 18 : [Berhuy, p.194]
Soit p un nombre premier.
Si G est d'ordre p^2, alors $G \cong \mathbb{Z}/p^2\mathbb{Z}$ ou $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Théorème 19 : [Berhuy, p.155]
Si G est un groupe cyclique d'ordre n, alors pour tout diviseur positif d de n, il existe un unique sous-groupe H_d d'ordre d de G et ce sous-groupe est cyclique.
De plus, si x_0 est un générateur de G, on a alors les égalités :

$$H_d = \left\langle x_0^{\frac{n}{d}} \right\rangle = \left\{ x \in G \text{ tq } x^d = e_G \right\}$$

Remarque 20 :
On a ici un cas où la réciproque du théorème de Lagrange est vraie !

Théorème 21 : [Berhuy, p.161]
Les groupes abéliens simples sont exactement les $\mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier.

Proposition 22 : [Rombaldi, p.283]
Soient a un entier relatif et n un entier naturel non nul.
$\overline{a}$ est un générateur du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, l'entier relatif a est premier avec n (ou encore si, et seulement si, $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$).

Théorème 23 : [Rombaldi, p.294] [ADMIS]
Le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si, et seulement si, $n = 2, 4, p^\alpha$ ou $2p^\alpha$ avec p premier impair et $\alpha \geq 1$.

II.2 Exposant d'un groupe

Définition 24 : Groupe d'exposant fini [Berhuy, p.344] :
On dit que G est **d'exposant fini** lorsqu'il existe un entier $n \in \mathbb{N}^*$ tel que pour tout $x \in G$, $x^n = e_G$.
Dans ce cas, on appelle **exposant de** G le plus petit entier $n \in \mathbb{N}^*$ vérifiant cette propriété et on le note $\exp(G)$.

Lemme 25 : [Berhuy, p.344]
Si G est un groupe d'exposant fini, alors $\exp(G) = \text{PPCM}(\{o(x),\ x \in G\})$.
De plus, si G est fini, on a $\exp(G)$ qui divise $\text{Card}(G)$.

Exemple 26 : [Berhuy, p.345]
$*$ Si G est cyclique d'ordre n, alors $\exp(G) = n$.
$*$ On a $\exp(D_4) = 4$ et $\exp(\mathfrak{S}_3) = 6$.

Proposition 27 : [Berhuy, p.345]
Si G est un groupe abélien d'exposant fini, alors il existe un élément $x \in G$ d'ordre $\exp(G)$.

Corollaire 28 : [Berhuy, p.345]
Si G est un groupe abélien fini, alors on a l'équivalence :

$$(\exp(G) = \text{Card}(G)) \iff (G \text{ cyclique})$$

Remarque 29 : [Berhuy, p.346]
L'ensemble $\mathfrak{S}_3$ montre que les deux résultats précédents sont faux si G n'est pas supposé abélien.

Théorème 30 : [Berhuy, p.346]
Soit $\mathbb{K}$ un corps commutatif quelconque.
Tout sous-groupe fini de $\mathbb{K}^\times$ est cyclique.

Remarque 31 : [Berhuy, p.346]
$*$ En particulier, on en déduit que tout sous-groupe de $\mathbb{F}_q^\times$ est cyclique (avec $q = p^n$ où p est un nombre premier et n un entier naturel non nul).
$*$ Si p est un nombre premier, on a alors que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique et on retrouve le résultat du théorème 23 dans le cas où $r = 1$.

II.3 Structure des groupes abéliens

Dans toute cette sous-partie, on suppose que $(G, *)$ est d'ordre fini et abélien.

Théorème 32 : Théorème de structure [ADMIS] [Berhuy, p.358] :
Il existe des entiers $d_1, ..., d_s \geq 2$ vérifiant $d_1 | d_2 | ... | d_s$ et tels que $G \cong \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$.
De plus, la suite d'entiers $(d_1, ..., d_s)$ est unique, et ne dépend que de la classe d'isomorphisme de G.

Définition 33 : Facteurs invariants [Berhuy, p.361] :
Les entiers $d_1, ..., d_s$ fournis par le théorème précédent sont appelés les **facteurs invariants de** G.

Corollaire 34 : [Berhuy, p.362]
Deux groupes abéliens finis sont isomorphes si, et seulement si, ils ont les mêmes facteurs invariants.

Exemple 35 : [Berhuy, p.363]
∗ Si $G = \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, alors $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$.
∗ Il y a exactement 3 groupes abéliens d'ordre 120 (à l'isomorphisme près).

Corollaire 36 :
Pour tout diviseur d de l'ordre de G, il existe un sous-groupe de G d'ordre d.

Théorème 37 : [ADMIS] [Berhuy, p.364]
Si G est un groupe abélien de type fini, alors il existe des entiers naturels r, s et des entiers $d_1, ..., d_s \geq 2$ vérifiant $d_1|d_2|...|d_s$ tels que $G \cong \mathbb{Z}^r \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$.
De plus, l'entier r et la suite d'entiers $(d_1, ..., d_s)$ sont uniques.

III Exemples de groupes non abéliens

III.1 Le groupe symétrique

Dans toute cette sous-partie, on considère un entier naturel $n \geq 2$. On notera $\mathfrak{S}_n$ le groupe symétrique sur $[\![1; n]\!]$ (de cardinal $n!$).

Théorème 38 : [Berhuy, p.204]
Toute permutation de $\mathfrak{S}_n$ se décompose en produit de cycles à supports disjoints et cette décomposition est unique à l'ordre des facteurs près.

Théorème 39 : [Berhuy, p.208]
L'ordre d'une permutation est le PPCM des longueurs des cycles à supports disjoints qui la composent.

Exemple 40 :
On considère $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 5 & 1 & 2 & 7 & 8 & 6 \end{pmatrix}$.
On a alors $\sigma = (1\ 4)(2\ 3\ 5)(6\ 7\ 8)$ et $o(\sigma) = \text{PPCM}(2, 3, 3) = 6$.

Proposition 41 : [Berhuy, p.212 + 213]
Le groupe $\mathfrak{S}_n$ est engendré par chacune des familles suivantes :
∗ Les cycles. ∗ Les transpositions. ∗ Les transpositions $(1\ i)$ pour $i \in [\![2; n]\!]$.
∗ Les transpositions $(i\ i+1)$ pour $i \in [\![1; n-1]\!]$. ∗ $(1\ 2)$ et $(1\ 2\ ...\ n)$.

Théorème 42 : [Combes, p.175]
Soit $\mathcal{E}$ un espace affine euclidien de dimension 3.
En notant $\mathcal{T}$ le tétraèdre régulier, on a $\text{Isom}^+(\mathcal{T}) \cong \mathfrak{A}_4$ et $\text{Isom}(\mathcal{T}) \cong \mathfrak{S}_4$.

Théorème 43 : [Combes, p.175]
Soit $\mathcal{E}$ un espace affine euclidien de dimension 3.
En notant $\mathcal{C}$ le cube régulier, on a $\text{Isom}^+(\mathcal{C}) \cong \mathfrak{S}_4$ et $\text{Isom}(\mathcal{C}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Définition 44 : Type d'une permutation [Berhuy, p.211] :
On considère $\sigma \in \mathfrak{S}_n$.
On appelle **type de** σ la liste $\lambda(\sigma) = [\lambda_1, ..., \lambda_n]$ où λ_1 est le nombre de points fixes de σ et λ_k le nombre de k-cycles dans la décomposition de σ.

Théorème 45 : [Berhuy, p.211]
Deux permutations de $\mathfrak{S}_n$ sont conjuguées si, et seulement si, elles ont le même type.

Proposition 46 : [Berhuy, p.212]
Le nombre total de classes de conjugaison dans le groupe symétrique $\mathfrak{S}_n$ est donné par $P(n) = \text{Card}\left(\left\{[\lambda_1, ..., \lambda_n] \text{ tq } \lambda_1, ..., \lambda_n \in \mathbb{N} \text{ et } \sum_{k=1}^{n} k\lambda_k = n\right\}\right)$.

Exemple 47 : [Berhuy, p.212]
$\mathfrak{S}_4$ possède 5 classes de conjugaison distinctes puisque $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$ et elles sont représentées par $(1\ 2\ 3\ 4)$, $(1\ 2\ 3)$, $(1\ 2)$, $(1\ 2)(3\ 4)$ et $\text{Id}_{[\![1;n]\!]}$.

Définition 48 : Signature [Berhuy, p.213] :
Il existe un unique morphisme de groupes $\varepsilon : \mathfrak{S}_n \longrightarrow \mathbb{C}^\times$ non trivial appelé **signature** tel que pour toute transposition σ, $\varepsilon(\sigma) = -1$ et pour toute permutation ρ qui s'écrit comme produit de s transpositions, on a $\varepsilon(\rho) = (-1)^s$.

On note $\mathfrak{A}_n$ le noyau de ε, aussi appelé groupe alterné sur $[\![1;n]\!]$ (de cardinal $\frac{n!}{2}$).

Remarque 49 : [Berhuy, p.301 + 302]
On a $\mathfrak{S}_n = \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$.
Autrement dit, on a la suite exacte scindée :

$$\left\{\text{Id}_{[\![1;n]\!]}\right\} \longrightarrow \mathfrak{A}_n \xrightarrow{\iota} \mathfrak{S}_n \underset{s}{\overset{\varepsilon}{\rightleftarrows}} \mathbb{Z}/2\mathbb{Z} \longrightarrow \left\{\text{Id}_{[\![1;n]\!]}\right\}$$

Développement 1 : [cf. ROMBALDI]

Théorème 50 : Simplicité de $\mathfrak{A}_n$ pour $n = 3$ ou $n \geq 5$ [Rombaldi, p.50] :
Pour $n = 3$ ou $n \geq 5$, le groupe $\mathfrak{A}_n$ est simple.

Remarque 51 : [Berhuy, p.219 + Perrin, p.28 + 37]
∗ En réalité, $\mathfrak{A}_5$ est le plus petit groupe simple non abélien (et tout groupe simple d'ordre 60 est isomorphe à $\mathfrak{A}_5$).
∗ Ce résultat est cohérent avec le théorème de Feit-Thompson (tout groupe simple fini et non abélien est d'ordre pair).
∗ Ce résultat a une importance historique majeure car il permet de montrer que pour $n \geq 5$, $\mathfrak{A}_n$ n'est pas résoluble et donc que les solutions des équations polynomiales de degré supérieur ou égal à 5 ne peuvent s'écrire à l'aide des quatre opérations élémentaires et de la racine carré.

Remarque 52 : [Perrin, p.30]
∗ Si $n = 4$, alors $\mathfrak{A}_n$ n'est pas simple car contient comme sous-groupe distingué $H = \left\{\text{Id}_{[\![1;4]\!]}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\right\}$.
∗ De plus, $\mathfrak{A}_4$ est le plus petit groupe (à l'isomorphisme près) qui ne vérifie pas la réciproque du théorème de Lagrange.

Proposition 53 : [Berhuy, p.219]
Si $n \geq 3$, alors le centre de $\mathfrak{S}_n$ est trivial.

Corollaire 54 : [Berhuy, p.220 + Delcourt p.139]
∗ Si $n \geq 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont exactement $\text{Id}_{[\![1;n]\!]}, \mathfrak{A}_n$ et $\mathfrak{S}_n$ et on a $D(\mathfrak{A}_n) = \mathfrak{A}_n$.
∗ De plus, on a $D(\mathfrak{S}_n) = \mathfrak{A}_n$.

Remarque 55 : [Berhuy, p.220]
Si $n = 4$, alors il faut rajouter à la liste précédente le sous-groupe H de $\mathfrak{S}_4$ (cf. remarque 50).

III.2 Le groupe diédral

Définition 56 : Groupe diédral [Berhuy, p.274] :
On appelle **groupe diédral d'ordre** $2n$ le groupe :

$$D_{2n} \cong \left\langle a, b \mid a^n = 1,\ b^2 = 1,\ bab^{-1} = a^{-1} \right\rangle$$

Proposition 57 : [Delcourt, p.98]
Le groupe diédral d'ordre $2n$ est un groupe non abélien de cardinal $2n$.

Remarque 58 : [Perrin, p.23]
Le groupe diédral d'ordre $2n$ possède une interprétation géométrique : il s'agit du groupe des isométries du plan euclidien conservant un polygone régulier à n côtés. Il est engendré par la rotation τ de mesure d'angle $\frac{2\pi}{n}$ et la symétrie orthogonale σ par rapport à l'axe (Ox).

Remarque 59 : [Perrin, p.23]
Le sous-groupe des rotations est distingué et isomorphe à $\mathbb{Z}/n\mathbb{Z}$. De plus, comme $\text{Card}(D_{2n}) = 2n$, on a donc une suite exacte :

$$\{\text{Id}\} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow D_{2n} \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow \{\text{Id}\}$$

et un isomorphisme $D_{2n} \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ car n'importe quelle réflexion fournit une section de p.

Proposition 60 : [Delcourt, p.139]
∗ Si n est impair, alors centre de D_{2n} est réduit au sous-groupe trivial.
∗ Si n est pair, alors le centre de D_{2n} est égal à $\left\{\text{Id}, \tau^{\frac{n}{2}}\right\}$.

Proposition 61 : [Delcourt, p.136]
∗ Si n est impair, alors le groupe dérivé de D_{2n} est égal à $<\tau>\cong \mathbb{Z}/n\mathbb{Z}$.
∗ Si $n = 2m$ est pair, alors le groupe dérivé de D_{2n} est égal à $\langle\tau^2\rangle \cong \mathbb{Z}/m\mathbb{Z}$.

Proposition 62 : [Berhuy, p. 310]
Soit p un nombre premier supérieur ou égal à 3.
Si G est d'ordre $2p$, alors G est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ ou à D_{2p}.

III.3 Le groupe des quaternions

Définition 63 : Groupe des quaternions [Delcourt, p.40] :
On appelle **groupe des quaternions** le groupe :

$$\mathbb{H}_8 \cong \langle a, b \mid a^4 = 1,\ b^4 = 1,\ ba = a^3b\rangle$$

Proposition 64 : [Delcourt, p.40]
Le groupe $\mathbb{H}_8$ possède 8 éléments dont : 1 élément d'ordre 1, 1 élément d'ordre 2 (a^2) et 6 éléments d'ordre 4.
En particulier, les groupes D_8 et $\mathbb{H}_8$ ne sont pas isomorphes.

Proposition 65 : [Delcourt, p.43 + 136]
Le groupe $\mathbb{H}_8$ (non commutatif!) possède 6 sous-groupes stricts et chacun est commutatif et distingué dans $\mathbb{H}_8$.
En particulier, $Z(\mathbb{H}_8) = \{-1; 1\}$.

IV Étude du groupe linéaire

Dans toute cette partie, on considère $\mathbb{K}$ un corps commutatif quelconque, n, m deux entiers naturels non nul et E un $\mathbb{K}$-espace vectoriel de dimension finie n.

IV.1 Le groupe linéaire

Définition 66 : Transvection [Rombaldi, p.145] :
On considère φ une forme linéaire non nulle sur E.
On appelle **transvection d'hyperplan** $\text{Ker}(\varphi)$ toute application $u \in \mathcal{L}(E)$ définie par :

$$\forall x \in E,\ u(x) = x + \varphi(x)a,\ a \in \text{Ker}(\varphi)$$

Théorème 67 : [Rombaldi, p.146]
∗ Un endomorphisme $u \in \mathcal{L}(E)$ est une transvection si, et seulement si, il existe un hyperplan H de E tel que $u|_H = \text{Id}_H$ et $\text{Im}(u - \text{Id}_E) \subseteq H$.
∗ Pour tout transvection $\tau_{\varphi,a}$, $\tau^2_{\varphi,2a}$ est une transvection.
∗ Une transvection $\tau_{\varphi,a}$ est dans $\text{GL}(E)$, son inverse est la transvection $\tau_{\varphi,-a}$, 1 est l'unique valeur propre de $\tau_{\varphi,a}$ et le sous-espace propre associé est $\text{Ker}(\varphi)$ pour $u \neq \text{Id}_E$.
∗ Le conjugué dans $\text{GL}(E)$ d'une transvection est une transvection.
∗ L'ensemble $T(H)$ des transvections d'hyperplan $H = \text{Ker}(\varphi)$ est un sous-groupe multiplicatif de $\text{GL}(E)$ isomorphe au groupe additif $(H, +)$.
∗ Une transvection u admet un polynôme minimal qui est $(X-1)$ lorsque $u = \text{Id}_E$ ou $(X-1)^2$ lorsque $u \neq \text{Id}_E$.

Théorème 68 : [Rombaldi, p.147]
Soit $u \in \mathcal{L}(E)\backslash\{\text{Id}_E\}$.
Les assertions suivantes sont équivalentes :
∗ u est une transvection.
∗ Il existe une base de E dans laquelle la matrice de u est de la forme suivante :
$T_n = \begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.
∗ Il existe une base de E dans laquelle la matrice de u est $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$ avec $\lambda \in \mathbb{K}^*$ et $1 \leq i \neq j \leq n$.
∗ $\text{rg}(u - \text{Id}_E) = 1$ et le polynôme caractéristique de u est $(X-1)^n$.

Corollaire 69 : [Rombaldi, p.148]
∗ Pour $\mathbb{K}$ infini, toute transvection différente de Id_E s'écrit comme produit de deux matrices diagonalisables inversibles.
∗ Si $n \geq 3$, alors toutes les transvections différentes de Id_E sont conjugués dans $\text{SL}(E)$.

Définition 70 : Dilatation [Rombaldi, p.150] :
On considère φ une forme linéaire non nulle sur E.
On appelle **dilatation d'hyperplan** $\mathrm{Ker}(\varphi)$ toute application linéaire $u \in \mathcal{L}(E)$ définie par :

$$\forall x \in E,\ u(x) = x + \varphi(x)a,\ a \in E \backslash \mathrm{Ker}(\varphi)$$

Théorème 71 : [Rombaldi, p.150]
Une dilatation $\delta_{\varphi,a}$ est dans $\mathrm{GL}(E)$ si, et seulement si, $\lambda = 1 + \varphi(a) \neq 0$.

Théorème 72 : [Rombaldi, p.150]
∗ Un automorphisme $u \in \mathrm{GL}(E)$ est une dilatation si, et seulement si, il existe un hyperplan H tel que $u|_H = \mathrm{Id}_H$ et u diagonalisable de valeurs propres 1 et $\lambda \in \mathbb{K}\backslash\{0;1\}$ (donc $E = \mathrm{Ker}(u - \mathrm{Id}_E) \oplus \mathrm{Ker}(u - \lambda \mathrm{Id}_E)$).
∗ Le conjugué dans $\mathrm{GL}(E)$ d'une dilatation est une dilatation de même rapport.
∗ Une dilatation u de rapport λ admet un polynôme minimal qui est $(X-1)(X-\lambda)$.
∗ L'inverse d'une dilatation de rapport λ est une dilatation de rapport $\frac{1}{\lambda}$.

Théorème 73 : [Rombaldi, p.152]
Soit $u \in \mathrm{GL}(E)$.
Les assertions suivantes sont équivalentes :
∗ u est une dilatation de rapport λ.
∗ Il existe une base de E dans laquelle la matrice de u est de la forme $I_n + (\lambda - 1)E_{n,n}$ avec $\lambda \in \mathbb{K}\backslash\{0;1\}$.

Développement 2 : [cf. ROMBALDI]

Théorème 74 : [Rombaldi, p.688]
Soit $A \in \mathrm{GL}_n(\mathbb{K})$.
A s'écrit sous la forme $A = \prod_{k=1}^{r} P_k D_n(\lambda) \prod_{j=1}^{s} Q_j$, où les P_k et Q_j sont des matrices de transvections et $\lambda = \det(A)$.

Corollaire 75 : [Rombaldi, p.689]
Les groupes $\mathrm{SL}_n(\mathbb{R})$, $\mathrm{SL}_n(\mathbb{C})$ et $\mathrm{GL}_n(\mathbb{C})$ sont connexes par arcs.

Corollaire 76 : [Rombaldi, p.689]
Le groupe $\mathrm{GL}_n(\mathbb{R})$ n'est pas connexe et ses deux composantes connexes sont $\mathrm{GL}_n^+(\mathbb{R})$ et $\mathrm{GL}_n^-(\mathbb{R})$.

Corollaire 77 : [Francinou, p.343]
Le groupe $\mathrm{GL}_n(\mathbb{R})$ est engendré par les matrices diagonalisables inversibles.

Théorème 78 : [Rombaldi, p.154]
Pour $n \geq 2$, on a :
∗ $D(\mathrm{SL}_n(\mathbb{K})) \subseteq D(\mathrm{GL}_n(\mathbb{K})) \subseteq \mathrm{SL}_n(\mathbb{K})$.
∗ Pour $n \geq 3$, $D(\mathrm{SL}_n(\mathbb{K})) = D(\mathrm{GL}_n(\mathbb{K})) = \mathrm{SL}_n(\mathbb{K})$.
∗ Pour $n = 2$, $\mathbb{K} \neq \mathbb{F}_2$ et $\mathbb{K} \neq \mathbb{F}_3$, $D(\mathrm{SL}_n(\mathbb{K})) = D(\mathrm{GL}_n(\mathbb{K})) = \mathrm{SL}_n(\mathbb{K})$.

IV.2 Le groupe orthogonal

Dans toute cette sous-partie, on suppose que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ et on muni E d'un produit scalaire noté $< \cdot;\cdot >$ de sorte que $(E, < \cdot;\cdot >)$ soit un espace euclidien de dimension $n \in \mathbb{N}^*$.

Théorème 79 : [Rombaldi, p.724]
$\mathrm{SO}_n(\mathbb{R})$ est un sous-groupe distingué de $\mathrm{O}_n(\mathbb{R})$ d'indice 2.

Proposition 80 : [Audin, p.62]
Le groupe $\mathrm{SO}_2(\mathbb{R})$ est abélien.

Théorème 81 : Théorème de Cartan-Dieudonné [Perrin, p.143] :
Tout élément f de $\mathrm{O}(E)$ est produit d'exactement $n - p$ réflexions (avec p la dimension de $\mathrm{Ker}(f - \mathrm{Id}_E)$).

Théorème 82 : [Audin, p.86]
Si E est de dimension 2, alors pour $f \in \mathrm{O}(E)$:
∗ Si $\det(f) = 1$, alors f est une rotation.
De plus, si $f \neq \mathrm{Id}_E$, alors l'ensemble $D = \{x \in E \text{ tq } f(x) = x\}$ est une droite de E et $f|_{D^\perp}$ est une rotation du plan vectoriel $D^\top$ (on dit que D est l'axe de la rotation f).
∗ Sinon $\det(f) = -1$ alors soit f est une réflexion par rapport à un plan, soit il existe une rotation $r \in \mathrm{SO}(E)$ d'axe D telle qu'en notant s la réflexion par rapport au plan $D^\perp$, on a $f = r \circ s = s \circ r$ (on dit que f est une antirotation).

Théorème 83 : [Audin, p.143]
Si E est de dimension 3, alors pour $f \in \mathrm{O}(E)$:
∗ Si $\det(f) = 1$, alors f est une rotation.
∗ Sinon $\det(f) = -1$ et f est une réflexion par rapport à une droite.

Théorème 84 : [Perrin, p. 143]
Pour $n \geq 3$, tout élément de $\mathrm{SO}_n(\mathbb{R})$ est produit d'au plus n renversements.

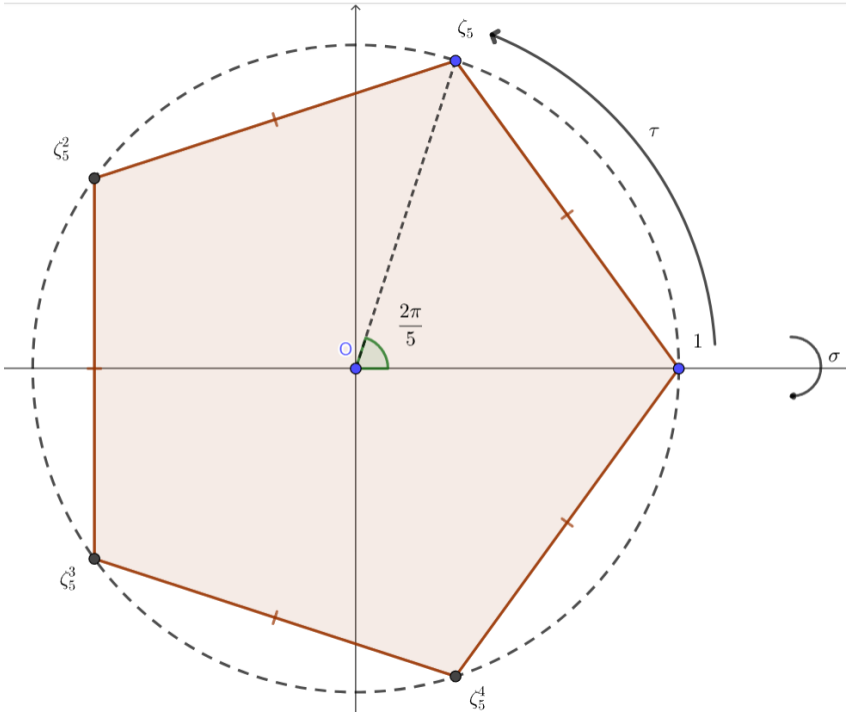
Théorème 85 : [Francinou (2), p.67]
Le groupe $\mathrm{SO}_3(\mathbb{R})$ est simple.

V Annexe

V.1 Correspondance entre $\mathfrak{S}_4$ et $\mathrm{Isom}(\mathcal{T})$

$\mathfrak{S}_4$	$\mathrm{Isom}(\mathcal{T})$	Cardinal
$\mathrm{Id}_{[\![1;n]\!]}$	Identité	1
(1 2)	Réflexion par rapport au plan médiateur d'une arête	6
(1 2 3)	Rotation d'axe une hauteur du tétraèdre et d'angle $\pm\frac{2\pi}{3}$	8
(1 2 3 4)	Anti-rotation d'axe passant par les milieux de deux arêtes opposées et d'angle $\pm\frac{\pi}{2}$	6
(1 2)(3 4)	Rotation d'axe passant par les milieux de deux arêtes opposées et d'angle $\pm\pi$	3

V.2 Illustration géométrique de D_{10}



V.3 Classification des isométries vectorielles en dimension 2

$\dim(\mathrm{Ker}(f-\mathrm{Id}_E))$	Isom. vect. f en dim. 2	$\det(f)$	Réduction matricielle
0	Rotation (différente de Id_E)	$+1$	$\begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix}$ dans toute B.O.N.
1	Réflexion par rapport à une droite	-1	$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ dans une B.O.N. bien choisie
2	Id_E	$+1$	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ dans une B.O.N. bien choisie

V.4 Classification des isométries vectorielles en dimension 3

$\dim(\mathrm{Ker}(f-\mathrm{Id}_E))$	Isom. vect. f en dim. 3	$\det(f)$	Réduction matricielle
0	Antirotation d'axe une droite	-1	$\begin{pmatrix}-1 & 0 & 0\\ 0 & \cos(\theta) & -\sin(\theta)\\ 0 & \sin(\theta) & \cos(\theta)\end{pmatrix}$ dans une B.O.N. bien choisie
1	Rotation d'axe une droite	$+1$	$\begin{pmatrix}1 & 0 & 0\\ 0 & \cos(\theta) & -\sin(\theta)\\ 0 & \sin(\theta) & \cos(\theta)\end{pmatrix}$ dans une B.O.N. bien choisie
2	Réflexion par rapport à un plan	-1	$\begin{pmatrix}-1 & 0 & 0\\ 0 & \cos(\theta) & -\sin(\theta)\\ 0 & \sin(\theta) & \cos(\theta)\end{pmatrix}$ dans une B.O.N. bien choisie
3	Id_E	$+1$	$\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$ dans toute B.O.N.

Remarques sur le plan

— Les parties génératrices sont très utiles car elles permettent de réduire l'étude d'un groupe à ses générateurs et d'en déduire des résultats sur la simplicité, de classification ou encore de propriétés sur des morphismes.

— On peut également insister sur la notion de groupe libre et de relations.

Liste des développements possibles

— Classification des groupes d'ordre p^2 et $2p$.

— Groupe des isométries du cube.

— Simplicité de $\mathfrak{A}_n$ pour $n = 3$ ou $n \geq 5$.

— Générateurs de $\mathrm{SL}_n(\mathbb{K})$ et $\mathrm{GL}_n(\mathbb{K})$.

— Simplicité de $\mathrm{SO}_3(\mathbb{R})$.

Bibliographie

— Grégory Berhuy, *Algèbre : le grand combat*.

— Daniel Perrin, *Cours d'algèbre*.

— Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et Géométrie*.

— François Combes, *Algèbre et géométrie*.

— Jean Delcourt, *Théorie des groupes*.

— Serge Francinou, *Exercices de mathématiques, Oraux X-ENS, Algèbre 2*.

— Michèle Audin, *Géométrie*.

— Serge Francinou, *Exercices de mathématiques, Oraux X-ENS, Algèbre 3*.