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

Développements :

Automorphismes de S_n, SO_3 est simple.

Bibliographie :

Rombaldi, Calais, Ulmer, Beruy, Combes, Perrin, OA, H2G2

Rapport du jury 2016 :

C'est une leçon qui doit être illustrée par des exemples très variés en relation avec les groupes de permutations et les groupes linéaires ou de leurs sous-groupes. La connaissance de parties génératrices s'avère très utile dans l'analyse des morphismes de groupes ou pour montrer la connexité de certains groupes. Tout comme dans la leçon 106, la présentation du pivot de Gauss et de ses applications est envisageable.

Rapport de jury 2017 :

C'est une leçon qui doit être illustrée par des exemples très variés qui peuvent être en relation avec les groupes de permutations, les groupes linéaires ou leurs sous-groupes ; les groupes Z/nZ, fournissent aussi des exemples intéressants. La connaissance de parties génératrices s'avère très utile dans l'analyse des morphismes de groupes ou pour montrer la connexité de certains groupes. Tout comme dans la leçon 106, la présentation du pivot de Gauss et de ses applications est envisageable.

1 Généralités

Définition 1 (Romb p11). *[Calais p29] Le sous-groupe engendré par X est l'intersection de tous les sous-groupes de G qui contiennent X. On le note $\langle X \rangle$.*

Remarque 2 (Romb p11). *[Calais p29] C'est le plus petit des sous-groupes qui contiennent X.*

Exemple 3. *$\mathbb{Z}$ est engendré par* 1.

Remarque 4 (Romb p11). *[Calais p29] Si X est formé d'un nombre fini d'éléments $(x_i)_{i=1..n}$, notation pour $\langle X \rangle$.*

Proposition 5 (Romb p11). *[Calais p29] Forme des éléments de $\langle X \rangle$.*

Définition 6 (Romb p11). *[Calais p29] X engendre G.*

Proposition 7. *Si G est un groupe engendré par une famille S (par exemple finie) et H est un sous-groupe distingué de G, alors les classes des éléments de S dans G/H engendrent ce quotient ; ainsi, si G admet une famille génératrice de cardinal n, il en va de même de G/H, tandis que l'analogue avec un sous-groupe au lieu d'un quotient est en général totalement faux*

Exemple 8. *$\mathbb{Q}$ est engendré par les $\{\frac{1}{p}, ppremier\}/$*

Exemple 9. *Sous-groupe engendré par $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.*

Définition 10 (Romb p13). *Le groupe dérivé est le sous-groupe engendré par les commutateurs.*

Remarque 11. *Si G est abélien, son groupe dérivé est G.*

Proposition 12 (Beruy p145). *Si $f : G \to G'$ est un morphisme de groupes alors $f(< S >) =< f(S) >$.*

2 Groupes abéliens finis

2.1 Groupes cycliques et monogènes

Définitions et exemples

Définition 13 (Romb p13). *Groupe monogène. Groupe cyclique. Ordre d'un élément.*

Remarque 14. *Un groupe monogène est abélien.*

Application 15. *SL_n et GL_n sont non monogènes.*

Remarque 16 (Romb p14). *Description de $\langle g \rangle$. Il est abélien. Description dans le cas où est G est cyclique.*

Exemple 17 (Calais p29). *[Romb p14] $\mathbb{Z}$ est monogène engendré par* 1. *Ses sous-groupes sont tous monogènes. $\langle m, n \rangle = (m \widehat{\wedge} n)\mathbb{Z}$.*
$\mathbb{Z}/n\mathbb{Z}$ est engendré par $\overline{1}$. Il est cyclique.
Le groupe multiplicatif des racines n-èmes de l'unité est cyclique d'ordre n.

Exemple 18 (Beruy p146). *$< a, b >= a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, $< a_i, i \in \mathbb{Z} >= pgcd(a_i)\mathbb{Z}$.*

Théorème 19 (Romb p14). *Un groupe monogène est isomorphe à $\mathbb{Z}$ou à $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 20 (Romb p15). *Un groupe de cardinal p premier est cyclique, isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et tout élément distinct du neutre engendre G.*

Contre exemple 21 (Ulmer p7). *$GL(2,2)$ est d'ordre 6 non cyclique.*

Théorème 22 (Romb p14). *Générateurs d'un groupe cyclique.*

Théorème 23 (Comb p59). *Ordre de a^k, générateur si et seulement si n et k premiers entre eux. $\phi(n)$ générateurs.*

Proposition 24 (Perrin p24). *Générateurs de $\mathbb{Z}/n\mathbb{Z}$.*

Exemple 25 (Combes p60). *Générateurs de $\mathbb{Z}/12\mathbb{Z}$.*

Proposition 26 (Romb p15). *Un groupe de cardinal p premier est cyclique.*

Contre exemple 27 (Romb p15). *S_3 d'ordre 6 non commutatif.*

Proposition 28. *Si G est monogène, l'image d'un morphisme de groupes de départ G est uniquement déterminé par son image sur g.*

Automorphismes

Proposition 29 (Combes p61). *$Aut(G)$ d'ordre $\phi(n)$ et ses éléments sont les $x \mapsto x^k$*

Proposition 30 (Perrin p24). *Automorphismes de $\mathbb{Z}/n\mathbb{Z}$. En particulier, il est abélien et de cardinal $\phi(n)$.*

Proposition 31 (Romb p294). *$Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$*

Sous-groupes

Théorème 32 (Romb p16). *Si G cyclique d'ordre n alors les sous-groupes de G sont tous cycliques d'ordre divisant n.*

Exemple 33 (Combes p62). *Sous-groupes de $\mathbb{Z}/20\mathbb{Z}$.*

Théorème 34 (Romb p17). *Si un groupe abélien fini d'ordre n est cyclique alors pour tout diviseur d de n il existe un unique sous groupe d'ordre d de G.*

Application 35 (Romb p18). *$n = \sum_{d|n} \phi(d)$*

Proposition 36 (Combes p71 ex3.2). *Nombre de morphismes de G dans G' (groupes cycliques).*

Exemple 37 (Combes p74). *Morphismes de $Z18\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$.*

Proposition 38 (Perrin p74). *F_q^* isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.*

Proposition 39 (Perrin p74). *Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.*

Exemple 40 (Combes p71 ex 3.6). *[Romb p38 ex 19] Sous-groupes finis de $\mathbb{C}^*$ sont cycliques d'ordre card(G).*

Contre exemple 41. *$\mathbb{U}$ sous groupe de $\mathbb{C}^*$.*

Application 42 (BMP). *Le symbole de Legendre est l'unique morphisme de F_p^*.*

2.2 Structure des groupes abéliens finis

Théorème 43 (Combes p63). *[Perrin p25] Théorème des restes chinois (à mettre pour les composantes primaires). Le produit de deux groupes cycliques est cyclique si et seulement si ils sont cycliques d'ordres premiers entre eux.*

Application 44 (Combes p63). *Calcul de $\phi(n)$.*

Théorème 45 (Combes p66). *Théorème de structure des groupes abéliens finis.*

Définition 46 (Combes p67). *Suite des invariants.*

Corollaire 47 (Combes p67). *Réciproque de Lagrange et décomposition en puissance de nombres premiers.*

Exemple 48 (Combes). *Groupes d'ordre 600.*

Exemple 49 (Combes p68). *$\mathbb{Z}/60\mathbb{Z} * \mathbb{Z}/72\mathbb{Z}$.*

Proposition 50 (Romb). *Un groupe abélien est cyclique si et seulement si pour tout diviseur d de n, il existe un sous-groupe d'ordre d.*

Proposition 51. *Existence d'un élément d'ordre le ppcm.*

3 Exemples pour des groupes non abéliens

3.1 Groupes symétrique et alternés

Définition 52 (Romb p43). *Groupe symétrique S_n.*

Définition 53. *Cycle*

Proposition 54 (Romb p43). *Une permutation est un cycle d'ordre r si et seulement si il n'y a qu'une seule σ-orbite non réduite à un point.*

Théorème 55 (Romb p45). *Décomposition d'un cycle en produit de cycles à supports disjoints. (S_n est engendré par les cycles).*

Proposition 56 (Romb p46). *S_n est engendré par les cycles, par les transpositions, par les $n-1$ transpositions $(1,k)$, $k \in \{2,..n\}$, par les $(n-1)$ transpositions $(k,k+1)$, $k \in \{1,..n-1\}$, par $(1,2),(1,2..,n)$. (Il n'est pas possible d'enlever une de ces transpositions.)*

Exemple 57 (Romb p47).

Définition 58 (Romb p48). *Signature. Elle est définie par l'intermédiaire des cycles qui engendrent S_n.*

Théorème 59 (Romb p49). *Si σ est produit de p transpositions alors $\epsilon(\sigma) = (-1)^p$. On utilise que les transpositions engendrent S_n.*

Théorème 60 (Romb p49). *ϵ est le seul morphisme surjectif de S_n dans $\mathbb{R}^*$.*

Définition 61 (Romb p51). *Une permutation est paire si elle s'écrit comme produit d'un nombre pair de transpositions.*

Définition 62 (Romb p51). *Groupe alterné : ensemble des permutations paires.*

Proposition 63 (Romb p52, p66). *A_n est engendré par les 3-cycles, par les $(1,2,k)$, $k \in \{3,..n\}$, $(k,k+1,k+2)$, $\left\{^{k\in\{1,..n-2}\right\}$.*

Proposition 64. *A_n est simple.*

Application 65. *Groupes dérivés de A_n et S_n.*

Application 66. *Isométries du cube et du tétraèdre.*

Proposition 67. *Les automorphismes de S_n sont intérieurs.*

3.2 Le groupe diédral

Définition 68 (Romb p87). *Un groupe multiplicatif G est diédral de type D_{2n} s'il est engendré par un élément ρ d'ordre n et un élément $\sigma \neq \rho$ d'ordre 2 tel que $\rho\sigma\rho\sigma = Id$.*

Proposition 69 (Romb p87). *Description de G. G est d'ordre $2n$.*

Proposition 70 (Romb p87). *De groupes diédraux de type D_{2n} sont isomorphes.*

Théorème 71 (Romb p88). *A isomorphisme près,le groupe diédral d'ordre $2n$ est le groupe des isométries d'un polygone régulier à n côtés dans $\mathbb{R}^2$.*

Proposition 72 (Ulmer p10). *Groupe dérivé de D_n selon la parité de n.*

Proposition 73 (Romb). *S_3 isomorphe à $Is(T_3)$.*

4 Parties génératrices en algèbre linéaire

4.1 Groupe linéaire

Définition 74 (Romb p125). *$GL_n(K)$, $SL_n(K)$.*

Définition 75 (H2G2). *Transvection, dilatation.*

Proposition 76 (Romb p140). *SL_n est engendré par les transvections.*

Proposition 77 (Ramis Warusfel). *Pivot de Gauss. Toute matrice de $GL_n(K)$ peut être transformée, par des transvections sur les colonnes en une matrice de la forme diag$(1,..,1,d)$. d est le déterminant de la matrice de départ.*

Proposition 78 (Romb p141). *GL_n est engendré par les dilatations et les transvections.*

Proposition 79 (Nourdin p226). *Deux dilatations sont conjuguées si et seulement si elles ont le même rapport. Deux transvections sont toujours conjuguées dans $GL(E)$. Si $n \geq 3$, elle le sont aussi dans $SL(E)$.*

Application 80 (??). *Algo du pivot de Gauss et décomposition LU pour résoudre les systèmes linéaires.*

Proposition 81 (Romb p141). *Groupes dérivés.*

Proposition 82. *Connexité.*

4.2 Groupe orthogonal

Définition 83 (Perrin p141). *$O_n(\mathbb{R})$, $SO_n(\mathbb{R})$ (ou $O(E)$?)*

Théorème 84 (Perrin p143). *Tout élément de O_n peut s'écrire comme produit d'au plus n réflexions.*
Tout éléments de SO_n est produit d'au plus n renversements.

Corollaire 85 (Perrin p143). *O_n est engendré par les réflexions orthogonales.*
SO_n est engendré par les renversements.

Proposition 86. *Groupes dérivés.*

Exemple 87 (Perrin). *$D(O_n) = SO_n$, $D(SO_n) = SO_n$.*

Proposition 88. *SO_3 est simple.*

4.3 Décompositions matricielles

Proposition 89. *Si A est une matrice carrée, il existe P tel que PA soit triangulaire. C'est la méthode de Gauss.*

Théorème 90. *Décomposition LU.*

Théorème 91. *Décomposition polaire.*

Application 92. *Résoudre les systèmes linéaires.*

Proposition 93. *$O_n(\mathbb{R})$ sous-groupe compact maximal de $GL_n(R)$.*