Université Claude Bernard–Lyon I
Agrégation de Mathématiques : Algèbre & géométrie
Année 2008–2009

Exemples de parties génératrices de groupes

Idée générale : Donner des parties génératrices de groupes "classiques", et *les utiliser* pour montrer des propriétés du groupe : simplicité, calcul du groupe dérivé, du centre, des automorphismes, etc.

Pour l'anecdote, voici un théorème (très) difficile, qui exprime que connaître une partie génératrice n'est pas la fin de tous les problèmes : tout groupe fini simple non abélien peut être engendré par deux éléments.

A ne pas manquer

- Groupes cycliques (rapidement), classification des groupes abéliens de type fini.
- Cœur de la leçon : parties génératrices de groupes "classiques" : groupes symétriques, groupes linéaires (GL, SL), groupes orthogonaux, voire groupes symplectiques.
- Dans chaque cas, on n'oubliera pas d'en tirer des propriétés structurelles du groupe.

Compléments (autres développements possibles)

- Le groupe modulaire $\mathrm{PSL}_2(\mathbb{Z})$ est engendré par S et T (pas très dur, voir V).
- Groupe présenté par générateurs et relations. Exemple du groupe symétrique (plus dur).

Quelques questions

- Tout groupe abélien de type fini est un quotient d'un $\mathbb{Z}^r$. Plus généralement, tout groupe de type fini, abélien ou non, est dénombrable. Le groupe additif $\mathbb{Q}$ est dénombrable, mais pas de type fini.
- Tout sous-groupe fini d'un corps commutatif est cyclique.
- Est-ce que le groupe $\mathbb{Z}^{(\mathbb{N})}$ des suites d'entiers presque nulles est libre ? Est-ce que le groupe $\mathbb{Z}^{\mathbb{N}}$ des suites d'entiers est libre ? (La deuxième question est délicate.)

I Groupes abéliens

1° Groupes cycliques

(a) Si un groupe est engendré par un seul élément, il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un unique $n \in \mathbb{N}$ (on autorise $n = 0$). Pour tout diviseur d de n, il a un unique sous-groupe d'indice d.
(b) Exemple *nécessaire* : tout sous-groupe fini d'un corps (commutatif !) est cyclique.

Réf. : A savoir par cœur. Ne pas s'apesantir sur cette partie facile.

2° Groupes abéliens de type fini

(a) Groupes abéliens libres. Une famille $(e_i)_{i\in I}$ est une base d'un groupe abélien G si tout élément de G s'écrit de façon unique sous la forme $\sum_{i\in I} n_i e_i$, où $(n_i)_{i\in I} \in \mathbb{Z}^{(I)}$ est une famille presque nulle d'entiers. Un groupe abélien est dit abélien libre s'il admet une base. Toutes les bases d'un groupe abélien libre ont le même cardinal, qu'on appelle son rang, noté $\operatorname{rg} G$.
Bien sûr, le groupe $\mathbb{Z}^{(I)}$ des familles presque nulles d'entiers indexée par un ensemble I est (trivialement) un groupe abélien libre, et (trivialement) tout groupe abélien libre est isomorphe à un tel groupe.

(b) Théorème de la base adaptée. Tout sous-groupe H d'un groupe abélien libre de type fini G est libre de type fini. Plus précisément, il existe une base $(e_1, \dots, e_n)$ de G, un entier $h \in \mathbb{N}$ et des entiers $(q_1, \dots, q_h) \in \mathbb{N}^h$, avec $q_1|q_2|\cdots|q_h \neq 0$ tels que $(q_1e_1, \dots, q_he_h)$ est une base de H. De plus, $n = \operatorname{rg} G$, $h = \operatorname{rg} H$ et $q_1, \dots, q_h$ sont uniques.

(c) Classification et structure. Tout groupe abélien de type fini est isomorphe à

$$\mathbb{Z}^r \oplus \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_h\mathbb{Z}, \quad \text{avec } q_1|q_2|\cdots|q_h \neq 0.$$

De plus, r (rang) et les q_i (diviseurs élémentaires ou facteurs invariants) sont uniques.

NB: même avec le théorème de la base adaptée, l'unicité est délicate, et demande la décomposition primaire (style "lemme chinois").

Exemple : groupe des inversibles de l'anneau des entiers d'une extension finie de $\mathbb{Q}$ ("théorème des unités") ; cas particuliers de (certaines) extensions quadratiques.

Réf. : Guin ou Goblot, par exemple.

II Groupes symétriques $\mathfrak{S}_n$ et alternés $\mathfrak{A}_n$

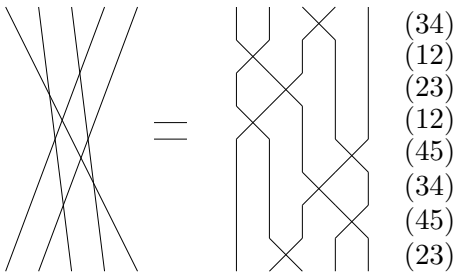
1° Engendrement par (toutes) les transpositions

(a) Preuve : récurrence sur le nombre de points fixes.

(b) Application : Unicité de la signature (morphisme non trivial $\varepsilon : \mathfrak{S}_n \to \mathbb{C}^\times$), donc de $\mathfrak{A}_n$.

2° Engendrement par les transpositions $(i, i+1)$ $(i = 1, \dots, n-1)$

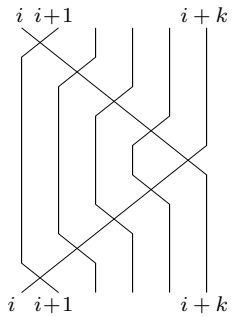
Interprétation géométrique :



$$(15234) = (23)(45)(34)(45)(12)(23)(12)(34).$$

Preuve pas très constructive : utiliser le cas précédent et la formule suivante :

$$\forall i = 1, \dots, n-1,\ \forall k = 1, \dots, n-i, \quad (i, i+k) = s_i s_{i+1} \cdots s_{i+k-2} s_{i+k-1} s_{i+k-2} \cdots s_{i+1} s_i.$$



Preuve constructive : utiliser le lemme suivant (voir la présentation de Coxeter IV**??**).

Lemme *Tout élément $w \in \mathfrak{S}_n$ peut s'écrire sous la forme :*

$$w = \underbrace{s_{i_{n-1}} s_{i_{n-1}+1} \cdots s_{n-2} s_{n-1}}\ \underbrace{s_{i_{n-2}} s_{i_{n-2}+1} \cdots s_{n-3} s_{n-2}}\ \cdots \underbrace{s_{i_k} s_{i_k+1} \cdots s_{k-1} s_k}\ \cdots$$

où $1 \leq i_k \leq k+1$ pour $k = 1, \dots, n-1$, avec la convention que si $i_k = k+1$, on n'écrit pas le "paquet" correspondant.

Sens du lemme : Tout élément s'obtient en supprimant les premières lettres de chaque paquet à partir de la décomposition suivante de l'élément le plus long :

$$w_0 = \underbrace{s_1 s_2 \cdots s_{n-2} s_{n-1}}\ \underbrace{s_1 s_2 \cdots s_{n-3} s_{n-2}}\ \cdots\ \underbrace{s_1 s_2 s_3}\ \underbrace{s_1 s_2}\ \underbrace{s_1} = (1,n)(2,n-1)(3,n-2)\cdots .$$

Preuve du lemme. On procède par récurrence sur n (rien à démontrer pour $n \leq 2$). Si n est fixe par w, l'hypothèse de récurrence donne une décomposition convenable, avec $i_{n-1} = n$ (on supprime tout le paquet $s_1 s_2 \ldots s_{n-1}$). Sinon, on pose $i_{n-1} = w(n)$. On utilise la formule suivante, pour $i < n$:

$$s_i s_{i+1} \cdots s_{n-1} = (i, i+1, \ldots, n-1, n).$$

Elle montre que $(s_{i_{n-1}} \cdots s_{n-1})^{-1} w$ fixe n, ce qui ramène au premier cas.□

3° Autres parties génératrices

(a) Engendrement par (12) et $(12\cdots n)$. Preuve : ramener au cas précédent en conjugant : $(12\cdots n)^i (12) (12\cdots n)^{-i} = (i+1, i+2)$.
Attention ! Il peut arriver qu'un n-cycle et une transposition n'engendrent pas $\mathfrak{S}_n$. Exemple : $\sigma = (1234)$ et $\tau = (13)$ dans $\mathfrak{S}_4$ satisfont : $\tau\sigma\tau^{-1} = \mathrm{Id}$, donc engendrent un groupe diédral (d'ordre 8, un 2-Sylow de $\mathfrak{S}_4$).
Si $n = p$ premier, en revanche, un n-cycle σ et une transposition (ij) engendrent $\mathfrak{S}_p$. En effet, σ possède une puissance qui est encore un p-cycle (la primalité de p joue ici), et qui envoie i sur j, ce qui ramène au cas précédent.

Application : Le groupe de Galois G de $P = X^5 - 6X + 3$ sur $\mathbb{Q}$ est $\mathfrak{S}_5$. En effet, P est irréductible par le critère d'Eisenstein. Si L est son corps de décomposition sur $\mathbb{Q}$, il contient le corps de rupture de P, donc le degré $[L : \mathbb{Q}]$ est divisible par 5, donc G contient un 5-cycle.
Par ailleurs, le polynôme a 3 racines réelles (vérifier !), donc la conjugaison complexe agit comme une transposition sur les 5 racines. Ainsi, G contient un 5-cycle et une transposition : on peut conclure.

(b) Engendrement du groupe alterné par les 3-cycles. (Récurrence sur le nombre de points fixes, qui vaut n ou est ≥ 3.) Engendrement par les doubles transpositions.

4° Applications

Sous-groupe dérivé de $\mathfrak{S}_n$ et $\mathfrak{A}_n$, des automorphismes (pour $n \neq 6$), simplicité de $\mathfrak{A}_n$ ($n \geq 5$).

Réf. : Perrin est excellent sur ces questions.

III Groupes de matrices

1° Groupe linéaire et avatars

(a) L'algorithme de Gauss peut s'exprimer par l'engendrement de GL_n par les matrices triangulaires et les matrices de permutation. Plus précisément, toute matrice est un produit $L_1 P L_2$, où L_1, L_2 sont triangulaires inférieures, et P et une matrice de permutation.
(b) Engendrement de SL_n par les transvections, de GL_n par les transvections et les dilatations.
Application : Simplicité de PSL_n (sauf $\mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z})$ et $\mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z})$). Groupes dérivés.

2° Groupes d'isométrie

(a) Engendrement du groupe orthogonal par les réflexions. Idem pour le groupe des isométries d'un espace affine euclidien.
Application : Calcul du centre de ces groupes.
(b) Engendrement de SO_3 par les demi-tours.
Application : Simplicité de SO_3. Tout automorphisme est intérieur. Pour montrer que "le" morphisme $\mathrm{SU}_2 \to \mathrm{SO}_3$ est surjectif, il suffit d'exhiber un demi-tour dans son image.

Réf. : Once again, Perrin est excellent sur ces questions. Voir aussi Lang, par exemple.

(c) Paradoxe de Banach-Tarski ou la multiplication des pains. Deux rotations dans $\mathrm{SO}_3(\mathbb{R})$ engendrent génériquement (presque partout) un groupe libre (voir ci-dessous). Ceci permet de montrer l'existence d'une partition d'une sphère de rayon 1 de $\mathbb{R}^3$ en un nombre *fini* de parties $A_1, \ldots, A_n, B_1, \ldots, B_p$, et des parties $A'_1, \ldots, A'_n, B'_1, \ldots, B'_p$ isométriques aux précédentes, telles que $\bigcup A'_i$ et $\bigcup B'_j$ soient deux sphères de rayon 1. Paradoxal, non ? Un développement peut consister à montrer que deux éléments convenablement choisis engendrent en effet un groupe libre.

Réf. : Ecrit du CAPES 2004 (voir un livre d'annales).

IV Générateurs et relations

Voir le texte sur les présentations de groupes :
`http://math.univ-lyon1.fr/~germoni/agreg/presentation.pdf`

V Sur le groupe modulaire

1° Motivation

Considérons le groupe $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$. On veut montrer de deux façons différentes que Γ est engendré par les classes des deux éléments

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

On fait opérer Γ par homographies sur le demi-plan de Poincaré $\mathcal{H} = \{z \in \mathbb{C} \ : \ \mathrm{Re}(z) > 0\}$:

$$\forall g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \ \forall z \in \mathcal{H}, \quad g \cdot z = \frac{az+b}{cz+d}.$$

Pour des raisons arithmétiques, on s'intéresse aux fonctions holomorphes $f : \mathcal{H} \to \mathbb{C}$ satisfaisant la relation de modularité (pour un certain $k \in \mathbb{Z}$) :

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \ \forall z \in \mathcal{H}, \quad f\left(\frac{az+b}{cz+d}\right) = \frac{1}{(cz+d)^k} f(z)$$

Un intérêt de savoir que Γ est engendré par S et T, c'est que pour montrer qu'une fonction $f(z)$ est modulaire, il suffit de vérifier qu'elle est invariante par T, i.e. ne dépend que de $q = \exp(i\pi z)$, et que l'on a une relation de la forme $f(-1/z) = z^{-k} f(z)$.

2° Approche géométrique

Ici, on suit Serre. L'étude de la géométrie de l'action (recherche et étude d'un domaine fondamental) donne le résultat. Comme mentionné par Serre, si on poursuit cette étude, on peut montrer que le groupe Γ est présenté par générateurs a et b et relations $a^2 = b^3 = 1$. En d'autres termes, tout élément de Γ s'écrit de façon unique sous l'une des formes :

$$\begin{array}{ll} ab^{1 \text{ ou } 2}ab^{1 \text{ ou } 2} \cdots b^{1 \text{ ou } 2}a, & b^{1 \text{ ou } 2}ab^{1 \text{ ou } 2} \cdots b^{1 \text{ ou } 2}a, \\ b^{1 \text{ ou } 2}ab^{1 \text{ ou } 2} \cdots b^{1 \text{ ou } 2}a, & b^{1 \text{ ou } 2}ab^{1 \text{ ou } 2} \cdots b^{1 \text{ ou } 2}. \end{array}$$

où a est la classe de $A = S$ et b est la classe de $B = S^{-1}T$.

Réf. : Serre, *Cours d'arithmétique*, Chap. 7, §1.

3° Approche arithmétique

On donne une interprétation matricielle de l'algorithme d'Euclide.
Pour commencer, on a : $S^2 = -\mathrm{Id}$ et $ST^{-1}S^{-1} = {}^tT$ (la transposée). Noter que multiplier à gauche par S (resp. par T^{-q}), c'est permuter les deux lignes en changeant un signe (resp. remplacer la première ligne L_1 par la combinaison $L_1 - qL_2$).

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Notons $\delta(A) = \max(|a|, |c|)$. On montre par récurrence sur $\delta(A)$ que A est dans le groupe engendré par S et T. Si $c = 0$, on vérifie sans peine que A ou $S^2A = -A$ est une puissance de T. Si $a = 0$, on vérifie que SA ou $S^{-1}A$ est une puissance de T.
Supposons $\delta(A) \neq 0$. Si $|a| > |c|$, on écrit la division euclidienne : $a = cq + r$, où $0 \leq r < |c|$. Alors $\delta(T^{-q}A) = \max(|a - cq|, |c|) < \delta(A)$. Si $|a| < |c|$, on procède de même avec ${}^tT$. Si $|a| = |c|$, le fait que $\det(A) = 1$ montre que $|a| = |c| = 1$ et c'est facile.

Réf. : J. Germoni, *Best of Algèbre, les meilleurs sujets corrigés*, Clermont-Ferrand, Dunod.

4° Variante : $\Gamma(2)$

Dans le même esprit, une récurrence sur $\max(|a|, |c|)$ permettent de montrer de même que le noyau de la projection naturelle $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$, est engendré par

$$U = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad -\mathrm{Id}.$$

Un joli argument géométrique montre que son image $\Gamma(2)$ dans Γ est un groupe libre (voir CAPES blanc).