

Leçon N° 108 Exemples de parties génératrices d'un groupe Applications

Dans toute cette leçon, G est un groupe.

I) Préliminaires.

1) Définitions et propriétés.

Lemme 1: L'intersection quelconque de sous groupes de G est un sous groupe de G .

Corollaire 2: Si X est une partie de G , l'intersection de tous les sous groupes de G qui contiennent X est un sous groupe de G .

Définition 3: Si X est une partie de G , le sous-groupe de G engendré par X est l'intersection de tous les sous groupes de G qui contiennent X .

Définition 4: Si X est une partie de G , on dit que X engendre G lorsque $G = \langle X \rangle$.

Définition 5: On dit que G est de type fini lorsqu'il admet une partie génératrice finie.

Remarque 6: Soient $P, Q \subseteq G$ et H un sous groupe de G .

1) $P \subseteq \langle P \rangle$

2) Si $P \subseteq H$, alors $\langle P \rangle \subseteq H$

3) $\langle P \rangle = P$ si P est un sous groupe de G .

4) Si $P \subseteq Q$, alors $\langle P \rangle \subseteq \langle Q \rangle$.

5) $\langle \emptyset \rangle = \{1_G\}$

Théorème 7: Soit P une partie de G . On note $P^{-1} = \{x^{-1} \mid x \in P\}$.

Alors $\langle P \rangle = \langle a_1, \dots, a_n, n > 0, n \in \mathbb{Z}, a_i \in P \cup P^{-1} \rangle$.

Corollaire 8: Si G est abélien et si $P = \{a_1, \dots, a_r\}$,
 $\langle P \rangle = \{a_1^{m_1} \dots a_r^{m_r} \mid (m_1, \dots, m_r) \in \mathbb{Z}^r\}$.

2) Premiers exemples.

Exemple 9: Soit $n \in \mathbb{Z}$, $\langle n \rangle = \{x^n \mid x \in \mathbb{Z}\}$.

Exemples 10: 1) $\mathbb{Z} = \langle 1 \rangle$

2) $\forall n \in \mathbb{N}^*, (\mathbb{Z}/n\mathbb{Z}, +) = \langle \overline{1} \rangle$

3) $\forall n \in \mathbb{N}^*, \langle n \rangle = \langle e^{2i\pi/n} \rangle$

Définition 11: Le groupe dérivé de G est le sous groupe $D(G)$ engendré par les commutateurs de G , i.e. $\{[a, b] = aba^{-1}b^{-1} \mid (a, b) \in G^2\}$

Proposition 12: Le groupe dérivé $D(G)$ est le plus petit sous groupe distingué H de G tel que G/H soit abélien.

Exemple 13: Si G est commutatif, $D(G) = \{1\}$.

Exemple 14: Soient $a, b \in \mathbb{Z}$, $d, m \in \mathbb{Z}$ tels que

$\langle a, b \rangle = a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$

Alors d est un p.g.c.d de a et b et m est un p.p.c.m de a et b .

3) Groupes monogènes et groupes cycliques

Définition 15: On dit que G est monogène lorsqu'il existe $g \in G$ tel que $G = \langle g \rangle$. Si de plus G est fini, on dit qu'il est cyclique.

Exemples 16: $(\mathbb{Z}, +)$ est monogène.

$\forall n \in \mathbb{N}^*, (\mathbb{Z}/n\mathbb{Z}, +)$ et $(U_n, \cdot)$ sont cycliques.

Théorème 17: Soit G un monogène, alors:

1) Si G est infini, $G \cong \mathbb{Z}$

2) Si G est fini, $G \cong \mathbb{Z}/n\mathbb{Z}$ avec $n = \#G$.

Proposition 18: Si $G = \langle g \rangle$ est cyclique d'ordre n , alors ses générateurs sont les g^k , $k \in \{1, n-1\}$ (i.e. $k, n = 1$).

Proposition 19: Un groupe de cardinal premier est cyclique.

Proposition 20: Un groupe commutatif d'ordre pq où p et q sont deux nombres premiers distincts, est cyclique.

Proposition 21: Si $n \geq 2$ est un entier premier avec $\varphi(n)$, alors l'ensemble commutatif d'ordre n est cyclique.

Théorème 22: Un groupe commutatif fini d'ordre $n \geq 1$ est cyclique si et seulement si n est premier.

Théorème 23: Soit $H \triangleleft G$. Les sous-groupes de G/H sont de la forme K/H où K est un sous-groupe de G qui contient H .

Application 24: $\forall n \geq 2$, $n = \prod_{i=1}^k p_i^{a_i}$ où p_i est l'indice de Euler.

II) Générateurs du groupe symétrique et du groupe alterné.

Soit $n \in \mathbb{N}^*$.

1) Le groupe symétrique.

Proposition 25: S_n est engendré par les transpositions.

Proposition 26: S_n est engendré par les $n-1$ transpositions $(1, 2), (2, 3), \dots, (n-1, n)$.

Proposition 27: S_n est engendré par les $n-1$ transpositions $(1, 2), (2, 3), \dots, (n-1, n)$.

Proposition 28: S_n est engendré par $(1, 2)$ et $(1, 2, \dots, n)$.

Exemple 29: Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix}$

$$\sigma = (1, 2, 3, 4, 5)(6, 7)$$

$$= (1, 2)(2, 3)(3, 4)(4, 5)(6, 7)$$

$$= (1, 3)(1, 2)(1, 3)(1, 4)(1, 3)(1, 4)(1, 5)(1, 4)(1, 6)(1, 7)(1, 6).$$

Proposition 30: Si $\sigma \in S_n$ est produit de p transpositions,

on a alors $\epsilon(\sigma) = (-1)^p$.

Application 31: Soit $\sigma \in \text{Sym}(1, 2)$, alors $\epsilon(\sigma) = \sum_{\tau \in S_n} \prod_{i=1}^n m_i \tau(i)$.

2) Le groupe alterné.

Définition 32: $A_n = \ker(\epsilon)$

Lemme 33: Si $n \geq 5$, A_n est engendré par les 3-cycles.

Lemme 34: Si $n \geq 5$, les 3-cycles sont conjugués dans A_n .

Lemme 35: Les double transpositions sont conjugués dans S_5 .

Théorème 36: Si $n \geq 5$, A_n est simple.

Corollaire 37: Si $n \geq 5$, $D(A_n) = A_n$.

Si $n \geq 2$, $D(S_n) = S_n$.

Contre-exemple 38: Si $n = 4$: $D(A_4) = \{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$

III) Groupes utiles en géométrie.

1) Le groupe diédral.

Définition 39: Soit $n \geq 2$. Le groupe diédral D_n est le groupe des isométries du plan euclidien conservant un polygone régulier à n côtés. On note O le centre du polygone.

Proposition 40: D_n est engendré par la rotation ρ et l'angle $2\pi/n$ et une réflexion par rapport à un droite passant par O et un sommet du polygone.

2) Les groupes orthogonaux et symétriques orthogonaux.

Définition 41: Soit E un espace vectoriel réel euclidien de dimension finie.

1) Une réflexion orthogonale de E est une symétrie orthogonale dont l'ensemble des points fixes est un hyperplan.

2) Un renversement orthogonale de E est une symétrie orthogonale dont l'ensemble des points fixes est un sous-espace vectoriel de E de dimension ≥ 1 .

Lemme 42: Soient $n \geq 1$ et τ_1, τ_2 deux réflexions, alors il existe σ_1, σ_2 deux renversements tels que $\tau_1 \tau_2 = \sigma_1 \sigma_2$.

Théorème 43: Soient E un espace vectoriel réel de dimension finie n , φ une forme quadratique sur E supposée définie positive.

- 1) $O(\varphi)$ est engendré par les réflexions orthogonales, plus précisément si $u \in O(\varphi)$, u est produit d'un plus ou réflexions.
- 2) $SO(\varphi)$, $n \geq 3$, est engendré par les renversements plus précisément, si $u \in SO(\varphi)$, alors u est produit d'un plus ou renversements.

Proposition 44: 1) $\forall n \geq 2, D(O(\varphi)) = O(\varphi)$

2) $\forall n \geq 3, D(SO(\varphi)) = SO(\varphi)$.

Théorème 45: $SO_3(\mathbb{R})$ est simple.

IV) Générateurs des groupes classiques.

Soit E un $\mathbb{K}$ -esp. de dimension finie $n \in \mathbb{N}^*$.

Définition 46: Soit φ une forme linéaire non nulle sur E . On appelle transvection l'application linéaire φ (à une application linéaire $\psi \in L(E)$) définie par $\forall x \in E, \psi(x) = x + \varphi(x) \cdot \alpha$ où $\alpha \in \mathbb{K} \setminus \{0\}$.

Définition 47: Soit φ une forme linéaire non nulle sur E . On appelle dilatation d'hyperplan ψ toute application linéaire $\psi \in L(E)$ définie par: $\forall x \in E, \psi(x) = x + \varphi(x) \cdot \alpha$ où $\alpha \in E \setminus \ker(\varphi)$.

Proposition 48: $SL(E)$ est engendré par les transvections.

Corollaire 49: $GL(E)$ est engendré par les transvections et les dilatations.

Application 50: (Pivot de Gauss).

Soit $A \in M_n, n(1, n)$. Il existe $P \in GL_n(\mathbb{K})$ produit de matrices de permutation et de transvections telle que PA

Soit échelonnée en lignes.

Proposition 51: 1) $D(SL(E)) \subseteq D(GL(E)) \subseteq SL(E)$.

2) $\forall n \geq 3, D(SL(E)) = D(GL(E)) = SL(E)$.

3) pour $n=2$ et $\mathbb{K} \neq \mathbb{F}_2, D(GL(E)) = SL(E)$.

4) pour $n=2$ et $\mathbb{K} \neq \mathbb{F}_2$ et $\mathbb{K} \neq \mathbb{F}_3, D(SL(E)) = D(GL(E)) = SL(E)$.