Nom:

Prénom:

Numéros des sujets tirés:

Intitulé du sujet choisi:

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

Numéro de Jury:

Dans toute cette leçon, G désignera un groupe dont on notera la loi multiplicativement.

I. Définitions et cardinal de parties génératrices

I. 1. Premières définitions

Def 1 : Pour S une partie non vide de G, on appelle sous groupe engendré par S le sous groupe de G : $\langle S \rangle := \bigcap_{H<G, S\subset H} H$

Rq 2 : - $\langle S\rangle$ est bien un sous groupe comme intersection de sous groupe de G

- $\langle S\rangle$ est le plus petit (au sens de l'inclusion) sous groupe de G contenant S.

Ex 3 : on définit le sous groupe dérivé de G par : $D(G) = \langle \{[g,h], g,h\in G\}\rangle$

Prop 4 : $\langle S\rangle = \{x_1x_2\dots x_m, m\in\mathbb{N}^*, x_i\in S$ ou $x_i^{-1}\in S \ \forall i\in[\![1,m]\!]\}$

Def 5 : Si S est une partie non vide de G telle que $\langle S\rangle = G$, on dit que S est une partie génératrice / un ensemble de générateurs.

Ex 6 : le groupe $(\mathbb{D},+)$ des nombres décimaux est engendré par $\{\frac{1}{10^m}, m\in\mathbb{N}\}$

Prop 7 : Soient G, H deux groupes et φ, ψ deux morphismes de $G\to H$. Ils sont égaux si et seulement si ils le sont sur une partie génératrice de G.

App 8 : $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{C}) \simeq \mu_n(\mathbb{C})$. le groupe des racines n-ièmes de l'unité.

Def 9 : On dit que G est de type fini s'il existe une partie génératrice finie.

Ex 10 : $(\mathbb{Z},+)$ est de type fini contrairement à $(\mathbb{Q}^*, \times)$.

Def 11 : on appelle ordre d'un groupe fini son cardinal et ordre d'un élément l'ordre du sous groupe qu'il engendre. Pour $x\in G$, on notera $o(x) = |\langle x\rangle|$.

Ex 12 : le groupe diédral D_n définit comme l'ensemble des isométries du plan conservant le polygone régulier à n sommets est d'ordre $2n$. Il est engendré par deux éléments : une rotation r d'ordre n et une symétrie s d'ordre 2.

Théo 13 : Théorème de Lagrange.
Si G est un groupe fini, l'ordre de tout sous groupe H de G divise l'ordre de G.
En particulier l'ordre de tout élément divise l'ordre de G.

App 14 : les groupes d'ordre premier n'ont pas de sous groupes non triviaux (ex : $\mathbb{Z}/p\mathbb{Z}$, p premier)

I.2. Cardinal des parties génératrices

Déf 15 : On appelle famille génératrice minimale une famille $(f_i)_{i\in I}$ telle que $\forall J \subsetneq I$ $(f_j)_{j\in J}$ n'est pas génératrice.

On appelle $g \in G$ un élément superflu / mou si pour toute famille génératrice $(g_1 \dots g_k, g)$ de G ($g_i \in G$ $\forall i \in [\![1,k]\!]$) alors $(g_1 \dots g_k)$ est encore génératrice.

Ex 16 : • $\{1\}$ et $\{2,3\}$ sont deux familles génératrices minimales de $\mathbb{Z}$ et 2 est un élément superflu de $\mathbb{Z}/4\mathbb{Z}$.

Rq 17 : toutes les familles génératrices minimales n'ont, en général, pas le même cardinal.

Déf 18 : • H un sous groupe de G est dit maximal si $H \neq G$ et $\forall H' < G$ tel que $H \subset H'$ alors $H' \in \{H, G\}$.

• le sous-groupe de Frattini de G est $F(G) = \bigcap_{M<G \text{ maximal dans } G} M$

Ex 19 : $(\mathbb{Q},+)$ n'a pas de sous groupe maximal. Donc $F(\mathbb{Q}) = \{0\}$.

Prop 20 : Le sous-groupe de Frattini est l'ensemble des éléments superflus.

DEV 1

Théo 21 : (Théorème de Frattini) Dans un p-groupe (un groupe de cardinal p^n avec p premier), toutes les familles génératrices minimales ont le même cardinal.

II. Exemples de groupes de type fini

II.1. Groupes monogènes et cycliques

Déf 22 : G est dit monogène s'il existe $g \in G$ tel que $G = \langle g \rangle$. Si de plus, G est fini, on dit que G est cyclique.

Prop 23. Tout groupe monogène est abélien

Ex 24 : • $(\mathbb{Z},+)$ est monogène engendré par 1.

• $(\mathbb{Z}/n\mathbb{Z},+)$ cyclique avec $k \in \mathbb{Z}$ générateur $\iff k \wedge n = 1$

Prop 25 : • tout groupe monogène infini est isomorphe à $\mathbb{Z}$

• tout groupe cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

App 26. Tout sous groupe d'un groupe monogène (resp. cyclique) est monogène (resp. cyclique).

Prop 27 : $G/Z(G)$ monogène $\Rightarrow$ G abélien avec $Z(G)$ le centre de G

App 28 : Si $\mathrm{card}(G) = p^2$ avec p premier, alors G abélien.

II.2. Structure des groupes abéliens de type fini

Théo 29 : Soit G un groupe abélien de type fini, alors : $\exists!\, r \geq 0$ et $(a_1 \dots a_k) \in \mathbb{N}\setminus\{0,1\}$ tels que $a_j \mid a_{j+1}$ $\forall j \in [\![1,k-1]\!]$ et $G \simeq \mathbb{Z}^r \times \mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_k\mathbb{Z}$.

Si de plus G est fini, $r = 0$.

Théo 30 : Théorème des restes chinois : avec m,n premiers entre eux, on a $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

App 31 : Tout sous groupe fini du groupe des inversibles $\mathbb{K}^\times$ d'un corps $\mathbb{K}$ est cyclique. En particulier $\mathbb{F}_q^\times$ est cyclique.

II.3. Le groupe symétrique $\mathfrak{S}_n$.

Déf 32. $\mathfrak{S}_n$ désigne l'ensemble des permutations de $[\![1,n]\!]$. $\gamma \in \mathfrak{S}_n$ est un r-cycle si $\exists j_1 \dots j_r \in [\![1,n]\!]$ tels que $\gamma(j_i) = j_{i+1}$ $\forall i \in [\![1,r-1]\!]$, $\gamma(j_r) = j_1$ et $\gamma|_{[\![1,n]\!]\setminus\{j_1 \dots j_r\}} = \mathrm{id}$. Une transposition est un 2-cycle.

Intercalaire N°

Intercalaire N°

<u>Théo 33</u> : toute permutation se décompose en un produit de cycles à supports disjoints / en produit de transpositions.

<u>Ex 34</u> : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (1\ 3\ 4)(2\ 5) = (1\ 3)(3\ 4)(2\ 5)$

<u>Coro 35</u> : les cycles engendrent $\mathfrak{S}_n$

<u>App 36</u> : l'ordre d'une permutation est le ppcm des longueurs des cycles dans sa décomposition.

<u>Coro 37</u> : les transpositions engendrent $\mathfrak{S}_n$

<u>App 38</u> - $F(\mathfrak{S}_n) = \{e\}$

- Isométries du tétraèdre : $Isom(T) \simeq \mathfrak{S}_4$.

<u>Prop 39</u> : les transpositions $(1\ i)$, $i \in [\![2, n]\!]$ engendrent $\mathfrak{S}_n$

DEV 2

<u>Coro 40</u> : tout automorphisme de $\mathfrak{S}_n$ qui envoie les transpositions sur les transpositions est un automor. intérieur

<u>App 41</u> : Pour $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont les automorphismes intérieurs.

<u>Def 42</u>. On définit $\mathcal{A}_n = \mathrm{Ker}\,\varepsilon$ le groupe alterné, avec ε la signature

<u>Prop 43</u> : $\mathcal{A}_n$ est engendré par les 3 cycles

<u>App 44</u> : $\mathcal{A}_n$ est simple pour $n = 3$ et $n \geq 5$.

III Groupe linéaire et ses sous groupes.

$\mathbb{K}$ désigne un corps et E un $\mathbb{K}$ espace vectoriel de dimension n.

III. 1 Groupe linéaire GL(E) et spécial linéaire SL(E)

<u>Def 45</u> : $GL(E)$ est le groupe des automorphismes $\mathbb{K}$ linéaire de E
. $SL(E)$ est l'ensemble des éléments de $GL(E)$ de déterminant 1

<u>Rq 46</u> : $GL(E) \simeq GL_n(\mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}),\ \det M \neq 0_{\mathbb{K}}\}$

$SL(E) \simeq SL_n(\mathbb{K}) = \{M \in GL_n(\mathbb{K}),\ \det M = 1_{\mathbb{K}}\}$

<u>Def 47</u> : Avec (E_{ij}) la base canonique de $\mathcal{M}_n(\mathbb{K})$. On dit que
- M est une matrice de transvection si $M = I_n + \lambda E_{ij}$ $\lambda \in \mathbb{K}$, $i \neq j$
- M est une matrice de dilatation si $M = I_n + (\alpha - 1)E_{ii}$, $\alpha \in \mathbb{K}^*$

<u>Prop 48</u> : $SL_n(\mathbb{K})$ est engendré par les matrices de transvection et $GL_n(\mathbb{K})$ par celles de transvection <u>et</u> de dilatation

<u>App 49</u> : $SL_n(\mathbb{K})$, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ est connexe par arcs

<u>Rq 50</u> : on a des résultats similaires en terme d'endomorphismes pour $GL(E)$ et $SL(E)$.

<u>Prop 51</u> $D(SL(E)) = SL(E)$ sauf si $n = 2$ et $\mathbb{K} = \mathbb{F}_2$ ou $\mathbb{F}_3$
$D(GL(E)) = SL(E)$ sauf si $n = 2$ et $\mathbb{K} = \mathbb{F}_2$.

III. 2. Groupe orthogonal O(E) et spécial orthogonal SO(E).

<u>Def 52</u>. $O(E)$ (resp $SO(E)$) est l'ensemble des isométries vectorielles de E (resp isométries positives) avec E euclidien

<u>Rq 53</u> $O(E) \simeq O_n(\mathbb{R}) = \{M \in \mathcal{M}_n(\mathbb{R}),\ {}^tMM = I_n\}$
$SO(E) \simeq SO_n(\mathbb{R}) = \{M \in O_n(\mathbb{R}) \mid \det M = 1\}$

<u>Def 54</u> : Soit s une symétrie orthogonale par rapport à $H \subset E$.
- si $\dim H = n - 1$ on appelle s une réflexion : dans une base convenable sa matrice est $\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & -1 \end{pmatrix}$.
- si $\dim H = n - 2$, on appelle s un renversement et dans une base convenable sa matrice est $\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & -1 & \\ & & & & -1 \end{pmatrix}$.

<u>Prop 55</u> : $O(E)$ est engendré par les réflexions $(n \geq 2)$ et $SO(E)$ par les renversements $(n \geq 3)$.

<u>App 56</u> : $D(SO(E)) = SO(E)$ $n \geq 3$
$D(O(E)) = SO(E)$ $n \geq 2$.

<u>App 57</u> : $SO_3(\mathbb{R})$ est simple.

Références :

* Josette Calais. <u>Eléments de théorie des groupes</u>, parties I.1 et II.3
* Massimo Zavidaque. <u>Un Max de Maths</u> : partie I.2 et DEV 1
* J.E. Rombaldi. <u>Algèbre et géométrie</u> partie II.1
* Felix Ulmer <u>Théorie des groupes</u>
* Daniel Perrin <u>Cours d'Algèbre</u> partie III.1/2 et DEV 2
* Michèle Audin <u>Géométrie</u> partie III.2