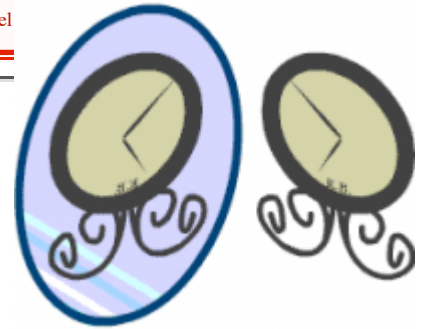


La Ticmatéma ou la Mathématique du Verlan

Une introduction aux commutateurs d'un groupe

Le 24 février 2010, par **Sylvain Barré**

Maître de conférence, Université de Bretagne-Sud ([page web](#))



Nous procédons tous au quotidien à des actions sur des espaces. L'ordre dans lequel nous appliquons ces actions est crucial. Se poser cette question : « Actions, commutez-vous ? » nous amène à la notion de groupe par une voie naturelle et à l'idée fondamentale de la conjugaison dans un groupe. Puis arrivent les fameux commutateurs....

Un exemple pour commencer

V OICI un tableau de 3 lignes et 3 colonnes.

1	2	3
4	5	6
7	8	9

Amusons-nous à permuter ses éléments en faisant glisser les lignes ou les colonnes.

Par exemple, notons L_2 l'opération qui consiste à faire glisser la deuxième ligne vers la droite et à ramener le dernier élément en première position. Le tableau suivant montre le résultat de cette opération.

1	2	3
6	4	5
7	8	9

Alors que le tableau ci-dessous correspond au glissement d'une unité vers le bas de la première colonne, notons C_1 cette opération.

7	2	3
1	5	6
4	8	9

Que se passe-t-il quand on combine ces opérations ? Voici une animation (élaborée par ma complice Katia) pour vous essayer.



Ci-dessous, on montre le résultat de l'action de L_2 suivie de celle de C_1 :

7	2	3
1	4	5
6	8	9

et l'action de C_1 suivie de celle de L_2 :

7	2	3
6	1	5
4	8	9

Vous constaterez que cela ne donne pas le même résultat. On dit que les **actions ne commutent pas** : $C_1 L_2 \neq L_2 C_1$. Ne nous arrêtons pas à ce constat. Notons C_1^{-1} l'*opération inverse* qui décale vers le haut d'une unité la colonne 1. Calculons alors le *commutateur* (on expliquera ce mot plus loin) de C_1 et L_2 , c'est-à-dire $[C_1, L_2] = C_1 L_2 C_1^{-1} L_2^{-1}$ ou encore l'action inverse de L_2 suivie de l'action inverse de C_1 suivie de l'action de L_2 puis de celle de C_1 dans cet ordre là. On trouve alors :

1	2	3
5	7	6
4	8	9

Il n'y a que trois chiffres qui sont permutés : (475). Exercez-vous à faire opérer des commutateurs, c'est toujours très utile comme nous allons le voir.

Qu'est-ce qu'un groupe ?

Pour commencer, considérons un ensemble de points, que nous noterons X . On appellera **permutation** de cet ensemble, une application $f : X \rightarrow X$ qui échange les points de cet ensemble (on parle dans un langage plus sophistiqué de « bijection »). Par exemple, si $X = \{x_1, x_2, x_3\}$ et $f(x_1) = x_2$, $f(x_2) = x_3$, $f(x_3) = x_1$ on dira que f permute **cycliquement** les éléments x_1, x_2, x_3 dans cet ordre. Dès qu'on a une permutation f , on a une

permutation inverse f^{-1} qui fait revenir à l'état initial : si $f(x) = y$ alors $f^{-1}(y) = x$. La permutation triviale, c'est-à-dire, celle qui ne bouge personne est appelée **identité** et notée Id . Quand on a deux permutations f et g d'un même ensemble, on peut appliquer d'abord f puis g , on aura alors défini une **permutation composée** qu'on notera $g \circ f$ (ou plus simplement gf dans ce sens-là car $gf(x) = g(f(x))$). On notera que composer avec l'identité est une opération neutre. On dit justement que l'identité est l'**élément neutre**. À l'instar d'Arthur Cayley, on donne la définition suivante :

Définition : *Un groupe, c'est l'ensemble de toutes les permutations d'un même ensemble X qu'on peut obtenir par composition à partir de certaines permutations préférées (et de leurs inverses) appelées générateurs.*

Par exemple, le groupe engendré par la seule application f précédente est composé de trois permutations : $f, f \circ f = f^2$ et $Id = f^3$. Dans ce cas il se trouve que l'inverse de f est f^2 .

Il y a d'autres définitions de la notion de groupe, équivalentes à celle-là. En général, on ne les présente que dans l'enseignement supérieur, car elles sont un peu abstraites. Celle qui est donnée ici est très concrète et pourrait bien être enseignée au lycée, voire même au collège. Sur ce même site, on pourra consulter un article sur ce sujet dans la rubrique « histoire des mathématiques » pour comprendre la découverte de cette notion fondamentale. **Histoire de Groupes**

Les translations entières

Considérons maintenant comme ensemble X , tous les points d'une droite. Notons t la translation d'une longueur l vers la droite : $t(x) = x + l$ si on pense la droite comme l'ensemble des nombres réels. La permutation inverse est la translation vers la gauche d'une même longueur. Plus généralement, la puissance n -ième de t opère sur la droite X comme cela : $t^n(x) = x + nl$.



Le groupe engendré par t

$$\dots, t^{-2}, t^{-1}, Id, t, t^2, \dots$$

peut se noter Z , avec le même symbole que celui utilisé pour l'ensemble des entiers relatifs, vous voyez pourquoi ?

Quel est donc ce groupe ?



On considère à présent deux triangles équilatéraux que l'on attache l'un à l'autre par un sommet. Notons x_1 le sommet commun, x_2, x_3 les deux autres sommets d'un triangle et enfin x_4, x_5 les deux derniers sommets. Notre ensemble X est composé de ces cinq éléments : $X = \{x_1, x_2, x_3, x_4, x_5\}$. Soit r la rotation de 120° qui fait tourner les trois sommets du premier triangle : r permute x_1, x_2, x_3 . Et soit r' la rotation qui fait tourner les trois sommets du second triangle : r' permute x_1, x_4, x_5 .

Combien d'éléments y-a-t-il dans le groupe engendré par r et r' ?

Commençons par calculer $r'r$. On voit que $r'r$ permute cycliquement x_1, x_2, x_3, x_4, x_5 dans cet ordre. Par contre, rr' permute cycliquement dans un autre ordre x_1, x_4, x_5, x_2, x_3 . Nous voyons donc que *ce groupe n'est pas commutatif*, en d'autres termes, l'ordre dans lequel on applique les éléments a de l'importance. En formule cela s'écrit :

$$rr' \neq r'r.$$

Le **cardinal** d'un groupe est son nombre d'éléments (on dit aussi son ordre, mais ce serait source de confusion ici). Essayez de montrer que le cardinal de ce groupe est **60**. Il suffit pour cela de voir qu'on peut réordonner les 5 sommets comme on veut, à la permutation de deux d'entre eux près, en utilisant les générateurs du groupe. Essayez-vous avec l'animation précédente.

Description du groupe diédral D_{10} .

Considérons un polygone régulier à cinq côtés. Il admet dix isométries :

- cinq *symétries orthogonales* par rapport aux droites joignant le centre aux divers sommets : A, B, C, D, E et

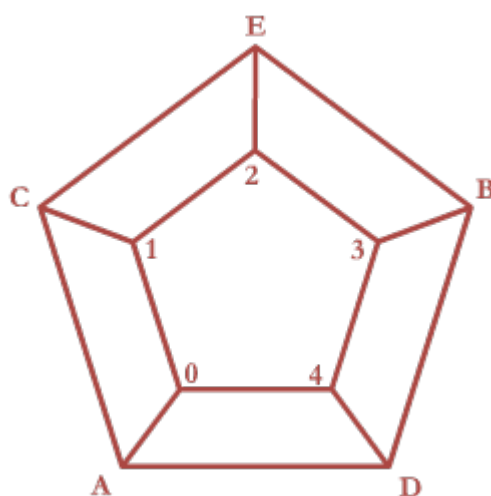
- cinq *rotations* : Id, r, r^2, r^3, r^4 , si r est la rotation d'un cinquième de tour.

Amusez-vous à comprendre comment se composent ces dix isométries.

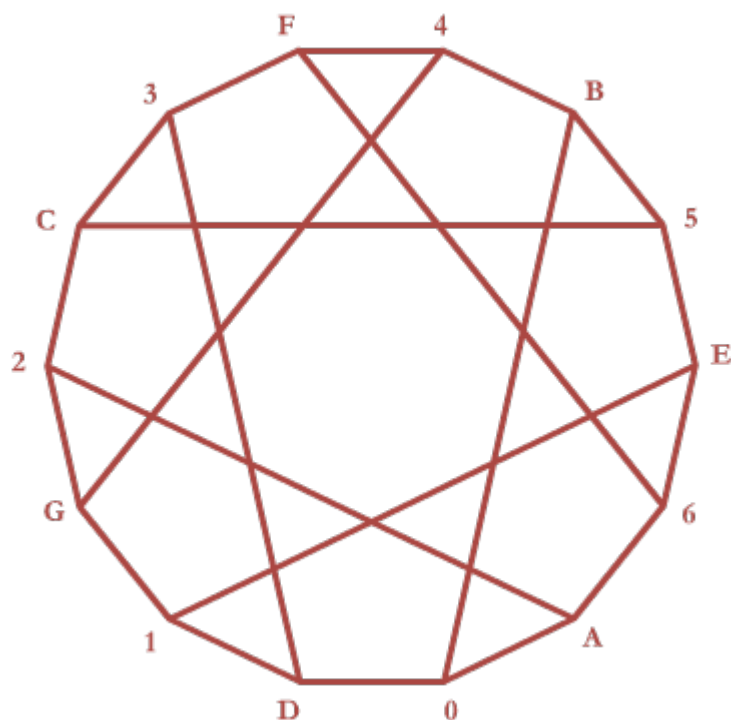


Dans cet exemple, on connaît à l'avance le cardinal du groupe (le **groupe diédral** D_{10}), mais sa structure n'est pas si simple que ça. En particulier, deux symétries commutent-elles ? Dans cette exemple, on peut aussi ne donner que deux générateurs : la rotation r et une symétrie s quelconque.

Essayez alors de “dessiner ce groupe” en représentant chacun de ses dix éléments par un point (sur une feuille de papier par exemple) et de relier deux de ces points par un trait si on saute de l'un à l'autre en utilisant un seul générateur ou son inverse. Cette représentation graphique du groupe s'appelle le **graphe de Cayley**. Sur la figure suivante, on a représenté le résultat, les puissances de la rotation sont notées avec des chiffres et les 5 symétries avec des lettres.



Amusez-vous aussi à comprendre le graphe de Cayley de D_{14} (l'analogue pour sept côtés) avec comme générateurs trois symétries A, B, D : ça vaut le coup ! (Ca fait des années que je dessine ce graphe au moins 3 fois par jours.)



Lorsque l'ordre des actions des éléments d'un groupe n'importe pas, on qualifie le groupe d'**abélien** (on dit encore **commutatif**). Par exemple le groupe Z vu plus haut est abélien. Vous pouvez aussi calculer son graphe de Cayley, tout comme celui de son analogue en dimension deux, engendré par une translation dans le plan vers la droite et une autre vers le haut (vous trouverez un quadrillage). Attention, dans un groupe il se peut que certains éléments commutent avec d'autres sans pour autant que le groupe soit commutatif.

Le groupe du « Rubik's carré »

J'ai choisi cette terminologie par analogie avec le Rubik's cube, qui lui, est bien connu et sera étudié juste après. Le carré est en dimension 2, ce que le cube est en dimension 3.

Considérons donc un carré de N lignes et N colonnes dont les petits carrés élémentaires sont numérotés x_1, \dots, x_{N^2} . L'ensemble X est composé de ces N^2 petits carrés.

Choisissons une ligne i et définissons la permutation élémentaire L_i qui décale les carrés de la ligne i d'un cran vers la droite et ramène le dernier en première position. De même on définit la permutation élémentaire de la j ème colonne C_j qui décale les cubes de la colonne j d'un cran vers le bas et ramène le dernier en haut de la colonne.

Retournez manipuler le carré du début. Mélangez donc les petits carrés (pour $N = 4$ par exemple, vous pouvez découper 16 petits carrés de papiers que vous ferez glisser) et essayez de les remettre à leur place en utilisant les générateurs du groupe que nous venons de définir. Utilisez donc les commutateurs introduits au tout début !

Le groupe du Rubik's cube

On considère le Rubik's cube usuel qui a neuf facettes de chaque couleur. On pourra commencer par consulter un des nombreux sites qui lui sont consacrés (si vous n'avez jamais manipulé ce cube) :



Découvrir le Rubik's Cube

Conservons pour ce cube, toujours la même orientation dans l'espace durant les mouvements : les facettes centrales ne font que pivoter sur elles-mêmes (nous ne les voyons pas tourner, on pourrait distinguer les quatre orientations de ces faces centrales, alors on définirait un groupe un peu plus gros : une *extension*). L'espace X est donc l'ensemble de toutes les photos du cubes.

Notons $F U R L$ les rotations élémentaires des faces respectives : de Face, du dessus (Up), de droite (Right), et de gauche (Left). Il y en aurait deux autres : dessous et derrière, mais le plus souvent on donne des formules qui ne les utilisent pas.

Comparez donc FU à UF .

La conjugaison

Se demander si deux éléments a et b d'un groupe commutent, c'est comparer ab à ba . Ou bien, ce qui revient au même, comparer aba^{-1} à b en composant par a^{-1} à droite. On appelle l'élément aba^{-1} le **conjugué** de b par a .

Reprenons l'exemple du groupe diédral d'ordre dix D_{10} . On peut calculer le conjugué d'une rotation par une symétrie, ou le contraire, ou encore le conjugué d'une symétrie par une autre symétrie. Par exemple, la conjuguée de la symétrie A par la rotation r est la symétrie B (dont l'axe est l'image de celui de A par la rotation r). Notez bien au passage que quand on conjugue par une symétrie s , il n'est pas utile de mettre la puissance -1 car $s = s^{-1}$ puisque $s^2 = Id$.

Essayons de comprendre ce que signifie l'opération de conjugaison. Imaginez comme espace X , une pièce de forme carrée avec en son centre un miroir (disposé parallèlement à un côté). Dans cette pièce, il y a deux tables, une de chaque côté de ce miroir, qui se correspondent exactement via la symétrie miroir. En d'autres termes, en regardant dans le miroir, on voit une image virtuelle d'une table qui se superpose parfaitement à l'autre table. Les deux actions sont les suivantes : a est la symétrie miroir (qui échange donc les deux tables) et b est la rotation de la table de droite d'un quart de tour dans le sens des aiguilles d'une montre. Calculons donc le conjugué de b par a : c'est la rotation de la table de gauche d'un quart de tour dans le sens inverse des aiguilles d'une montre.

De façon générale, conjuguer b par a c'est considérer b au travers le miroir défini par a .

Sur l'exemple du groupe du Rubik's carré, on peut calculer, à l'aide de l'animation « carrés à manipuler », des conjugués d'un générateur par un autre : ça donne des cycles tordus toujours de longueur trois. Voici par exemple l'action du conjugué de L_2 par C_2 :

1	2	3
6	5	8
7	4	9

Pour approfondir un peu, vous pouvez vous demander si dans un groupe diédral comme D_{10} ou D_{14} déjà rencontrés ou encore plus simplement D_4 , deux symétries sont toujours conjuguées.

Un commutateur

On a vu que les éléments a et b commutent si et seulement si le conjugué de b par a est égal à b ou ce qui revient au même, si $aba^{-1}b^{-1} = Id$.

Il est judicieux de dénommer cet élément le **commutateur** de a et b . On le note :

$$[a, b] = aba^{-1}b^{-1}.$$

Ce commutateur est le composé de a et du conjugué de a^{-1} par b .

Calculons des commutateurs dans le groupe du « Rubik's carré » de taille N . Commençons par le commutateur de L_i et C_j . Vous constaterez que ce commutateur permute cycliquement trois cases seulement quelle que soit la taille N du grand carré. Ces commutateurs vous permettent d'obtenir presque toutes les permutations du grand carré (et même toutes dans le cas où N est un nombre pair). Vous pouvez vous exercer avec l'animation « carrés à manipuler », ou avec vos carrés de papier.

Prenons pour ensemble X un cercle de centre O et pour générateurs du groupe toutes les symétries orthogonales par rapport aux diamètres et toutes les rotations de centre O de tous les angles. Ça fait beaucoup de générateurs pour ce groupe : on a mis tous les éléments du groupe ! On pourrait en prendre moins : par exemple parmi les rotations d'ordre fini (c'est-à-dire quand il existe n tel que $r^n = Id$), ne garder que celles d'ordre premier (la composée d'une rotation d'ordre 2 et d'une autre d'ordre 3 et une rotation d'ordre 6). On vérifie que le conjugué d'une symétrie par une rotation d'un certain angle a est une symétrie par rapport à une droite tournée d'un même angle. Et la composée de deux symétries est une rotation (d'un angle double de celui déterminé par les deux droites de symétrie). On vient donc de démontrer que :

Dans le groupe des isométries du cercle, toute rotation est un commutateur.

En effet une rotation R est le produit d'une symétrie s quelconque, par la conjuguée rsr^{-1} où r est la rotation d'angle moitié de celui de R :

$$R = [s, r]$$

On peut vérifier aussi que tout commutateur est une rotation (c'est le produit d'une isométrie par la conjuguée de son inverse, donc, soit le produit de deux symétries, soit le produit de deux rotations). Notez au passage que dans ce groupe il y a un élément qui commute avec tous les autres : c'est la symétrie centrale (ou rotation d'angle π). Un élément qui a cette propriété est qualifié de **central** en général. Dans le groupe du rubik's cube, il y a un élément différent du neutre qui est central, cherchez-le ! [Réponse : la seule opération qui soit invariante par conjugaison par tous les générateurs est celle qui retourne chacune des 12 arêtes] .

Pour aller plus loin...

Dans un groupe, un élément n'est pas toujours un commutateur, ni même un produit de commutateurs. On dit qu'un groupe est PARFAIT si tout élément est un produit de commutateurs.

Si un élément est un produit de commutateurs, on peut aussi chercher à connaître le **nombre minimal de commutateurs** nécessaires pour le composer.

Pour résoudre le Rubik's Cube, on développe de nombreuses formules. La plupart sont des produits de commutateurs des générateurs. Seulement la plupart car le groupe du cube n'est pas parfait (mais presque : un élément sur deux est un produit de commutateurs).

Une formule simple très pratique : $FURU^{-1}R^{-1}F^{-1}$ est le conjugué par F du commutateur $[U, R]$. Vous pouvez vérifier que c'est aussi le commutateur des conjugués : $[FUF^{-1}, FRF^{-1}]$.

Sans se restreindre à des commutateurs, on peut chercher à résoudre le Rubik's cube avec un nombre minimal de générateurs. Ce problème est encore ouvert ! (on sait depuis peu, que moins de 26 opérations élémentaires suffisent toujours).

On cherche souvent à majorer le nombre minimal de commutateurs sur un groupe donné, ou sur une famille de groupes... Par exemple, le carré d'un commutateur est-il un commutateur ? La réponse est non en général. Par contre, le cube d'un commutateur est le produit de seulement deux commutateurs, et ce quel que soit le groupe, comme le montre la magnifique formule de M. Culler suivante [extraite de l'article de Christophe Bavard « Longueur stable des commutateurs » paru dans la revue l'Enseignement Mathématique (2) 37 (1991)] :

$$[a, b]^3 = [aba^{-1}, b^{-1}aba^{-2}][b^{-1}ab, b^2].$$

Vérifiez-la ! Et demandez-vous comment il a été possible de penser à une telle formule...

Pour finir, voici un exemple concret où l'on cherche à minimiser le nombre de commutateurs. L'espace X est l'ensemble de tous les vecteurs du plan, avec un point d'attache. On peut penser à un vecteur comme à une voiture sur un grand parking (ou plutôt seulement une roue avant, disons un monocycle !). Décrivons deux générateurs. Le premier, t , avance les voitures d'un mètre en avant, en suivant la flèche. Le second, r , tourne les voitures d'un dixième de tour dans

le sens des aiguilles d'une montre (en pivotant suivant le point base). Vous calculerez facilement le commutateur de ces deux éléments : c'est une translation du vecteur, mais cette fois dans une direction transverse. Pour **se garer en créneau**, on a souvent besoin d'utiliser un tel commutateur, parfois il en faut plusieurs...on cherche à en faire le moins possible !

Il y a de nombreux articles en ce moment sur le sujet. Ce nombre garde encore beaucoup de secrets. Une des grandes questions est de savoir si, pour un groupe donné infini, il existe un majorant pour cette longueur de commutateurs.

Un grand merci aux relecteurs et en particulier à **Étienne Ghys** pour ses nombreuses suggestions.

► **Crédits images**

Pour citer cet article : **Sylvain Barré**, **La Ticmatéma ou la Mathématique du Verlan**. *Images des Mathématiques*, CNRS, 2010. En ligne, URL : <http://images.math.cnrs.fr/La-Ticmatema-ou-la-Mathematique-du.html>