# Calcul effectif avec les groupes

Dans cette note on donne quelques informations sur la manière dont les ordinateurs effectuent des calculs avec les groupes.

## 1 Stockage

Rappelons qu'un *bit* (symbole : b) est une unité d'information de base dans un ordinateur (en général représenté par 0 ou 1) ; un *octet* (symbole : o) est un paquet de 8 bits ; un *byte* (symbole : B) est la plus petite unité « logiquement » adressable par un programme sur un ordinateur. Aujourd'hui, les bytes de 8 bits = 1 octet se sont généralisés, mais en principe ce n'est pas une règle absolue. C'est pourquoi les mémoires sont données tantôt avec le format 2 Go, tantôt avec le format 2 GB.

La machine représente les nombres entiers en base 2, donc $n = n_r 2^r + \cdots + n_1 r + n_0$ nécessite le stockage de $r \sim \log_2(n)$ bits. Les processeurs actuels ont une implémentation native de l'arithmétique des nombres de moins de 32 bits, ce qui suffit la plupart du temps.

## 2 Modes de représentation

Pour représenter un groupe, les deux manières les plus importantes sont sans doute les suivantes :

(1) comme *groupe de symétries* ;
(2) par *générateurs et relations*.

La manière (1) est plus concrète ; le groupe est représenté comme un sous-groupe, le plus souvent sous-groupe de $\mathfrak{S}_n$ pour des symétries d'ensembles finis, ou sous-groupe de $\mathrm{GL}_n$ pour des symétries d'objets d'algèbre linéaire ou de géométrie. La manière (2) est plus abstraite ; le groupe est représenté comme un quotient, plus précisément un quotient d'un groupe libre $L_X$. Ces deux modes de représentation sont utilisés en machine. Ils reposent de manière essentielle sur les groupes $\mathfrak{S}_n$, $\mathrm{GL}_n$ et $L_X$ qui jouent un rôle fondamental et dont la bonne implémentation dans les logiciels de calcul formel conditionne l'efficacité de tous les calculs.

## 3 Exemple : les groupes symétriques

Regardons comment stocker un groupe avec l'exemple des groupes symétriques. Une permutation est simplement stockée comme une liste des images des $n$ symboles permutés (appelons-les des points). Si $n \leqslant 2^{16} = 65536$, on peut faire avec 16 bits par point, c'est-à-dire 2 octets (et en général on s'en sort en tout cas avec 4 octets par point) ; il nous faut donc $2n$ octets de mémoire. Si on manipule un groupe de permutation agissant sur 1000 points, i.e. $G \subset \mathfrak{S}_{1000}$, chaque permutation prend 2 ko. Sur une machine avec 2 Go, en consommant toute la mémoire on pourrait stocker jusqu'à un million de permutations, mais notez qu'un million est ridicule comparé avec $|\mathfrak{S}_{1000}| = 1000! \approx 4 \cdot 10^{2567}$...

Il est donc hors de question de stocker tout le groupe ; plutôt, on se contentera de stocker des générateurs. Il se trouve que de nombreux groupes peuvent être engendrés par un petit nombre d'éléments.

# 4 Petites familles génératrices

Un groupe $G$ possède de nombreuses parties génératrices. On sait que selon l'utilisation que l'on veut en faire, différentes qualités de ces parties peuvent être pertinentes. Par exemple, pour démontrer que le groupe alterné $G = \mathfrak{A}_n$ avec $n \geqslant 5$ est simple, la méthode classique est d'utiliser la partie génératrice composée des 3-cycles car ceux-ci sont à la fois simples individuellement (ils ont beaucoup de points fixes) et collectivement (ils sont tous conjugués). Mais cette partie génératrice est de grande taille. Pour d'autres questions, notamment pour la question du stockage machine évoquée plus haut, il est beaucoup plus intéressant de disposer de petites familles génératrices. Or $\mathfrak{A}_n$ peut être engendré par les deux éléments

$$c = (1,2,3) \quad \text{et} \quad \sigma = \begin{cases} (3,4,...,n) \text{ si } n \text{ est impair,} \\ (1,2)(3,4,...,n) \text{ si } n \text{ est pair.} \end{cases}$$

La quantité suivante joue donc un rôle primordial.

**Définition.** On appelle *rang* de $G$ le cardinal minimal d'une partie génératrice, noté $\mathrm{rg}(G)$.

# 5 Quelques faits sur le rang

Faisons une liste de remarques et exemples, nous donnerons quelques justifications ensuite.

(1) **Rang comparé à la taille.** Si $G$ est un groupe fini, on a $\mathrm{rg}(G) \leqslant \log_2 |G|$ avec égalité si et seulement si $G \simeq (\mathbb{Z}/2\mathbb{Z})^r$ pour un certain $r$.

(2) **Rang des groupes finis simples.** Si $G$ est un groupe fini simple non abélien, on a $\mathrm{rg}(G) = 2$. (Difficile : cela résulte de la classification des groupes finis simples).

(3) **Rang des groupes abéliens de type fini.** Si $G$ est un groupe abélien de type fini, d'après le théorème de structure, il existe un isomorphisme $G \simeq \mathbb{Z}^s \times (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_t\mathbb{Z})$ avec des entiers $s, t \geqslant 0$ et $2 \leqslant d_1 \mid \cdots \mid d_t$ uniques (on convient que la liste des $d_i$ est vide si $t = 0$). On a alors $\mathrm{rg}(G) = s + t$. En particulier :

(3.a) si $G \simeq (\mathbb{Z}/n\mathbb{Z})^t$ on a $\mathrm{rg}(G) = t$,
(3.b) si $G \simeq \mathbb{Z}^s$ on a $\mathrm{rg}(G) = s$.

(4) **Rang des quotients.** Si $Q$ est un quotient de $G$, alors $\mathrm{rg}(Q) \leqslant \mathrm{rg}(G)$. Si $\Phi(G)$ désigne le sous-groupe de Frattini de $G$, pour tout sous-groupe $1 \subset N \subset \Phi(G)$ on a $\mathrm{rg}(G) = \mathrm{rg}(G/N)$. Si $G$ est un $p$-groupe, le groupe $G/\Phi(G)$ est un $\mathbb{F}_p$-espace vectoriel (aussi appelé *$p$-groupe élémentaire abélien*) et $\mathrm{rg}(G) = \mathrm{rg}(G/\Phi(G)) = \dim_{\mathbb{F}_p}(G/\Phi(G))$.

(5) **Rang des sous-groupes.** Si $H$ est un sous-groupe de $G$, on ne peut rien dire : on peut avoir $\mathrm{rg}(H) \gg \mathrm{rg}(G)$ ou $\mathrm{rg}(H) \ll \mathrm{rg}(G)$, car les groupes de rang arbitrairement grand contiennent des groupes cycliques (de rang 1) et sont inclus dans des groupes symétriques (de rang 2).

# 6 Quelques justifications

Nous donnons quelques indications de démonstration sur les faits (1) à (5) précédents, sans chercher à être exhaustif.

(1) Démonstration de l'inégalité. Soient $r = \mathrm{rg}(G)$ et $\{g_1, \dots, g_r\}$ une partie génératrice de cardinal minimal. Pour tout $k$ notons $G_k = \langle g_1, \dots, g_k \rangle$. Alors $g_{k+1} \notin G_k$ donc les parties $G_k$ et $g_{k+1}G_k$ sont disjointes dans $G_{k+1}$. Comme elles ont même cardinal, on déduit que $|G_{k+1}| \geqslant 2|G_k|$. On en déduit par récurrence que $|G| = |G_r| \geqslant 2^r$.

(2) Il n'y a pas grand'chose de plus à dire que cela découle de la classification des groupes finis simples ; voir par exemple cette question sur MathOverflow.

(3) Il s'agit de voir que le groupe $\mathbb{Z}^s \times (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_t\mathbb{Z})$ ne peut pas être engendré par moins de $s + t$ éléments. Nous laissons ceci en exercice.

(4) Le fait que $\mathrm{rg}(Q) \leqslant \mathrm{rg}(G)$ provient de ce que l'image dans $Q$ d'une partie génératrice de $G$ est génératrice. Ensuite rappelons que le sous-groupe de Frattini $\Phi(G)$ est l'intersection des sous-groupes maximaux de $G$. C'est aussi l'ensemble des éléments appelés *superflus*, qui sont les $x$ tels que pour toute partie $S \subset G$ telle que $\langle S, x \rangle = G$, on a $\langle S \rangle = G$ (certains auteurs disent *mous* ou *non-générateurs*). En effet :

- ⋆ si $x \in \Phi(G)$ et $\langle S, x \rangle = G$, alors aucun sous-groupe maximal $M$ ne peut contenir $S$ (car contenant aussi $x$, il contiendrait $G$, impossible), donc $\langle S \rangle = G$ (on utilise ici le fait que tout sous-groupe strict est inclus dans un sous-groupe maximal). Donc $x$ est superflu.
- ⋆ si $x$ est superflu et $M \subset G$ est un sous-groupe maximal, on a $\langle M \rangle \neq G$ donc $\langle M, x \rangle \neq G$ puisque $x$ est superflu, donc $x \in M$ puisque $M$ est maximal. Ainsi $x \in \Phi(G)$.

Cette propriété a pour conséquence que si $1 \subset N \subset \Phi(G)$ et $\pi : G \to G/N$ désigne le morphisme de quotient, alors une partie $S \subset G$ est génératrice si et seulement si l'image $\pi(S)$ est génératrice. Le fait que $\mathrm{rg}(G) = \mathrm{rg}(G/N)$ en découle. Les propriétés supplémentaires dans le cas des $p$-groupes se trouvent par exemple dans Calais [Ca84] (voir les 4 derniers exercices du chapitre VII) ou Zavidovique [Za13].

(1) Démontration du cas d'égalité. Notons $r = \mathrm{rg}(G)$ et $n = |G|$. Si $r = \log_2 n$, alors $n = 2^r$ donc $G$ est un 2-groupe. D'après (4) on en déduit que $r = \mathrm{rg}(G/\Phi(G)) = \dim_{\mathbb{F}_2}(G/\Phi(G))$. Alors le morphisme surjectif $G \to G/\Phi(G)$ a une source et un but de même cardinal $2^r$, donc c'est une bijection, c'est-à-dire $G \simeq G/\Phi(G) \simeq (\mathbb{Z}/2\mathbb{Z})^r$.

# Références


[Ca84] Josette Calais, *Éléments de théorie des groupes*, PUF, 1984.

[Za13] Maxime Zavidovique, *Un max de maths*, Calvage & Mounet, 2013.