108

Exemple de parties génératrices d'un groupe. Applications

Thibaut BAGORI

I Introduction :

déf 1 : Soit G un groupe et $S \subseteq G$ non vide. On désigne par $\mathcal{H}_S$ l'ensemble des groupes de G contenant S et on pose :
$$\langle S \rangle = \bigcap_{H \in \mathcal{H}_S} H$$
Alors $\langle S \rangle$ est un sous-groupe de G appelé sous-groupe engendré par S.

Prop 2 : Soit $S \subseteq G$ non vide, on a :
$$\langle S \rangle = \{ x_1 x_2 \dots x_n / n \in \mathbb{N}^*, x_i \in S \text{ ou } x_i^{-1} \in S \}$$

déf 3 : • Si $S \subseteq G$ non vide est telle que $\langle S \rangle = G$, on dit que S est une partie génératrice du groupe G.
• S'il existe $S \subseteq G$ non vide et fini telle que $\langle S \rangle = G$, on dit que G est de type fini.

Prop 4 : Soit G un groupe et P une propriété sur les éléments du groupe. Si on a :
(i) $\exists S$ tq $\langle S \rangle = G$ et telle que $\forall s \in S$, $P(s)$ est vraie
(ii) P est compatible avec G : si $P(x)$ et $P(y)$, alors $P(xy^{-1})$
Alors, on a $\forall x \in G$, $P(x)$ est vraie.

Ex 5 : • Si φ et ψ deux morphismes de groupes $\langle S \rangle \to H$ tels que $\varphi_{|S} = \psi_{|S}$, alors $\varphi = \psi$.
• $\langle S \rangle$ est abélien ssi les éléments de S commutent deux à deux.

I. Groupes abéliens

déf 6 : Un groupe engendré par un seul élément (ie $\exists x \in G$ tq $G = \langle x \rangle$) est dit monogène. Il est dit cyclique si G est de plus fini.

Ex 7 : • $(\mathbb{Z}, +)$ est monogène.
• $(\mathbb{Z}/n\mathbb{Z})$ est cyclique.

Prop 8 : Toute image homomorphe d'un groupe monogène est monogène.

Cor 9 : Si G est un groupe monogène, alors G vérifie l'une des conditions suivantes : (1) $G \simeq \mathbb{Z}$, dans ce cas G est monogène infini
(2) $\exists n > 0$ tq $G \simeq \mathbb{Z}/n\mathbb{Z}$ alors G est cyclique d'ordre n.

Cor 10 : (i) deux groupes monogènes infinis sont isomorphes
(ii) deux groupes cycliques d'ordre n et m sont isomorphes ssi $n = m$

Prop 11 : Un groupe monogène infini possède exactement deux générateurs distincts.

déf 12 : Pour $n \geq 2$, on note $\varphi(n) = \# \{ h \in [\![0, n-1]\!], h \wedge n = 1 \}$

Prop 13 : Soit G un groupe cyclique d'ordre n et a un générateur de G. Pour tout $h \in \mathbb{Z}$, l'ordre de $a^h \in G$ est $\mathrm{ord}(a^h) = \frac{n}{n \wedge h}$
En particulier, a^h est générateur ssi $n \wedge h = 1$. Il existe donc exactement $\varphi(n)$ générateurs distincts de G.

Cor 14 : Soit G un groupe cyclique d'ordre n. Le groupe $\mathrm{Aut}(G)$ est d'ordre $\varphi(n)$ et ses éléments sont les applications de : $x \mapsto x^h$, avec $h \wedge n = 1$.

Thm 15 : Tout sous-groupe fini du groupe multiplicatif d'un corps (commutatif) est cyclique.

Cor 16 : $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique et $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z} = \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$

Prop 17 : Soit G un groupe cyclique d'ordre n et a un générateur de G. Tout sous-groupe de G est cyclique et pour tout diviseur d de n, il existe un unique ss-gpe de G d'ordre d qui est :
$$H_d = \{ x \in G, x^d = 1 \} = \langle a^{n/d} \rangle$$

Prop 18 : Le produit $G_1 \times G_2$ de deux groupes est cyclique ssi G_1 et G_2 sont cycliques d'ordre n et m avec $n \wedge m = 1$.
Dans ce cas, $\langle \{(a, b)\} \rangle = G_1 \times G_2$ ssi $\langle \{a\} \rangle = G_1$ et $\langle \{b\} \rangle = G_2$

Cor 19 (Th Chinois) : Pour n, m entiers ≥ 1,
$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z} \quad \text{ssi} \quad n \wedge m = 1.$$

I. 2 Groupes abéliens libres de type fini :

déf 20 : Étant donnée une famille $\{G_i\}_{i \in I}$ de groupes abéliens, où I est un ensemble quelconque, le sous-groupe Γ du groupe $\prod_{i \in I} G_i$, formé par l'ensemble des $x \in \prod G_i$ qui n'ont qu'un nombre fini de composantes non-nulles est appelé somme directe des groupes abéliens G_i, noté : $\Gamma = \bigoplus_{i \in I} G_i$

déf 21 : On dit qu'un groupe abélien est libre s'il est somme directe de groupes monogènes infinis. Il s'écrit donc sous la forme : $F = \bigoplus_{i \in I} \langle x_i \rangle$, $I \neq \emptyset$ et $\langle x_i \rangle \simeq \mathbb{Z}$ $\forall i$

déf 22 : Soit F un groupe abélien libre. Alors $X = \{x_i\}_{i \in I}$ est appelé une base de F. On notera alors $F(X)$.

Prop 23 : On a $F(X) \simeq \mathbb{Z}^{(X)}$

Rq 24 : A isomorphisme près, il existe un seul groupe abélien libre sur X.

Th 25 : Un groupe abélien libre est de type fini ssi il a une base finie. Dans ce cas, toutes ses bases ont même nombre d'éléments (= rang).

Th26 : Si H est un sous groupe de F gpe abélien libre. Alors H est libre et $rg(H) \leq rg(F)$

I.3 Groupes abéliens de type fini

déf 27 : Les éléments d'ordre fini de G sont appelés éléments de torsion du groupe. On dit que G est de torsion (resp. sans torsion) si $Tor(G) = G$ (resp. $tor(G) = \emptyset$).

Prop 28 : Si G est un gpe abélien de t.f. et sans torsion, alors G est libre de rang fini.

Cor 29 : Soit G abélien de t.f. Il existe H ss-gpe de G libre tq $G \simeq H \oplus Tor(G)$ et $Tor(G)$ est fini

Th 30 : Soit G un groupe abélien de type fini. Alors $\exists ! n \in \mathbb{N}$, $\exists ! (p_1, \dots, p_k)$ premiers et pour $1 \leq i \leq k$ une unique suite $n_{i,1} \geq \dots \geq n_{i,a_i} \geq 1$ tq $G \simeq \mathbb{Z}^n \times \prod_{1 \leq i \leq k} (\mathbb{Z}/p_i^{n_{i,1}}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p_i^{n_{i,a_i}}\mathbb{Z})$

II - Exemples de groupes non abéliens

II - 1 Groupe symétrique

déf 31 : Pour tout entier $n \geq 1$, le groupe symétrique S_n est le groupe de permutation de l'ensemble $[\![1, n]\!]$.

Prop 32 : $|S_n| = n!$ et S_n non abélien pour $n > 2$.

déf 33 : Soit $\sigma \in S_n$, le support de σ est $Supp(\sigma) = \{i, \sigma(i) \neq i\}$

Prop 34 : $\forall \sigma, \sigma' \in S_n$, $supp(\sigma) \cap supp(\sigma') = \emptyset \Rightarrow \sigma\sigma' = \sigma'\sigma$

déf 35 : A toute permutat° $\sigma \in S_n$, on associe les orbites de l'action de σ sur $[\![1, n]\!]$.

$$\mathcal{O}_\sigma(i) = \{\sigma^n(i), n \in \mathbb{Z}\}$$

déf 36 : Une permutation est un cycle ssi toute orbite sauf au plus une est réduite à un point.

Th 37 : Toute permutat° $\sigma \in S_n$ s'écrit comme produit de cycles à supports disjoints.

Cor 38 : (i) Les transposit° (cycles de lg 2) engendrent S_n

(ii) $\{(1,2); (1,3); \dots; (1,n)\}$ engendre S_n

(iii) $< \{(1,2), (2,3), \dots, (n-1,n)\} > = S_n$

(iv) $<\{(1,2), (1\,2 \dots n)\}> = S_n$

Appli 39 : Pour $n \neq 6$, on a $Aut(S_n) = Int(S_n)$

Prop 40 : Il existe un unique morphisme de groupes non trivial $\varepsilon : S_n \to \mathbb{C}^*$ de noyau noté $\mathfrak{A}_n$.

Prop 41 : Pour $n \geq 3$, les 3-cycles engendrent $\mathfrak{A}_n$.
Pour $n \geq 5$, ils sont conjugués dans $\mathfrak{A}_n$.

Appli 42 : Ssi $n \neq 4$ $\mathfrak{A}_n$ est simple. Dévt 1

Déf 43 : $D(H) = <\{xyx^{-1}y^{-1}, x, y \in H\}> \Leftrightarrow H/D(H)$ plus grand quotient abélien

Appli 44 : Si $n \geq 5$, $D(S_n) = D(\mathfrak{A}_n) = \mathfrak{A}_n$.

Prop 45 : Si $n \neq 4$, les seuls ss-gpes distingués de S_n sont $\{Id\}$, $\mathfrak{A}_n$ et S_n.

II - 2 Groupe diédral.

déf 46 : Pour $n \in \mathbb{N}^*$, on note P_n un polygone régulier à n sommets dans le plan. Soit D_n l'ens. des isométries du plan qui conservent P_n.
Alors D_n est un ssgpe de O_n appelé gpe diédral.

Th 47 : $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ de cardinal 2n et $D_n = <r, s>$  A_0

Où r est la rotat° d'angle $\frac{2\pi}{n}$ et s est la symétrie orthogonale d'axe (OA_0).
On a $sor = r^{-1}os$

III - Groupes en algèbre linéaire

Soit $\mathbb{K}$ un corps (commutatif).

III - 1. Groupe linéaire

déf 48 : On appelle groupe linéaire l'ensemble des $\mathbb{K}$-automorphismes de E, noté $GL(E)$.

déf 49 : le noyau du morphisme de groupes $\det$ est appelé groupe spécial linéaire et est noté $SL_n(\mathbb{K})$

Prop 50 : $GL_n(\mathbb{K}) = SL_n(\mathbb{K}) \rtimes \mathbb{K}^*$

déf/prop 51 : On appelle dilatation un élément qui fixe un hyperplan H et vérifie l'une des propriétés équivalentes suivantes :

(i) $\det(u) = \lambda \neq 1$

(ii) u admet une valeur propre $\lambda \neq 1$ et u est diagonalisable

(iii) $\mathrm{Im}(u - \mathrm{Id}) \not\subset H$.

(iv) Il existe une base de $\mathbb{K}^n$ dans laquelle u a pour matrice $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$

déf/prop 52 : On appelle transvection un élément u fixant un hyperplan H qui vérifie l'une des prop. équivalentes suivantes :

(i) $u \neq \mathrm{id}$ et $\det u = 1$

(ii) Si f est une forme lin. telle que $H = \ker f$, alors $\exists a \in H$ tq $u(x) = x + f(x)a$.

(iii) u n'est pas diagonalisable

(iv) $\{0\} \neq \mathrm{Im}(u - \mathrm{Id}) \subset H$.

(v) Dans une certaine base $\mathrm{Mat}(u) = \begin{pmatrix} 1 & & 0 \\ & \ddots & 1 \\ & & 1 \end{pmatrix}$

Th 53 : (i) $SL_n(\mathbb{K})$ est engendré par les transvections

(ii) $GL_n(\mathbb{K})$ est engendré par les transvections et les dilatations.

Appli 54 : Pivot de Gauss.

III - 2 Groupe orthogonal.

déf 55 : On appelle isométrie de E (relativement à q) les automorphismes $u \in GL(E)$ qui vérifient $q(u(x)) = u(x)$ $\forall x \in E$.

(où q forme quadratique).

déf 56 : On note $O^+(q)$ le groupe des isométries de déterminant 1.

déf 57 : Si une isométrie a comme matrice $\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{pmatrix}$ dans une certaine base, on dit que c'est une ~~isom~~ symétrie.

Prop 58 : les symétries sont les éléments d'ordre 2 de $O(E)$.

Déf 59 : Si $\begin{cases} \dim(\ker(u+id)) = 1, \text{ on dit } u \text{ réflexion} \\ \dim(\ker(u+id)) = 2, \text{ on dit } u \text{ renversement} \end{cases}$

Th 60 : (i) Les réflexions engendrent $O(E)$

(ii) Les retournements engendrent $O^+(E)$ pour $\dim E \geq 3$

Dév 2