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

Dans cette leçon on considère $(G, \cdot)$ un groupe.

1 Généralités et groupe abélien

1.1 Parties génératrices

Proposition 1. *Soit G un groupe, l'intersection d'une famille quelconque $(H_i)_{i\in I}$ de sous groupes de G est un sous groupe de G.*

Définition 2.
1. Soit $X \subset G$, le sous groupe de G engendré par X noté $\langle X\rangle$ est l'intersection de tous les sous groupes de G contenant X.
2. Soit $X \subset G$, on dit que X engendre G lorsque $\langle X\rangle = G$. On dit que G est de type fini lorsqu'il admet une partie génératrice finie.

Théorème 3. *1. En notant $X^{-1} = \{x^{-1} | x \in X\}$, les éléments de $\langle X\rangle$ sont de la forme $x_1 \dots x_r$ avec $x_i \in X \cup X^{-1}$ pour tout $k \in [\![1, r]\!]$.*

2. Pour tout $p \in \mathbb{N}^*$ et tout p-uplet $(g_1, \dots, g_p) \in G^p$ qui commutent 2 à 2 on a $\langle g_1, \dots, g_p\rangle = \{\prod_{k=1}^{p} g_k^{\alpha_k} | \alpha_k \in \mathbb{Z}\}$ et ce groupe est commutatif.

Définition 4. L'ordre du groupe G est son cardinal et l'ordre d'un élément $g \in G$ est $o(g) = Card(\langle g\rangle)$.

Proposition 5. *Pour $g \in G$ et $n \in \mathbb{N}^*$ les assertions suivantes sont équivalentes :*
- *g est d'ordre n,*
- *$g^n = e_G$ et $g^k \neq e_G$ pour tout $k \in [\![1, n-1]\!]$,*
- *Pour $k \in \mathbb{Z}$, on a $g^k = e_G$ si et seulement si $n|k$.*

Définition 6. Le groupe dérivé de G est le sous groupe engendré par les commutateurs $[a, b] = aba^{-1}b^{-1}$ avec $a, b \in G$ on le note $D(G) = \langle [a, b]\rangle$

Théorème 7. *Le groupe dérivé de G est le plus petit sous groupe distingué H tel que G/H soit commutatif.*

1.2 Groupes monogènes

Définition 8. On dit que G est monogène lorsqu'il existe $g \in G$ tel que $G = \langle g\rangle$. Si de plus G est fini, il est dit cyclique.

Théorème 9. *Si G est monogène infini alors il est isomorphe à $(\mathbb{Z}, +)$. Si G cyclique d'ordre n alors il est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Théorème 10. *Si $G = \{g\}$ cyclique d'ordre n, ses générateurs sont alors les g^k où $k \in [\![1, n]\!]$ premier avec n.*

Théorème 11. *Tout groupe d'ordre premier est cyclique.*

Théorème 12. *Les assertions suivantes sont équivalentes :*
- *$\mathbb{Z}/n\mathbb{Z}$ est un corps,*
- *$\mathbb{Z}/n\mathbb{Z}$ intègre,*
- *n est premier.*

Corollaire 13. *Le groupe des inversible $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ est donc cyclique.*

Exemple 14. Pour n non premier c'est totalement faux, par exemple $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ n'a que 4 éléments.

Théorème 15. *Si p premier impair et $\alpha \in \mathbb{N}\backslash\{0, 1\}$ alors $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.*

Théorème 16. *Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = 2$, $n = 4$, $n = p^\alpha$ ou $n = 2p^\alpha$ avec p premier impair et $\alpha \geqslant 1$ entier.*

Théorème 17. *Un groupe commutatif d'ordre pq avec p et q premiers distincts est cyclique.*

Corollaire 18. *Si $p \geqslant 2$ premier et G un p-groupe opérant sur un ensemble X fini, alors $|X^G| \equiv |X| \mod p$*

Corollaire 19. *Soit G un groupe fini qui opère sur lui même par conjugaison, en notant $\Omega(x_1), \ldots, \Omega(x_r)$ toutes les orbites 2 à 2 distinctes, on a :*

$$|G| = |Z(G)| + \sum_{\substack{i=1 \\ |\Omega(x_i)|\geqslant 2}}^{r} |\Omega(x_i)| = |Z(G)| + \sum_{\substack{i=1 \\ |\Omega(x_i)|\geqslant 2}}^{r} \frac{|G|}{|Stab(x_i)|}$$

Théorème 20. *Pour tout nombre premier p, le centre d'un p-groupe n'est pas réduit à $\{1\}$.*

Théorème 21. *Tout groupe d'ordre p^2 avec p premier est commutatif. Il est isomorphe soit à $\mathbb{Z}/p^2\mathbb{Z}$ soit à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Proposition 22. *Soit p premier impair, si G groupe d'ordre $2p$ alors G est isomorphe soit à $\mathbb{Z}/2p\mathbb{Z}$ soit à D_{2p}.*

2 Groupe symétrique

2.1 Introduction et générateurs

Définition 23. Le groupe symétrique à n éléments est $\mathcal{S}_n$ l'ensemble des bijections de $[\![1, n]\!]$ dans lui même.

Définition 24. Soit $2 \leqslant r \leqslant n$. On appelle r-cycle toute permutation $\sigma \in \mathcal{S}(E)$ qui permute circulairement r éléments et laisse fixe les autres. C'est-à-dire qu'il existe $\{x_1, \ldots, x_r\} \subset E$ telle que : $\forall k \in \{1, \ldots, r-1\}, \sigma(x_k) = x_{k+1}$; $\sigma(x_r) = x_1$; $\forall x \in E \backslash \{x_1 \ldots, x_r\}, \sigma(x) = x$. On notera un tel cycle $(x_1, \ldots, x_r)$.

Proposition 25. *L'inverse d'un r-cycle est un r-cycle, précisément $(x_1, \ldots, x_r)^{-1} = (x_r, \ldots, x_1)$.*

Définition 26. Un 2-cycle est appelé transposition.

Proposition 27. *Soit $2 \leqslant r \leqslant n$. Le conjugué dans $\mathcal{S}_n$ d'un r-cycle est encore un r-cycle. Plus précisément pour tout $\sigma = (x_1, \ldots, x_r)$ et toute permutation τ on a $\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1), \ldots, \tau(x_r))$. Réciproquement deux cycles de même longueur sont conjugués dans $\mathcal{S}_n$.*

Théorème 28. *Le groupe symétrique $\mathcal{S}_n$ est de cardinal $n!$.*

Théorème 29. *Toute permutation $\sigma \in \mathcal{S}(E) \backslash \{Id\}$ se décompose en produit de cycles à support disjoints. Cette décomposition est unique à l'ordre près.*

Lemme 30. *Pour $2 \leqslant r \leqslant n$, tout r-cycle s'écrit comme produit $r-1$ transpositions.*

Théorème 31. *Toute permutation $\sigma \in \mathcal{S}(E)$ se décompose en produit de transpositions.*

Lemme 32.
1. *$\mathcal{S}_n$ est engendré par les $n-1$ transpositions $(1\ k)$ où $2 \leqslant k \leqslant n$.*
2. *$\mathcal{S}_n$ est engendré par les $n-1$ transpositions $(k\ k+1)$ où $1 \leqslant k \leqslant n-1$.*
3. *$\mathcal{S}_n$ est engendré par $(1\ 2)$ et $(1\ 2\ \ldots n)$.*

2.2 Groupe alterné

Définition 33. La signature d'une permutation $\sigma \in \mathcal{S}_n$ est l'élément $\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)} \in \{-1, 1\}$.

Exemple 34. On a $\varepsilon(Id) = 1$, pour un r-cycle σ on a $\varepsilon(\sigma) = (-1)^{r-1}$

Lemme 35. *Pour tout $\sigma \in \mathcal{S}_n$ et toute transposition $\tau \in \mathcal{S}(E)$, on a $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.*

Théorème 36. *Si $\sigma \in \mathcal{S}_n$ est produit de p transpositions, on a alors $\varepsilon(\sigma) = (-1)^p$.*

Définition 37. Le groupe alterné $\mathcal{A}(E)$ est le sous ensemble de $\mathcal{S}(E)$ formé des permutations σ de signature $\varepsilon(\sigma) = 1$.

Théorème 38. *Le sous groupe $\mathcal{A}(E)$ est un sous groupe normal du groupe $\mathcal{S}(E)$.*

Proposition 39. *Pour tout $n \in \mathbb{N}^*$, $\mathcal{A}_n$ est un sous groupe d'indice 2 de $\mathcal{S}_n$ et on a $|\mathcal{A}_n| = \frac{n!}{2}$.*

Lemme 40. *Le produit de 2 transpositions est un produit de 3-cycles. Précisément pour $x, y, z, t \in [\![1, n]\!]$ distincts on a : $(x\ y)(x\ z) = (x\ z\ y)$ et $(x\ y)(z\ t) = (x\ y\ z)(y\ z\ t)$.*

Théorème 41. *Pour $n \geqslant 3$, $\mathcal{A}_n$ est engendré par les 3-cycles.*

Théorème 42. *Pour $n \geqslant 5$ les sous groupes normaux de $\mathcal{S}_n$ sont $\{Id\}, \mathcal{A}_n$ et $\mathcal{S}_n$.*

Théorème 43. *Pour $n = 3$ ou $n \geqslant 5$ le groupe $\mathcal{A}_n$ est simple.*

Dev 1 : Classification des groupes d'ordre p^2 18, 19,20 et 21
Dev 2 : An est simple 40,41 et 43

Références

[BER18] Grégory BERHUY : Algèbre le grand combat. Calvage et Mounet, 2018.

[PER96] Daniel PERRIN : Cours d'algèbre. Ellipses, 1996.

[ROM17] JeanÉtienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Superieur, 2017.

RAPPORT DU JURY :
La leçon doit être illustrée par des exemples de groupes très variés, dont il est indispensable de donner des parties génératrices. La description ensembliste du groupe engendré par une partie doit être connue et les groupes monogènes et cycliques doivent être évoqués. Les groupes $\mathbb{Z}/n\mathbb{Z}$ fournissent des exemples naturels tout comme les groupes de permutations, les groupes linéaires ou leurs sous-groupes (par exemple $SL_n(\mathbb{K}), O_n(\mathbb{R})$ ou $SO_n(\mathbb{R})$). Ainsi, on peut s'attarder sur l'étude du groupe des permutations avec différents types de parties génératrices en discutant de leur intérêt (ordre, simplicité de A5 par exemple). On peut, en utilisant des parties génératrices pertinentes, présenter le pivot de Gauss, le calcul de l'inverse ou du rang d'une matrice, le groupe des isométries d'un triangle équilatéral. Éventuellement, il est possible de discuter des conditions nécessaires et suffisantes pour que $(\mathbb{Z}/n\mathbb{Z})^*$ soit cyclique ou la détermination de générateurs du groupe diédral. On illustre comment la connaissance de parties génératrices s'avère très utile dans certaines situations, par exemple pour l'analyse de morphismes de groupes, ou pour montrer la connexité par arcs de certains sous-groupes de $GL_n(\mathbb{R})$.
Pour aller plus loin,on peut s'intéresser à la présentation de certains groupes par générateurs et relations. Il est également possible de parler du logarithme discret et de ces applications à la cryptographie (algorithme de Diffie-Hellman, cryptosystème de El Gamal).