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

Références : Berhuy, Rombaldi, Perrin, Caldero (Nouvelles...), Ladegaillerie

I - Généralités sur les parties génératrices

1) Définitions et sous-groupe

2) Ordre d'un élément

II - Groupes abéliens

1) Groupes monogènes et cycliques

2) Structure des groupes abéliens de type fini

III - Groupes non abéliens

1) Groupe symétrique

2) Groupes diédraux

IV - Groupes en algèbre linéaire et en géométrie affine

1) Générateurs du groupe linéaire

2) Le groupe orthogonal

3) Groupe des isométries affines

DEV 1 : $\mathfrak{A}_n$ est simple

DEV 2 : Cartan-Dieudonné

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

Soit $(G, *)$ un groupe noté G par la suite. Son neutre est e_G.

I - Généralités sur les parties génératrices

1) Définitions et sous-groupe dérivé [BERH]

DEF 1 : Soit $P \subset G$. Le sous-groupe de G engendré par P, noté $\langle P \rangle$ est l'intersection de tous les sous-groupes de G contenant P. C'est le plus petit sous-groupe de G contenant P.

THM 2 : Soit $P \subset G$. On note $P^{-1} = \{x^{-1} / x \in P\}$. Alors on a :
$\langle P \rangle = \{x_1 \cdots x_n / n \geqslant 0, x_i \in P \cup P^{-1}\}$.

REM 3 : Si $P = \{a_1, \dots, a_n\}$, $\langle P \rangle = \langle a_1, \dots, a_n \rangle$

PROP 4 : Soit $x \in G$. $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$.

PROP 5 : Si G est abélien et $P = \{a_1, \dots, a_n\}$, on a :
$\langle P \rangle = \{a_1^{m_1} \cdots a_n^{m_n} \mid m_1, \dots, m_n \in \mathbb{Z}\}$.

DEF 6 : Soit $P \subset G$. On dit que P engendre G si $G = \langle P \rangle$. On dit aussi que P est une partie génératrice ou un système de générateurs de G.

REM 7 : La notion de partie génératrice est utile pour simplifier les calculs : pour montrer que $H \subset H'$, si $H = \langle P \rangle$, il suffit de montrer $P \subset H'$.

DEF 8 : On définit le sous-groupe dérivé de G par :
$D(G) = \langle xyx^{-1}y^{-1} / x, y \in G \rangle$.

REM 9 : Si G est abélien, $D(G) = \{e_G\}$.

THM 10 : $D(G) \triangleleft G$ et $D(G) = \bigcap_{\substack{H \triangleleft G \\ G/H \text{ abélien}}} H$

2) Ordre d'un élément [BERH]

DEF 11 : On dit que $x \in G$ est d'ordre fini lorsque le sous-groupe $\langle x \rangle$ est fini. Dans ce cas, l'ordre de x est l'ordre de $\langle x \rangle$. On le note $o(x)$.

THM 12 : Soit $x \in G$. x est d'ordre fini si et seulement s'il existe $m > 0$ tel que $x^m = e_G$. Dans ce cas, l'ordre de x est le plus petit entier $n > 0$ vérifiant $x^n = e_G$.

COR 11 : On a $\langle x \rangle = \{e_G, x, \dots, x^{o(x)-1}\}$. De plus, pour tout $m \in \mathbb{Z}$, $x^m = e_G \Leftrightarrow o(x) \mid m$.

COR 12 : Avec le théorème de Lagrange, on a, si $\#G < \infty$, $o(x) \mid \#G$ et donc $x^{\#G} = e_G$.

PROP 13 : Soit x d'ordre fini dans G. Pour tout $d \geqslant 1$, x^d est d'ordre fini et $o(x^d) = \frac{o(x)}{d \wedge o(x)}$.

II - Groupes abéliens

On suppose G abélien

1) Groupes monogènes et groupes cycliques [BERH]

DEF 14 : On dit que G est monogène lorsqu'il est engendré par un élément, et cyclique lorsqu'il est monogène fini.

EX 15 :
- $\mathbb{Z}$ est monogène engendré par 1.
- $\forall n \geqslant 1$, $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n engendré par $\bar{1}$.

THM 16 : (1) Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.
(2) Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
En particulier, deux groupes cycliques sont isomorphes si et seulement s'ils ont même ordre.

COR 17 : Soit p un nombre premier, $\#G = p$. Alors G est cyclique et $G \simeq \mathbb{Z}/p\mathbb{Z}$.

THM 18 : Soit G un groupe cyclique d'ordre n. Pour tout $d \mid n$, il existe un unique sous-groupe H_d d'ordre d et H_d est cyclique. Si $G = \langle x_0 \rangle$, alors $H_d = \langle x_0^{\frac{n}{d}} \rangle$

EX 19 : $\mu_n = \{z \in \mathbb{C} / z^n = 1\}$ est cyclique d'ordre n.
$\mathfrak{S}_3$ n'est pas cyclique.

2) Structure des groupes abéliens de type fini [BERH]

DEF 20 : On dit que G est de type fini lorsqu'il est engendré par une famille finie.

THM 21 : [ADMIS] Soit G abélien fini. Alors il existe $d_1, \dots, d_s \geqslant 2$ vérifiant $d_1 \mid \cdots \mid d_s$ tels que $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$.
De plus, la suite d'entiers $(d_1, \dots, d_s)$ est unique et ne dépend que de la classe d'isomorphisme de G.

DEF 22 : La suite $(d_1, \dots, d_s)$ s'appelle la suite des invariants de similitude de G.

EX 23: $G = \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^3 \times \mathbb{Z}/8\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$

COR 24: Deux groupes abéliens finis sont isomorphes si et seulement s'ils ont mêmes invariants de similitude.

THM 25 [ADMIS]: On suppose G abélien de type fini. Alors il existe $r, s \geq 0$ et $d_1, \dots, d_s \geq 2$ vérifiant $d_1 | \dots | d_s$ tels que :

$$G \simeq \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}.$$

De plus, r et $(d_1, \dots, d_s)$ sont uniques

III - Groupes non abéliens

1) Le groupe symétrique

Soit $n \geq 2$ [BERH]

L'action naturelle de $\mathfrak{S}_n$ sur $[\![1;n]\!]$ se restreint en une action du sous-groupe $\langle\sigma\rangle$ sur $[\![1;n]\!]$ et une orbite sous cette action, appelée σ-orbite est de la forme :

$$Orb_\sigma(a) = \{\sigma^m(a) \,/\, m \in \mathbb{Z}\} \quad a \in [\![1;n]\!].$$

LEMME 26: Soit $\sigma \in \mathfrak{S}_n$ et ω une σ-orbite à p éléments et $a \in \omega$. Alors, p est le plus petit entier strictement posit. tel que $\sigma^p(a) = a$ et $\omega = \{a, \sigma(a), \dots, \sigma^{p-1}(a)\}$.

LEMME 27: Soit $\sigma \in \mathfrak{S}_n$ et $\omega \in \Omega$ une orbite non réduite à un élément. Pour $a \in [\![1;n]\!]$, on pose $\sigma_\omega(a) = \begin{cases} \sigma(a) & \text{si } a \in \omega \\ a & \text{sinon} \end{cases}$

σ_ω est un cycle de support ω et pour tout $a \in \omega$, on a $\sigma_\omega = (a\ \sigma(a) \dots \sigma^{p-1}(a))$, où $p = \#\omega$. De plus, tout p-cycle de $\mathfrak{S}_n$ est de cette forme.

THM 28: Soit $\sigma \in \mathfrak{S}_n$. Alors, σ se décompose en produit de cycles à supports disjoints, et cette décomposition est unique à l'ordre des facteurs près. Cette décomposition est donnée par : $\sigma = \prod_{\omega \in \Omega^*} \sigma_\omega$ où Ω^* est l'ensemble des σ-orbites non réduites à un singleton.

REM 29: Cela donne donc que $\mathfrak{S}_n$ est engendré par les cycles.

COR 30: $\mathfrak{S}_n$ est engendré par les transpositions.

PROP 31: Un p-cycle est d'ordre p. Si $\sigma = \sigma_1 \dots \sigma_n$ où σ_i sont des cycles à supports disjoints, alors, l'ordre de σ est le ppcm des ordres des cycles σ_i.

THM 32: Deux permutations sont conjuguées dans $\mathfrak{S}_n$ si et seulement si les listes (avec répétition) des longueurs des cycles à supports disjoints qui les composent sont les mêmes à l'ordre près.

THM 33: Le groupe $\mathfrak{S}_n$ est engendré par chacune des familles :
(1) les transpositions $(1\ i)$, $i \in [\![2;n]\!]$
(2) les transpositions $(i\ i{+}1)$, $i \in [\![1;n-1]\!]$
(3) les permutations $(1 2)$ et $(1 2 \dots n)$.

THM 34: Il existe un unique morphisme de groupes non trivial de $\mathfrak{S}_n$ dans $\mathbb{C}^*$. Ce morphisme s'appelle la signature et est noté ε.

DEF 35: Le noyau de ε, noté $\mathfrak{A}_n$, s'appelle le groupe alterné.

PROP 36: Pour $n \geq 3$, $\mathfrak{A}_n$ est engendré par les 3-cycles [DEV 1]

PROP 37: Pour $n \geq 5$, tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

THM 38: Pour $n = 3$ et $n \geq 5$, $\mathfrak{A}_n$ est simple.

2) Le groupe diédral

[ROM] [PER]

DEF 39: On dit que G est diédral de type D_{2n} lorsqu'il est engendré par un élément ρ d'ordre n et un élément $\sigma \neq \rho$ d'ordre 2 tel que $\rho\sigma\rho\sigma = e_G$.

THM 40: Si G est diédral de type D_{2n}, alors on a :
$G = \{e_G, \rho, \dots, \rho^{n-1}\} \cup \{\sigma, \sigma\rho, \dots, \sigma\rho^{n-1}\}$.
- Deux groupes diédraux de type D_{2n} sont isomorphes.

REM 41: Le groupe diédral D_{2n} possède une interprétation géométrique : il s'agit du groupe des isométries du plan conservant un polygône régulier à n côtés. Il contient les n rotations ρ d'angle $\frac{2k\pi}{n}$, $k \in [\![0;n-1]\!]$ de centre O (centre du polygône), et les n réflexions par rapport aux droites passant par O et les sommets ou les milieux des côtés du polygone.

PROP 42: D_{2n} n'est pas abélien.

PROP 43: On a une suite exacte :

$$1 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow D_{2n} \xrightarrow{f} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

IV - Groupes en algèbre linéaire et en géométrie affine

1) Générateurs du groupe linéaire [CAL]

DEF 44: On définit les matrices élémentaires suivantes:

- dilatation: $D_i(\alpha) = \begin{pmatrix} 1 & & & (0) \\ & \ddots & & \\ & & \alpha & \\ (0) & & & \ddots \\ & & & & 1 \end{pmatrix} = I_n + (\alpha-1)E_{i,i}$ $\alpha \in K \setminus \{0\}$
- transvection: $T_{i,j}(\lambda) = \begin{pmatrix} 1 & & \lambda & (0) \\ & \ddots & & \\ (0) & & \ddots & \\ & & & 1 \end{pmatrix} = I_n + \lambda E_{i,j}$ $(i \neq j)$
- permutation: $P_{i,j} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 0 & 1 & \\ & & 1 & 0 & \\ & & & & \ddots \end{pmatrix}$

PROP 45: Effectuer des opérations élémentaires sur les lignes (les colonnes) d'une matrice $A \in \mathcal{M}_{n,m}(K)$ revient à multiplier A à gauche (à droite) par une matrice élémentaire

Opération	$D_i(\alpha)A$	$T_{i,j}(\lambda)A$	$P_{i,j}A$
Résultat	$L_i \leftarrow \alpha L_i$	$L_i \leftarrow L_i + \lambda L_j$	$L_i \leftrightarrow L_j$
Opération	$AD_i(\alpha)$	$AT_{i,j}(\lambda)$	$AP_{i,j}$
Résultat	$C_i \leftarrow \alpha C_i$	$C_j \leftarrow C_j + \lambda C_i$	$C_i \leftrightarrow C_j$

PROP 46 Ces matrices sont inversibles et $D_i(\alpha)^{-1} = D_i(\frac{1}{\alpha})$
$T_{i,j}(\lambda)^{-1} = T_{i,j}(-\lambda)$, $P_{i,j}^{-1} = P_{i,j}$

THM 47: Toute matrice $A \in GL_n(K)$ s'écrit $A = \prod_{k=1}^{r} P_k D_n(\alpha) \prod_{j=1}^{s} Q_j$ où $P_1, \dots, P_r, Q_1, \dots, Q_s$ sont des matrices de transvection et $\alpha = \det(A)$.

REM 48: $GL_n(K)$ est donc engendré par les matrices de transvection et de dilatation. $SL_n(K)$ est engendré par les matrices de transvection

COR 49: Les groupes $SL_n(\mathbb{R})$, $SL_n(\mathbb{C})$ et $GL_n(\mathbb{C})$ sont connexes par arcs.

COR 50: Les ensembles $GL_n^+(\mathbb{R})$, $GL_n^-(\mathbb{R})$ sont connexes par arcs et ce sont les composantes connexes de $GL_n(\mathbb{R})$.

2) Le groupe orthogonal [PER]

Soit E un espace euclidien de dimension finie $n \in \mathbb{N}^*$. On note $O(E)$ le groupe orthogonal constitué des isométries vectorielles et $O_n(\mathbb{R})$ le groupe des matrices orthogonales. On note $SO(E)$ le groupe spécial orthogonal des isométries directes, $SO_n(\mathbb{R})$ le groupe des matrices associées.

THM 51: Le groupe $O(E)$ est engendré par les réflexions orthogonales. Plus précisément, si $u \in O(E)$, u est produit d'au plus $p_u = rg(u - Id_E)$ réflexions.

PROP 52: Ce nombre p_u est minimal. $u \in O(E)$ est donc produit d'exactement p_u réflexions.

THM 53: Pour $n \geq 3$, $SO(E)$ est engendré par les renversements : tout $u \in SO(E)$ est produit d'au plus n renversements.

3) Groupe affine et isométries affines [LAP]

Soit $(E, \vec{E})$ un espace affine euclidien.

DEF 54: Une application $f: E \to F$ est une isométrie lorsque $\forall (M,N) \in E^2$, $\|\overrightarrow{MN}\| = \|\overrightarrow{f(M)f(N)}\|$

THM 55: Les isométries $f: E \to F$ sont les applications affines dont la partie linéaire est une isométrie vectorielle.

PROP 56: L'ensemble $Is(E)$ des isométries affines est un groupe

THM 57: Toute isométrie affine f de E s'écrit de façon unique comme le produit commutatif $f = t_{\vec{u}} \circ g = g \circ t_{\vec{u}}$ de g isométrie à point fixe et de $t_{\vec{u}}$ translation où $\vec{u} \in \ker(\vec{f} - Id_{\vec{E}})$

REM 58: Le THM 51 permet la classification des isométries vectorielles en dimension 2 et 3.
Grâce au THM 57, on classifie les isométries affines en dimension 2 et 3.

THM 59: $Is(\text{tétraèdre}) \simeq \mathfrak{S}_4$
$Is(\text{cube}) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$