Exemples de parties génératrices d'un groupe. Applications.

I) Partie génératrice

Déf 1 : Soit $(G, \cdot)$ un groupe et X une partie non vide de G.
Le groupe engendré par X est : $\langle X \rangle = \left\{ \prod_{i=1}^{n} x_i^{\varepsilon_i},\ x_i \in X,\ \varepsilon_i \in \{-1,0,1\},\ n \in \mathbb{N} \right\}$

Exple 2 : Le groupe dérivé de G est $D(G) = \langle [a,b],\ a,b \in G \rangle$.

Déf 3 : Soit $x \in G$, on note $\langle x \rangle := \langle \{x\} \rangle = \{x^n,\ n \in \mathbb{Z}\}$ le groupe engendré par x.

Exple 4 : Les sous groupes de $(\mathbb{R},+)$ sont de la forme $a\mathbb{Z}$, $a \geq 0$ ou bien sont denses dans $\mathbb{R}$.

Appli 5 : • $\exists!\, \pi > 0$ tq $\ker(\exp) = 2i\pi\mathbb{Z}$.
• $\forall \theta \notin \pi\mathbb{Q}$, $\{e^{in\theta},\ n \in \mathbb{Z}\}$ est une partie dense de $\mathbb{U}$.

II) Groupes monogènes

1) Classification des groupes monogènes

Déf 6 : On dit qu'un groupe G est monogène si $\exists\, g \in G$ tel que $G = \langle g \rangle$
On dit que G est cyclique si G est monogène et fini.

Exple 7 : $\mathbb{Z} = \langle 1 \rangle$ est monogène. De plus, 1 ou -1 sont les générateurs possibles.
$\forall n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est cyclique. Il possède $\varphi(n)$ générateurs, les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Th 8 : Soit G un groupe monogène, alors G est abélien. De plus,
si $|G| = +\infty$, alors $G \simeq \mathbb{Z}$ et si $|G| = n$, alors $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Exple 9 : $\forall n \in \mathbb{N}^*$, $\mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$ est engendré par l'une des $\varphi(n)$ racines $n^{\text{ièmes}}$ primitives.

2) Propriétés des groupes cycliques

Prop 10 : Si $G = \langle g \rangle$ est d'ordre n, ses générateurs sont les g^k, $k \in [\![1, n-1]\!]$, $k \wedge n = 1$

Prop 11 : Les sous groupes de G sont tous cycliques, d'ordre divisant $|G|$.

Th 12 : Pour tout d diviseur positif de $n = |G|$, il existe un unique ss groupe d'ordre d de G.
Ce groupe est le groupe cyclique $H = \langle g^{\frac{n}{d}} \rangle$.

3) Groupe des inversible d'un corps fini

Th de Wedderburn : Soit $\mathbb{K}$ un corps fini, alors $(\mathbb{K}^*, \times)$ est commutatif.

Prop 15 : Soit G un groupe abélien fini, alors $\exists\, x \in G$ tq $o(x) = \mathrm{ppcm}_{g \in G}\, o(g)$

Th 16 : $(\mathbb{F}_q^*, \times)$ est cyclique. En particulier, $\mathbb{F}_q^* \simeq \mathbb{Z}/(q-1)\mathbb{Z}$

DVPT ①

Appli 17 : Soit G un groupe d'ordre pq avec $p, q \in \mathbb{P}$, $p < q$.
• Si $q \not\equiv 1\ [p]$, alors $G \simeq \mathbb{Z}/pq\mathbb{Z}$
• Si $q \equiv 1\ [p]$, alors $G \simeq \mathbb{Z}/pq\mathbb{Z}$ ou bien $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$
où $\alpha : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est la seule action non triviale

Appli 18 : Théorème de Gauss-Wantzel
Soit $N \geq 2$. Le N-gône est constructible (à la règle et au compas)
$\Leftrightarrow N = 2^\alpha p_1 \cdots p_r$ avec $\alpha \in \mathbb{N}$, $p_1, \dots, p_r$ nbs 1^{ers} de Fermat distincts

III) Parties génératrices de groupes finis

1) Groupes abéliens finis

Soit $(G, \cdot)$ un groupe abélien fini.

Prop 19 : G et son groupe dual $\widehat{G}$ ont le même exposant.

Th de structure des groupes abéliens finis :

$\exists!\, r \in \mathbb{N}^*$, $\exists!\, n_1, \dots, n_r \geq 2$ tel que $n_1 | n_2 | \dots | n_r$ et $G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$.

Rq 21 : Dans ce cas, G est engendré par exactement r éléments

Expl 22 : Il existe, à isomorphisme près, 3 groupes abéliens d'ordre 24 :

$\mathbb{Z}/24\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

2) Groupe symétrique

Déf 23 : $\forall n \in \mathbb{N}^*$, on note σ_n le groupe des permutations d'un ensemble à n éléments.

On a $|\sigma_n| = n!$

Prop 24 : Toute permutations de σ_n peut se décomposer en produit d'au plus $n-1$ transpositions.

Prop 25 : $\sigma_n = \langle (1, i) \,,\, i \in [\![2, n]\!] \rangle$ ou $\sigma_n = \langle (i, i+1) \,,\, i \in [\![1, n-1]\!] \rangle$

Appli 26 : On a $\sigma_4 \simeq \mathrm{Isom}^+(\text{cube})$.

On peut alors donner la table des caractères de σ_4.

Appli 27 : $\forall n \neq 6$, les automorphismes de σ_n sont intérieurs.

Appli 28 : Il existe un unique morphisme ε de σ_n dans $\mathbb{C}^*$ appelé signature.

Déf 29 : On pose $A_n = \mathrm{Ker}(\varepsilon)$ le groupe alterné d'indice n. On a $|A_n| = \frac{n!}{2}$.

Prop 30 : $\forall n \geq 3$, A_n est $n-2$ transitif

Prop 31 : $\forall n \geq 3$, A_n est engendré par les 3-cycles

DV (2) **Appli 32 :** $\forall n \geq 5$, A_n est simple

Coro 33 : $\forall n \geq 5$, $D(A_n) = A_n$ et $D(\sigma_n) = A_n$.

Th 34 : $\sigma_n = \langle (1,2) \,,\, (1, 2, \dots, n) \rangle$

3) Groupe diédral

Déf 35 : Soit $n \geq 3$. On note $\mathbb{D}_n$ le groupe des isométries affines du plan qui laissent invariant le n-gône.

Prop 36 : On note r la rotation de centre O et d'angle $\frac{2\pi}{n}$

et s la symétrie par rapport à l'axe des abscisses.

alors : $r^4 = 1$; $s^2 = 1$ et $srs = r^{-1}$.

Prop 37 : On a $|\mathbb{D}_n| = 2n$ et $\mathbb{D}_n = \langle r, s \rangle$

Prop 38 : On a $\mathrm{Mat}_{\mathcal{B}_c}(r) = \begin{pmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix}$ et $\mathrm{Mat}_{\mathcal{B}_c}(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Appli 39 : On en déduit la table des caractères de $\mathbb{D}_4$

IV Parties génératrices de groupes (potentiellement) infinis

Soit $\mathbb{K}$ un corps commutatif et E un $\mathbb{K}$-ev de dimension $n \in \mathbb{N}^*$.

1) Le groupe linéaire

Déf 40 : On note $GL(E)$ le groupe des isomorphismes linéaires de E.
et $SL(E) = \mathrm{Ker}(\det)$ le groupe spécial linéaire de E.

Déf - Prop 41 : Soit H un hyperplan de E et $u \in GL(E)$ tq $u_{|H} = Id_H$. Alors :
$\det(u) = \lambda \neq 1$. (ie $u \notin SL(E)$)
$\iff$ u admet une valeur propre $\lambda \neq 1$.
$\iff$ $\mathrm{Im}(u - Id) \not\subset H$
$\iff$ Dans une base convenable, on a $Mat_B(u) = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$ pour $\lambda \neq 1$

On dit alors que u est une dilation d'hyperplan $H = \mathrm{Ker}(u - Id)$, de droite $D = \mathrm{Im}(u - Id)$ et de rapport λ.

Déf - Prop 42 : Soit H un hyperplan de E d'équation $f \in E^*$ et $u \in GL(E)$, $u_{|H} = Id_H$, $u \neq Id_E$
$\det(u) = 1$. (ie $u \in SL(E)$)
$\iff$ u n'est pas diagonalisable
$\iff$ $D = \mathrm{Im}(u - Id) \subset H$
$\iff$ $\exists\, a \in H \setminus \{0\}$ tq $\forall x \in E$, $u(x) = x + f(x)\, a$
$\iff$ Dans une base convenable, on a $Mat_B(u) = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & 1 \\ 0 & & & 1 \end{pmatrix}$

On dit alors que u est une transvection d'hyperplan H et de droite D.

Lemme : Soient $x, y \in E \setminus \{0\}$. Il existe une transvection u v tel que $u(x) = y$ ou $uv(x) = y$

Th 44 : Les transvections engendrent $SL(E)$
Les transvections et les dilations engendrent $GL(E)$.

Appli 45 : $SL_n(\mathbb{R})$ est connexe par arcs ; $GL_n(\mathbb{C})$ est connexe par arcs.

2) Le groupe orthogonal

Ici E est un espace euclidien

Déf 46 : on note $O(E)$ le groupe des isométries linéaires de E
et $SO(E) = O(E) \cap \det^{-1}(\{1\})$ le groupe spécial orthogonal

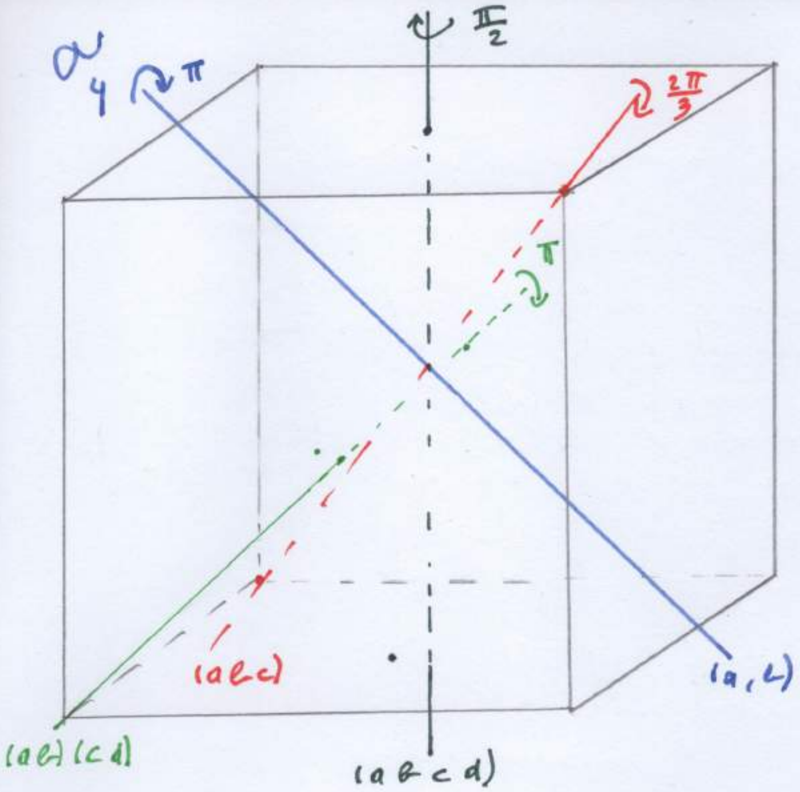
Déf - Prop 47 : Soit $u \in O(E)$ tq $u^2 = Id$. On note $E_1 = \mathrm{Ker}(u - Id)$ et $E_{-1} = \mathrm{Ker}(u + Id)$
alors $E = E_1 \oplus E_{-1}$; $u_{E_1} = Id_{E_1}$ et $u_{E_{-1}} = -Id_{E_{-1}}$.

Si $u \neq Id_E$, on dit que u est une symétrie ;
Si $\dim(E_{-1}) = 1$, on dit que u est une réflexion ;
Si $\dim(E_{-1}) = 2$, on dit que u est un renversement.

Th 48 : Tout élément $u \in O(E)$ est produit d'au plus n réflexions.
Tout élément $u \in SO(E)$ est produit d'au plus n renversements.

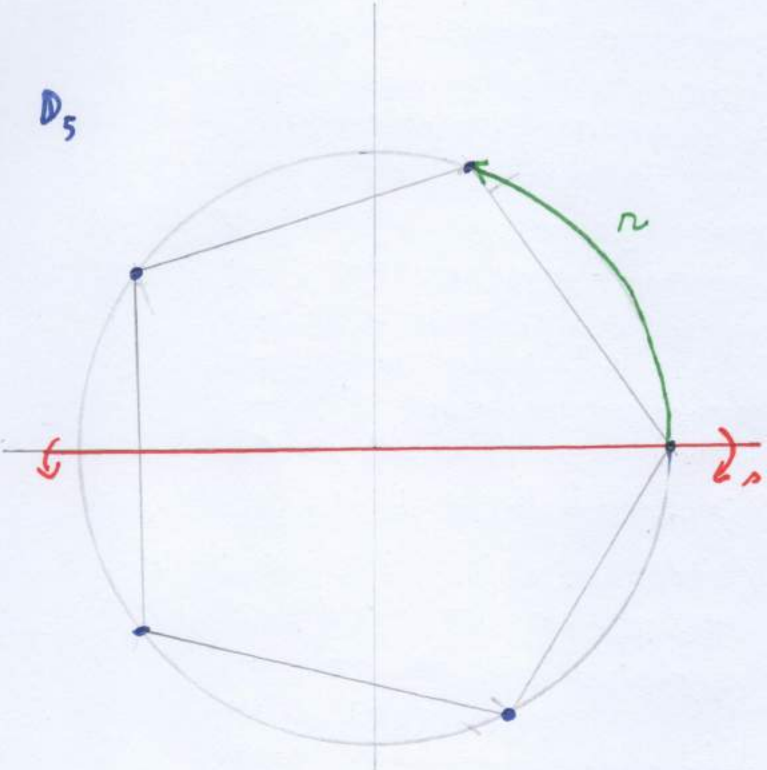
Appli 49 : $SO_3(\mathbb{R})$ est simple.

Appli 50 : $SO_n(\mathbb{R})$ est connexe par arcs.



σ_4	[1]	[2]	[2,2]	[3]	[4]
1	1	1	1	1	1
ε	1	-1	1	1	-1
χ_4	2	0	2	-1	0
χ_s	3	1	-1	0	-1
χ_c	3	-1	-1	0	1

D_5



D_4	Id	-Id	r	s	rs
1	1	1	1	1	1
χ_r	1	1	-1	1	-1
χ_s	1	1	1	-1	-1
χ_{rs}	1	1	-1	-1	1
χ_4	2	-2	0	0	0

$5 = 2^0 . (2^2 + 1)$

Le pentagone est constructible

<u>Référence</u> : Perrin (cours + dev x 2)