VULGARISATION DE MA THÈSE

COLIN JAHEL, AVEC L'AIDE DE CHARLES VALENTIN

Ce document s'adresse à ma famille et à mes ami·e·s non-mathématicien·ne·s. J'essaye de résumer ce à quoi je m'intéresse en utilisant un langage qui soit (autant que possible) compréhensible par tous·tes. J'ai fait le choix de laisser des erreurs et des imprécisions pour rendre la lecture plus fluide, j'espère que mes camarades mathématicien·ne·s me pardonneront les crispations que leur donnera sans aucun doute la lecture de ce document.

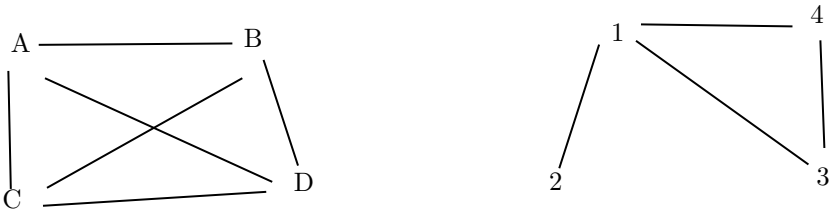
1. Les graphes

Un graphe est un ensemble de sommets et des relations entre ces sommets, qu'on appelle des arêtes. Il s'agit de points dont certains sont reliés entre eux. Des exemples d'objets de la vie courante qu'on représente parfois par des graphes sont généralement les liens d'amitié sur les réseaux sociaux, ou les réseaux de transport. Il y a des individus (les sommets) et des liens (les arêtes). Ci-dessous, deux exemples de graphes.

Les deux graphes précédents sont, stricto sensu, différents. Cependant, si on change le nom des sommets, on peut passer de l'un à l'autre : en effet, si on change A en 1, B en 2 et C en 3, on obtient le même graphe. Dans ce cas, on dit que les deux graphes sont isomorphes : ils ont la même forme.

Par exemple, les graphes suivants ne sont pas isomorphes. En effet, le premier a quatre sommets, alors que l'autre en a trois.

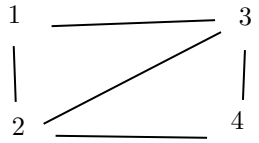
Les deux exemples suivants ne sont pas non plus isomorphes, car dans le premier, toutes les paires de points sont reliés entre elles, mais pas dans le second.



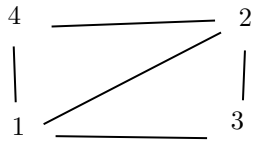
Supposons maintenant que nous avons un graphe donné. On s'interesse à des transformations, ou réarrangements, des sommets de notre graphe. Un réarrangement des sommets de notre graphe qui préserve les arêtes (et l'absence d'arêtes !) s'appelle un **automorphisme**. Un automorphisme est essentiellement une transformation

des sommets qui préserve la structure de graphe. Pour se clarifier les idées, regardons quelques exemples.

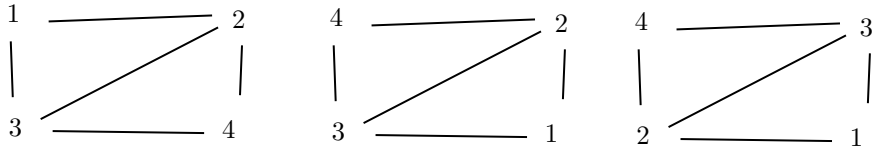
Regardons tout d'abord comment une transformation des sommets agit sur un graphe. Prenons le graphes suivant dont les sommets sont $1, 2, 3$ et 4.



La transformation qui change $(1, 2, 3, 4)$ en $(4, 1, 2, 3)$ donne donc le graphe suivant:



Les deux graphes ne se ressemblent pas, cette transformation n'est donc pas un automorphisme. Les automorphismes de ce graphes sont en fait la transformation qui envoie $(1, 2, 3, 4)$ sur $(1, 3, 2, 4)$ ou $(4, 3, 2, 1)$ ou $(4, 2, 3, 1)$.



On peut remarquer qu'appliquer la transformation $(1, 2, 3, 4) \mapsto (4, 3, 2, 1)$ revient exactement à appliquer $(1, 2, 3, 4) \mapsto (1, 3, 2, 4)$ puis $(1, 2, 3, 4) \mapsto (4, 2, 3, 1)$. Ce pouvoir de composer deux automorphismes fait de l'ensemble des automorphismes ce qu'on appelle un groupe, et c'est l'objet de la section suivante.

2. Groupe d'automorphismes du graphe aléatoire

Je vais maintenant pouvoir décrire l'objet archétypique sur lequel je travaille : le graphe aléatoire, ou graphe de Rado. On considère une infinité (dénombrable[1]) de sommets et on met une arête entre deux sommets avec probabilité $1/2$, et on réitère cette opération pour toute paire de sommets.

A priori, on peut obtenir n'importe quel graphe par cette méthode : si je n'ai pas de chance par exemple, je mettrai une arête entre chaque paire de point. Il se trouve que cette situation ne peut pas arriver, ou en tout cas c'est tellement rare qu'on ne considère pas ce cas là. On dit qu'il a une probabilité 0 d'arriver.

Il se passe en réalité quelque chose d'intéressant : on peut montrer que le graphe ainsi obtenu est toujours le même. Pas dans le sens où j'ai toujours les mêmes arêtes au même endroit, mais dans le sens où il existe toujours un automorphisme entre deux réalisations de mon graphe. Tous les graphes ainsi obtenus se ressemblent. On peut donc parler de R, le graphe ainsi obtenu.

Ce graphe est homogène, c'est à dire que si deux parties finies A et B de R définissent les mêmes graphes, alors il existe un automorphisme de R (une transformation des sommets de R) qui envoie A sur B.

Comme nous l'avons remarqué précédemment, on peut appliquer un automorphisme puis un autre autormorphisme, et obtenir encore un automorphisme : on peut composer les automorphismes. Plus formellement, si on a f et g des automorphismes de R, on peut définir $f \circ g$ comme l'automorphisme qui a x associe le somment que f associe à $g(x)$.

[1]Voir la section Les différents types d'infinis

Cette propriété de composition fait de l'ensemble des automorphismes de R un **groupe**. Un groupe est un ensemble qui possède une opération (ici la composition) qui à deux éléments de notre ensemble associe un autre élément de notre ensemble. Les groupes (et plus spécifiquement les groupes d'automorphismes) sont centraux dans mon travail.

Un groupe G agit sur un espace X si à tout élément g de G et tout élément de X on peut associer un élément de X noté $g \cdot x$. On demande aussi que si on a deux éléments g et h de notre groupe, $(g \circ h) \cdot x = g \cdot h \cdot x$. L'étude des actions de groupes constitue ce qu'on appelle **la dynamique** et c'est mon domaine de recherche.

3. Mesures et Probabilités

La notion de mesure est fondamentale dans la théorie moderne des probabilités.

Une mesure assigne un nombre positif à chaque partie d'un espace. Il y a une correspondance avec la notion intuitive de mesure : mesurer une longueur, c'est assigner un nombre à un segment.

Une mesure doit vérifier quelques propriétés pour être considérée comme telle : on doit assigner 0 à l'ensemble vide, et la réunion d'ensembles disjoints doit avoir une mesure égale à la somme des mesures des ensembles. Comme pour les graphes, il y a des analogies avec des mesures de la vie réelle, mais on s'intéresse ici aux mesures en tant qu'objets abstraits.

Une mesure sur un ensemble X est une **mesure de probabilités** si elle associe à l'ensemble tout entier la valeur 1. En particulier, la mesure de n'importe quelle autre partie de X aura un nombre associé plus petit que 1. La mesure qui est associée à une partie de X est alors appelée la probabilité de cette partie.

Prenons l'exemple d'un dé à 6 faces. L'ensemble sur lequel on travaille est $\{1, 2, 3, 4, 5, 6\}$. Si notre dé est équilibré, la probabilité qui le représente est la mesure qui à toute partie associe son cardinal divisé par 6. En revanche si le dé est pipé et tombe sur 6 à chaque fois, la probabilité qui décrit ce dé est celle qui associe à une partie le nombre 1 si elle contient 6 et 0 sinon.

On peut maintenant combiner la notion de mesure et celle d'action de groupe. Prenons un espace X et un groupe G qui agit sur X. Une mesure est dite **invariante** si pour toute partie A de X le nombre que notre mesure associe à A est le même nombre que ce qu'elle associe à $g \cdot A$, où $g \cdot A$ correspond à l'ensemble des $g \cdot a$ pour tout a dans A.

Pour un premier exemple, reprenons notre dé à 6 faces. L'ensemble sur lequel on travaillait, $\{1, 2, 3, 4, 5, 6\}$, possède un groupe de bijection qu'on appelle S_6. Exercice : montrer que ce groupe à 720 éléments. Ce groupe agit naturellement sur $\{1, 2, 3, 4, 5, 6\}$. La mesure qui correspond au dé équilibré est invariante sous l'action de S_6, en effet, la taille d'une partie ne change pas lorsqu'on lui applique une bijection de S_6. En revanche, pour le dé pipé, la mesure n'est pas invariante puisque contenir 6 n'est pas une propriété stable sous l'action de S_6 : une partie qui contient 6 peut être envoyée sur une partie qui ne contient pas 6.

Un autre exemple : l'ensemble des nombres réels $\mathbb{R}$ (vu comme des vecteurs) agit sur $\mathbb{R}$ (vu comme des points sur une droite) par translation, c'est à dire qu'un nombre réel x transforme un autre nombre réel y en $x + y$. On peut mesurer la longueur d'un segment de droite, et cette longueur ne change pas si on translate ce segment. Cette propriété se généralise à toute partie[2] de la droite : on ne change pas sa mesure quand on la translate. Ainsi, cette mesure est invariante par l'action du groupe $\mathbb{R}$ sur lui-même.

Un dernier exemple, plus important dans mes travaux, donc aussi plus compliqué. Le groupe d'automorphismes de R agit naturellement sur l'espace des ordres sur les

[2]du moins quasi-toute ...

sommets du graphe. Cette action a une mesure invariante qui peut être décrite de la manière suivante : soit $x_1, ..., x_n$ des sommets de R, la probabilité que $x_1 < \ldots < x_n$ est $1/n!$, le nombre de permutations d'un ensemble de taille n.

4. Du coup, de quoi parle ma thèse

Dans ma thèse, je m'intéresse à certaines actions de certains groupes. La question que je me suis posée repose sur l'observation suivante. Prenons un groupe ressemblant au groupe d'automorphismes du graphe aléatoire. Pour n'importe quelle action du groupe, si il y a une mesure invariante pour l'action, alors il n'y en a qu'une seule. Cela peut paraître anodin, mais le caractère unique de certains objets titille souvent l'attention des mathématicien·ne·s.

Mon travail a consisté à étayer cette observation. Déjà en étudiant des exemples intéressants de groupes, puis en trouvant des propriétés générales sur la classe de groupes qui m'intéressent... Pour essayer d'en savoir plus, vous pouvez maintenant écouter ma soutenance.

Les différents types d'infinis

Nous allons dans ce paragraphe expliquer comment on peut mathématiquement distinguer différents types d'infini. Pour cela, revenons aux bases : qu'est-ce que compter ? Oubliez temporairement tout ce que vous savez, vos tables de multiplication, vos algorithmes préférés de division, et retrouvez votre âme d'enfant : pour compter, on utilise ses doigts, les uns après les autres. Avoir cinq bonbons, c'est être capable de relier chacun des bonbons à un doigt de sa main.

On voit apparaître la notion de **bijection** : une bijection entre deux ensembles X et Y, c'est une manière d'associer les éléments de X et ceux de Y de manière biunivoque : à chaque élément de X correspond un et un seul élément de Y, et inversement. Dans le cas des automorphismes d'un graphe, on souhaitait des bijections qui conservaient également les arêtes du graphe. Ici, ce n'est pas le cas, on considère des ensembles sans structures supplémentaires, ce sont simplement des collections d'objets.

Ce qui permet de compter les éléments d'un ensemble fini, c'est la capacité à établir une bijection entre cet ensemble et un autre ensemble qu'on connaît mieux. En fait, la notion de **nombres entiers** est simplement une manière efficace de résumer ce qu'on sait sur la taille d'un ensemble, mais la notion première est celle de bijection. Avoir cinq éléments, cela veut exactement dire être en bijection avec n'importe quel autre ensemble à cinq éléments.

La définition précédente a un sens également pour des ensembles infinis : on dit que deux ensembles ont le même **nombre cardinal**[3] (ou simplement cardinal) s'il on peut établir une bijection entre les deux. Par exemple, l'ensemble des entiers naturels $\mathbb{N} = \{0, 1, 2, \ldots\}$ est en bijection avec l'ensemble des suites finis de lettres de l'alphabet. En effet, on peut numéroter toutes les suites de lettres de la manière suivante : on commence par les suites d'une seule lettre rangé dans l'ordre alphabétique ("a" a le numéro 0, "b" le numéro 1, etc...), puis celle de deux lettres, ("aa" a le numéro 26, "ab" le numéro 27, etc...) et ainsi de suite. On a ainsi établi une bijection.

Quand un ensemble est en bijection avec l'ensemble des entiers naturels, on dit qu'il est **dénombrable**.

[3]En linguistique, un adjectif numéral cardinal désigne un nombre : "un", "deux", etc... qu'on distingue de la notion d'adjectif numéral ordinal : "premier", "deuxième", etc... Cette deuxième notion a également une généralisation aux ensembles infinis, qu'on appelle nombres ordinaux. Nous n'en parlerons pas ici, mais il y a des choses à dire ...

Un résultat contre-intuitif au premier abord (mais on s'y habitue), c'est qu'un ensemble infini peut être en bijection avec une de ses parties. Par exemple, $\mathbb{N}^* = \{1, 2, \ldots\}$ est une partie de $\mathbb{N}$ mais pourtant les deux ensembles sont en bijection, par exemple via la bijection qui a un entier non-nul n associe l'entier $n-1$. Cette situation est impossible avec des ensembles finis (si j'ai cinq bonbons et que j'en perds un, je n'en ai plus cinq !).

On montre également que $\mathbb{Z}$ (l'ensemble des entiers relatifs, c'est-à-dire des entiers positifs ou négatifs) est également dénombrable. Par exemple, l'application suivante est une bijection entre $\mathbb{N}$ et $\mathbb{Z}$: $0 \mapsto 0, 1 \mapsto 1, 2 \mapsto -1, 3 \mapsto 2, 4 \mapsto -2$, etc ... (on numérote les entiers relatifs en commençant par 0, puis en prenant un nombre positif, puis un négatif, etc...)

Exercice : montrer que l'ensemble des nombres rationnels $\mathbb{Q}$ (c'est-à-dire les nombres de la forme $\frac{p}{q}$ où p et q sont des entiers, et q non nul) est également dénombrable !

On peut avoir l'impression que $\mathbb{Q}$ est bien plus gros que $\mathbb{N}$, mais le résultat précédent montre que non. On peut alors se demander si, par des astuces similaires, on pourrait établir une bijection entre n'importe quel ensemble infini et $\mathbb{N}$.

Il n'en est rien, c'est un célèbre théorème du mathématicien Georg Cantor, prouvé en 1874, qui nous dit que $\mathbb{R}$, l'ensemble des nombres réels (c'est-à-dire l'ensemble des nombres qu'on peut positionner sur une droite, par exemples $\sqrt{2}$ ou π et beaucoup d'autres encore) ne peut pas être mis en bijection avec $\mathbb{N}$. On dit qu'il est **non-dénombrable**.

On peut même montrer qu'il y a un ensemble plus gros que $\mathbb{R}$, et un autre encore plus gros, et ainsi de suite. Il y a en fait une infinité d'infinis, l'étude et la classification de ces infinis est l'un des points de départ de ce qu'on appelle la **théorie des ensembles**.

Une autre question que l'on peut se poser est la suivante : existe-t-il un infini entre la taille de $\mathbb{N}$ et la taille de $\mathbb{R}$, c'est-à-dire, existe-t-il un ensemble X qui contienne tous les entiers, et ne contenant que des nombres réels, mais qui ne soit en bijection ni avec $\mathbb{N}$, ni avec $\mathbb{R}$? Cette question s'appelle **l'hypothèse du continu**, et la réponse est un peu surprenante : (accrochez-vous) les règles usuelles du raisonnement mathématique ne permettent ni de prouver l'existence d'un tel ensemble, ni de prouver qu'il n'en existe pas ! On dit que ce problème est **indécidable** (dans l'axiomatique usuelle).