108 Exemples de parties génératrices d'un groupe et applications.

Déf 1: Soit $S \subset G$, on peut définir la partie engendrée par S, $\langle S \rangle$ de deux façons : • de l'extérieur $\langle S \rangle = \bigcap_{S \subset H} H$ (H sous-groupe de G)
• de l'intérieur $\langle S \rangle = \{s_1, \dots, s_n,\ s_i \in S \cup S^{-1}\}$

Déf 2: Soit G un groupe. Si S est une partie non vide de G tq $\langle S \rangle = G$, on dit que S est une partie génératrice de G.

Rem 3: Un groupe possède toujours au moins une partie génératrice : $G = \langle G \rangle$.

Ex 4: Pour $a \in G$, $\langle a \rangle = \{a^k, k \in \mathbb{Z}\}$ ou $\{ka, k \in \mathbb{Z}\}$.

Ex 5: Le groupe dérivé, ie le groupe engendré par les commutateurs noté $D(G) = \langle \{xyx^{-1}y^{-1} \mid x, y \in G\} \rangle$

Thm 6: $\langle A \rangle$ est un sous-groupe de G contenant A (partie non vide de G). Pour tout sous-groupe H de G : $A \subset H \Rightarrow \langle A \rangle \subset H$. Donc $\langle A \rangle$ est le plus petit sous-groupe de G contenant A.

I - GROUPES ABÉLIENS :

A - Groupes monogènes et cycliques :

Déf 7: S'il existe $x \in G$ tq $G = \langle x \rangle$, on dit que G est monogène.

Rem 8: Tout groupe monogène est abélien.

Prop 9: Soient G, G' deux groupes et $f : G \to G'$ un morphisme surjectif. Alors : G monogène $\Rightarrow$ G' monogène.

Déf 10: Un groupe cyclique est un groupe monogène fini.

Ex 11: $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique. Les générateurs sont les $m \in \mathbb{Z}$ tq $m \wedge n = 1$

Thm 12: Soit G un groupe cyclique d'ordre n et $g \in G$ tq $G = \langle g \rangle$. Alors les générateurs de G sont les g^k avec $k \in [\![1, n]\!]$ et $k \wedge n = 1$.

Déf 13: L'indicatrice d'Euler : $\varphi : \mathbb{N}^* \to \mathbb{N}^*$
$n \mapsto \mathrm{card}(\{m \in \mathbb{N}^*, m < n, m \wedge n = 1\})$

App 14: $\varphi(n)$ est donc le nombre de générateurs d'un groupe cyclique d'ordre n.

Rem 15: Dans un groupe G d'ordre fini premier, tout élément ($\neq e_G$) engendre G.

Thm 16: Description des groupes monogènes
Soit G un groupe monogène. Si $\mathrm{card}(G) < +\infty$ alors $G \simeq \mathbb{Z}/n\mathbb{Z}$ Sinon $G \simeq \mathbb{Z}$.

Coro 17: Tout groupe fini d'ordre p premier est cyclique et donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

App 18: L'ensemble des racines cubiques de l'unité $\Gamma_3 = \{1, j, j^2\}$ est isomorphe à $\mathcal{A}_3$.

B - Groupes abéliens de type fini :

Déf 19: S'il existe $S \subset G$ finie $S \neq \emptyset$ tq $\langle S \rangle = G$ alors G est de type fini.

Rem 20: ⚠ fini ≠ de type fini ⚠ c-ex : $\mathbb{Z} = \langle 1 \rangle$ de type fini mais pas fini.

Déf 21: Soit A abélien, $n \in \mathbb{Z}$, $\underline{a} = (a_1, \dots, a_n)$ avec $\forall i \in [\![1, n]\!]$ $a_i \in A$.
$\varphi_{\underline{a}} : \mathbb{Z}^n \to A$
$(m_1, \dots, m_n) \mapsto \sum_{i=1}^{n} m_i a_i$
$\underline{a}$ est une base $\Leftrightarrow \varphi_{\underline{a}}$ bijective
Lorsqu'il existe une telle base $A \simeq \mathbb{Z}^n$ et on dit que A est libre

Déf 22: $x \in G$ est de torsion si $\exists b \in \mathbb{Z}^*$ tq $bx = 0$. $G_{Tors} = \{x \in G, x \text{ de torsion}\}$
G est sans torsion si $G_{Tors} = \{0\}$ et de torsion si $G_{Tors} = G$.

Prop 23: G_{Tors} sous-groupe de G.
G/G_{Tors} est sans torsion
G libre $\Rightarrow$ G sans torsion

Prop 24: Si $G \simeq \mathbb{Z}^q \oplus \mathbb{Z}/(d_1) \oplus \dots \oplus \mathbb{Z}/(d_r)$ avec $\forall i\ d_i \neq 0$ et $d_1 | \dots | d_r$.
i) $G_{Tors} \simeq \mathbb{Z}/(d_1) \oplus \dots \oplus \mathbb{Z}/(d_r)$.
ii) $G/G_{Tors} \simeq \mathbb{Z}^q$.

Thm 25: Structure des groupes abéliens de type fini.
Soit G abélien de type fini. Alors il existe un entier $q \geq 0$, il existe une unique suite $d_1, \dots, d_r$ d'entiers ≥ 2 tq :

i) $d_1 | \dots | d_r$

ii) $G \simeq \mathbb{Z}^q \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/d_r\mathbb{Z}$

II LES GROUPES SYMÉTRIQUES ET ALTERNÉS

A - Le groupe symétrique S_n :

Déf 26 : On note, $\forall n \in \mathbb{N}^*$, S_n le groupe des permutations de $\{1, \dots, n\}$. Le groupe $(S_n, \circ)$ est appelé le groupe symétrique de degré n.

Rem 27 : $\text{Card}(S_n) = n!$

Déf 28 : Pour toute permutation $\sigma \in S_n$, on peut considérer la relation d'équivalence $\mathcal{R}_\sigma$ sur $\{1, \dots, n\}$ définie par :
$i \mathcal{R}_\sigma j \iff \exists r \in \mathbb{Z}$ tq $j = \sigma^r(i)$.
$\forall \sigma \in S_n$, $\forall i \in [\![1, n]\!]$ $\Omega_\sigma(i) = \{\sigma^r(i), i \in \mathbb{Z}\}$ la classe d'équivalence de i modulo $\mathcal{R}_\sigma$, appelée σ-orbite de i.

Déf 29 : $\sigma \in S_n$ est un cycle s'il existe au plus une σ-orbite O, telle que $\text{Card}(O) > 1$. Dans ce cas, $\text{card}(O)$ est la longueur du cycle et σ son support.

Déf 30 : Un 2-cycle est une transposition.

Prop 31 : Un n-cycle est un élément d'ordre n.

Ex 32 : Dans S_5, $(1\,3\,5)$ est un 3-cycle de support $\{1, 3, 5\}$

CEx 33 : Dans S_4, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ n'est pas un cycle

Prop 34 : Toute permutation s'écrit de manière unique (à l'ordre près des facteurs), comme un produit de cycles à supports disjoints

Déf 35 : On dit que deux permutations ont la même structure orbitale si elles ont le même nombre de 2, 3, ..., n-cycles dans leur décomposition en cycle à support disjoints.

Prop 36 : Dans S_n, deux permutations sont conjuguées ssi, elles ont même structure orbitale.

Thm 37 : S_n est engendré par les transpositions.

Rem 38 : On peut réduire à 2 le nombre de générateurs de S_n :
$$S_n = \langle (1, 2) ; (1, \dots, n) \rangle.$$

Thm 39 : Il existe un unique morphisme surjectif $\varepsilon : S_n \longrightarrow \{\pm 1\}$
$$\sigma \longmapsto \prod_{j<i} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Déf 40 : Le morphisme est appelé la signature de S_n.

Ex 41 : Les transpositions sont de signature -1

B - Le groupe alterné $\mathcal{A}_n$:

Déf 42 : Le noyau du morphisme signature est appelé le groupe alterné, noté $\mathcal{A}_n$. $\quad \text{Ker}(\varepsilon) = \mathcal{A}_n$.

Rem 43 : $\mathcal{A}_n$ est l'ensemble des permutations qui se décomposent en un produit pair de transpositions.

Rem 44 : $\text{Card}(\mathcal{A}_n) = \frac{n!}{2}$

Thm 45 : Pour $n \geqslant 3$, $\mathcal{A}_n$ est engendré par les 3-cycles.

Déf 46 : Soit G un groupe et H un sous-groupe de G. On dit que H est distingué dans G si : $\forall x \in G$, $xH = Hx$. On note $H \lhd G$.

Rem 47 : Tout sous-groupe d'un groupe abélien est distingué.

Prop 48 : Soit G un groupe : $H \lhd G \iff (\forall x \in G \; xHx^{-1} = H)$

Déf 49 : Un groupe simple est un groupe non trivial qui ne possède pas de sous-groupe distingué autre que e_G et G.

Thm 50 : Pour $n \geqslant 5$, le groupe $\mathcal{A}_n$ est simple.] Dvp 1

Prop 51 : • Soit G un groupe. Si c est un commutateur de G
Alors : $\forall x \in G$ $\; xcx^{-1}$ est aussi un commutateur (stable par conj.)
• $D(G)$ est un sous-groupe distingué de G.

App 52 : $\forall n \geqslant 5 \quad D(\mathcal{A}_n) = D(S_n) = \mathcal{A}_n$.

III - GROUPE LINÉAIRE ET GROUPE SPÉCIAL LINÉAIRE

A - $GL_n(K)$:

On se place dans le cadre où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Déf 53 : On note $GL_n(K)$ l'ensemble des matrices inversibles de $\mathcal{M}_n(K)$.

Prop 54 : Soit $A \in \mathcal{M}_n(K)$, $A \in GL_n(K) \iff \det(A) \neq 0$.

Déf 55 : Soient $i, j \in [\![1,n]\!]$, soit $\lambda \in \mathbb{K}^*$, on définit la matrice de transvection : $T_{ij}(\lambda) = I_n + \lambda E_{ij}$. $(i \neq j)$

Déf 56 : Soient $i \in [\![1,n]\!]$, soit $\lambda \in K^*$, on définit la matrice de dilatation par $D_i(\lambda) = I_n + (\lambda - 1) E_{ii}$.

Thm 57 : $GL_n(K)$ est engendré par les dilatations et les transvections.

B - $SL_n(K)$:

Déf 58 : $SL_n(K)$ est le noyau du morphisme de groupe $\det : GL_n(K) \to K^*$. On appelle $SL_n(K)$ le groupe spécial linéaire.

Thm 59 : $SL_n(K)$ est engendré par les transvections.

App 60 : $SL_n(K)$ est connexe par arcs.

Déf 61 : On définit le centre d'un groupe par :
$Z(G) = \{g \in G, \forall x \in G, gx = xg\}$.

Ex 62 : $Z(SL_n(K)) = \{\lambda I_n, \lambda \in K \text{ tq } \lambda^n = 1\}$.

Déf 63 : Le groupe projectif de $SL_n(K)$ est $PSL_n(K) = \dfrac{SL_n(K)}{Z(SL_n(K))}$

Prop 64 : Deux transvections sont conjuguées.

Thm 65 : $PSL_n(\mathbb{K})$ est simple

App 66 : $D(GL_n(K)) = D(SL_n(K)) = SL_n(K)$

Références : Gourdon, Algèbre
Bouvier, Richard, Groupes
Tauvel, Cours d'algèbre.
Perrin, Cours d'algèbre
Ulmer, Théorie des groupes.

$\boxed{\text{SIMPLICITÉ DE } A_n \text{ pour } n \geqslant 5.}$

Posons $E = [\![1, n]\!]$. Soit H un sous-groupe de $\mathcal{A}_n$ tel que $H \lhd \mathcal{A}_n \setminus \{id\}$. Soit $\sigma \in H \setminus \{id\}$.

① Construire un ensemble à 5 éléments.

Comme $\sigma \neq id$, il existe $a \in E$ tq $\sigma(a) = b \neq a$.
Soit $c \in E$ tq $c \notin \{a, b, \sigma(b)\}$
Soit τ le 3-cycle $(a\,c\,b) \in \mathcal{A}_n$. On a $\tau^{-1} = (a\,b\,c)$.
Posons $\rho = (\tau \sigma \tau^{-1}) \sigma^{-1} \in H$

$$\rho = \tau(\sigma \tau^{-1} \sigma^{-1}) = (a\,c\,b)\,(\sigma\,(a\,b\,c)\,\sigma^{-1})$$

$$\rho = (a\,c\,b)\,(\sigma(a)\,\sigma(b)\,\sigma(c)).$$

Posons également $F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\} = \mathrm{Supp}(\rho)$.
Comme $b = \sigma(a)$; F a au plus 5 éléments.
Quitte à rajouter des éléments dans F, on peut supposer $|F| = 5$
De plus, $\rho|_{E \setminus F} = id_{E \setminus F}$.

② Trouver un sous-groupe distingué dans F.

Posons $A(F)$ l'ensemble des permutations paires d'éléments de
$A(F)$ est isomorphe à $\mathcal{A}_5$.
Considérons le morphisme d'injection suivant :

$$i : \begin{array}{ccc} A(F) & \hookrightarrow & \mathcal{A}_n \\ u & \longmapsto & \bar{u} \end{array}$$

avec $\bar{u}$ tel que $\bar{u}|_F = u$ et $\bar{u}|_{E \setminus F} = id_{E \setminus F}$

On construit alors $H_0 = \{u \in A(F) \text{ tq } \bar{u} \in H\}$, l'image réciproque de H par i. H_0 est un sous-groupe de $A(F)$ car H est un sous-groupe de $\mathcal{A}_n$.

De plus, puisque H est distingué dans $\mathcal{A}_n$ et que i est un morphisme, on sait que H_0 est distingué dans $A(F)$

$$H \triangleleft \mathcal{A}_n \Rightarrow \underbrace{i^{-1}(H)}_{H_0} \triangleleft A(F).$$

③ Montrer que $H_0 = A(F)$:

On sait que $H_0 \neq \{id\}$ car $\rho|_F \in H_0$.
De plus, comme $\mathcal{A}_5$ est simple et que $A(F) \simeq \mathcal{A}_5$, on déduit que $A(F)$ est simple, et donc $A(F) = H_0$.

④ Montrer que $H = \mathcal{A}_n$:

Pour $\sigma \in A(F)$, on sait que $o(\sigma) = 3$, donc on déduit que $o(\bar{\sigma})$ divise 3, d'où $o(\bar{\sigma}) = 1$ ou 3.
Or i est injective donc $\mathrm{Ker}(i) = \{0\}$.
Donc $i(\sigma) = \bar{\sigma} \neq e_{\mathcal{A}_n}$, donc $o(\bar{\sigma}) \neq 1$; ainsi $o(\bar{\sigma}) = 3$.

On déduit ainsi que $\bar{\sigma}$ est un produit de 3-cycles car le ppcm de la décomposition est 3.

De plus, puisque $\sigma \in A(F)$, on a $|\mathrm{supp}(\sigma)| \leq 5$ et donc $|\mathrm{supp}(\bar{\sigma})| \leq 5$.
D'où $\bar{\sigma}$ est un 3-cycle.
On sait également que puisque $\sigma \in H_0$, $\bar{\sigma} \in H$.
De plus, tous les 3-cycles sont conjugués dans $\mathcal{A}_n$ (puisqu'ils ont la même structure orbitale) et H est distingué dans $\mathcal{A}_n$ donc H contient tous les 3-cycles.
Donc H contient le sous-groupe engendré par les 3-cycles qui n'est autre que $\mathcal{A}_n$.
Ainsi $H = \mathcal{A}_n$.

SIMPLICITÉ DE $\mathcal{A}_5$

① Dénombrement :

$\text{card}(\mathcal{A}_5) = \frac{5!}{2} = 60$. et soit $\sigma \in \mathcal{A}_5$, $|\text{supp}(\sigma)| \leq 5$.

* éléments d'ordre 5 : $\frac{5!}{5} = 24$ (grâce à ⊛)
* éléments d'ordre 3 : $\frac{5 \times 4 \times 3}{3} = 20$ (grâce à ⊛)
* éléments d'ordre 2 : $60 - 24 - 20 - 1 = 15$ (grâce à ⊛)
* neutre.

② Sous-groupe distingué :

⊛ Dans $\mathcal{A}_5$, les éléments d'ordre 3 sont les 3-cycles, les éléments d'ordre 5 sont les 5-cycles et les éléments d'ordre 2 sont de la forme $(ab)(cd)(e)$ $(a,b,c,d,e \in [\![1,n]\!])$.

Tous les éléments d'ordre 2, 3, 5 ont respectivement la même structure orbitale, ils sont donc conjugués dans $\mathcal{A}_5$.

Soit H un sous-groupe distingué de $\mathcal{A}_5 \setminus \{id\}$.
Par conjugaison, si H contient un élément d'ordre 2, 3 ou 5 alors il les contient tous.

③ Problème de cardinal :

De plus, on sait que $|H| \mid |\mathcal{A}_5|$. Les diviseurs de 60 sont : 1 2 3 4 5 6 10 12 15 20 30 60.

Si H contient les 3-cycles : $|H| = 1+20 = 21 \nmid 60$.

Si H contient les 5-cycles : $|H| = 1+24 = 25 \nmid 60$

Si H contient les éléments d'ordre 2 : $|H| = 1+15 = 16 \nmid 60$.

Donc H contient au moins 2 des 3 types.

Mais : $|H| \geqslant 15+20+1 = 36$

Donc $|H| = 60$ et ainsi $H = \mathcal{A}_5$

$SL_n(\mathbb{K})$ ($\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$) CONNEXE PAR ARC

Soit $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$, soit $M \in SL_n(\mathbb{K})$. Montrons que toute matrice de $SL_n(\mathbb{K})$ peut être reliée par un chemin continu à I_n.

① <u>Montrons que $GL_n(\mathbb{K})$ et $SL_n(\mathbb{K})$ sont engendrés par les transvections et les dilatations.</u>

On note E_{ij} la matrice avec un 1 en position (i,j) et des 0 ailleurs. On rappelle qu'une matrice de transvection est de la forme $T_{ij}(\lambda) = I_n + \lambda E_{ij}$ avec $i \neq j$, et une matrice de dilatation de la forme $D_i(\lambda) = I_n + (\lambda - 1)E_{ii}$ où det
On a alors $\det(T_{ij}(\lambda)) = 1$ et $\det(D_i(\lambda)) = \lambda$.

On remarque que multiplier à droite par $T_{ij}(\lambda)$ revient à effectuer l'opération sur les colonnes : $C_j \leftarrow C_j + \lambda C_i$ et multiplier à gauche revient à effectuer l'opération sur les lignes $L_i \leftarrow L_i + \lambda L_j$.
Soit $M = (m_{ij}) \in GL_n(\mathbb{K})$. On raisonne par récurrence sur
* Si $n=1$, alors $M = D_1(\det M)$.

* Si $n \geqslant 2$, supposons que toute matrice de $GL_{n-1}(\mathbb{K})$ soit un produit de transvections et dilatations.
– Dans un premier temps, supposons que l'un au moins des coefficients m_{i1} pour $i \geqslant 2$ est non nul. On effectue alors l'opération $L_1 \leftarrow L_1 - \left(\frac{m_{11}-1}{m_{i1}}\right) L_i$, ce qui revient à multiplier M à gauche par $T_{1i}\left(-\frac{m_{11}-1}{m_{i1}}\right)$. Dans ce cas, le coefficient en

position $(1,1)$ obtenu est 1.

- Si tous les coefficients m_{i1} $(i \geq 2)$ sont nuls, alors forcément m_{11} n'est pas nul car M est inversible.
On effectue alors les opérations $L_1 \leftarrow L_1 + L_2$; $L_2 \leftarrow L_2 - L_1$ puis $L_1 \leftarrow L_1 + L_2$. Cela entraîne, par multiplication par des transvections, que le coefficient m_{21} est non nul et on se reporte au cas précédent.

Enfin, pour $i \in [\![2, n]\!]$, on effectue les opérations $L_i \leftarrow L_i - m_{i1} L_1$ et $C_i \leftarrow C_i - m_{1i} C_1$ successivement ce qui annule tous les coefficients de la première colonne et de la première ligne, sauf le coefficient $m_{11} = 1$.
On obtient alors une matrice de la forme $\begin{pmatrix} 1 & 0 \cdots 0 \\ 0 & \\ \vdots & M' \\ 0 & \end{pmatrix}$ où $M' \in GL_{n-1}(\mathbb{K})$. Donc en appliquant l'hypothèse de récurrence à M', on obtient le résultat suivant :
$\exists (T^1), \ldots, (T^r)$, $(S^1), \ldots, (S^s)$ des matrices de transvections telles que :

$$(T^r)^{-1} \ldots (T^1)^{-1} M (S^s)^{-1} \ldots (S^1)^{-1} = D_n(\det M')$$

On a $\det M = \det M'$, d'où : $M = T^r \ldots T^1 D_n(\det M) S^1 \ldots S^s$
Donc M est bien le produit de matrices de transvections et dilatations.

→ De plus, si $M \in Sl_n(\mathbb{K})$, alors $D_n(\det M') = I_n$ et donc $Sl_n(\mathbb{K})$ est bien engendré par les transvections seules.

② Connexité par arc

$M \in Sl_n(\mathbb{K})$ donc il existe $T^1, \dots, T^r$ des transvections, telles que : $M = T^1 \dots T^r$.

Considérons l'application suivante : $\phi : [0,1] \longrightarrow Sl_n(\mathbb{K})$
$t \longmapsto T^1 \dots T^r(t)$.

Chaque matrice T^k est associée à un couple (i,j) $i \neq j$ et à $\lambda_k \in \mathbb{K}$ de manière à ce que $T^k = T_{ij}(\lambda_k)$ et donc $T^k(t) = T_{ij}(\lambda_k t)$.

ϕ est continue.

$$\phi(0) = T^1 \dots T^r(0) = \underbrace{I_n \dots I_n}_{r \text{ fois}} = I_n$$

$$\phi(1) = T^1 \dots T^r(1) = M.$$

Ce qui nous donne bien un chemin continu de $[0,1]$ dans $Sl_n(\mathbb{K})$. Donc $Sl_n(\mathbb{K})$ est connexe par arc.

Le cas $Gl_n(\mathbb{C})$ est plus délicat car l'application $t \mapsto D_n(t$ n'est pas à valeurs dans $Gl_n(\mathbb{C})$. On ne peut donc pas utiliser la même technique. Mais en remarquant que $\mathbb{C}^*$ est connexe par arcs, on déduit qu'il existe une application continue f_λ de $[0,1]$ dans $\mathbb{C}^*$ telle que $f_\lambda(0) = 1$ et $f_\lambda(1) = \lambda$.
Dans ce cas l'application $t \mapsto D_n(f_\lambda(t))$ est à valeurs dans $Gl_n(\mathbb{C})$, et on peut ainsi conclure de la même manière.