

Nom:

Numéro de Jury:

Prénom:

Numéros des sujets tirés:

108

Intitulé du sujet choisi:

Exemples de parties génératrices d'un groupe. Applications.

Définition 1: Soit G un groupe et $A \subset G$. Le sous-groupe engendré par A , noté $\langle A \rangle$, est le plus petit sous-groupe de G contenant A : $\langle A \rangle = \bigcap_{\substack{H \leq G \\ A \subset H}} H$.

Définition 2: Soit G un groupe et $A \subset G$. On dit que A est une partie génératrice de G lorsque $\langle A \rangle = G$.

I - Groupes monogènes

Définition 3: Un groupe G est dit:

- monogène s'il est engendré par un seul élément
- cyclique s'il est monogène et fini.

Exemple 4: Pour $n \geq 1$, le sous-groupe de $(\mathbb{C}^*, \times)$ des racines n -ièmes de l'unité est cyclique d'ordre n .

Proposition 5: Un groupe monogène est abélien.

Théorème 6: Soit G un groupe monogène.

- Si G est infini, alors $G \cong \mathbb{Z}$.
- Si G est fini d'ordre $n \geq 1$, alors $G \cong \mathbb{Z}/n\mathbb{Z}$.

Théorème 7: Soit $n \geq 1$. Les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les classes $k\mathbb{Z}$ où $k \wedge n = 1$.

Définition 8: On appelle indicatrice d'Euler la fonction $\varphi: \mathbb{N}^* \rightarrow \mathbb{N}^*$ qui à $n \in \mathbb{N}^*$ associe le nombre $\varphi(n)$ de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Exemple 9: Les générateurs de $\mathbb{Z}/10\mathbb{Z}$ sont $\bar{1}, \bar{3}, \bar{7}, \bar{9}$ donc $\varphi(10) = 4$.

Proposition 10: $\forall n \in \mathbb{N}^*, n = \sum_{d|n} \varphi(d)$.

Application 11: Soit K un corps fini et E/K une extension finie. Alors il existe $\alpha \in E$ tel que $E = K(\alpha)$.

II - Groupe dérivé

Définition 12: Le groupe dérivé d'un groupe G , noté $D(G)$, est le sous-groupe engendré par les commutateurs de G :

$$D(G) = \langle \{xyx^{-1}y^{-1} \mid x, y \in G\} \rangle$$

Remarque 13: Le groupe dérivé d'un groupe abélien est trivial.

Exemple 14: $D(S_3) = 2\mathbb{Z}_3 \cong \mathbb{Z}/3\mathbb{Z}$.

Proposition 15: Soit $\varphi: G \rightarrow G'$ un morphisme de groupes. Alors $\varphi(D(G)) \subset D(G')$.

Corollaire 16: $D(G)$ est un sous-groupe caractéristique (donc distingué) de G .

Proposition 17: Soit $H \triangleleft G$. G/H est abélien si et seulement si $D(G) \subset H$.

Exemple 18: Le sous-groupe V de $2L_4$ engendré par les bitranspositions contient $D(2L_4)$.

III - Groupes de permutations

Pour $n \geq 2$, on note S_n le groupe symétrique sur $[1, n]$ et $2L_n$ son sous-groupe alterné.

Définition 19: Pour $r \in [2, n]$, on appelle r -cycle toute permutation de la forme $(i_1 \dots i_r)$ où $i_1, \dots, i_r \in [1, n]$ sont 2 à 2 distincts. Un 2-cycle est appelé transposition.

Théorème 20: Toute permutation se décompose en produit de cycles à supports disjoints. De plus, cette décomposition est unique à ordre des cycles près.

Exemple 21: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix} = (1 \ 4 \ 2)(5 \ 6)$.

Application 22: Deux permutations de S_n sont conjuguées si et seulement si leurs décompositions en produit de cycles à supports disjoints contiennent le même nombre de r -cycles pour tout $2 \leq r \leq n$.

Théorème 23: Toute permutation se décompose en produit de transpositions.

Exemple 24: $(1 \ 4 \ 2) = (1 \ 4)(4 \ 2)$.

Remarque 25: • Cette décomposition n'est pas unique.

• On peut se limiter aux transpositions $(i \ i+1)$ pour $1 \leq i \leq n-1$ et $(1 \ i)$ pour $2 \leq i \leq n$.

Application 26: Si $n \neq 6$, alors les automorphismes de S_n sont intérieurs. Si de plus $n \geq 3$, $\text{Aut } S_n = \text{Int } S_n \cong S_n$.

Application 27: Si $n \geq 3$, alors $2L_n$ est engendré par les 3-cycles.

Exemple 28: Cette décomposition n'est pas unique:

$$\begin{aligned} (1 \ 2)(3 \ 4) &= (1 \ 2 \ 3)(1 \ 2 \ 4)(1 \ 3 \ 2)(1 \ 4 \ 2) \\ &= (1 \ 2 \ 3)(1 \ 3 \ 4)(1 \ 3 \ 2)(1 \ 4 \ 3) \end{aligned}$$

Proposition 29: Si $n \geq 5$, alors les 3-cycles sont conjugués dans $2L_n$.

Application 30: Pour $n \geq 5$, $D(S_n) = D(2L_n) = 2L_n$.

Application 31: Pour $n \geq 5$, $2L_n$ est simple.

Remarque 32: $2L_3$ est simple, mais $2L_4$ n'est pas simple car $D(2L_4) = V \neq 2L_4, \{\text{id}\}$.

IV - Groupe linéaire

Soit K un corps et E un K -espace vectoriel de dimension finie $n \geq 1$.

1) Pivot de Gauss

Définition 33: On définit les matrices élémentaires de $GL_n(K)$:
• les transvections $I_n + \lambda E_{ij}$ pour $\lambda \in K^*$ et $1 \leq i \neq j \leq n$;

- les dilatations $I_n + (\lambda - 1)E_{ii}$ pour $\lambda \in K^*$ et $1 \leq i \leq n$.

Théorème 34 (Pivot de Gauss): Soit $A \in M_n(K)$. Il existe des matrices élémentaires $E_1, \dots, E_k$ telles que la matrice $E_k \dots E_1 A$ soit échelonnée en lignes et réduite.

Corollaire 35: $GL_n(K)$ est engendré par les transvections et les dilatations. $SL_n(K)$ est engendré par les transvections.

Application 36: $Z(GL_n(K)) = K^* I_n$ et $Z(SL_n(K)) = \mu_n(K) I_n$.

Application 37: $GL_n(\mathbb{C})$, $SL_n(\mathbb{C})$ et $SL_n(\mathbb{R})$ sont connexes par arcs.

Remarque 38: $GL_n(\mathbb{R})$ possède deux composantes connexes par arcs.

Application 39: Soit $A \in GL_n(K)$ et $b \in K^n$. L'algorithme du pivot de Gauss permet de résoudre $Ax = b$ d'inconnue $x \in K^n$ avec une complexité en $O(n^3)$.

Proposition 40: Si $n \geq 3$, les transvections sont conjuguées dans $GL_n(K)$ et $SL_n(K)$.

Application 41: Si $n \geq 3$, $D(GL_n(K)) = D(SL_n(K)) = SL_n(K)$.

2) Groupe orthogonal

On suppose $K = \mathbb{R}$ et on munit E d'un produit scalaire.

Définition 42: On appelle groupe orthogonal le sous-groupe $O(E) = \{u \in GL(E) \mid \forall x, y \in E, \langle u(x), u(y) \rangle = \langle x, y \rangle\}$ de $GL(E)$, et groupe spécial orthogonal le sous-groupe $SO(E) = \{u \in O(E) \mid \det u = 1\}$.

Définition 43: On appelle :

- réflexion toute symétrie orthogonale $s \in O(E)$ par rapport à un hyperplan

- renversement toute symétrie orthogonale $s \in SO(E)$ par rapport à un sous-espace vectoriel de dimension $n-2$.

Théorème 44: Toute isométrie $u \in O(E)$ (resp. $SO(E)$) s'écrit comme produit d'au plus n réflexions (resp. renversements).

Proposition 45: Les renversements sont conjugués dans $SO_3(\mathbb{R})$.

Application 46: $SO_3(\mathbb{R})$ est simple.

3) Application en géométrie.

On considère l'action de $SL_2(\mathbb{Z})$ sur le demi-plan de Poincaré $\mathbb{H} = \{z \in \mathbb{C} \mid \text{Im } z > 0\}$ par homographie :

$$\begin{aligned} SL_2(\mathbb{Z}) \times \mathbb{H} &\rightarrow \mathbb{H} \\ \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, z \right) &\mapsto \frac{az+b}{cz+d} \end{aligned}$$

On note $D = \{z \in \mathbb{H} \mid |z| \geq 1 \text{ et } -\frac{1}{2} \leq \text{Re } z \leq \frac{1}{2}\}$.

Proposition 47: L'action de $SL_2(\mathbb{Z})$ sur $\mathbb{H}$ est bien définie.

Théorème 48: $SL_2(\mathbb{Z}) = \langle S, T \rangle$ où $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ et $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

Application 49: Le groupe $PSL_2(\mathbb{Z}) := SL_2(\mathbb{Z}) / \{\pm I_2\}$ agit sur $\mathbb{H}$ avec D , i.e.:

$$\mathbb{H} = \bigcup_{\bar{A} \in PSL_2(\mathbb{Z})} A \cdot D$$

$$\forall \bar{A}, \bar{B} \in PSL_2(\mathbb{Z}), \bar{A} \neq \bar{B} \Rightarrow A \cdot D \cap B \cdot D = \emptyset.$$

Algorithme du pivot.

Entrée : $A = [a_{ij}]_{1 \leq i \leq m, 1 \leq j \leq p} \in \mathcal{M}_{m,p}(K)$

Sortie : Forme échelonnée réduite de A

Traitement :

$i_0, j_0 \leftarrow -1, 1$

Tant que $i_0 \leq m$ et $j_0 \leq p$:

Si la colonne j_0 est nulle :

$j_0 \leftarrow j_0 + 1$

Sinon :

Si $a_{i_0, j_0} = 0$:

Chercher $i \in \llbracket 1, m \rrbracket$ tel que $a_{ij_0} \neq 0$

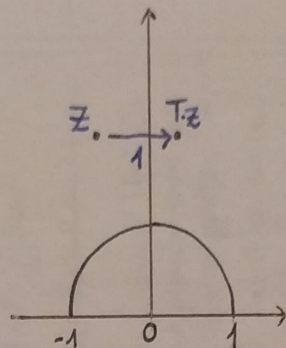
$L_{i_0} \leftarrow L_{i_0} + L_i$

$L_{i_0} \leftarrow a_{i_0, j_0}^{-1} L_{i_0}$

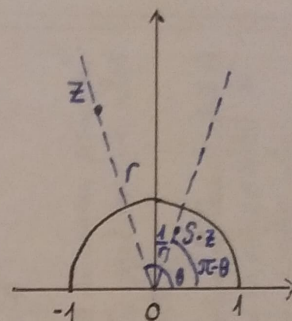
Pour $i \neq i_0$ allant de 1 à n :

$L_i \leftarrow L_i - a_{ij_0} L_{i_0}$

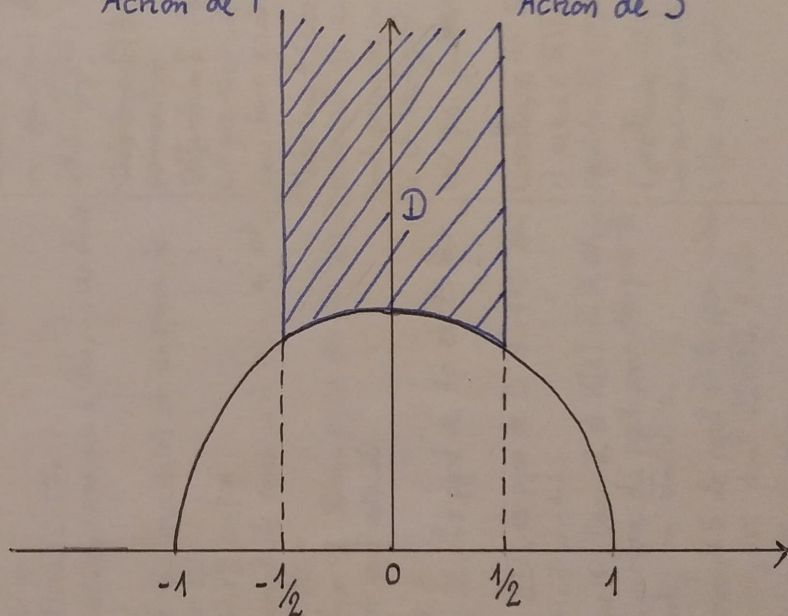
$i_0, j_0 \leftarrow i_0 + 1, j_0 + 1$.



Action de T



Action de S



Domaine D .