on peut rajouter: $f : \langle a \rangle \to G'$ déterminée par $f(a)$. (*)

108

Exemples de parties génératrices d'un groupe. Applications.

Dans la suite G et G' sont des groupes, notés multiplicativement.

Def 1 : Soit $S \subset G$, on peut définir la partie engendrée par S, $\langle S \rangle$ de deux façons : • de l'extérieur : $\langle S \rangle = \bigcap_{\substack{S \subset H \\ H \text{ sg de } G}} H$

• de l'intérieur : $\langle S \rangle = \{ s_1 \dots s_n,\ s_i \in S \cup S^{-1} \}$.

Def 2 : Si S est une partie non vide de G tq $\langle S \rangle = G$, on dit que S est une partie génératrice de G.

Rq 3 : Un groupe possède toujours au moins une partie génératrice $G = \langle G \rangle$.

Ex 4 : • Pour $a \in G$, $\langle a \rangle = \{ a^k, k \in \mathbb{Z} \}$

• Le groupe dérivé $D(G)$ est le groupe engendré par les commutateurs $D(G) = \langle \{ xyx^{-1}y^{-1},\ x, y \in G \} \rangle$

Thm 5 : $\langle S \rangle$ est un sous groupe de G, contenant S. Pour tout sous groupe H de G, $S \subset H \Rightarrow \langle S \rangle \subset H$. Ainsi $\langle S \rangle$ est le plus petit sous groupe de G contenant S.

Perrin Calais

I. GROUPES ABÉLIENS

1. Groupes monogènes et cycliques. Calais

Def 6 : On dit que G est monogène s'il existe $x \in G$ tq $G = \langle x \rangle$.

Rq 7 : • En général, il existe plusieurs générateurs

• Tout groupe monogène est abélien

Ex 8 : $(\mathbb{Z}, +)$ est engendré par $\{1\}$

Prop 9 : Soit $f \in \mathrm{Hom}(G, G')$ surject^f. G monogène $\Rightarrow$ G' monogène.

Def 10 : On dit que G est cyclique s'il est monogène et fini.

Appl 11 : $\forall n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique.

Thm 12 (Description des groupes monogènes). Si G est monogène alors

× $\mathrm{Card}(G) < \infty$ et alors $\exists n \geq 1$ $G \simeq \mathbb{Z}/n\mathbb{Z}$, ainsi G est cyclique

ou × $G \simeq \mathbb{Z}$ ainsi G est monogène infini.

Ex 13 : • $\mathbb{U}_n$ est un groupe cyclique d'ordre n.

• Si G est fini d'ordre p premier, il est cyclique

Prop 14 : • Tout sg non trivial d'un gpe monogène infini est monogène infini

• Tout sg d'un gpe cyclique est cyclique.

Thm 15 : Si $G = \langle x \rangle$ cyclique d'ordre n, pour tout diviseur d de n, il existe un unique sg d'ordre d dans G. Il est engendré par x^k où $kd = n$.

Thm 16 : Si $G = \langle x \rangle$. Alors,

× G infini : les seuls générateurs sont x et x^{-1}

ou × G est cyclique d'ordre n : les générateurs sont les x^k tq $k \wedge n = 1$

Ex 17 : × générateurs de $\mathbb{Z}/12\mathbb{Z}$, de $\mathbb{U}_{18}$. Combes p 60

Def 18 : L'indicatrice d'Euler : $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ tq $\varphi(1) = 1$ et $\varphi(n)$ = nb de générateurs de $\mathbb{Z}/n\mathbb{Z}$

Rq 19 : $\varphi(n) = \mathrm{Card}(\{ k \in \mathbb{N}^*,\ k < n,\ k \wedge n = 1 \})$.

Ex 20 : • $\varphi(12) = \varphi(4)\varphi(3) = 2 \times 2 = 4$

• $n = \sum_{d \mid n} \varphi(d)$ Combes p 63

App 21 : • $(\mathbb{Z}/n\mathbb{Z})^\times$ sont les générateurs de $\mathbb{Z}/n\mathbb{Z}$, gpe multiplicatif d'ordre $\varphi(n)$

• Si G est d'ordre fini premier, tout élt non trivial engendre G.

• $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ Combes p 61 (*)

2. Groupes abéliens de type fini. Ulmer

Def 22 : G est de type fini s'il existe $S \subset G$ finie, $S \neq \emptyset$ tq $G = \langle S \rangle$.

Ex 23 : Tout gpe monogène est de type fini.

Rq 24 : "fini" $\neq$ "type fini" : $\mathbb{Z} = \langle 1 \rangle$.

gpe libre, torsion, sans torsion.

Thm 25 (Structure des groupes abéliens de type fini).

Tout groupe G abélien de type fini est isomorphe à un pd direct $\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^r$ $r, k \in \mathbb{N}$. $m_i \in \mathbb{N}^*$ avec $m_1 \mid m_2 \mid \dots \mid m_k$.

Les entiers $r, k, m_1, \dots, m_k$ sont déterminés de manière uniq. Ce sont les invariants du groupe G.

Ex 26 : Invariants du groupe $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$

II. GROUPES SYMÉTRIQUES ET DIÉDRAUX.

1. Groupes symétriques et alternés. Ulmer et Calais

voir 105

Def 27 : On note, pour $n \in \mathbb{N}^*$, $\mathfrak{S}_n$ le groupe des permutations de $\{1, \dots, n\}$. $\mathrm{Card}(\mathfrak{S}_n) = n!$. (a gpe symétrique)

Def 28 : À $\sigma \in \mathfrak{S}_n$, on associe la relation d'équivalence $i \mathcal{R}_\sigma k \Leftrightarrow \exists r \in \mathbb{Z}$ $\sigma^r(i) = k$.

On note $\mathcal{O}_\sigma(i)$ la σ-orbite de i (classe d'équivalence de i modulo $\mathcal{R}_\sigma$), i.e. $\mathcal{O}_\sigma(i) = \{ \sigma^r(i),\ r \in \mathbb{Z} \}$.

Def 29 : σ est un cycle de longueur r s'il existe $i_1, \dots, i_r$, élts distincts de $[\![1, n]\!]$ tq $\sigma(j) = j$ si $j \notin \{ i_1, \dots, i_r \}$ et $\sigma(i_k) = i_{k+1}$ (où l'indice est pris modulo r). On le note $(i_1, \dots, i_r)$. d'ordre r

Un cycle de longueur 2 est appelé transposition.

peut être pas besoin d'en rajouter

Def 30 : Le support de $\sigma \in \mathfrak{S}_n$ = supp $\sigma = \{i \in [\![1,n]\!], \sigma(i) \neq i\}$.

Ex 31 : Dans $\mathfrak{S}_5$, $(1\,3\,5)$ est un 3-cycle de support $\{1,3,5\}$.

Prop 32 : Deux permutations à support disjoints commutent.

Thm 33 : Toute permutation $\sigma \neq e$ se décompose en produit de cycles à support disjoint. Cette décomposition est unique à l'ordre des facteurs près.

Ex 34 : Exemple d'une décomposition.

Thm 35 : Toute permutation $\sigma \neq e$ se décompose en produit de transpositions, non permutables en général.

Rq 36 : Décomposition non unique pour $n \geq 2$.

Ex 37 : Exemple d'une décomposition.

Rq 38 : * $\mathfrak{S}_n$ est engendré par l'ensemble des transpositions de la forme $(1, i)$, $2 \leq i \leq n$

* $\mathfrak{S}_n$ est engendré par $(1,2)$ et $(1,\dots,n)$.

b- Groupe alterné

Thm 39 : Il existe un unique morphisme surjectif $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$.

Def 40 : Ce morphisme est appelé signature. Pour $\sigma \in \mathfrak{S}_n$

$$\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Prop 41 : Si $\sigma = \tau_1 \dots \tau_k$ où les τ_i sont des transpositions, $\varepsilon(\sigma) = (-1)^k$

Def 42 : Le noyau de ε est appelé groupe alterné, noté $\mathfrak{A}_n$. (Il est distingué dans $\mathfrak{S}_n$.)

Rq 43 : $\mathfrak{A}_n$ est l'ensemble des permutations qui se décomposent en un produit pair de transpositions.

Thm 44 : Pour $n \geq 3$, $\mathfrak{A}_n$ est engendré par les cycles de la forme $(1, i, j)$ $i \neq j$. En particulier, $\mathfrak{A}_n$ est engendré par les 3-cycles.

Prop 45 : Pour $n \geq 2$, $D(\mathfrak{S}_n) = \mathfrak{A}_n$, $D(\mathfrak{A}_n) = \mathfrak{A}_n$, $n \geq 5$

• $\mathfrak{A}_n$ est le seul groupe d'indice 2 de $\mathfrak{S}_n$.

App 46 : Isométrie du tétraèdre et du cube. [DVLPT]

Thm 47 : Pour $n \geq 5$, $\mathfrak{A}_n$ est simple

App 48 : Si $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont les automorphismes intérieurs de $\mathfrak{S}_n$ (DVLPT)

à abréger c'est pas la leçon 105!

$D(\mathfrak{A}_1) = \{e\}$
$D(\mathfrak{A}_2) = \{e\}$
$D(\mathfrak{A}_3) =$
$D(\mathfrak{A}_4) = \{id, (12)(34), (13)(24), (14)(23)\}$

2- Groupes diédraux. Ulmer p8

Def 49 : Soit $n \in \mathbb{N}$, $n \geq 3$. Dans $\mathbb{C} \simeq \mathbb{R}^2$, on considère le polygône régulier convexe P_n à n sommets formés par les affixes des racines n-èmes de l'unité $\omega_k = \exp(2i\pi k/n)$. Le groupe diédral D_n est le sous groupes des isométries du plan affine qui laissent P_n invariant.

Prop 50 : Pour $n \geq 3$, D_n est d'ordre $2n$. Il est engendré par la symétrie axiale s et la rotation r d'angle $\theta = \frac{2\pi}{n}$ définis par

$$s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ et } r = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

Rq 51 : • $r^n = e$, $s^2 = e$ et $srs = r^{-1}$, $sr^i = r^{-i}s$

• $D_n = \langle r, s \mid r^n, s^2, (sr)^2 \rangle$

• $D_n = \{s^i r^j, i \in [\![0,1]\!], j \in [\![0, n-1]\!]\}$

Prop 52 : Le sous groupe $\langle r \rangle \subset D_n$ est un sg distingué de D_n d'ordre n.

Prop 53 : • $D(D_{2m}) = \langle r^2 \rangle$

• $D(D_{2m+1}) = \langle r \rangle$.

Ex 54 : ~~Table de multiplicatio~~ de D_3 et D_4 + table de caractères

III. AUTOUR DU GROUPE LINÉAIRE.

1. GL(E) et SL(E). Perrin

Ici E est un K-ev de dim finie, K étant un corps de caractéristique quelconque.

Def 55 : $GL(E)$ est le groupe des K-automorphismes de E.

Rq 56 : La donnée d'une base de E définit un isomorphisme de $GL(E)$ sur $GL_n(K)$

Def 57 : $SL(E)$ est le noyau de $\det : GL(E) \to K^*$. Il est appelé groupe spécial linéaire.

Rq 58 : $SL(E) \simeq SL_n(K)$ matrices de déterminant 1.

Prop 59 : Soit H un hyperplan de E, $u \in GL(E)$ tq $u_{|H} = Id_H$.

* $\det u = \lambda \neq 1$

$\Leftrightarrow$ * u admet une vp $\lambda \neq 1$ et u est diagonalisable

$\Leftrightarrow$ * $Im(u - Id) \not\subset H$.

$\Leftrightarrow$ * Dans une base convenable, u a pour matrice $diag(1, \dots, 1, \lambda)$ avec $\lambda \in K^*$, $\lambda \neq 1$

On dit que u est une dilatation d'hyperplan H, de rapport λ. $H = \ker(u - Id)$

Prop 60 : Soit H un hyperplan de E ($H = \ker f$), $u \in GL(E)$, $u \neq id$
tq $u_{|H} = id_H$.
× $\det u = 1$
$\Leftrightarrow$ × u n'est pas diagonalisable
$\Leftrightarrow$ × $D = \mathrm{Im}(u - Id) \subset H$
$\Leftrightarrow$ × il existe $a \in H$ $a \neq 0$ tq $\forall x \in E$ $u(x) = x + f(x)a$. $D = (a)$.
$\Leftrightarrow$ × Dans une base convenable, u a pour matrice $\left(\begin{array}{c|c} Id & 0 \\ \hline 0 & \begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} \end{array}\right)$
On dit que u est une transvection d'hyperplan H et de droite D.

Thm 61 : • Les transvections engendrent $SL(E)$
• Les transvections et les dilatations engendrent $GL(E)$ DVLPT

App 62 : $SL(E)$ est connexe par arcs.

Thm 63 : × $D(GL(n,K)) = SL(n,K)$ pour $n \neq 2$ $K \neq \mathbb{F}_2$
× $D(GL(2,\mathbb{F}_2)) = \mathfrak{S}_3$
× $D(SL(n,K)) = SL(n,K)$ sauf pour $(n=2, K=\mathbb{F}_2)$ / $(n=2, K=\mathbb{F}_3)$.
× $D(SL(2,\mathbb{F}_2)) = \mathfrak{A}_3$.
× $D(SL(2,\mathbb{F}_3)) = H_8$.

Perrin

Perrin p141 **2. Groupe orthogonal $O(E)$.**

Ici E est un $\mathbb{R}$-ev de dim finie n $q(x) = \sum_{i=1}^{n} x_i^2$, f forme polaire $\langle \cdot, \cdot \rangle$.

Def 64 : • On appelle isométries de E (relativement à q) les automorphismes $u \in GL(E)$ qui vérifient
$\forall x, y \in E$ $f(u(x), u(y)) = f(x, y)$
L'ensemble des isométries forme le groupe orthogonal.
• Le sous groupe de $O(E)$ formé des isométries de déterminant 1 est distingué et s'appelle groupe spécial orthogonal, $SO(E)$
• $u \in O(E)$ est un retournement si $\det u = -1$

Prop 65 $O(E)$ est isomorphe à $O(n, \mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}), {}^tAA = I\}$.
$SO(E)$ est isomorphe à $SO_n(\mathbb{R})$

Def 66 : $u \in O(E)$ est une reflexion si $\dim E^- = 1$ et $u^2 = 1$
renversement $= 2$ $u^2 = 1$

Thm 67 : • $O(E)$ est engendré par les reflexions orthogonales.
• pour $n \geq 3$, $SO(E)$ est engendré par les renversements

App 68 : $SO(3)$ est simple (DVLPT)

(**3. Homographies.** Perrin p98 + Audin)

Ici E est un $\mathbb{C}$-ev de dimension finie n.

Prop 69 : $Z(GL(E)) = \{x \mapsto \lambda x, \lambda \in \mathbb{C}^\times\} (\simeq \mathbb{C}^\times)$
$Z(SL(E)) = \{x \mapsto \lambda x, \lambda x, \lambda^n = 1\} (\simeq \mu_n(\mathbb{C}))$

Def 70 : Le quotient de $GL(E)$ par son centre est appelé groupe projectif linéaire, $PGL(E)$. Pour $SL(E)$, c'est $PSL(E)$

Def 71 : • L'espace projectif $P(E)$ est l'ensemble des droites vectorielles de E Audin p191
• Une homographie $h : P(E) \to P(E)$ est une application tq il existe un isomorphisme linéaire $g : E \to E$ tq $p \circ f = g \circ p$ où $p : E \setminus \{0\} \to P(E)$ est la projection.
Les homographies de $P(E)$ dans $P(E)$ forme $PGL(E)$

Prop 72 : $PGL_2(\mathbb{C})$ est engendré par les similitudes directes ($z \mapsto az + b$ avec $a \neq 0$) et l'application $z \mapsto 1/z$ p201

App 73 : Les éléments de $PGL(2, \mathbb{C})$ conservent les angles orientés.