108 - Exemples de parties génératrices de groupe. Applications.

I) Définitions et Généralités.

[1] **Def 1** Soit G un groupe et $A \subset G$. Il existe un plus petit sous groupe (noté sg) de G contenant A. Il s'écrit comme produit de A et d'inverses de A. On l'appelle sous groupe engendré par A : $H = \langle A \rangle$. Si A est fini alors on note $H = \langle x_1, \dots, x_n \rangle$

[3] **Ex 2** Soit $n \in \mathbb{N}$, le groupe Diédral D_n est le groupe des isométries du plan euclidien conservant un polygone régulier à n côtés. Il possède n rotations de centre O le centre du polygone et n symétries par rapport aux droites passant par O et par les sommets du polygone (si n est pair) ou par les milieux des côtés (si n est impair). On a : $D_n = \langle s, r \rangle$ où $o(s) = 2$, $o(r) = n$ et $o(sr) = 2$. De plus si on appelle $D(D_n)$ le groupe dérivé de D_n, c'est à dire le plus petit sg distingué de D_n engendré par les commutant : $srs^{-1}r^{-1}$, on a : $D(D_{2n}) = \langle r \rangle$ et $D(D_{2n+1}) = \langle r^2 \rangle$ où $o(r) = n$.

[1] **Def 3** Un groupe G est dit de type fini si il existe un nombre fini d'éléments $a_1, \dots, a_n \in G$ tels que $G = \langle a_1, \dots, a_n \rangle$

Ex 4 D_n, $\mathbb{Z}^n = \langle (1,0,\dots,0), (0,1,0,\dots,0), \dots, (0,\dots,0,1) \rangle$

[4] **Cex 5** $(\mathbb{Z}[X], +)$ est engendré par $\{1, X, \dots, X^k, \dots\}$.

[5] **Def 6** Soit $g \in G$, g est un élément mou si $\forall a_1, \dots, a_k \in G$ tels que $\langle g, a_1, \dots, a_k \rangle = G$ alors $\langle a_1, \dots, a_k \rangle = G$.

Ex 7 L'élément neutre est mou, $\overline{2}$ est mou dans $\mathbb{Z}/2n\mathbb{Z}$.

Def 8 Une partie génératrice de G est dite minimale si elle n'engendre plus G lorsque l'on lui retire un élément.

[4] **Def 9** G est un p-groupe (p premier) si $|G| = p^k$, $k \in \mathbb{N}^*$

Ex 10 Soit p premier $(\mathbb{Z}/p\mathbb{Z})^k$ est un p groupe $\forall k \in \mathbb{N}^*$

Def 10 Soit G un groupe. On appelle groupe de Frattini de G (noté) $\Phi(G)$ l'intersection de tous ses sg maximaux.

Ex 12 $\Phi(\mathbb{Q}) = \mathbb{Q}$ pour $(\mathbb{Q}, +)$.

[5] **prop 13** Soit G un groupe. $\Phi(G)$ est l'ensemble des éléments mou de G.

[4] **thm 14** Soit G un p-groupe. Les familles génératrices minimales ont même cardinal.

Def 15 On appelle $\mathbb{F}_n$ le groupe libre à n éléments construit par concaténation des éléments $\{a_1, \dots, a_n\}$ un ensemble de caractères. On identifie deux mots une fois enlevé les syllabes de la forme $a_i a_i^{-1}$ et $a_i^{-1} a_i$. Si $m \in \mathbb{F}_n$ alors $m = a_{i_1}^{\varepsilon_1} \cdots a_{i_s}^{\varepsilon_s}$ où $\forall j$ $\varepsilon_j \in \{-1, 1\}$ et $a_{i_j} \in \{a_1, \dots, a_n\}$.

Def-prop 16 Soit G un groupe et $b_1, \dots, b_n \in G$. Il existe un unique morphisme $\varphi : \mathbb{F}_n \to G$ tel que $\forall i \in \{1, \dots, n\}$ $\varphi(a_i) = b_i$. Ce morphisme est surjectif ssi les $(b_i)_{1 \le i \le n}$ engendrent G. En particulier, dans ce cas $G \simeq \mathbb{F}_n / \ker \varphi$. On appelle présentation de G par générateurs et relations la donnée de générateurs $(b_i)_i$ et d'une partie génératrice du sous groupe distingué $\ker \varphi$ appelée relation.
On note alors $G = (b_1, \dots, b_n \mid r_1, \dots, r_p)$.

[4] **Ex 17** $D_n = (r, s \mid s^2 = 1, r^n = 1, srs = r^{-1})$. On notera par la suite $D_n = (r, s \mid s^2, r^n, srsr)$.

II] Groupes monogènes, $\mathbb{Z}/n\mathbb{Z}$.

[1] **Def 18** Soit G un groupe. On dit que G est monogène s'il est engendré par un seul élément : $\exists a \in G$ tel que $G = \langle a \rangle$

Ex 19 $(n\mathbb{Z}, +)$ est engendré par n, $\forall n \geq 1$.

[1] **Prop 20** Tous les groupes monogènes sont abéliens.

[5] **Def 21** $(n\mathbb{Z}, +)$ est distingué dans $(\mathbb{Z}, +)$. On définit alors le quotient $\mathbb{Z}/n\mathbb{Z}$.

[5] **Prop 22** $\mathbb{Z}/n\mathbb{Z}$ est cyclique, il est engendré par $\bar{1}$.

[5] **Prop 23** Soit G un groupe monogène. G est isomorphe à $\mathbb{Z}$ ou à un $\mathbb{Z}/n\mathbb{Z}$.

Ex 24 Le groupe des racines n'ième de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Prop 25 Soit $k \in \mathbb{Z}$. On a:
$k \wedge n = 1 \iff \langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z} \iff \bar{k} \in (\mathbb{Z}/n\mathbb{Z})^*$

Ex 26 $\mathbb{Z}/n\mathbb{Z}$ possède $\varphi(n)$ générateurs où φ est l'indicatrice d'Euler.

[1] **Prop 27** Tout sous groupe d'un groupe cyclique est cyclique et pour tout diviseur d de n, il existe un unique sous groupe H_d de G d'ordre d. En posant $\delta = n/d$, ce sous groupe est caractérisé par :
$$H_d = \{x \in G \,/\, x^d = e\} = \langle a^{\delta} \rangle \text{ où } G = \langle a \rangle.$$

[1] **Thm 28** Théorème Chinois. Soit $k \wedge n = 1$, on a alors
$$\mathbb{Z}/nk\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$$

Ex 29 $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Ex 30 $\mathbb{Z}/6\mathbb{Z} = \langle x \mid x^6 \rangle = \langle x, y \mid x^2, y^3, xyx^{-1}y^{-1} \rangle$ [6]
avec les morphismes : $\varphi_6 : \mathbb{F}_1 \to \mathbb{Z}/6\mathbb{Z}$, $x^i \mapsto \bar{i}$
et $\varphi_{2,3} : \mathbb{F}_2 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$x^i \mapsto (\bar{i}, \hat{0})$
$y^j \mapsto (\bar{0}, \hat{j})$

Thm 31 Théorème de Structure des groupes abélien fini. [7]
Soit G un groupe abélien fini d'ordre $n \geq 2$. Il existe des uniques $q_1 | \dots | q_k$ des entiers tels que $G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_k\mathbb{Z}$

Thm 32 Théorème de structure des groupes abéliens de type fini: [2]
Soit G un groupe abélien de type fini. Il existe un unique r et $q_1 | \dots | q_k$ entiers naturels tels que : $G \simeq \mathbb{Z}^r \times \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_k\mathbb{Z}$

III Groupe Symétrique:

Def 33 Soit $n \in \mathbb{N}^*$. On note S_n le groupe des permutations de $\{1, \dots, n\}$ (muni de la loi de composition). Le groupe S_n est appelé groupe symétrique d'indice n. Si $\sigma \in S_n$, on note $\sigma := \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$. De plus, $\mathrm{Card}\, S_n = n!$

Def 34 Soit $\sigma \in S_n$. On appelle point fixe de σ un élément invariant par σ. On appelle support de σ [1]
le complémentaire des points fixe dans $\{1, \dots, n\}$.

Ex 35 $\sigma_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$ possède 4 et 5 comme point fixe et $\mathrm{Supp}\, \sigma = \{1, 2, 3\}$.

Prop 36 Soient $\sigma_1, \sigma_2 \in S_n$. Si $\mathrm{Supp}\, \sigma_1 \cap \mathrm{Supp}\, \sigma_2 = \emptyset$ alors σ_1 et σ_2 commutent

Def 37 Soit $l \in \mathbb{N}^*$ et $i_1, \dots, i_l \in \{1, \dots, n\}$ distincts. La permutation $\sigma \in S_n$ définie par $\operatorname{supp}\sigma = \{i_1, \dots, i_l\}$ et $\sigma(i_k) = i_{k+1}$ si $1 \leq k < l$ et $\sigma(i_l) = i_1$ est appelé cycle de longueur l. Un cycle de longueur 2 est appelé transposition. On écrit alors $\sigma_0 = (1\,2\,3)$ (ex 35)

[1] Th 38 Toute permutation s'écrit de manière unique en produit de cycles à supports disjoints.

[1] Th 39 Tout cycle s'écrit en produit de transpositions.

[1,2] Thm 40 S_n est engendré par les parties suivantes :
- l'ensemble des transpositions
- l'ensemble des transpositions adjacentes : $(i\ i+1)$ $i \in [\![1, n-1]\!]$
- $\{(1\ i),\ i \in \{2, \dots, n\}\}$
- $\{\tau, c\}$ où τ est une transposition et c un n-cycle. [4]

DEV 2 Thm 41 S_n est présenté par les transpositions adjacentes et les relations : $r_1 = \{a_i^2, \forall i \in \{1, \dots, n-1\}\}$, $r_2 = \{(a_i a_{i+1})^3, 1 \leq i \leq n-2\}$, $r_3 = \{a_i a_j a_i^{-1} a_j^{-1}, 1 \leq i < j-1 \leq n-2\}$

[2] Def 42 Soit $\sigma \in S_n$, on définit la signature de σ :
$$\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

[2] Prop 43 La signature est un morphisme de S_n dans $(\mathbb{Q}^*, \times)$ et $\varepsilon(S_n) = \{-1, 1\}$. $\varepsilon(\tau) = -1$ pour une transposition et

[2] Def 44 Le noyau du morphisme signature est un sous groupe distingué de S_n noté A_n et appelé le groupe alterné.

[2] Thm 45 A_n est engendré par les 3-cycles.

[2] Thm 46 A_n est simple pour $n \geq 5$.

IV Sous groupes de $GL(E)$, E est un $\mathbb{k}$ espace vectoriel

Def 47 Le groupe linéaire $GL(E)$ est le groupe des $\mathbb{k}$ (corps commutatif) automorphisme de E. Le groupe spécial linéaire $SL(E)$ est le sous groupe de $GL(E)$ formé des automorphismes de déterminant 1. [3]

Thm 48 Soit H un hyperplan et $u \in GL(E)$ tel que $u_{|H} = id_H$. [3]
Il y a équivalence entre :
- $\det u = \lambda \neq 1$
- u admet une valeur propre $\lambda \neq 1$ et u diagonalisable
- $\operatorname{Im}(u - id) \not\subset H$
- Il existe une base dans laquelle la matrice de u est de la forme :

$$\left(\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & 0 \\ 0 & & 1 & \\ \hline & 0 & & \lambda \end{array}\right), \lambda \neq 1.$$

On dit alors que u est une dilatation d'hyperplan H de droite $D = \operatorname{Im}(u - id)$.

Thm 49 Soit H un hyperplan, $f \in E^*$ tel que $\ker f = H$ et $u \in GL(E)$ différent de l'identité tel que $u_{|H} = id_H$. [3]
Il y a équivalence entre :
- $u \in SL(E)$
- u non diagonalisable
- $D = \operatorname{Im}(u - id) \subset H$
- $\bar{u} : E/H \longrightarrow E/H$ induit l'identité de E/H
- $\exists a \neq 0 \in H$ tel que $\forall x \in E$, $u(x) = x + f(x)a$
- Il existe une base dans laquelle la matrice de u est de la forme :

$$\left(\begin{array}{ccc|c} 1 & & 0 & 0 \\ & \ddots & & 0 \\ 0 & & 1 & 1 \\ \hline 0 & \cdots & 0 & 1 \end{array}\right)$$

On dit alors que u est une transvection d'hyperplan H et de droite D. On a $D = (a)$ et $D \subset H$.

Thm 50 Les transvections engendrent $SL(E)$. [3]

Thm 51 Les transvections et les dilatations engendrent $GL(E)$. [3]