108

Exemples de parties génératrices d'un groupe. Applications.

Soit G un groupe.

Def 1: Une partie $H \subset G$ est génératrice si $G = \langle H \rangle$. G est dit de type fini s'il existe une partie génératrice finie. [1]

Ex 2: Le groupe dérivé $D(G)$ est engendré par les commutateurs $[x,y] = xyx^{-1}y^{-1}$, $x, y \in G$.

I) Cas des groupes abéliens

On suppose ici G abélien.

A] Groupes monogènes, groupes cycliques

Def 3: G est dit monogène s'il existe un générateur $g \in G$. Si $|G| < +\infty$, G est dit cyclique.

Ex 4: $(\mathbb{Z}, +)$ est monogène engendré par 1.

Ex 5: Pour $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique engendré par $\bar{1}$.

Thm 6: Si G est monogène infini, $G \simeq (\mathbb{Z}, +)$. Si G est cyclique d'ordre $n \in \mathbb{N}^*$, $G \simeq (\mathbb{Z}/n\mathbb{Z}, +)$.

Thm 7: Soit G un groupe cyclique d'ordre $n \in \mathbb{N}^*$ et de générateur g. Alors les autres générateurs de G sont les g^k avec $k \wedge n = 1$. [1]

Ex 8: Les générateurs de $(\mathbb{Z}/p\mathbb{Z}, +)$ avec p premier sont les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$.

App 9: Soit $\mathbb{U}_n$ le groupe des racines n-ème de l'unité. $\mathbb{U}_n \simeq (\mathbb{Z}/n\mathbb{Z}, +)$ donc les générateurs de $\mathbb{U}_n$ sont les $\exp\left(\frac{2ik\pi}{n}\right)$ avec $k \wedge n = 1$.

App 10: Si p est premier, $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$.

Thm 11: Soit G un groupe cyclique généré par $g \in G$, d'ordre n. Pour tout diviseur d de n, il existe un unique sous-groupe G d'ordre d: $H = \langle g^{n/d} \rangle$.

App 12: Pour tout $d | n$, il existe un élément de G d'ordre d, pour G cyclique d'ordre n. [7]

B] Groupes abéliens finis, de type finis

Lem 13: Soit G fini et soit $a \in G$ d'ordre maximal. $\forall y \in G/\langle a \rangle$, $\exists x \in G$, $o(x) = o(\bar{y})$ avec $o(x)$ est l'ordre de x.

Thm 14: Si G est fini, il existe des entiers $q_1 \dots q_k$ uniques tels que $G \simeq \prod_{i=1}^{k} \mathbb{Z}/q_i\mathbb{Z}$. Ces entiers sont les facteurs invariants de G. [4]

Rem 15: Ceci donne un système de générateurs de G à isomorphisme près.

Ex 16: $\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/360\mathbb{Z}$.

App 17: Si G est abélien fini, il existe un élément d'ordre le ppcm des ordres des éléments de G.

App 18: Pour pour $d | n = |G|$ avec G abélien fini, il existe un sous-groupe de G d'ordre d.

Prop-def 19: Si G est de type fini, il est dit libre si $\exists r \geq 0$, $G \simeq \mathbb{Z}^r$. r est unique et est le rang de G.

Def 20: Le groupe de torsion de G est l'ensemble des éléments d'ordre fini.

Thm 21: Soit T le groupe de torsions de G, de type fini. $\exists! r \in \mathbb{N}$, $G \simeq \mathbb{Z}^r \times T$. [6]

Rem 22: Couplé au thm 14, ceci classifie les groupes abéliens de type fini.

App 23: Un groupe abélien de type fini sans torsion est libre.

II] Groupes symétriques et diédraux

A] Groupes symétriques

Soit $n \in \mathbb{N}^*$. On définit S_n comme le groupe des bijections de $[\![1;n]\!]$ dans lui-même.

[1] **Def 24** : Soit $\sigma \in S_n$. Son support est $supp(\sigma) = \{x \in [\![1;n]\!] \mid \sigma(x) \neq x\}$. On dit que c'est un p-cycle, $p \in [\![1;n]\!]$ si il existe $a_1, \dots, a_p \in [\![1;n]\!]$ avec $\sigma(a_i) = a_{i+1}$ $\forall i \in [\![1;p-1]\!]$, $\sigma(a_p) = a_1$. On le note $(a_1 \dots a_p)$. Si $p=2$, on parle de transpositions.

Thm 25 : Tout élément $\sigma \in S_n$ se décompose de façon unique comme produit de cycles à supports disjoints.

Cor 26 : Les cycles, et plus particulièrement les transpositions, sont des générateurs de S_n.

Cor 27 : Soient τ une transposition et σ un n-cycle. Alors ce sont des générateurs de S_n.

Rem 28 : Si $n \geq 3$, on ne peut faire mieux puisqu'alors S_n n'est plus abélien.

[4] **Def 29** : Soit $\sigma \in S_n$. On écrit sa décomposition donnée en Thm 25 : $\sigma = c_{p_1} \dots c_{p_k}$ où $p_1 \leq \dots \leq p_k$ et c_{p_i} est un p_i-cycle. Le type de σ est le vecteur $(p_1 ; \dots ; p_k)$.

Thm 30 : (DEV1) Soient $\sigma, \sigma' \in S_n$. σ et σ' sont conjugués si et seulement si ils ont même types.

App 31 : σ et σ' sont conjugués si et seulement si leurs matrices de permutation sur un corps de caractéristique nulle sont semblables.

App 32 : Il y a autant de classes de conjugaisons de S_n que de façons d'écrire n comme somme d'entiers.

[1] **Thm 33** : Soit A_n le groupe des permutations paires, $n \geq 3$. Alors A_n est engendré par les 3-cycles.

Rem 34 : Ceci permet d'en déduire aussi les classes de conjugaison de A_n.

App 35 : (DEV2) $\forall n \geq 5$, A_n est simple. [1]

Rem 36 : Pour $n = 4$, cette proposition ne tient plus.

B] Groupes diédraux

Def 37 : On appelle polygone régulier à n côtés l'enveloppe convexe dans $\mathbb{C}$ des points d'affixes $(\omega^k)_{0 \leq k \leq n-1}$ où $\omega = e^{\frac{2i\pi}{n}}$. On note P_n ce polygône.

Def 38 : On définit le groupe diédral D_n d'indice n comme $D_n = Is(P_n)$ les isométries stabilisant P_n.

Ex 39 : Soit r la rotation linéaire d'angle $\frac{2\pi}{n}$. Alors $r \in D_n$. [7]

Ex 40 : Soit s la symétrie orthogonale d'axe $(0,(1,0))$. Alors $s \in D_n$.

Thm 41 : D_n est engendré par r et s. De plus, on a la relation $rs = sr^{-1}$.

App 42 : $D_3 \simeq S_3$.

Thm 42 : Les isométries positives de D_n forment un groupe cyclique de générateur r.

III) Générateurs dans le groupe linéaire

A] Groupe linéaire, groupe spécial linéaire

Soit k un corps commutatif et $n \in \mathbb{N}^*$.

Def 43 : On définit le groupe linéaire par $GL_n(k) = \{M \in \mathcal{M}_n(k) \mid \det M \neq 0\}$ et le groupe spécial linéaire $SL_n(k) = \{M \in GL_n(k) \mid \det M = 1\}$. [2]

Rem 44 : On aurait pu de même définir $GL(E)$ et $SL(E)$ où E est un k-espace vectoriel de dimension n.

[2] On a alors $GL(E) \simeq GL_n(\mathbb{k})$ et $SL(E) \simeq SL_n(\mathbb{k})$.
Soit $(E_{ij})_{1\leq i,j\leq n}$ la base canonique de $\mathcal{M}_n(\mathbb{k})$.

<u>Def 45</u>: On définit les matrices de :
- transvection de la forme $T_{ij}(\lambda) = I_n + \lambda E_{ij}$, $i\neq j$, $\lambda \in \mathbb{k}^*$
- [3] dilatation de la forme $D(\alpha) = \operatorname{diag}(1,\dots,1,\alpha)$, $\alpha \in \mathbb{k}^*$.

<u>Rem 46</u>: Soit $A \in \mathcal{M}_n(\mathbb{k})$. On note $L_1,\dots,L_n$ ses lignes et $C_1,\dots,C_n$ ses colonnes.
- $T_{ij}(\lambda)A$ revient à faire $L_i \to L_i + \lambda L_j$
- $A T_{ij}(\lambda)$ revient à faire $C_j \to C_j + \lambda C_i$

<u>Meth 47</u>: La méthode de Gauss consiste à échelonner une matrice $A \in GL_n(\mathbb{k})$:
- Si $a_{11} = 0$, soit $i \in [\![1;n]\!]$ tel que $a_{i1} \neq 0$. On fait $A \to T_{1i}(\lambda)A$
[5] où $\lambda = \frac{1}{a_{i1}}$
- Pour $j \in [\![2;n]\!]$, on annule a_{j1} via $A \to T_{j1}(\lambda)A$ avec $\lambda = -a_{j1}$
- On réitère sur $(A_{ij})_{2\leq i,j\leq n}$

<u>Rem 48</u>: Si $A \in \mathcal{M}_n(\mathbb{k})$, la méthode s'applique aussi mais il faut éventuellement permuter les colonnes (on peut tomber sur des colonnes nulles).

<u>Rem 49</u>: On peut raisonner de la même manière sur les colonnes. On obtient alors :

<u>Thm 50</u>: $SL_n(\mathbb{k})$ est engendré par les matrices de
[2] transvections.

<u>Cor 51</u>: $GL_n(\mathbb{k})$ est engendré par les matrices de transvections et de dilatation.

<u>Rem 52</u>: Les isomorphismes de Rem 44 donnent aussi des générateurs de $GL(E)$ et $SL(E)$.

<u>App 53</u>: Les composantes connexes de $GL_n(\mathbb{R})$ sont
[1] $\det^{-1}(\mathbb{R}_+^*)$ et $\det^{-1}(\mathbb{R}_-^*)$.

[2] <u>App 54</u>: Si $\operatorname{car}(\mathbb{k}) = 0$, $D(GL_n(\mathbb{k})) = D(SL_n(\mathbb{k})) = SL_n(\mathbb{k})$

B] <u>Groupe des isométries</u>

<u>Def 55</u>: On définit le groupe orthogonal $O_n(\mathbb{R}) = \{M \in \mathcal{M}_n(\mathbb{R}) \mid {}^tMM = I_n\}$ et le groupe spécial orthogonal $SO_n(\mathbb{R}) = O_n(\mathbb{R}) \cap \det^{-1}\{1\}$

<u>Rem 56</u>: Si E est un espace euclidien, $O(E) = \{u \in \mathcal{L}(E) \mid \forall x,y \in E, \langle u(x) | u(y)\rangle = \langle x|y\rangle\}$ et $SO(E) = O(E) \cap \det^{-1}\{1\}$
Alors $O(E) \simeq O_n(\mathbb{R})$ et $SO(E) \simeq SO_n(\mathbb{R})$ où $n = \dim E$. [2]

<u>Lem 57</u>: Soit $u \in \mathcal{L}(E)$ telle que $u^2 = id$. Alors $E = \operatorname{Ker}(u - id) \oplus \operatorname{Ker}(u+id)$.

<u>Def 58</u>: Dans ce cas, si $\dim \operatorname{Ker}(u+id) = 1$, on parle de réflexion. Si $\dim \operatorname{Ker}(u+id) = 2$, on parle de retournement.

<u>Thm 59</u>: Les réflexions orthogonales engendrent $O(E)$.

<u>Cor 60</u>: Si $n \geq 3$, les renversements engendrent $SO(E)$.

> <u>App 61</u>: (DEV 3) Soit G le groupe des quaternions de module 1. Alors $SO_3(\mathbb{R}) \simeq G/\{\pm 1\}$

<u>App 62</u>: $D(O_n(\mathbb{R})) = SO_n(\mathbb{R})$ pour $n \geq 2$.
$D(SO_n(\mathbb{R})) = SO_n(\mathbb{R})$ pour $n \geq 3$

<u>Rem 63</u>: $SO_2(\mathbb{R})$ étant abélien, $D(SO_2(\mathbb{R})) = \{I_2\}$.

Références :

- Algèbre et géométrie, Rombaldi [1]
- Cours d'algèbre, Perrin [2]
- Algèbre, Gourdon [3]
- Algèbre et géométrie, Combes [4]
- Algèbre linéaire, Grifone [5]
- Théorie des groupes, Calais [6]
- Cours de géométrie, Mercier [7]