108 — Exemples de parties génératrices d'un groupe. Applications.

Introduction : deux définitions équivalentes.

Soit G un groupe, noté multiplicativement, et $A \subset G$ une partie.

Déf : On note $\langle A \rangle = \bigcap_{A \subset H} H$ l'intersection des sous-groupes de G contenant A, c'est le groupe engendré par A.

Déf : A est une partie génératrice de G si $\langle A \rangle = G$.

Prop : $\langle A \rangle = \{x \in G \mid \exists n \geq 1, \exists x_1, \dots, x_n \in A \cup A^{-1}, x = x_1 \dots x_n\}$.

I – Groupes abéliens

1) Groupes monogènes.

Déf : Un groupe est dit monogène s'il est engendré par un seul élément, et cyclique s'il est monogène et fini.

Exple : Pour tout $n \geq 1$, le sous-groupe de $\mathbb{C}^*$ des racines n-ièmes de l'unité est cyclique.

Prop : Tout groupe monogène G est abélien, et plus précisément G est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$ pour un entier $n \geq 1$.

Prop : Soit $a \in \mathbb{Z}$ et $n \geq 1$. Sont équivalents :

(1) $\bar{a}$ engendre $\mathbb{Z}/n\mathbb{Z}$

(2) a est premier avec n.

(3) $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$.

Application : $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.

Thm : Soit K un corps. Tout sous-groupe fini de K^* est cyclique.

(NB : une preuve simple repose sur la notion d'exposant)

Exple : $(\mathbb{Z}/7\mathbb{Z})^*$ est un groupe cyclique d'ordre 6, $\bar{3}$ et $\bar{5}$ sont des générateurs.

2) Groupes abéliens finis.

Prop : Soit p un nombre premier et G un p-groupe abélien fini. Alors il existe une unique suite $m_1 \geq \dots \geq m_r \geq 1$ tel que $G \simeq \mathbb{Z}/p^{m_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{m_r}\mathbb{Z}$.

Prop : Soit G abélien fini, et p premier. L'ensemble $G(p)$ des éléments de G d'ordre une puissance de p est un sous-groupe.

Th ("Facteurs élémentaires") $G \simeq G(p_1) \times \dots \times G(p_s)$

Th ("Facteurs invariants") Soit G abélien fini (non trivial). Il existe une unique suite $(a_i)_{i=1}^{s}$, $a_{i+1} \mid a_i$, $a_s \geq 2$ tel que $G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \dots \mathbb{Z}/a_s\mathbb{Z}$. En particulier, a_1 est l'exposant de G et $\prod_{i=1}^{s} a_i$ son ordre.

DEV 1

<u>Exple</u> : A isomorphisme près il existe quatre groupes abéliens d'ordre 36 :

$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \simeq \mathbb{Z}/6 \times \mathbb{Z}/6$

$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/9 \simeq \mathbb{Z}/18 \times \mathbb{Z}/2$

$\mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \simeq \mathbb{Z}/12 \times \mathbb{Z}/3$

$\mathbb{Z}/4 \times \mathbb{Z}/9 \simeq \mathbb{Z}/36$

3) Groupes abéliens de type fini.

<u>Def</u> : Un groupe est de <u>type fini</u> s'il est engendré par une partie finie.

<u>Exple</u> : Pour tout $n \geq 1$, $\mathbb{Z}^n$ est un groupe infini de type fini.

<u>Contre-exemple</u> : $\mathbb{Q},+$ n'est pas de type fini.

<u>Thm</u> : Tout groupe abélien de type fini est isomorphe à un produit $\mathbb{Z}^n \times G$ avec $n \geq 0$ et G abélien fini.

II - <u>Groupes symétriques</u>

1) Groupe S_n.

<u>Prop</u> : Le groupe S_n est engendré par les k-cycles, et plus précisément tout $\sigma \in S_n$ s'écrit de façon unique (à l'ordre près) comme un produit de cycles à support disjoint.

<u>Cor</u> : le groupe S_n est engendré par :

(a) les transpositions $(i\,j)$

(b) les transpositions $(1\,i)$

(c) les transpositions $(i\;\,i+1)$

(d) (12) et $(12 \dots n)$.

<u>Application</u> : Le morphisme <u>signature</u> est l'unique morphisme non trivial de S_n vers $\mathbb{C}^*$.

2) Groupe alterné A_n

<u>Prop</u> : (1) $\forall n \geq 2$, A_n est engendré par les 3-cycles.

(2) $\forall n \geq 5$, les 3-cycles sont deux à deux conjugués dans A_n.

<u>Application</u> : le groupe A_n est simple pour $n \geq 5$.

III - <u>Groupes de matrices</u>

1) Quelques groupes classiques.

<u>Def</u> : Une matrice de <u>dilatation</u> est une matrice conjuguée dans $GL_n(K)$ à $\begin{pmatrix} \lambda & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix}$ avec $\lambda \neq 1$.

Une matrice de <u>transvection</u> est une matrice conjuguée à $\left(\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 1 & \\ \hline 0 & & \begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix} \end{array}\right)$.

Prop : Soit K un corps, et $n \geq 1$.

(1) $SL_n(K)$ est engendré par les transvections.

(2) Si car $K \neq 2$, $GL_n(K)$ est engendré par les dilatations.

Application : $PSL_n(K)$ est simple pour $n \geq 2$, sauf dans les cas $n=2$ et $K = \mathbb{F}_2, \mathbb{F}_3$.

Def : Dans le groupe orthogonal $O_n(\mathbb{R})$, une réflexion est une matrice conjuguée à $\mathrm{diag}(-1,1,\dots,1)$ et un renversement une matrice conjuguée à $\mathrm{diag}(-1,-1,1,\dots,1)$.

Prop : $O_n(\mathbb{R})$ est engendré par les réflexions et $SO_n(\mathbb{R})$ est engendré par les renversements.

2) Groupe diédral

Def : Le groupe des isométries du plan préservant un polygone régulier à n côtés est appelé groupe diédral, noté D_n.

Prop : D_n est d'ordre $2n$, et le sous-groupe des rotations dans D_n est cyclique d'ordre n.

Prop : Tout groupe engendré par 2 involutions a, b est isomorphe au groupe diédral D_n, avec $n =$ ordre (ab).

Variante : Tout groupe engendré par a d'ordre 2 et b d'ordre n, tel que $(ab)^2 = 1$, est isomorphe à D_n.

3) Groupe $SO_3(\mathbb{R})$

Application : Le critère précédent est utile dans la classification des sous-groupes finis de $SO_3(\mathbb{R})$.

Prop : $SO_3(\mathbb{R})$ est compact et connexe. Précisément, $SO_3(\mathbb{R})$ est la composante connexe de l'identité dans $O_3(\mathbb{R})$.

Application : Le groupe $SO_3(\mathbb{R})$ est simple.

Thm : Il existe un isomorphisme "exceptionnel"

$$SU_2(\mathbb{C}) / \pm id \simeq SO_3(\mathbb{R}).$$

DEV 2

Remarque : Le fait que les renversements engendrent admet une preuve simple dans le cas $n=3$.

Application : Tout groupe fini d'ordre impair dans $SU_2(\mathbb{C})$ est cyclique.

chaque vecteur non nul ${}^t(x, y, z, t)$ le vecteur tangent ${}^t(-\,y, x, -t, z)$, ou ${}^t(-\,z, t, x, -y)$, ou ${}^t(-\,t, -z, y, x)$, qui ne s'annulent pas.

À nouveau, si l'on juxtapose le point de la sphère et les trois vecteurs tangents choisis, on retrouve la représentation matricielle réelle des quaternions.

En dimension 8

Le cas $n = 8$ du théorème d'Adams peut être réalisé dans l'espace de dimension 8 des octonions, qui engendre stupeur et tremblements quand on sait que la chose est munie d'une multiplication non commutative et non associative... Voir l'exercice C.5.

3. Applications à SO(3)

C'est ici que l'on comprendra pourquoi $\mathbb{H}$ fut le Graal d'Hamilton : un outil puissant pour faire de la géométrie en dimension 3.

La norme $N(h) = h\overline{h}$ est une forme quadratique réelle définie positive sur $\mathbb{H}$; la base $(\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k})$ est orthonormée et la forme bilinéaire symétrique associée est donnée par :

$$\forall h, h' \in \mathbb{H}, \quad \langle h, h' \rangle = \frac{1}{2}(h\overline{h}' + h'\overline{h}).$$

(On l'a sans calcul par unicité de la forme bilinéaire symétrique associée.)

Notons que le sous-espace $\mathbb{I}$ des imaginaires de $\mathbb{H}$ est l'orthogonal de $\mathbb{R} = \mathbb{R}\mathbf{1}$ et que $\mathrm{SU}(2) \simeq \mathbf{S}^3$ agit sur $\mathbb{H}$ par automorphismes d'algèbres :

$$\begin{array}{rcl} \varphi : \mathrm{SU}(2) & \longrightarrow & \mathrm{Aut}(\mathbb{H}) \\ h & \longmapsto & \varphi_h : \mathbb{H} \longrightarrow \mathbb{H} \\ & & \qquad u \longmapsto huh^{-1}. \end{array}$$

L'application φ_h est linéaire et respecte la norme de $\mathbb{H}$, car $N(huh^{-1}) = N(u)$. Comme $\mathbf{1}$ est central dans $\mathbb{H}$, l'action de $\mathrm{SU}(2)$ préserve $\mathbb{R}$, donc elle préserve aussi son orthogonal $\mathbb{I}$. Considérons alors :

$$\begin{array}{rcl} \varphi : \mathrm{SU}(2) & \longrightarrow & \mathrm{O}(\mathbb{I}) \\ h & \longmapsto & \varphi_h : \mathbb{I} \longrightarrow \mathbb{I} \\ & & \qquad u \longmapsto huh^{-1}. \end{array}$$

Via le choix d'une base, qui donne un isomorphisme entre les isométries de $\mathbb{I}$ et le groupe orthogonal $\mathrm{O}(3)$, on définit un morphisme, noté avec un abus par la même lettre : $\varphi : \mathrm{SU}(2) \to \mathrm{O}(3)$.

Par continuité (on n'utilise que des additions, des multiplications et des inverses non nuls), on peut affirmer que l'image $\varphi(\mathrm{SU}(2))$ est connexe et, comme elle contient l'identité, que l'on dispose d'un morphisme φ qui applique SU(2) dans SO(3).

Montrons que ce morphisme est surjectif.

3.1. Rappel. Le résultat suivant est prouvé dans l'annexe A.

- Un système de générateurs de $\mathrm{O}(n)$ est donné par les réflexions orthogonales, qui ont pour matrice, dans une base orthonormée convenable :

$$\begin{pmatrix} \mathrm{I}_{n-1} & \\ & -1 \end{pmatrix}.$$

- Un système de générateurs de $\mathrm{SO}(n)$ est donné par les retournements (demi-tours), qui ont pour matrice, dans une base orthonormée convenable :

$$\begin{pmatrix} \mathrm{I}_{n-2} & \\ & -\mathrm{I}_2 \end{pmatrix}.$$

Pour la surjectivité, il suffit donc de montrer que tous les retournements de $\mathrm{SO}(\mathbb{I}) \simeq \mathrm{SO}(3)$ sont dans $\varphi(\mathrm{SU}(2))$.

Soit $h \in \mathbb{I} \cap \mathbf{S}^3$ et r_h le retournement d'axe $\mathbb{R}h$. On montre que $r_h = \varphi_h$. Pour cela, il suffit de montrer que l'on a :

1. $\varphi_h(h) = h$,
2. $\varphi_h(h') = -h'$ si $\langle h, h' \rangle = 0$.

La première assertion est claire, car l'on a : $\varphi_h(h) = hhh^{-1} = h$.

Quant à la deuxième, on fixe h' orthogonal à h. Il vient : $h'\overline{h} + h\overline{h'} = 0$ donc, puisque h est imaginaire pur : $h'(-h) + h(-h') = 0$, et de là, facilement : $hh'h^{-1} = -h'$.

Donc, l'application $\varphi : \mathrm{SU}(2) \to \mathrm{SO}(3)$ est surjective.

De plus, le noyau de φ est l'intersection du centre de $\mathbb{H}$ avec la sphère unité, il est donc isomorphe, par 1.1.8, au groupe des réels de norme 1. Il vient donc $\operatorname{Ker}\varphi = \{\pm \mathrm{I}_2\}$, d'où l'isomorphisme (par passage au quotient) apparaissant dans la proposition suivante.

3.2. Proposition. *Il existe un* isomorphisme exceptionnel *explicite de groupes*

$$\overline{\varphi} : \mathrm{SU}(2)/\{\pm \mathrm{I}_2\} \simeq \mathrm{SO}(3).$$

De plus :

$$\overline{\varphi} : \mathbb{H}^*/\mathbb{R}^* \simeq S^3 \simeq \mathrm{SU}(2).$$

3.3. Remarque

- On a en prime une interprétation topologique : SO(3) est homéomorphe à $\mathbb{P}^3(\mathbb{R})$, quotient $\mathbf{S}^3/\{\pm \mathrm{I}_3\}$ de la sphère $\mathbf{S}^3$ par l'antipode.
- Application en calcul formel, et dans les logiciels de simulation de vol, où les calculs de rotations sont effectués dans $\mathbb{H}$ plutôt que dans SO(3) directement.
- Voici un supplément pour les lecteurs qui ont quelques bases de topologie algébrique. Comme SU(2) est la sphère $\mathbf{S}^3$, donc simplement connexe, et comme $\{\mathrm{I}_2, -\mathrm{I}_2\}$ est discret, cela prouve que SU(2) est le revêtement universel de SO(3) et donc que le groupe fondamental de SO(3) est $\mathbb{Z}/2\mathbb{Z}$. En illustration, on a le fameux principe de l'assiette à soupe : si l'on pose sur sa main une assiette et que l'on fait faire à son bras deux rotations de 360^o dans le même sens en maintenant l'assiette horizontale, le bras ne se tord pas deux fois, mais revient à sa position initiale. En aucun cas, la rédaction n'est responsable d'accidents survenus en expérimentant ce beau théorème de topologie.

4. Applications à SO(4)

Avec un tout petit effort supplémentaire, nous allons aussi réaliser SO(4). Bien sûr, cette fois-ci, SU(2) tout seul, trop petit, ne va pas suffire. On considère donc l'action de SU(2) × SU(2) sur $\mathbb{H}$ par automorphismes :

$$\begin{array}{rcl} \psi : \mathrm{SU}(2) \times \mathrm{SU}(2) & \longrightarrow & \mathrm{Aut}(\mathbb{H}) \\ (h,k) & \longmapsto & \psi_{h,k} : \mathbb{H} \longrightarrow \mathbb{H} \\ & & \qquad\quad u \longmapsto huk^{-1}. \end{array}$$

Comme avant, on obtient un morphisme : $\psi : \big(SU(2) \times \mathrm{SU}(2)\big) \to \mathrm{SO}(4)$. Montrons qu'il est surjectif.

Soit P un plan quelconque de $\mathbb{H}$, on veut montrer que le retournement par rapport à P est dans l'image de ψ. Pour cela, choisissons une base orthonormée (p,q) de P. On calcule :

$$\overline{p^{-1}q} = \overline{q}\,\overline{p^{-1}} = \overline{q}\,p = -\overline{p}\,q = -p^{-1}q.$$

Par suite, $v := p^{-1}q \in \mathbb{I}$.

D'après le paragraphe sur SO(3), cela implique que $\psi_{v,v}$ est un retournement, et donc que son conjugué $\psi_{p,1}\psi_{v,v}\psi_{p^{-1},1} = \psi_{pvp^{-1},v}$ est aussi un retournement.

De plus, on vérifie facilement que $\psi_{pvp^{-1},v}(p) = p$ et $\psi_{pvp^{-1},v}(q) = q$. C'est donc bien le retournement cherché.

Leçons où l'on peut utiliser le développement "Isomorphisme exceptionnel $\mathrm{SU}_2\,/\pm 1 \simeq \mathrm{SO}_3$":

- 101. Groupe opérant sur un ensemble. Exemples et applications.
- 106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E).Applications.
- 108. Exemples de parties génératrices d'un groupe. Applications.
- 154. Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.
- 160. Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).
- 161. Isométries d'un espace affine euclidien de dimension finie. Applications en dimensions 2 et 3.
- 170. Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.
- 171. Formes quadratiques réelles. Coniques. Exemples et applications.
- 182. Applications des nombres complexes à la géométrie.
- 183. Utilisation des groupes en géométrie.

Leçons où l'on peut utiliser le développement "Structure des groupes abéliens finis":

- 102. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.
- 103. Exemples de sous-groupes distingués et de groupes quotients. Applications.
- 104. Groupes finis. Exemples et applications.
- 107. Représentations et caractères d'un groupe fini sur un C-espace vectoriel. Exemples.
- 108. Exemples de parties génératrices d'un groupe. Applications.
- 110. Structure et dualité des groupes abéliens finis. Applications.
- 159. Formes linéaires et dualité en dimension finie. Exemples et applications.

Leçons où l'on peut utiliser le développement "Simplicité de A_n pour $n \geq 5$":

- 101. Groupe opérant sur un ensemble. Exemples et applications.
- 103. Exemples de sous-groupes distingués et de groupes quotients. Applications.
- 104. Groupes finis. Exemples et applications.
- 105. Groupe des permutations d'un ensemble fini. Applications.
- 108. Exemples de parties génératrices d'un groupe. Applications.