Exemples de parties génératrices d'un groupe. Applications.

108

DVP 1

I – Propriétés algébriques des parties génératrices

1. Parties génératrices, groupes monogènes

Déf 1. Soient G un groupe et $A \subset G$. Le plus petit sous-groupe de G contenant A existe et est noté $\langle A \rangle$. C'est le sous-groupe engendré par A. Il est égal à l'intersection des sous-groupes de G contenant A, et à $\{s_1 \dots s_k : s_i \in A \cup A^{-1}\}$. Si $\langle A \rangle = G$, on dit que A est une partie génératrice ; si $|A| = 1$ on dit que $\langle A \rangle$ est monogène. On a toujours $G = \langle G \rangle$.

Exm 2. Les seuls groupes monogènes (à iso près) sont $\mathbb{Z}$ et les groupes cycliques $\mathbb{Z}/n\mathbb{Z}$.

Exm 3. Des exemples non-abéliens sont :
- $D_n = \langle$ rotation d'angle $2\pi/n$, réflexion d'axe $Ox \rangle$;
- $\mathfrak{S}_n = \langle (i\ j) : i < j \rangle$; $\mathfrak{S}_n = \langle (1\ j) : 1 < j \rangle$;
- $\mathfrak{S}_n = \langle (i\ i+1) : i < n \rangle$; $\mathfrak{S}_n = \langle (1\ 2), (1\ 2 \dots n) \rangle$;
- $\mathfrak{A}_n = \langle 3\text{-cycles} \rangle$.

Déf 4. L'ordre d'un élément g d'un groupe est l'ordre de $\langle g \rangle$.

Prop 5. $\mathbb{Z}/p\mathbb{Z}$ est le seul groupe d'ordre p (à iso près, p premier). Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont isomorphes à $\mathbb{Z}/d\mathbb{Z}$ avec $d|n$. Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$.

App 6. Si $G/Z(G)$ est cyclique alors G est abélien.

Prop 7. Si k est un corps, tout sous-groupe fini de $k^\times$ est cyclique.

Thm 8. $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique lorsque $n = 4$ ou lorsque n est de la forme p^r ou $2p^r$ avec p premier impair.

Prop 9. Si H est un sous-groupe strict de G alors $G \setminus H$ est une partie génératrice de G.

Prop 10. Si $G = \langle S \rangle$ et $H = \langle T \rangle$ alors $(S \times 1) \amalg (1 \times T)$ est une partie génératrice de $G \times H$.

Déf 11. Le sous-groupe dérivé $D(G)$ d'un groupe G est le sous-groupe engendré par les commutateurs :
$$D(G) = \langle [a,b] = aba^{-1}b^{-1} : a,b \in G \rangle.$$
C'est le plus petit sous-groupe distingué de G tel que le quotient $G^{ab} = G/D(G)$ soit abélien.

App 12. Si G est un groupe topologique connexe alors $D(G)$ est aussi connexe.

2. Minimalité

Prop 13. Si G est un groupe fini, on peut toujours en trouver une partie génératrice de cardinal $\leq \lfloor \log_2 |G| \rfloor$.
On peut parfois faire beaucoup mieux : D_n et $\mathfrak{S}_n$ sont toujours engendrés par deux éléments mais $|D_n| = 2n$ et $|\mathfrak{S}_n| = n!$.

Lem 14. Si $[G:H]$ est le plus petit diviseur premier de $|G|$ alors H est distingué dans G.

Thm 15. (de la base de Burnside)
Les parties génératrices minimales d'un p-groupe fini ont toutes le même cardinal.

Exm 16. Le groupe quaternionique $\mathbb{Q}_8$ est un 2-groupe et ses parties génératrices minimales sont toutes de cardinal 2.

Exm 17. Le groupe symétrique $\mathfrak{S}_n$ avec $n \geq 3$ n'est pas un p-groupe, il a des parties génératrices minimales de cardinaux différents.

Exm 18. Le p-groupe de Prüfer $\mathbb{Z}_{p^\infty} \simeq \{z \in \mathbb{C} \mid \exists \alpha \in \mathbb{N},\ z^{p^\alpha} = 1\}$ est un p-groupe mais n'a aucune partie génératrice minimale.

II – Groupes de type fini

1. En général

Déf 19. Soit X un ensemble. Le groupe F_X des mots de la forme $x_1^{\varepsilon_1} \dots x_s^{\varepsilon_s}$ avec $x_i \in X$ et $\varepsilon_i = \pm 1$, modulo les relations $xx^{-1} = x^{-1}x = 1$ pour $x \in X$ et muni de la concaténation des (classes de) mots s'appelle le groupe libre sur X. C'est l'unique groupe (à iso. près) vérifiant la propriété universelle :
pour tout groupe G et toute application $X \to G$, il existe un unique morphisme $F_X \to G$ tel que $X \to F_X$ commute, $X \to F_X$ envoyant x sur x.

Déf 20. Un groupe est de type fini s'il admet une partie génératrice finie.

Exm 21. Les groupes finis, les $\mathbb{Z}^r$, $PSL(2,\mathbb{Z})$ ou encore $GL(n,\mathbb{F}_q)$ sont de type fini. $\mathbb{Q}$ et $\mathbb{Q}^\times$ ne sont pas de type fini.

Rmq 22. Si G n'est pas de type fini alors toute partie génératrice de G a le même cardinal que G.

Prop 23. Les groupes de type fini sont exactement les quotients des groupes libres sur un nombre fini de générateurs. Ainsi, un quotient d'un groupe de type fini est aussi de type fini.

Exm 24. Un sous-groupe d'un groupe de type fini n'est pas forcément de type fini : le sous-groupe dérivé $D(F_2)$ du groupe libre à deux générateurs est libre, à une infinité dénombrable de générateurs.

Déf 25. Soit $G = \langle g_1, \dots, g_m \rangle$ un groupe de type fini. D'après la propriété universelle, G est isomorphe à un quotient de groupe libre F_X/R, où $X = \{x_1, \dots, x_m\}$ avec R le noyau du morphisme $F_X \longrightarrow G$ envoyant x_i sur g_i. Si $R = \langle r_1, \dots, r_n \rangle$, on appelle présentation par générateurs et relations l'écriture :

$$G = \langle g_1, \dots, g_m \mid r_1, \dots, r_n \rangle .$$

Exm 26. $\mathbb{Z}/n\mathbb{Z} = \langle x \mid x^n \rangle$. $D_n = \langle r, s \mid r^n, s^2, (rs)^2 \rangle$.
$\mathfrak{S}_3 = \langle a, b \mid a^3, b^2, (ab)^2 \rangle$.
$A_4 = \langle a, b \mid a^3, b^2, (ab)^3 \rangle$.
$G_4 = \langle a, b \mid a^3, b^2, (ab)^4 \rangle$.
$A_5 = \langle a, b \mid a^3, b^2, (ab)^5 \rangle$.

2. Les groupes abéliens de type fini

DVP2

Thm 27. (forme normale de Smith)
Soient A un anneau euclidien et $M \in \mathcal{M}_{m,n}(A)$. Alors il existe des éléments $f_1, \dots, f_r \in A$ tels que $f_1 | f_2 | \dots | f_r$ et uniques à association près, tels que M soit équivalente à :

$$\begin{bmatrix} f_1 & & & 0 \\ & f_2 & & \\ & & \ddots & \\ & & & f_r \\ 0 & & & 0 \end{bmatrix}.$$

Cor 28. (classification des groupes abéliens de type fini)
Soit G un groupe abélien de type fini. Alors il existe un unique entier $r \in \mathbb{N}$ et une unique suite d'entiers positifs $(s_1, \dots, s_k)$ tels que $s_1 | \dots | s_k$ et

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/s_1\mathbb{Z} \times \dots \times \mathbb{Z}/s_k\mathbb{Z} .$$

Rmq 29. On en déduit directement que de tout groupe G abélien fini d'ordre $p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ on peut trouver une partie génératrice de cardinal $\alpha_1 + \dots + \alpha_s$, mieux, de cardinal $1 + \max \alpha_i$.

Thm 30. Soit $G = \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$. Pour tout premier p, on note d_p le nombre de i tels que $p | n_i$. Alors le cardinal minimal d'une partie génératrice de G est exactement $\max d_p$.

III – Parties génératrices en géométrie

1. Groupes matriciels

Soient k un corps et E un k-espace vectoriel de dimension finie.

Thm 31. Les transvections engendrent $SL(E)$. Les transvections et dilatations engendrent $GL(E)$.

Prop 32. Les transvections sont toutes conjuguées dans $GL(E)$. Elles le sont aussi dans $GL(E)$ si $\dim E \geq 3$.

Thm 33. (Algorithme du pivot de Gauss)
Toute matrice inversible à coefficients dans k est équivalente à une matrice de dilatation via des opérations élémentaires de transvections. Ainsi $GL(n,k)$ est engendré par les matrices de dilatations et transvections, et $SL(n,k)$ par les matrices de transvections.

Cor 34. Si $k = \mathbb{R}$ ou $\mathbb{C}$ alors $SL(n,k)$ est connexe par arcs.

Cor 35. $GL(n,k)$ est engendré par les matrices (inversibles et) diagonalisables.

Thm 36. Le groupe dérivé $D(GL(n,k))$ est $SL(n,k)$ sauf si : $n=2$, $k = \mathbb{F}_2$.
De même, $D(SL(n,k)) = SL(n,k)$ sauf si : $n=2$, $k = \mathbb{F}_2$ ou $\mathbb{F}_3$.

Thm 37. $PSL(n,k)$ est simple sauf si $n=2$ et $k = \mathbb{F}_2$ ou $\mathbb{F}_3$.

Thm 38. Si q est une forme quadratique non-dégénérée alors le groupe orthogonal $O(q)$ est engendré par les réflexions.
Mieux (Cartan-Dieudonné) : tout élément de $O(q)$ est produit d'au plus $\dim(E)$ réflexions.

Thm 39. $SO(q) = \langle$retournements$\rangle$ et de même, tout élément de $SO(q)$ est produit d'au plus $\dim(E)$ retournements, lorsque $\dim(E) \geq 3$.

Cor 40. $SO(3, \mathbb{R})$ est simple.

2. Graphes de Cayley

Déf 41. Le graphe de Cayley d'un groupe G selon une partie génératrice finie S, noté $\Gamma(G,S)$, est le graphe orienté :
- dont les nœuds sont étiquetés par les éléments de G ;
- avec pour chaque nœud x et chaque générateur $s \in S$, un arc de x vers xs, étiqueté par s.

Exm 42 Annexe ① : graphe de Cayley de $\langle a,b \mid a^3, b^2, (ab)^4 \rangle$ selon $S = \{a,b\}$. C'est un cube tronqué.

Rmq 43. Le graphe de Cayley dépend de la partie génératrice choisie ! Le groupe précédent admet un graphe de Cayley qui est un octaèdre tronqué.

Rmq 44. Par construction, le groupe G agit simplement transitivement sur chacun de ses graphes de Cayley. Ainsi, si un groupe H agit aussi simplement transitivement sur $\Gamma(G,S)$ alors $G \cong H$.

Prop 45. Le groupe $\mathfrak{S}_4$ agit simplement transitivement sur le cube tronqué en annexe ①. Ainsi :

$$\mathfrak{S}_4 \cong \langle a, b \mid a^3, b^2, (ab)^4 \rangle.$$

C'est la présentation donnée en Exm 26.

IV -- Aspects pratiques

1. Application en cryptographie : le système El Gamal

Déf 46. Soient G un groupe cyclique et $g \in G$ un générateur. Pour $0 \leq i < |G|$, le logarithme discret de g^i est l'entier i.

Principe 47 Le cryptosystème El Gamal permet d'envoyer un message $M \in \{0, \dots, |G|-1\}$ de façon sécurisée grâce à la difficulté pratique du calcul du logarithme discret dans $G = (\mathbb{Z}/p\mathbb{Z})^\times$ (ou plus généralement $G = \mathbb{F}_q^\times$, qui est cyclique, en vertu de la Prop 7).

Chiffrement 48. (cf. Annexe ②). Alice souhaite envoyer un message à Bob. Bob possède une clé publique (p_b, g_b, β_b) et une clé privée α_b, telles que :

- p_b est un (grand) nombre premier ;
- g_b est un générateur de $(\mathbb{Z}/p_b\mathbb{Z})^\times$;
- $0 \leq \alpha_b < p_b$ et $\beta_b = g_b^{\alpha_b}$.

Pour envoyer le message M à Bob, Alice choisit $k_a \leq p_b - 1$ (qu'elle devra changer régulièrement), puis envoie à Bob le couple chiffré :

$$(y_1, y_2) = (g_b^{k_a}, \beta_b^{k_a} M).$$

Déchiffrement 49. Pour lire le message, Bob calcule $y_2 (y_1^{\alpha_b})^{-1}$ pour obtenir M modulo p_b.

Sécurité 50. On ne sait pas décrypter les messages interceptés sans connaître la clé privée α_b. Les meilleurs algorithmes de calcul des logarithme discret pour retrouver α_b sont actuellement en $O\left(e^{C\sqrt{\log_2(p)\log_2(\log_2(p))}}\right)$.

2. Vérifier l'associativité d'une table de multiplication

Rmq 51 Étant donnée une table de multiplication de taille $n \times n$, on peut vérifier qu'elle admet un élément neutre et que chaque élément a un inverse en temps $O(n^2)$. Pour vérifier l'associativité, l'algorithme naïf consistant à vérifier que $a(bc) = (ab)c$ pour tous a, b et c s'exécute en $O(n^3)$ opérations.

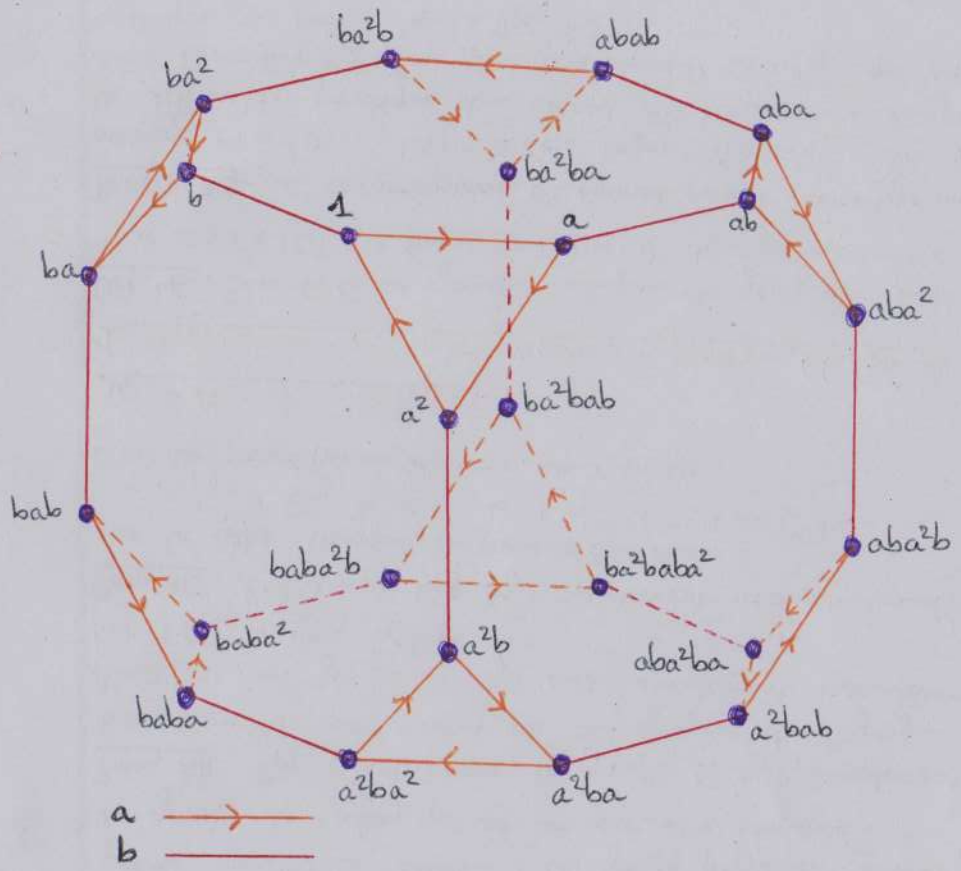
Prop 52. Soit $(G, \cdot)$ un magma admettant une partie génératrice Γ. Alors $\cdot$ est associative si et seulement si $a(bc) = (ab)c$ pour tous $a, b \in G$ et $c \in \Gamma$.

Cor 53. Grâce à la proposition 13, on obtient un test d'associativité en $O(n^2 \log n)$.

Thm 54. Étant donnée la table de multiplication d'un magma $(G, \cdot)$, après avoir vérifié qu'il admettait un élément neutre et tous les inverses, on peut en trouver une partie génératrice et vérifier son associativité en $O(n^2)$ opérations élémentaires.

Cor 55 On sait donc reconnaître une table de multiplication d'un groupe en $O(n^2)$.

Annexe ① : Graphe de Cayley de $\langle a, b \mid a^3, b^2, (ab)^4 \rangle$.



Annexe ② : Système El Gamal

ALICE
- Veut transmettre M
- Choisit $k_a \leq p_b - 1$ (et change souvent)

envoie
$(y_1, y_2) = (g_b^{k_a}, \beta_b^{k_a} M)$

CHARLIE
intercepte (y_1, y_2)
↓
Ne sait pas le décoder car il lui faut connaître α_b.

BOB
Public : p_b, g_b, β_b
Privé : α_b

décode
$M = y_2 (y_1^{\alpha_b})^{-1}$

- Perrin
- Berhuy, Modules: Théorie, pratique
- Boyer, Petit compagnon des nombres
- Debreil, Groupes finis et treillis de leurs sous-groupes
- Debreil, Mneimné, Le groupe S4 et ses métamorphoses
- Zavidovique (dvt 1)
- Objectif Agreg et 131 Développements (dvt 2: présenter l'algo pour l'existence, pas la méthode de 131 Dvt)