NOM : SÉRAPHIN Prénom : Carine Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi :

Autre sujet : 108 Exemple de partie génératrice d'un groupe. Applications

Soit G un groupe. Soit $n \in \mathbb{N}^*$. $S \subseteq G$

I Généralités [G]

Def 1 : Soit G un groupe et $S \subseteq G$.
On appelle sous groupe de G engendré par S (noté $\langle S \rangle$) l'intersection de tous les sous-groupes de G contenant S.

Ex 2 : - $\langle \emptyset \rangle = \{1_G\}$
- dans $(\mathbb{Z},+)$, $\langle 1 \rangle = \mathbb{Z}$
- Soit $a \in G$, $\langle a \rangle = \{a^n, n \in \mathbb{Z}\}$ (G multiplicatif)

Prop 3 : Soit $S \subseteq G$ non vide. Alors $\langle S \rangle$ est un groupe et $\langle S \rangle = \{s_1^{\varepsilon_1} \dots s_n^{\varepsilon_n} \mid n \in \mathbb{N}, s_1, \dots s_n \in S, \varepsilon_1 \dots \varepsilon_n \in \{\pm 1\}\}$

ex 4 : . dans $\mathbb{Z}/6\mathbb{Z}$ $\langle 2 \rangle = \{0, 2, 4\}$

Def 5 : $S \subseteq G$ est une $\boxed{\text{partie génératrice}}$ si $\langle S \rangle = G$
G est $\boxed{\text{monogène}}$ s'il existe $g \in G$ tel que $G = \langle g \rangle$
G est $\boxed{\text{cyclique}}$ s'il est monogène et fini.

Prop 6 Soit P une propriété sur les éléments de G
si i) il existe $S \subseteq G$ tel que $\langle S \rangle = G$ et $\forall s \in S$ $P(s)$ est vraie
ii) $\forall x, y \in G$, si $P(x) \wedge P(y) \Rightarrow P(x^{-1}y)$
alors $\forall g \in G$ $P(g)$ est vraie

Appli 7 Soit G' un groupe et $\varphi, \psi : \langle S \rangle \to G'$
si $\varphi(s) = \psi(s)$ $\forall s \in S$ alors $\varphi = \psi$

II Groupe abélien

1) Groupes monogènes et cycliques [combes] [P]

Rem 8 : Tout groupe monogène est abélien

ex 9 : - $\mathbb{Z}$ est monogène
- $\mathbb{U}_n = \{1, \xi, \dots \xi^{n-1}\}$ le groupe multiplicatif des racines de l'unité est cyclique de générateur $\xi = \exp\left(\frac{2i\pi}{n}\right)$

Prop 10 : Si G est monogène alors G est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$ pour un $n \in \mathbb{N}^*$ si G est fini.

Exercice 11 : Si $|G| = p$ avec p premier alors $G \simeq (\mathbb{Z}/p\mathbb{Z}, +)$

Prop 12 : les sous-groupes d'un groupe monogène (resp. cyclique) sont monogènes (resp. cycliques)

Prop 13 : Soit $n \geq 2$, $\forall s \in \mathbb{Z}$ on note $\bar{s}$ son image dans $\mathbb{Z}/n\mathbb{Z}$. Les propositions suivantes sont équivalentes
i) s est premier avec n
ii) $\bar{s}$ est générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$
iii) $\bar{s} \in (\mathbb{Z}/n\mathbb{Z})^*$ (groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$)

Def 14 (fonction d'Euler)
On note $\varphi(n) = \mathrm{Card}\{x \mid x \wedge n = 1, 1 \leq x \leq n\} = |\mathbb{Z}/n\mathbb{Z}^*|$

Prop 15 : Soient $n \in \mathbb{N}^*$, d tel que $d \mid n$, G cyclique, $|G| = n$.
Il existe alors un unique sous-groupe de G d'ordre d isomorphe à $\mathbb{Z}/d\mathbb{Z}$

Cor 16 $n = \sum_{d \mid n} \varphi(d)$

appli 17 Pour tout corps fini $\mathbb{F}_q$, $\mathbb{F}_q^*$ est cyclique (donc tous ses sous-groupes aussi) < ex 17 bis $(\mathbb{Z}/13\mathbb{Z})^* \simeq (\mathbb{Z}/12\mathbb{Z}, +)$

Prop 18 : . $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$

ex 19 : $(\mathbb{Z}/4\mathbb{Z})^* = \{\bar{1}, \bar{3}\} \simeq (\mathbb{Z}/2\mathbb{Z}, +)$
. $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) = \{id, \bar{1} \mapsto \bar{3}\}$

2) Groupes abéliens finis [P] [Combes]

Soit G un groupe fini

Prop 20 : $|G|$ est premier si et seulement si G est cyclique et simple (ses seuls sous-groupes distingués sont $\{1_G\}$ et G)

Prop 21 : Soit H un sous-groupe du centre de G, $Z(G)$, tel que G/H soit cyclique. Alors G est abélien

Prop 22 : Si $|G| = p^m$ avec p premier et $m \in \mathbb{N}^*$ alors $Z(G)$ n'est pas réduit à $\{1_G\}$

Appli 23 : Si $|G| = p^2$ alors G est abélien.

Prop 24 (lemme chinois)

Si p et q sont premiers entre eux, on a :

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

Appli 25 : trouver $x \in \mathbb{Z}/pq\mathbb{Z}$ tel que $x \equiv a\,[p]$ et $x \equiv b\,[q]$ revient à chercher l'inverse de (a, b) par l'isomorphisme

Théo 26 (de structure)

Soit G abélien fini. Il existe $d_1, \dots, d_n$ pour un certain n tel que $d_1 | d_2 | \dots | d_n$, uniques, tel que $G \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/d_n\mathbb{Z})$

Exercice 27 : Trouver tous les groupes abéliens d'ordre 12

Cor 28 : Soit G abélien fini. Il existe $x \in G$ tel que son ordre soit le ppcm des ordres des éléments de G.

Contre-ex 29 : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \not\simeq \mathbb{Z}/4\mathbb{Z}$

III Groupes symétriques et diédraux

1) Groupe symétrique et Alterné [P]

Def 30 : $\mathfrak{S}_n$ est le groupe des permutations de $[\![1, n]\!]$. $\mathfrak{A}_n$ est le groupe des permutations de signature 1 de $[\![1, n]\!]$

Prop 31 : $\mathfrak{S}_n$ est engendré par :
- les transpositions
- les transpositions $(1, i)$ $i \in [\![2, n]\!]$
- $(1, 2)$ et $(1, \dots, n)$
- les cycles

Théo 32 : $\forall s \in \mathfrak{S}_n$, s se décompose en un unique produit (à ordre près) de cycles à supports disjoints.

Rem 33 : Le théorème repose sur le fait que les cycles du produit sont les $\{s^k(x) | k \in \mathbb{N}\}$ avec $x \in [\![1, n]\!]$

Prop 34 : $\varepsilon(i\,j) = -1$ $\forall i, j \in [\![1, n]\!]$, $i \neq j$

Appli 35 : Les générateurs de $\mathfrak{A}_n$ sont :
- les doubles transpositions
- pour $n \geq 3$, les cycles d'ordre 3
- les permutations s^2 avec $s \in \mathfrak{S}_n$

Lemme 36 : $n \geq 3$. Si H est un sous-groupe distingué de $\mathfrak{A}_n$ contenant un 3-cycle alors $H = \mathfrak{A}_n$

Théo 37 : pour $n \geq 5$, $\mathfrak{A}_n$ est simple

Rem 38 : $D_2 = \{id, (12)(34), (13)(24), (14)(23)\}$ est un sous-groupe distingué de $\mathfrak{A}_4$.

Appli 39 : Si $n \geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\mathfrak{A}_n$, $\{id\}$ et $\mathfrak{S}_n$

Ex 40 : $D(\mathfrak{A}_n) = \mathfrak{A}_n$ et $D(\mathfrak{S}_n) = \mathfrak{A}_n$ pour $n \geq 2$

DEV 1

2) Groupe diédral [P] [Calais]

Def 41 : D_n est le groupe des isométries du plan euclidien conservant le polygone régulier à n côtés

Prop 42 : Soit ρ la rotation d'angle $\frac{2\pi}{n}$ et de centre O, et s la symétrie d'axe (Ox). On a alors $D_n = \langle \rho, \sigma \rangle$

Appli 43 : $|D_n| = 2n$

Prop 44 : $D_n \simeq (\mathbb{Z}/n\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$

Rem 45 : tout groupe G engendré par a, b tels que $a^2 = 1$, b d'ordre n et ab d'ordre 2 est isomorphe à D_n (~~le groupe de présentation de D_n est $\langle a, b, a^2 = b^n = ab^2 = 1 \rangle$~~)

III Groupes en algèbre linéaire [P] [FGN2]

Soit $\mathbb{K}$ un corps à au plus 2 éléments, et E un $\mathbb{K}$-ev de dim n

1) $GL(E)$ et $SL(E)$

Def 46 : • $GL(E)$ est le groupe des applications $\mathbb{K}$-linéaires bijectives de E dans E, isomorphe au groupe des matrices inversibles de $\mathcal{M}_n(\mathbb{K})$

• $SL(E)$ sous-groupe de $GL(E)$ isomorphe au groupe des matrices de $\mathcal{M}_n(\mathbb{K})$ de $\det = 1$

Prop 47 : $GL(E) = SL(E) \rtimes \mathbb{K}^*$

Def 48 : Soit $n \geq 2$. Une matrice de transvection est une matrice de la forme $T_{ij}(\lambda) = I_n + \lambda E_{ij}$ où $i \neq j$ et $\lambda \in \mathbb{K}$. Une matrice de dilatation est une matrice diagonale de la forme $D_i(\alpha) = I_n + (\alpha - 1) E_{ii}$ avec $\alpha \in \mathbb{K}^*$

Théo 49 : $SL_n(\mathbb{K})$ est engendré par les transvections

- $GL_n(E)$ est engendré par les transvections et les dilatations.

appli 50 Le pivot de Gauss permet algorithmiquement de trouver l'inverse d'une matrice (multiplier à gauche (resp à droite) M par une matrice de transvection $T_{ij}(\lambda)$ revient à faire $L_i \leftarrow L_i + \lambda L_j$ (resp $C_j \leftarrow C_j + \lambda C_i$) avec (L_i) et (C_i) les lignes et les colonnes de M. Multiplier à gauche (resp à droite) M par une matrice de dilatation $D_i(\alpha)$ revient à faire $L_i \leftarrow \alpha L_i$ (resp $C_i \leftarrow \alpha C_i$). Ainsi, appliquer le pivot de Gauss à M c'est le décomposer en transvections et dilatations).

Cor 51 : $Z(GL_n) = \{\lambda Id \mid \lambda \in K^*\}$

$Z(SL_n) = \{\lambda Id \mid \lambda^n = 1\}$.

Cor 52 pour $K = \mathbb{R}$ ou $\mathbb{C}$, $SL_n(K)$ est connexe par arc

2. Groupe orthogonal [P]

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie n muni d'une norme euclidienne

Def 55 $O(E)$ est le groupe des isométries de E

Rem 56 $O(E) < GL(E)$

Def 57 $SO(E)$ est le sous-groupe de $O(E)$ des isométries de déterminant 1.

Théo 58. $O(E)$ est engendré par les réflexions orthogonales. De plus, si $u \in O(E)$ alors u est le produit d'au plus n réflexions

- si $n \geq 3$ $SO(E)$ est engendré par les renversements. De plus, si $u \in SO(E)$, u est produit d'au plus n renversements.

Def 57bis : Soit $u \in GL(E)$ tel que $u^2 = Id$. Il existe deux sous-espaces E^+ et E^- tels que : $E = E^+ \oplus E^-$ et $u|_{E^+} = Id_{E^+}$, $u|_{E^-} = -Id_{E^-}$

Dans une certaine base on a

$$Mat(u) = \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & -1 & \\ 0 & & & & \ddots \\ & & & & & -1 \end{pmatrix}$$

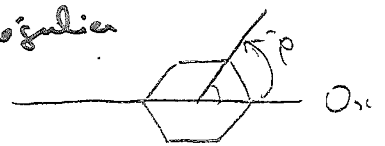
- Si $u^2 = Id$, $u \neq Id$ alors u est une involution
- Si $\dim E^- = 1$ u est une réflexion
- Si $\dim E^- = 2$ u est un renversement.

Prop 59 Soit H le corps gauche des quaternions, isomorphe à $\mathbb{R}^4$ en tant que $\mathbb{R}$-espace vectoriel, muni de la norme $N : a + ib + jc + dk \mapsto a^2 + b^2 + c^2 + d^2$. Soit G le sous-groupe de H des quaternions de norme 1 (identifié à la sphère de $\mathbb{R}^4$). Alors

$$G/_{\{+1,-1\}} \xrightarrow{\sim} SO_3(\mathbb{R})$$

DEV 2
Perrin, Cours d'algèbre

Annexe :
polygone régulier à 6 côtés



Ref : Perrin Cours d'algèbre
FGN algèbre 2
Combes Cap's agrégation
Calais
Gourdon algèbre

Pour développements :
Tauvel Corps commutatifs et théorie de Galois
Perrin Cours d'algèbre