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

Références : Rombaldi, Perrin, Algèbre Gourdon, Cortella,

Cadre : Soit (G,+) un groupe.

1 Génération d'un groupe

1.1 Sous-groupe engendré

Lintersection d'une famille quelquonque de sous-groupe de G est un sous-groupe de G.

Définition 1. Soit X une partie de G.
L'intersection des sous-groupes de G qui contiennnent X est un sous-groupe de G. On l'appelle sous-groupe engendré par X, et on le note $\langle X \rangle$.
De plus, si $G =< X >$, alors X est appelée partie génératrice de G.

Théorème 2. *Soit X, Y deux parties de G.*

- $X \subset < X >$
- *si* $X \subset Y$, *alors,* $< X > \subset < Y >$.
- *Les éléments de X sont de la forme* $x_1^{a_1} ... x_r a_r$ *avec* $r \in \mathbb{N}^*$, $a_i = \pm 1$ *et* $x_i \in X$.

Exemple 3.
- $\forall a \in G, < a >= \{a^m \mid m \in \mathbb{Z}\}$
- si a et b commutent dans G, $< a, b >= \{a^m b^n \mid (m,n) \in \mathbb{Z}^2\}$. On à une généralisation pour p éléments qui commutent deux à deux.

Définition 4.
- Si G est engendré par une partie génératrice X finie, il est dit de type finie.
- G est dit monogène si il est engendré par un unique élément x.
- G est dit cyclique si il est fini et monogène

Exemple 5.
- Le groupe $(\mathbb{Z}, +)$ est monogène engendré par 1.
- Ses sous-groupes sont les $(n\mathbb{Z}, +)$ ($0 \neq n$), qui sont monogènes engendrés par n.

Définition 6. On appelle groupe dérivée de G le groupe engendré par les commutateurs, c'est-à-dire les éléments de la forme $aba^{-1}b^{-1}$. Il s'agit d'un sous-groupe de G

Remarque 7. Si G est abélien, alors son groupe dérivée est $\{e\}$.

1.2 Ordre d'un élément

Définition 8. Un élément a de G est dit d'ordre $p \in \mathbb{N}^*$ si le sous-groupe $< a >$ est finie de cardinal p. On à alors $< a >= \{e, a, a^2, ..., a^{p-1}\}$. Si cet ensemble n'est pas finie, a est dit d'ordre infinie.

Exemple 9.
- e est d'ordre 1 dans G
- 1 est d'ordre infini dans $(\mathbb{Z}, +)$
- Dans S_n, un cycle de longueur l est d'ordre l.
-

Théorème 10. *Si G est fini d'ordre n, alors l'ordre de tout élément de G divise n.*

Théorème 11. *Soit a un élément de G d'ordre p. On à l'équivalence* $a^q = e \iff p \mid q$

Théorème 12. *Soit G d'ordre fini. Soit et g dans G qui commutent.*
- *hg est d'ordre finie qui divise* $\theta(h) \vee \theta(g)$.
- *Si* $< h > \bigcap < g >= \{e\}$, *alors* $\theta(hg) = \theta(h) \vee \theta(g)$
- *si les ordres de h et g sont premiers entre eux, alors* $\theta(hg) = \theta(h)\theta(g)$

Théorème 13. *Soit G d'ordre fini abélien. Alors il existe un élément d'ordre le PPCM de tout ses éléments. Il est appelé l'exposant de G.*

2 Etude des groupes abéliens

2.1 Groupes cycliques

Exemple 14.
- Le groupe $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$ est cyclique à n éléments.
- Le groupe des racines n-ème de l'unité $_n$ est cyclique à n éléments.

Théorème 15. *Tout groupe cyclique à n élément est isomorphe à* $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$.

Théorème 16. *Soit* $G =< a >$ *cyclique à n élément.* $G =< a^k > \iff k \wedge n = 1$

Corollaire 17. *Soit G cyclique à n éléments. G possède* $\varphi(n)$ *éléments générateurs.*

Corollaire 18. *Un groupe de cardinal p premier est cyclique, et tout élément de G en est un générateur.*

Théorème 19 (Sous-groupe d'un groupe cyclique). *Soit G cyclique d'ordre n,* $G =< a >$.

— *Les sous-groupes de G sont tous cyclique d'ordre d qui divise n.*

— *Soit d un diviseur de n. Alors il existe un unique sous-groupe de G d'ordre d, il s'agit de* $H =< a^{\frac{n}{d}} >= \{x \in G \mid \theta(x) \mid\}$. *Les générateurs de H sont les éléments d'ordre d.*

Application 20. *Soit* $n \in \mathbb{N}^*$. $n = \sum_{d|n} \varphi(d)$.

Application 21. *Soit* $\mathbb{K}$ *un corps. Tout sous-groupe du groupe multiplicatif* $(\mathbb{K}^*, \times)$ *est cyclique.*

2.2 Théorème de structure des groupes abéliens finis

Dans toute cette partie, G est un groupe abélien fini.

Lemme 22. *Soit H un sous-groupe de G. Tout morphisme de groupe de H dans* $\mathbb{C}^*$ *peut se prolonger en un morphisme de* $G \mapsto \mathbb{C}^*0$

Lemme 23. *Soit* g_0 *d'ordre m l'exposant de G. On suppose que* $m \neq n-1$ *et on note* $K =< g_0 >$. *Alors*

— *Il existe un unique morphisme* $\varphi_0 : K \mapsto \mathbb{C}^*0$ *tel que* $\varphi_0(g_0) = w = e^{\frac{2i\pi}{m}}$

— *Le morphisme précédent se prolonge en* φ *sur G, et l'application :*
$$\begin{array}{ccc} :< g_0 > \times \ker(\varphi) & \to & G \\ (g_0^k, h) & \mapsto & g_0^k h \end{array}$$
est un isomorphisme de groupe.

Théorème 24 (Théorème de structure des groupes abéliens finis). *Il existe une suite d'entiers* $(n_i)_i$ *finis tel que* $n_1|n_2|...|n_r$ $(n_1 > 1)$ *et tel que G est isomorphe au produit de groupe cyclique* $\prod_{i=1}^{r} \frac{\mathbb{Z}}{n_i\mathbb{Z}}$.

3 Le groupe symétrique S_n

3.1 Les générateurs de S_n

Théorème 25 (Décomposition en cycle à support disjoinct). *Toute permutation* $\sigma \in S_n$ *se décompose en un produit de cycle à support disjoinct. Cette décomposition est unique à l'ordre près.*

Exemple 26. On donne un exemple simple.

Application 27. *Soit* $\sigma \in S_n$ *et* $\prod_{i=1}^{r} c_i$ *sa décomposition en cycle à support disjoinct. Alors l'ordre de* σ *est égal au ppcm des longueurs des cycles* c_i.

Théorème 28. *Tout* $\sigma \in S_n$ *se décompose en un produit de transpositions. Les transpositions engendrent donc* S_n.

Exemple 29. On reprend l'exemple précédent que l'on simplifie.

Proposition 30. *Les familles suivantes engendrent* S_n *:*

— $\{(1,k) \mid 1 < k < n+1\}$

— $\{(k,k+1) \mid 1 < k < n+1\}$

— $\{(1,2),(1,2,...,n)\}$

Définition 31. φ est un automorphisme intérieur de S_n si il existe α tel que $\varphi(g) = \alpha g \alpha^{-1}$ $\forall g \in S_n$.

Théorème 32. *Pour* $n \neq 6$, *tout les automorphismes de* S_n *sont intérieurs.*

3.2 Sous-groupes de S_n

Proposition 33. *Si* $n > 2$, $Z(S_n) = \{Id\}$

Définition 34. On définit la signature de $\sigma \in S_n$ par $\varepsilon(\sigma) = (-1)^p$ où σ est le produit de p transpositions.

Théorème 35. *L'application* ε *est l'unique morphisme de* $S_n\mathbb{C}^*$ *non-trivial.*

Définition 36. On appelle groupe altérnée A_n le noyau de ε. Il s'agit d'un sous-groupe de S_n.

Proposition 37. *Les familles suivantes engendrent* A_n *:*

— *Les 3-cycles*

— $\{(1,2,k) \mid 2 < k < n+1\}$

— $\{(k,k+1,k+2) \mid 2 < k < n+1\}$

Exemple 38. On décompose une permutation de A_7 en 3-cycle (voir rombaldi)

Lemme 39. *Pour* $n > 4$ *Les 3-cycles sont conjuguées dans* A_n.

Théorème 40. *Pour* $n > 4$, A_n *est simple.*

Proposition 41. *Pour* $n > 4$, *le groupe dérivée de* A_n *est* A_n.

4 Application en algèbre linéaire

4.1 Le groupe linéaire $Gl(E)$

Cadre : Soit E un $\mathbb{K}$ espace vectoriel de dimension finie n.

Définition 42. On appelle groupe linéaire de E l'ensemble des endomorphismes de E dans E muni de la loi composition.
Il est isomorphe à $Gl_n(\mathbb{K})$, l'ensemble des matrices inversibles de taille $n \times n$ à coefficients dans $\mathbb{K}$.
On note $Sl_n(\mathbb{K})$ l'ensemble des matrices de $Gl_n(\mathbb{K})$ de déterminant 1. C'est un sous-groupe de $Gl_n(\mathbb{K})$.

Définition 43. Soit $\lambda \in \mathbb{K}^*$.
On appelle transvection toute matrice de la forme $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$.
On appelle dilatation toute matrice de la forme $D_i(\lambda) = I_n + (\lambda - 1)E_{i,i}$. *
Leurs effets par multiplication sur une matrice M sont les suivants :

$MT_{i,j}(\lambda)$	$T_{i,j}(\lambda)M$	$MD_i(\lambda)$	$D_i(\lambda)M$
$C_j \leftarrow C_j + \lambda C_i$	$L_i \leftarrow L_i + \lambda L_j$	$C_i \leftarrow \lambda C_i$	$L_i \leftarrow \lambda L_i$

Pivot de Gauss. On explique le principe du pivot de Gauss pour une matrice inversible.

Exemple 44. Exemple sur une matrice 3×3.

Théorème 45. *Les matrices de transvections engendrent $SL_n(\mathbb{K})$. Les matrices de transvections et dilatations engendrent $Gl_n(\mathbb{K})$.*

4.2 Le groupe orthogonal

[Gri]

Définition 46. On appelle groupe orthogonal de $Gl_n(\mathbb{K})$ l'ensemble $\{P \in Gl_n(\mathbb{K}) \mid {}^tPP = I_n$. Il s'agit d'un sous-groupe de $Gl_n(\mathbb{K})$.

Exemple 47. On donne une matrice simple dans $O_n(\mathbb{K})$

Théorème 48 (Réduction des matrices orthogonales).

Définition 49.
— On définit les retournements
— On définit les réflexions

Théorème 50. *Les réflexions et les retournements engendrent $O_n(\mathbb{R})$.*