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

1. Partie génératrice, générateurs et relations. —

- Def : Groupe engendré par une partie.
- Def : Partie génératrice d'un groupe.
- Ex : Le groupe dérivé $D(G)$ est engendré par les $xyx^{-1}y^{-1}$ pour $x, y \in G$.
- Def : Groupe libre $\mathscr{F}(A)$ engendré par une partie A.
- Pro : Morphisme entre $\mathscr{F}(A)$ et $G =< A >$.
- Def : Présentation d'un groupe par générateurs et relations.

2. Groupes abéliens. —

1. Groupes monogènes et groupes cycliques. —

- Def : Un groupe G est abélien si pour tous x, y, $xy = yx$.
- Def : Un groupe G est dit monogène s'il existe $x \in G$ tel que $G =< x >$.
  Si de plus G est fini, on dit qu'il est cyclique.
- Rem : Un groupe monogène est abélien.
  Pour tout $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ est cyclique.
- $\mathbb{Z}/n\mathbb{Z}$ a un générateur x de relation $x^n = e$.
- App : Pour tout $a \in G$, $< a >$ est isomorphe à $\mathbb{Z}$ ou à un $\mathbb{Z}/n\mathbb{Z}$.
- Ex : Le groupe U_n des racines n-ièmes de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
- Pro : Soit $n \geq 1$. Si $a \in \mathbb{Z}$, notons $\overline{a}$ son image dans $\mathbb{Z}/n\mathbb{Z}$. On a l'équivalence :
  i) a est premier avec n.
  ii) $\overline{a}$ est un générateur du groupe $\mathbb{Z}/n\mathbb{Z}$.
  iii) $\overline{a}$ est un inversible de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
- Pro : Si l'ordre de G est un nombre premier p, alors G est cyclique, et tout $x \in G$ différent de e engendre G.
- Pro : Soit G un groupe cyclique d'ordre n, de générateur a, et soit $k \geq 1$.
  On a : $ord(a^k) = \frac{n}{pgcd(k,n)}$.
  En particulier, a^k est un générateur ssi $pgcd(n, k) = 1$.
- App : Pour G cyclique d'ordre n, tout sous-groupe de G est cyclique.
  Pour tout $d|n$, il existe un unique sous-groupe d'ordre d.
- Def : On appelle indicatrice d'Euler de n, $\phi(n)$, le nombre de générateurs du groupe $Z/n\mathbb{Z}$.
- Pro : Pour $d|n$, le nombre d'éléments de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d est $\phi(d)$.
  Ainsi, $n = \sum_{d|n} \phi(d)$.
- Pro : Pour $G =< a >$ cyclique d'ordre n, G' un groupe, et $f : G \to G'$ morphisme de groupes, f est entièrement déterminé par l'image de a, qui est un élément de G' d'ordre $d|n$.
- App : Si G et G' sont cycliques d'ordres m, n, alors il existe $pgcd(m, n)$ morphismes de groupes de G vers G'.
- Pro : Pour G et G' cycliques d'ordres m, n, l'ordre des éléments de $G \times G'$ divise $pgcd(m, n)$.
  De plus, il existe un élément d'ordre $pgcd(m, n)$ dans $G \times G'$.
- App : Le produit direct de k groupes $G_1 \times .. \times G_k$ est cyclique ssi les G_i sont cycliques d'ordres premiers entre eux deux à deux.

2. Groupes abéliens de type fini. —

- Def : Un groupe G est abélien de type fini ssi il est abélien et si il est engendré par un nombre fini d'éléments.
- Ex : Les groupes abéliens finis sont de type fini.
- Théorème de structure des groupes abéliens de type fini : Soit G abélien de type fini.
  Alors il existe $r \geq 1$ et des entiers non-nuls $d_1|..|d_s$ tels que $G \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times .. \times (\mathbb{Z}/d_s\mathbb{Z}) \times \mathbb{Z}^r$.
  De plus, $r, d_1, .., d_s$ sont uniques. On les appelle invariants de G.
- Ex : Un groupe abélien d'ordre 24 est isomorphe soit à $\mathbb{Z}/24\mathbb{Z}$, soit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.
- Rem : Un groupe abélien de type fini est fini ssi $r = 0$.
- Pro : Un groupe G abélien fini est cyclique ssi pour tout $d|n$ il existe au plus un sous-groupe d'ordre d dans G.
- Pro : Pour G un groupe abélien d'ordre n, on note $exp(G) = ppcm_{x \in G}(ord(x))$.
  Alors il existe $x \in G$ d'ordre $exp(G)$.

3. Groupes symétriques et diédraux. —

1. Groupes symétriques, alternés. —

- Def : Pour tout $n \geq 1$, on note Σ_n le groupe des bijections de $\{1, .., n\}$, appelé n-ième groupe symétrique.
- Thm : Soit $n \geq 2$. On a :
  i) Les transpositions engendrent Σ_n.
  ii) Les transpositions $(1, i)$, $\forall 2 \geq i \geq n$ engendrent Σ_n.
  iii) Les transpositions $(i, i+1)$, $\forall 1 \geq i \geq n-1$ engendrent Σ_n.
  iv) Les permutations $(1, 2)$ et $(1, 2, .., n)$ engendrent Σ_n.
- Def+Pro : On appelle n-ième groupe alterné A_n le sous-groupe des éléments de Σ_n qui sont des produits de carrés.
  L'application signature $\varepsilon : \sigma \in \Sigma_n \mapsto \begin{cases} 1 \text{ si } \sigma \text{ est un produits de carrés} \\ -1 \text{ sinon} \end{cases}$ est un morphisme de groupes de Σ_n vers $\{-1, 1\}$, de noyau A_n.
  On a $\varepsilon((i, j)) = -1$.
- App : Pour $n \geq 3$, A_n est engendré par les 3-cycles (i, j, k).
- **Dev** : Pour tout $n \geq 5$, le groupe alterné A_n est simple.
- App : Pour tout $n \geq 2$, $D(\Sigma_n) = A_n$. Pour tout $n \geq 5$, $D(A_n) = A_n$.
- Thm : Pour tout $n \neq 6$, tout automorphisme de Σ_n est de la forme $\sigma \mapsto \tau.\sigma.\tau^{-1}$ pour un $\tau \in \Sigma_n$.

2. Groupes diédraux. —

- Def : Soit $n \geq 2$. Dans le plan complexe $\mathbb{C}$ identifié $\mathbb{R}^2$, considérons le polygone régulier connexe P_n à n sommets, formé par les affixes des $exp^{2i\pi\frac{k}{n}}$.
  Le groupe diédral D_n est le sous-groupe des isométries affines du plan qui laissent P_n invariant.
- Pro : D_n est d'ordre $2n$, et il est engendré par la symétrie axiale s et la rotation d'angle $\theta = \frac{2\pi}{n}$ données par $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $r = \begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix}$.
  Ces générateurs satisfont aux relations $r^n = e$, $s^2 = e$ et $srsr = e$.
  Les éléments de D_n sont ainsi exactement les $r^k.s^\varepsilon$ avec $0 \leq k \leq n-1$ et $\varepsilon \in \{0, 1\}$.
  Le sous-groupe $< r >$ est d'ordre n et distingué dans D_n.
- Ex : Présentation de D_n : $\{x, y \text{ tq } x^n = e, y^2 = e, xyxy = e\}$.
- Pro : $D(D_{2m}) =< r^2 >$ et $D(D_{2m+1}) =< r >$.

4. Autour du groupe linéaire. —

Ici, K est un corps de caractéristique quelconque et E est un K-ev de dimension finie.

1. $GL(E)$ et $SL(E)$. —

- Def : Le groupe linéaire $GL(E)$ est le groupe des isomorphismes linéaires de E.
  Le noyau de l'application déterminant $GL(E) \to K^*$ est noté $SL(E)$.
- Pro+Def : Soit H un hyperplan de E et $u \in GL(E)$ tq $u|_H = Id_H$. On a l'équivalence :
  i) $det(u) = \lambda \neq 1$. (càd $u \notin SL(E)$)
  ii) u admet une valeur propre $\lambda \neq 1$. (donc une droite propre)
  iii) $Im(u - Id) \nsubseteq H$.
  iv) Dans une base convenable, la matrice de u est $Diag(1, .., 1, \lambda)$ pour $\lambda \neq 1$.
  On dit alors que u est une dilatation d'hyperplan $H = Ker(u - Id)$, de droite $D = Im(u - Id)$ et de rapport λ.
- Pro+Def : Soit H un hyperplan de E d'équation $f \in E^*$ et $u \in GL(E)$ tq, $u \neq Id_E$ $u|_H = Id_H$. On a l'équivalence :
  i) $det(u) = 1$. (càd $u \in SL(E)$)
  ii) u n'est pas diagonalisable.
  iii) $D = Im(u - Id) \subset H$.
  iv) Le morphisme induit $\overline{u} : E/H \to E/H$ est l'identité de E/H.
  v) Il existe $a \in H - \{0\}$ tel que pour tout $x \in E$, $u(x) = x + f(x).a$.
  vi) Dans une base convenable, u a pour matrice (une matrice de transvection).
  On dit alors que u est une transvection d'hyperplan H et de droite D.
- Thm : Les transvections sont toutes conjuguées dans $SL(E)$ et engendrent $SL(E)$.
- Cor : Les transvections et les dilatations engendrent $GL(E)$.
- App : 1) On a $D(Gl_n(K)) = Sl_n(K)$ pour $n \geq 3$ et $car(K) \neq 2$.
  2) On a $D(Sl_n(K)) = Sl_n(K)$ pour $n \geq 3$ et $car(K) \neq 2$.
- App : Le centre de $Gl_n(K)$ est l'ensemble des matrices $\lambda.I_n$. Il est isomorphe au groupe K^*.
  Le centre de $Sl_n(K)$ est l'ensemble des matrices $\lambda.I_n$ avec $\lambda^n = 1$. Il est isomorphe au groupe des racines n-ièmes de l'unité dans K.
- App : Pour $K = \mathbb{R}, \mathbb{C}$, $Sl_n(K)$ est connexe par arcs.
  $Gl_n(\mathbb{R})$ a deux composantes connexes.

2. Groupe orthogonal $O(E)$. —

Ici, E est un ev euclidien de dimension n.

- Def : L'ensemble des isométries linéaires de E est un groupe appelé groupe orthogonal et noté $O(E)$.
- Pro : L'ensemble $SO(E) := O(E) \cap det^{-1}(\{1\})$ est un sous-groupe distingué de $O(E)$ appelé groupe spécial orthogonal.
- Pro+Def : Soit $u \in Gl(E)$ tq $u^2 = Id$. Alors pour $E_1 = Ker(u + Id)$, $E_2 = Ker(u - Id)$, on a $E = E_1 \oplus E_2$, et $u|_{E_1} = -Id_{E_1}$, $u|_{E_2} = Id_{E_2}$.
  Si $u \neq id$, on dit que u est une involution (ou symétrie).
  Si $dim(Ker(u + Id)) = 1$ (resp 2) on dit que u est une réflexion (resp un renversement).
- Pro : Soit u une involution. u est une isométrie ssi $E_1 \perp E_2$.
- Thm : Le groupe $O(E)$ est engendré par les réflexions orthogonales.
  Tout $u \in O(E)$ est produit d'au plus n réflexions.
- Rem : Si $u \in SO(E)$, u est produit d'un nombre pair de réflexions.
- Thm : Pour $n \geq 3$, $SO(E)$ est engendré par les renversements orthogonaux.
  Tout $u \in SO(E)$ est produit d'au plus n renversements.
- Lem : Soit $n \geq 3$ et τ, τ' des réflexions. Alors il existe des renversements σ, σ' tels que $\tau.\tau' = \sigma.\sigma'$.
- App : Pour $n \geq 2$, on a $D(O(E)) = SO(E)$.
  Pour $n \geq 3$, on a $D(SO(E)) = SO(E)$.
- Rem : Pour $n = 2$, $SO(E)$ est commutatif et on a $D(SO(E)) = \{Id\}$.
- App : Le groupe $SO_3(\mathbb{R})$ est simple.
- $SO_n(\mathbb{R})$ est connexe par arcs.
- **Dev** : Soit G le groupe des quaternions de norme 1. Alors $G/\{\pm 1\} \simeq SO_3(\mathbb{R})$.
- Rem : Cet isomorphisme, permet de ramener le calcul de l'image d'un vecteur de $\mathbb{R}^3$ par une rotation à des produits dans $\mathbb{H}$ en identifiant les vecteurs $\overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k}$ du repère orthonormé canonique de $\mathbb{R}^3$ aux éléments i,j,k de $\mathbb{H}$.

3. Homographies. —

- Def : La relation $xRy \Leftrightarrow \exists \lambda \in \mathbb{K}$ tq $x = \lambda y$ est une relation d'équivalence sur $E^2 - \{0\}$.
  On définit $P(E) := (E^2 - \{0\})/R$, et on note $dim(P(E)) = dim(E) - 1$.
  On note $P_1(\mathbb{K}) := P(\mathbb{K}^2)$ la droite projective sur $\mathbb{K}$.

- Def : Soient E,E' deux $\mathbb{K}-ev$. On appelle homographie une application $g : P(E) \to P(E')$ telle qu'il existe une application linéaire bijective $f : E \to E'$ telle que le diagramme suivant commute :
$$\begin{array}{ccc} E-\{0\} & \to_f & E'-\{0\} \\ \downarrow P & & \downarrow P \\ P(E) & \to_g & P(E') \end{array}$$
- Pro : Les homographies de $P_1(\mathbb{C})$ sont de la forme $z \mapsto \frac{az+b}{cz+d}$ avec $ad-bc \neq 0$, en choisissant pour convention de prolonger $z \mapsto \frac{1}{z}$ par ∞ en 0 et par 0 en ∞.
- Pro : Les homographies sont des bijections sur $P_1(\mathbb{C})$.
- Ex : Les similitudes directes sont des homographies. (dont les translations, rotations, homothéries)
- Ex : La fonction inverse est une homographie.
- Def : On note $PGl_2(\mathbb{C})$ le groupe des homographies de $P_1(\mathbb{C})$.
- Pro : $PGl_2(\mathbb{C})$ est engendré par les similitudes directes et la fonction inverse.
- Pro : Les homographies envoient les cercles et droites sur des cercles et droites.
- **Dev** : Les homographies engendrées par les éléments de $Sl_2(\mathbb{Z})$ préservent le demi-plan de Poincaré $H := \{Im(z) > 0\}$. Pour $D := \{z \in H \text{ tq } |z| \geq 1, |Re(z)| < \frac{1}{2}\}$, $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$et $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, on a les propriétés suivantes :
  i) L'orbite de tout élément de H par $< S, T >$ rencontre D.
  ii) Si $z \in \overset{\circ}{D}$ et $\gamma \in Sl_2(\mathbb{Z})$, $\gamma z \in D$ ssi $\gamma = \pm I_2$.
  iii) $Sl_2(\mathbb{Z}) =< S, T >$.

Références

Perrin : Sous-groupe engendré, partie génératrice, groupe dérivé. Groupes monogènes, $\mathbb{Z}/n\mathbb{Z}$. Groupe symétrique, éléments générateurs, groupe alterné, signature, groupes dérivés, automorphismes intérieurs, Groupe linéaire, dilatations, transvections, génération, groupes dérivés, applications. Groupe orthogonal, involutions, réflexions, génération, groupes dérivés, applications. $SO_3(\mathbb{R})$ et les quaternions.(Dev)
Combes : Groupes cycliques, produit direct de groupes cycliques, morphismes sur un groupe cyclique, propriétés, exemples.
Ulmer : Présentation par générateurs et relations. Th de structure des groupes abéliens de type fini, exemples. Propriétés de Σ_n. Groupes diédraux, propriétés, exemples.
Caldero, Germoni :$SO_3(\mathbb{R})$ et les quaternions.(Dev)
Lang : A_n est simple.(Dev)
Gourdon : Groupes monogènes, générateurs.
Audin : Homographies, propriétés.
Alessandrini : Action du groupe modulaire sur le demi-plan de Poincaré.(Dev)

September 18, 2017

Vidal Agniel, École normale supérieure de Rennes