Also sprach Marc Schaul

Mathe für alle und keinen

Table des matières

Un peu de théorie des ensembles

1 Une théorie sur des bases frêles

1.1 Manipuler des ensenbles

Qu'est-ce qu'un ensemble ? Tout, et rien à la fois. C'est un objet formel sur lequel on se donne uniquement une chose : la relation d'appartenance, $\in$. Comment alors en pratique construire et utiliser des ensembles ? On peut penser qu'un ensemble est simplement défini par la donnée d'une propriété, éventuellement en langage naturel : $x \in A \iff$ Quelque chose est vrai de x. On verra plus tard que cette approche connaît de graves problèmes qui motiveront une axiomatisation plus rigoureuse de la théorie des ensembles. Mais pour l'instant, elle suffit à explorer quelques notions de base et à introduire du vocabulaire.

Définition 1

Soient A et B deux ensembles. On appelle union de A et B l'ensemble $A \cup B = \{x | x \in A \vee x \in B\}$, et intersection de A et B l'ensemble $A \cap B = \{x | x \in A \wedge x \in B\}$.

Définition 2

Soient A et B deux ensembles. On dit que A est inclus dans B, ce qu'on note $A \subset B$, quand $\forall x \in A, x \in B$.

Définition 3

Soit $A \subset B$. On appelle complémentaire de A dans B l'ensemble $B \backslash A = \{x \in B | \neg x \in A\}$

Un poil plus compliqué : définir le produit cartésien $A \times B$, c'est à dire l'ensemble des couples (x, y) avec $x \in A$ et $y \in B$. Pour ce faire, il faut trouver une façon purement ensembliste de définir un couple ordonné (sachant qu'un ensemble n'est justement pas ordonné). Une des solutions possibles :

Définition 4 (Couples de Kuratowski)

On note couple (x, y) l'ensemble $\{x, \{x, y\}\}$.

Cette définition permet de préserver l'ordre de la paire : $(x, y) \neq (y, x)$. On peut maintenant définir de façon purement ensembliste une relation binaire

Définition 5 (Relation binaire)

Soit E un ensemble. On appelle relation binaire $\mathcal{R}$ sur (E, F) (ou si $E = F$, tout simplement sur E) un sous ensemble de $E \times F$. On dit que le couple (x, y) de $E \times E$ vérifie la relation $\mathcal{R}$, ce qu'on note $x\mathcal{R}y$ quand (x, y) appartient à cet ensemble $\mathcal{R}$.

Intuitivement, une fonction de E dans F est un objet qui à tout x de E associe un unique y de F. On formalise ceci à l'aide d'une relation binaire.

Définition 6

Soit ϕ une relation binaire sur (E, F). f est une application quand $\forall (x, y, z) x\phi y \wedge x\phi z \implies y = z$. On notera à l'avenir $\phi(x) = y$.

Toutes les relations binaires ne sont pas des applications. Une application doit associer à tout élément une image unique.
On définit encore diverses propriétés sur ces relations.

Définition 7 (Premières définitions)

Soit $\mathcal{R}$ une relation binaire de E. On dit que :
- $\mathcal{R}$ est réflexive si $\forall x \in E$, $x\mathcal{R}x$.
- $\mathcal{R}$ est symétrique si $\forall (x, y) \in E^2$, $x\mathcal{R}y \implies y\mathcal{R}x$.
- $\mathcal{R}$ est antisymétrique si $\forall (x, y) \in E^2$, ($x\mathcal{R}y$ et $y\mathcal{R}x$) $\implies x = y$
- $\mathcal{R}$ est transitive si $\forall (x, y, z) \in E^3$, ($x\mathcal{R}y$ et $y\mathcal{R}z$) $\implies x\mathcal{R}z$.

Définition 8 (Relation d'équivalence)

On dit qu'une relation binaire $\mathcal{R}$ sur E est une relation d'équivalence si elle est réflexive, symétrique et transitive. On la note en général $\sim$.

Définition 9 (Relation d'ordre)

On dit qu'une relation binaire $\mathcal{R}$ sur E est une relation d'ordre si elle est réflexive, antisymétrique et transitive. On note en général $\leq$ plutôt que $\mathcal{R}$.

Entiers, principe de récurrence et suites

Encore de la logique et de la théorie des ensembles

Structures algébriques

Groupes, anneaux, corps, corps de fractions

Polynômes

Construction et propriétés de $\mathbb{K}[X]$, de $\mathbb{K}[X,Y]$

Arithmétique

Arithmétique dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$

Limites et continuité

Un peu de topologie ridiculement générale

Construction de $\mathbb{R}$ et de $\mathbb{C}$

Suites de Cauchy, coupures de Dedekind, théorèmes fondamentaux pour l'analyse

1 Motivation et suites de Cauchy

1.1 Pourquoi $\mathbb{R}$?

Qu'est ce que l'ensemble des réels ? Intuitivement, c'est l'ensemble des nombres rationnels dont on a "rempli les trous". Mais que sont donc ces trous ? Par exemple, une solution de $x^2 = 2$:

Une preuve de l'irrationnalité de $\sqrt{2}$

On suppose qu'il existe deux entiers p, q premiers entre eux tels que $\left(\frac{p}{q}\right)^2 = 2$.
Alors $p^2 = 2q^2$, donc p^2 est pair. Mais tout entier ayant la même parité que son carré, p est également pair. Avec $p = 2k$, il vient $4k^2 = 2q^2$, d'où $2k^2 = q^2$, et rebelote : q est pair.
On avait supposé la fraction irréductible, et pourtant $\text{PGCD}(p, q) \geq 2$.... C'est impossible, donc $\sqrt{2}$ est irrationnel.

Comment faire sens alors d'une telle solution ?
Peut être d'une façon approchée : par exemple, en construisant une suite de rationnels dont le carré converge vers 2.

Exercice 1 (Méthode de Héron pour l'approximation de $\sqrt{2}$)

On définit par récurrence la suite rationnelle suivante :

$$\begin{cases} u_0 = 2 \\ u_{n+1} = \frac{1}{2}(u_n + \frac{2}{u_n}) \end{cases}$$

1. Montrer que $u_n^2 > 2$.
2. Montrer (sans utiliser le théorème de la limite monotone, puisqu'il n'est pas valable pour des suites rationelles) que la suite définie par $v_0 = 2$ et $v_{n+1} = (\frac{v_n}{2})^2$ tend vers 0.
3. Montrer que $u_n^2 \to 2$, en procédant par majoration de $u_n^2 - 2$ par v_n.

Les termes de cette suite sont successivement, en valeur approchée, [...]. Ils semblent être de plus en plus proches les uns des autres. On peut formaliser cette notion.

Définition 1

On dit qu'une suite (u_n) est de Cauchy quand :

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, (m \geq N \text{ et } n \geq N) \implies |u_n - u_m| < \varepsilon$$

Intuitivement, cela veut dire que les termes sont de plus en plus proches deux à deux.
On notera $\mathcal{C}_{\mathbb{Q}}$ l'ensemble des suites de Cauchy rationnelles.

Propriété 1

Toute suite convergente est de Cauchy.

On rappelle que $u_n \to l$ quand :

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, n \geq N \implies |u_n - l| < \varepsilon$$

Soit $u_n \to l$ et $\varepsilon > 0$.

$$\exists N \in \mathbb{N}, n \geq N \implies l - \varepsilon/2 < u_n < l + \varepsilon/2$$

Alors si $n \geq N$et $m \geq N$:

$$l - \varepsilon/2 < u_n < l + \varepsilon/2$$

$$l - \varepsilon/2 < u_m < l + \varepsilon/2$$

D'où :

$$-\varepsilon < u_n - u_m < \varepsilon$$

Autrement dit, $|u_n - u_m| < \varepsilon$ et donc (u_n) est de Cauchy.

On va immédiatemment montrer que la réciproque est fausse dans $\mathbb{Q}$.

Exercice 2

La suite (u_n) est celle définie précédemment.

1. En se souvenant que $u_n^2 > 2$, montrer que (u_n) décroit.
2. En se souvenant que $u_n^2 \to 2$, déduire que $\forall p, \lim_{n \to +\infty} |u_{n+p} - u_n| = 0$.
3. En conclure que (u_n) est de Cauchy.

Vue depuis le monde rationnel, cette suite n'est pourtant pas convergente, puisque $\sqrt{2}$ est irrationelle. Ceci nous fournit un contre-exemple à la réciproque de la propriété 1. Pourtant, les termes semblent bien se rapprocher "de quelque chose" : ce quelque chose, c'est le nombre réel $\sqrt{2}$, qu'il reste encore à définir.

1.2 Quelques propriétés des suites de Cauchy

Avant d'attaquer la construction, on montre ici quelques propriétés qu'il sera utile d'avoir en tête :

Propriété 2

Toute suite de Cauchy est bornée.

Soit $\varepsilon > 0$. Il existe un rang N tel que si $n, m \geq N$ alors $|u_n - u_m| < \epsilon$. En particulier, $|u_N - u_n| < \varepsilon$, c'est à dire $u_n \in [u_N - \varepsilon, u_N + \varepsilon]$. Mais alors $\forall n \in \mathbb{N}, u_n \leq \max(\{u_k | k < N\} \cup \{u_N + \varepsilon\})$, et de même $u_n \geq \min(\{u_k | k < N\} \cup \{u_N - \varepsilon\})$. Finalement, (u_n) est majorée et minorée, donc bornée.

Propriété 3

Toute suite de Cauchy ne convergeant pas vers 0 est non nulle à partir d'un certain rang.

Supposons l'inverse : pour tout $N \in \mathbb{N}$ aussi grand soit-il, il existe un $n \geq N$ tel que $u_n = 0$. Soit $\varepsilon > 0$. Il existe $N \in \mathbb{N}$ tel que si $m > N$ et $p > N$, $|u_m - u_p| < \varepsilon$. Soit $n > N$ avec $u_n = 0$: alors $\forall m \geq N$, $|u_m - u_n| < \varepsilon$ soit $|u_m| < \varepsilon$. D'où $u_n \to 0$.

Théorème 1 (Analogue au théorème de la limite monotone)

Toute suite rationnelle monotone bornée est de Cauchy.

On fait une démonstration par dichotomie dans le cas croissante et majorée.
Soit $(u_n) \in \mathbb{Q}^{\mathbb{N}}$ croissante et majorée par un rationnel M. Pour tout n, $u_0 \leq u_n \leq M$. On pose $a_0 = u_0$ et $b_0 = M$.
On va construire par récurrence deux suites :

- Si $[a_n, \frac{a_n+b_n}{2}]$ contient une infinité de termes de la suite, alors $[\frac{a_n+b_n}{2}, b_n]$ n'en contient aucun. On pose $a_{n+1} = a_n$ et $b_{n+1} = \frac{a_n+b_n}{2}$.
- Sinon, $[\frac{a_n+b_n}{2}, b_n]$ contient tous les termes de la suite à partir d'un certain rang. On pose $a_{n+1} = \frac{a_n+b_n}{2}$ et $b_{n+1} = b_n$.

On a $|a_n - b_n| = \frac{1}{2^n}$.
De plus, par construction, pour tout n il existe un rang N_n à partir duquel tous les termes de la suite sont dans $[a_n, b_n]$. Pour tout $m, p > N_n$ on a donc $|u_m - u_p| < \frac{1}{2^n}$.
Soit maintenant $\varepsilon > 0$. Soit n le plus petit entier tel que $2^n > \frac{1}{\varepsilon}$. Il existe un rang N à partir duquel $|u_m - u_p| < \frac{1}{2^n}$. Mais par définition, $\frac{1}{2^n} < \varepsilon$. D'où finalement, (u_n) est de Cauchy.

Exercice 3

Reprendre la démonstration ci dessus dans le cas décroissante et minorée, et ainsi achever la démonstration du théorème 1.

2 Une construction de $\mathbb{R}$ par les suites de Cauchy

2.1 Les réels

On rappelle les notions suivantes :

Définition 2

Une relation d'équivalence sur E est une relation binaire $\sim$ sur E :

- réfléxive $(\forall x \in E, x \sim x)$;
- transitive $((x \sim y \wedge y \sim z) \implies x \sim z)$;
- symétrique $(x \sim y \iff y \sim x)$

On appelle classe d'équivalence de x l'ensemble noté $[x] = \{y \in E | y \sim x\}$.
Remarquons que si $x \sim y$, $[x] = [y]$.

Propriété 4

L'ensemble des classes d'équivalence est une partition de E. On l'appelle ensemble quotient de E par $\sim$, noté $E/\sim$.

L'idée est de définir une relation d'équivalence R sur les suites rationnelles :

$$(a_n)R(b_n) \iff a_n - b_n \to 0$$

On vérifie bien que c'est une relation d'équivalence :
- $a_n - a_n = 0 \to 0$,
- si $a_n - b_n \to 0$, alors $b_n - a_n = -(a_n - b_n) \to -0 = 0$,
- si $a_n - b_n \to 0$ et $b_n - c_n \to 0$, alors $a_n - b_n + b_n - c_n = a_n - c_n \to 0$.

On peut donc partitionner $\mathcal{C}_{\mathbb{Q}}$: cette partition est $\mathbb{R}$. Chaque classe d'équivalence est alors un réel, représenté par toutes les suites rationnelles qui l'approximent.
En identifiant tout rationnel q à la classe d'équivalence de la suite stationnaire dont tous les termes sont égaux à q, $\mathbb{Q} \subset \mathbb{R}$.

2.2 Leur structure algébrique

On peut ensuite définir les opérations usuelles sur $\mathbb{R}$:

Définition 3

1. $[(a_n)] + [(b_n)] = [(a_n + b_n)]$
2. $[(a_n)] \times [(b_n)] = [(a_n b_n)]$

Il faut ici vérifier que quelque soit la suite rationelle qu'on a choisi pour représenter un réel, l'addition et la multiplication donnera le même résultat. Autrement dit :
1. Si $(a_n)R(a'_n)$, $[(a_n + b_n)] = [(a'_n + b_n)]$.
2. Si $(a_n)R(a'_n)$, $[(a_n b_n)] = [(a'_n b_n)]$.

En effet comme attendu :
1. $a_n - a'_n = (a_n + b_n) - (a'_n + b_n)$, donc si $a_n - a'_n \to 0$, $(a_n + b_n)R(a'_n + b_n)$ soit $[(a_n + b_n)] = [(a'_n + b_n)]$.
2. Si $a_n - a'_n \to 0$, comme (b_n) est de Cauchy donc bornée, $b_n(a_n - a'_n) \to 0$. D'où $(a_n b_n)R(a'_n b_n)$ soit $[(a_n b_n)] = [(a'_n b_n)]$.

On définit de plus une relation d'ordre sur $\mathbb{R}$:

Définition 4

Soit $x = [(a_n)] \in \mathbb{R}$. x est positif si $x \neq 0$ et si il existe un rang N tel que $\forall n \geq N, a_n > 0$.

Il faut encore vérifier que cette définition a un sens, c'est à dire que si $a_n - b_n \to 0$ et (a_n) ne tend pas vers 0, si (a_n) finit par n'avoir que des termes positifs, alors (b_n) aussi.
Supposons que $\forall N, \exists n \geq N, b_n \leq 0$. $a_n - b_n \to 0$ c'est à dire $\forall \varepsilon > 0, \exists N, n \geq N \implies |a_n - b_n| < \varepsilon$.
Soit $\varepsilon > 0$. $\exists N, n \geq N \implies |a_n - b_n| < \frac{\varepsilon}{2}$. De plus, comme (a_n) est de Cauchy, $\exists N', n, p \geq N' \implies |a_n - a_p| < \frac{\varepsilon}{2}$.
Enfin, $\exists m \geq \max(N, N'), b_m \leq 0$. Mais alors comme $b_m - \frac{\varepsilon}{2} < a_m < b_m + \frac{\varepsilon}{2}$, $\forall n \geq \max(N, N'), |a_n - a_m| < \frac{\varepsilon}{2}$, $b_m - \varepsilon < a_n < b_m + \varepsilon$ d'où $0 < a_n \leq \varepsilon$. D'où $a_n \to 0$.

On achève maintenant la définition de la relation d'ordre :

Définition 5

Soit $(x, y) \in \mathbb{R}^2$. On dit que $x \geq y$ si $x - y$ est positif ou si $x = y$.

C'est bien une relation d'ordre :
- $x = x$ donc $x \geq x$,
- antisymétrie
- transitivité

On peut maintenant montrer que $\mathbb{R}$ est un corps ordonné.

3 Une autre construction de $\mathbb{R}$

3.1 Les réels, version 2

3.2 Leur structure algébrique

4 Les propriétés fondamentales de $\mathbb{R}$

On suppose au début de cette partie qu'on a bien le droit de parler de $\mathbb{R}$ comme d'un "unique objet", qu'il est été construit à partir des coupures de Dedekind ou des suites de Cauchy. À la fin de cette partie, on montrera qu'elles sont effectivement isomorphes, c'est à dire que d'un point de vue structurel, elles sont parfaitement identiques. On prouvera même mieux : toutes les structures possédant certaines propriétés "$\mathbb{R}$-esques" sont isomorphes. C'est cette unicité à isomorphisme près qui permet à vos camarades

un peu moins braves de se passer totalement de la construction de $\mathbb{R}$ et de l'introduire sur le mode axiomatique.

4.1 La complétude, à partir des suites de Cauchy

On rappelle que la borne supérieure d'une partie d'un ensemble est le plus petit de ses majorants.

Propriété 5 (Caractérisation séquentielle de la borne supérieure)

Une première conséquence importante :

Théorème 2 (Théorème de la limite monotone)

Toute suite bornée et monotone converge.

On considère $\ell = \sup\{u_n | n \in \mathbb{N}\}$. Soit $\forall \varepsilon > 0$. $\exists n_0 \in \mathbb{N}, \ell - \varepsilon < u_{n_0} \leq \ell$ puisque sinon $\ell - \varepsilon$ serait un majorant de $\{u_n | n \in \mathbb{N}\}$, ce qui est impossible. Mais comme (u_n) est croissante, $\forall n \geq n_0, \ell - \varepsilon < u_n < \ell$. Autrement dit, $u_n \to \ell$.

Une deuxième conséquence importante :

Définition 6 (Suites adjacentes)

Deux suites réelles (u_n) et (v_n) sont dites adjacentes si
- L'une est croissante et l'autre décroissante.
- $u_n - v_n$ tend vers 0.

Théorème 3 (Théorème des suites adjacentes)

Deux suites adjacentes convergent vers la même limite.

Soient (a_n) et (b_n) deux suites adjacentes, avec (a_n) croissante et (b_n) décroissante.
Commençons par montrer que $\forall n \in \mathbb{N}, a_n \leq b_n$. Soit $n \in \mathbb{N}$. Supposons l'inverse. Alors $\forall p > n, b_p \leq b_n < a_n \leq a_p$ et donc $\forall p > n, |b_p - a_p| > |a_n - b_n|$. Mais comme $|b_p - a_p| \to 0$, ceci est absurde.
On sait maintenant que $\forall n \in \mathbb{N}, a_0 \leq a_n \leq b_n \leq b_0$. On peut donc appliquer le théorème de la limite monotone : (a_n) est croissante et majorée par b_0 et (b_n) est décroissante et minorée par a_0. Les deux suites convergent donc vers ℓ_1 et ℓ_2. Enfin comme $a_n - b_n \to 0$ $\ell_1 - \ell_2 = 0$ donc les deux suites convergent vers la même limite.

On peut enfin montrer que dans $\mathbb{R}$, toute suite de Cauchy converge. On a ainsi bien défini tous les "quelque chose" qu'on évoquait en fin de paragraphe 1.1.

Théorème 4 (Critère de Cauchy ou Cauchy-complétude)

Toute suite réelle de Cauchy converge.

Soit (u_n) une suite de Cauchy et $\varepsilon > 0$:

$$\exists N \in \mathbb{N}, p \geq N \implies |u_N - u_p| < \varepsilon$$

L'idée de cette preuve est d'encadrer les termes de la suite entre deux suites adjacentes.
Pour tout $n \in \mathbb{N}$, on pose $a_n = \inf\{u_k | k \geq N\}$ et $b_n = \sup\{u_k | k \geq n\}$.
Comme $\{u_k | k \geq n+1\} \subset \{u_k | k \geq n\}$, on a bien $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$.
De plus, soit $\varepsilon \geq 0$ Comme (u_n) est de Cauchy, il existe N tel quel $\forall n \geq N, |u_N - u_n| < \frac{\epsilon}{2}$. On a $\{u_k | k \geq N\} \subset]u_N - \frac{\varepsilon}{2}, u_N + \frac{\varepsilon}{2}[$ soit $b_N - a_N < \varepsilon$. Mais par croissance/décroissance, $\forall n \geq N, b_n - a_n \leq b_N - a_N < \varepsilon$, d'où $b_n - a_n \to 0$.

Cette propriété de $\mathbb{R}$ est importante et se généralise aux espaces métriques.

Définition 7 (Suite de Cauchy)

Soit (E, d) un espace métrique et $(u_n) \in E^{\mathbb{N}}$. (u_n) est de Cauchy quand

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall p, q > N, d(u_p, u_q) < \varepsilon$$

Avec la distance usuelle sur les nombres rationnels $d(a, b) = |a - b|$ on retrouve bien la précédente définition.

4.2 La propriété de la borne supérieure, à partir des coupures de Dedekind

4.3 Ces deux constructions sont équivalentes

Théorème 5 (Existence et unicité de $\mathbb{R}$)

Il existe un corps totalement ordonné vérifiant la propriété de la borne supérieure, unique à isomorphisme près.

4.4 $\mathbb{R}$ n'est pas dénombrable

Cette dernière partie concerne le cardinal de $\mathbb{R}$. Dans le chapitre 2, on a établi une théorie général des cardinaux transfinis. On a évoqué l'hypothèse du continu, c'est à dire le problème initialement posé par Cantor sur les cardinaux entre $\aleph_0$, cardinal de $\mathbb{N}$ et $2^{\aleph_0}$, cardinal de $\mathcal{P}(\mathbb{N})$.
On justifie ici l'appelation "hypothèse du continu" en montrant que $2^{\aleph_0}$ est le cardinal de $\mathbb{R}$.

Théorème 6

$\mathbb{R}$ est équipotent à $\mathcal{P}(N)$.

Théorème 7 ($\mathbb{R}$ n'est pas dénombrable)

La propriété précédente nous permet directement de conclure grâce au théorème de Cantor qu'il n'existe aucune bijection entre $\mathbb{N}$ et $\mathbb{R}$.

Dérivation

Dérivée, série de Taylor, fonction exponentielle

Intégration

Convergence et analyse asymptotique

Convergence de suites et de séries numériques, développements limités et asymptotiques, un peu d'arithmétique

Théorème 1 (Théorème de réarrangement de Riemann)

Groupe symétrique et déterminant

Polynômes caractéristiques, théorème de Cayley-Hamilton

1 Le groupe symétrique

Définition 1 (Groupe symétrique (ou groupe des permutations))

Pour tout entier naturel $n \geq 1$, on note l'ensemble fini $\mathbb{N}_n = \{1, \dots, n\} = [\![1, n]\!]$. On note alors $\mathfrak{S}_n$ ou $\mathcal{S}_n$ le groupe symétrique (ou groupe des permutations) d'indice n qui correspond au groupe de toutes le permutations de $\mathbb{N}_n$, c'est à dire toutes les bijections de $\mathbb{N}_n$ sur lui-même.

Une bijection σ de $\mathfrak{S}_n$, c'est à dire une permutation, est une application de $\mathbb{N}_n$ dans $\mathbb{N}_n$ représente par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

Avec $\mathbb{N}_n = \{\sigma(k) \mid k \in \mathbb{N}_n\}$.

Exemple 1

Dans $\mathfrak{S}_3$ une permutation possible serait :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Et alors $\sigma(1) = 3$; $\sigma(2) = 1$ et $\sigma(3) = 2$
Les éléments de l'ensemble de départ étant toujours dans l'ordre on se permet parfois d'écrire uniquement $\sigma = \begin{pmatrix} 3 & 1 & 2 \end{pmatrix}$ ce qui signifie la même permutation.

Propriété 1 (Structure de groupe)

L'ensemble $\mathfrak{S}_n$ muni de la composition $\circ$ forme un groupe.

- Loi interne de composition : Soit σ et σ' deux permutations de $\mathfrak{S}_n$, alors $\sigma' \circ \sigma$ et une bijection de $\mathbb{N}_n$ dans $\mathbb{N}_n$ par composé et $\sigma' \circ \sigma \in \mathfrak{S}_n$.
- Élément neutre : Il est facile de voir que la fonction identité est un élément neutre, en effet $\forall k \in \mathbb{N}_n, \mathrm{Id}(k) = k$ et $\sigma \circ \mathrm{Id}(k) = \sigma(k)$ alors $\sigma \circ \mathrm{Id} = \sigma$ Réciproquement $\forall k \in \mathbb{N}_n, \mathrm{Id}(\sigma(k)) = \sigma(k)$ et $\mathrm{Id} \circ \sigma = \sigma$.
- Existence d'un inverse : Simplement pour toute permutation σ on associe σ^{-1} la permutation suivante : $\forall k \in \mathbb{N}_n \ \sigma^{-1}(\sigma(k)) = k$ c'est alors une bijection entièrement définie et $\sigma^{-1} \circ \sigma = \mathrm{Id}$. C'est alors la bijection réciproque de σ et $\sigma \circ \sigma^{-1} = \mathrm{Id}$

Propriété 2 (Cardinal de $\mathfrak{S}_n$)

L'ordre ou le cardinal de $\mathfrak{S}_n$, noté $|\mathfrak{S}_n|$ ou $\mathrm{Card}(\mathfrak{S}_n)$ vaut $n!$

En effet une permutation σ de $\mathfrak{S}_n$ est entièrement déterminée par le n-uplet $(\sigma(1), \dots, \sigma(n))$, on comprend facilement en commençant par 1, on a n possibilités différentes pour $\sigma(1)$, puis alors $n-1$ pour $\sigma(2)$ car il ne peut plus prendre la valeur prise par $\sigma(1)$, puis $n-2$ possibilités pour $\sigma(3)$ et ainsi de suite. On a donc bien $n!$ permutation distinctes dans $\mathfrak{S}_n$.

Exemple 2 ($\mathfrak{S}_1$,$\mathfrak{S}_2$, et $\mathfrak{S}_3$)

— Pour $\mathfrak{S}_1$, comme $\mathbb{N}_1 = \{1\}$, la seul permutation possible est $\sigma(1) = 1$, $\sigma = \mathrm{Id}$ et $\mathfrak{S}_1 = \{\mathrm{Id}\}$

— Pour $\mathfrak{S}_2$ on a $2! = 2$ permutation, trivialement $\sigma = \begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix} = \mathrm{Id}$ et $\sigma' = \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$

— Pour $\mathfrak{S}_3$ on a $3! = 6$ permutations.
$\mathrm{Id} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$, $\sigma = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$, $\sigma' = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$, $\tau_1 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$, $\tau_2 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$, $\tau_3 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$

On peut alors se demander si le groupe est commutatif avec par exemple un table de groupe ;

Exemple 3 (Table de groupe (ou table de Pythagore ou table de Cayley))

On va le faire avec $\mathfrak{S}_3$, pour le remplir on calcul les différents produits, on peut aussi utiliser le fait que tout les éléments doivent apparaitre exactement une fois dans chaque ligne ou colonne (comme un sudoku).
Pour les produits de permutation on applique l'une après l'autre.
$\tau_3 \circ \sigma' = (3 \quad 2 \quad 1)(2 \quad 3 \quad 1) = \begin{pmatrix}2 & 3 & 1\\ 3 & 2 & 1\end{pmatrix} = (1 \quad 3 \quad 2) = \tau_2$, (il faut s'entrainer)
Il faut faire suffisamment de calcul pour remplir le reste par sudoku, on obtient la table :

$\circ$	Id	τ_1	τ_2	τ_3	σ	σ'
Id	Id	τ_1	τ_2	τ_3	σ	σ'
τ_1	τ_1	Id	σ	σ'	τ_2	τ_3
τ_2	τ_2	σ'	Id	σ	τ_3	τ_1
τ_3	τ_3	σ	σ'	Id	τ_1	τ_2
σ	σ	τ_3	τ_1	τ_2	σ'	Id
σ'	σ'	τ_2	τ_3	τ_1	Id	σ

Ce qui se lit l'élément de la ligne fois celui de la colonne. On voit que la table n'est pas symétrique par rapport à la diagonale donc le groupe n'est commutatif.

Définition 2 (Orbite par permutation)

On appelle orbite de $p \in \mathbb{N}_n$ d'une permuation $\sigma \in \mathfrak{S}_n$ l'ensemble $\{\sigma^k(p) \mid k \in \mathbb{N}\}$

2 Cycles et transpositions

Définition 3 (Cycle)

Dans $\mathfrak{S}_n$ avec $n \geq 2$, pour $p \geq 2$, $p \in \mathbb{N}_n$ on dit que $\sigma \in \mathfrak{S}_n$ est un cycle de longueur p s'il existe p éléments $a_1, a_2, \ldots, a_p$ distincts de $\mathbb{N}_n$ tel que : $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, … , $\sigma(a_{p-1}) = a_p$ et $\sigma(a_p) = a_1$ Et que pour tout élément b de $\mathbb{N}_n \backslash \{a_1, \ldots, a_p\}$, $\sigma(b) = b$, on dit que b est invariant σ. L'ensemble $\{a_1, a_2, \ldots, a_p\}$ est appelé support du cycle σ, généralement on écrit ce cycle $(a_1, a_2, \ldots, a_p)$.
Dans $\mathfrak{S}_n$, on appelle permutation circulaire un cycle de longueur n ; càd de support $\mathbb{N}_n$.
Dans $\mathfrak{S}_1$, la seule permutation est l'identité, on peut la considéré comme un cycle à un seul élément.

Exemple 4

$\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 5 & 6 & 3 & 1 & 2 & 4 & 7\end{pmatrix}$ est le cycle $(1 \quad 5 \quad 2 \quad 6 \quad 4)$

Définition 4

On dit que deux cycles $\sigma = (a_1, a_2, \ldots, a_p)$ et $\sigma' = (b_1, b_2, \ldots, b_q) \in \mathfrak{S}_n$ ont des supports disjoints si $\{a_1, a_2, \ldots, a_p\} \cap \{b_1, b_2, \ldots, b_q\} = 0$

Propriété 3 (Sur les cycles)

— l'inverse du cycle $(a_1 \quad a_2 \quad \ldots \quad a_p)$ vaut $(a_p \quad a_{p-1} \quad \ldots \quad a_1)$
— Soit σ un cycle de longueur p alors $\sigma^p = \mathrm{Id}$, on a fait un tour du cycle. On en déduit que pour un entier relatif $m = pq + r$, $\sigma^m = \sigma^r$.
— Deux cycle à support disjoint commutent

Définition 5 (Transposition)

Dans $\mathfrak{S}_n$ avec $n \geq 2$, on dit que la permutation $\sigma \in \mathfrak{S}_n$ est une transposition si c'est un cycle de longueur 2, c'est à dire qu'il existe $i, j \in \mathbb{N}_n$ distinct tel que $\sigma(i) = j$ et $\sigma(j) = i$ et que $\forall k \in \mathbb{N}_n \backslash \{i, j\}$, $\sigma(k) = k$.
On note souvent cette transposition $\begin{pmatrix} i & j \end{pmatrix}$ ou $\begin{pmatrix} j & i \end{pmatrix}$ ou encore $\tau_{i,j}$.

Propriété 4 (Sur les transposition)

Comme on peut le voir avec la notation $\tau_{i,j} = \tau_{j,i}$, on a aussi facilement $\tau_{i,j}^2 = \mathrm{Id}$ et donc $\tau_{i,j} = \tau_{i,j}^{-1}$

Théorème 1 (Décomposition de permutations)

Toute permutation de $\mathfrak{S}_n$(avec $n \geq 1$) se décompose en un produit de cycles à supports deux à deux disjoints. Cette décomposition est unique à l'ordre des facteurs près.

Existence par récurrence : $\mathcal{H}_n$:Toute permutation de $\mathfrak{S}_n$(avec $n \geq 1$) se décompose en un produit de cycles à supports deux à deux disjoints.
Pour $n = 1$, la seule permutation est l'identité, c'est le cycle à 1 éléments
Soit n tel que $\forall k \in \mathbb{N}_n$, $\mathcal{H}_k$.Soit $\sigma \in \mathfrak{S}_{n+1}$, on pose $A = \{\sigma^k(1) \mid k \in \mathbb{N}\}$ le support de 1 par σ et $B = \mathbb{N}_{n+1} \backslash A$ A est un sous-ensemble de $\mathbb{N}_{n+1}$, il est donc de cardinal fini. Donc il existe une infinité d'entier $k \in \mathbb{N}$ tel que $\exists k' \in [\![1, k-1]\!], \sigma^{k'}(1) = \sigma^k(1)$. Comme tout sous-ensemble de $\mathbb{N}$ admet un plus petit élément, on peu posé p le plus petit entier vérifiant $\exists p' \in [\![1, p-1]\!], \sigma^{p'}(1) = \sigma^p(1)$. On montre alors que $\sigma^p(1) = 1$, en effet si $p \geq 1, \sigma \circ \sigma^{p'-1}(1) = \sigma \circ \sigma^{p-1}(1)$ et par injectivité $\sigma^{p'-1}(1) = \sigma^{p-1}(1)$ ce qui contredit le caractère minimal de p. On se retrouve finalement avec $A = \{\sigma^k(1) \mid k \in \mathbb{N}_{p-1}\}$, on pose $c = (1, \sigma(1), \sigma^2(1), \ldots, \sigma^{p-1}(1))$, et donc $\forall x \in A, c(x) = \sigma(x)$. Alors si $A = \mathbb{N}_{n+1}$, c'est à dire $\mathrm{Card}(A) = n + 1$, c est un cycle donc on a $\mathcal{H}_{n+1}$ Sinon on a $1 \leq \mathrm{Card}(B\mathbb{N}_{n+1} \backslash A) \leq n$ car 1 est forcement dans A, et B invariant par c. On considérant σ' la restriction de σ à B, $\sigma' \in \mathfrak{S}_n$ et par hypothèse de récurrences σ' se décompose en produit de cycle à support disjoint.

Théorème 2 (Développement d'un déterminant)

Blabla

Pour une matrice $A \in \mathcal{M}_n(\mathbb{K})$, $n \geq 2$ de terme général a_{ij} de déterminant $\Delta = \det A$, on donne les définitions suivantes :

Définition 6 (Mineur d'un matrice A)

On appelle mineur (i, j) de A ou mineur de a_{ij} dans A le déterminant souvent noté Δ_{ij} ou $(\det A)_{ij}$ qui correspond au déterminant de A ou l'on à supprimé la ligne i et la colonne j.

Définition 7 (Cofacteur d'une matrice A)

On appelle cofacteur (i, j) de A ou cofacteur de a_{ij} dans A, souvent noté γ_{ij} le scalaire $\gamma_{ij} = (-1)^{i+j}\Delta_{ij}$ avec Δ_{ij} la mineur (i, j) de A.

Définition 8 (Comatrice d'une matrice A)

La comatrice de A, noté $\mathrm{Com}(A)$ est la matrice des cofacteurs de A, c'est a dire la matrice de terme générale γ_{ij}.

Propriété 5 (Caractérisation suivant les lignes ou les colonnes d'un cofacteur)

(Rarement utilisé en pratique mais utile pour certaine démonstration),Soit $e = \{e_1, \dots, e_n\}$ une base canonique de $\mathbb{K}^n$, en désignant par $(C_1, C_2, \dots, C_n)$ le système des vecteurs colonnes de A et par $(L_1, L_2, \dots, L_n)$ le système des vecteurs lignes de A on a $\forall i, j \in \mathbb{N}_n$ le cofacteur :

$$\gamma_{ij} = \det_e(C_1, \dots, C_{j-1}, e_i, C_{j+1}, \dots, C_n) = \det_e(L_1, \dots, L_{j-1}, e_j, L_{j+1}, \dots, L_n)$$

On part de $D_C = \det_e(C_1, \dots, C_{j-1}, e_i, C_{j+1}, \dots, C_n)$ pour montrer l'égalité.

$$D_C = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1(j-1)} & 0 & a_{1(j+1)} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2(j-1)} & 0 & a_{2(j+1)} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{(i-1)1} & a_{(i-1)2} & \cdots & a_{(i-1)(j-1)} & 0 & a_{(i-1)(j+1)} & \cdots & a_{(i-1)n} \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ a_{(i+1)1} & a_{(i+1)2} & \cdots & a_{(i+1)(j-1)} & 0 & a_{(i+1)(j+1)} & \cdots & a_{(i+1)n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{n(j-1)} & 0 & a_{n(j+1)} & \cdots & a_{nn} \end{vmatrix}$$

On effectue un premier cycle sur les colonnes $\begin{pmatrix} C_n & C_{n-1} & \cdots & C_{j+1} & C_j \end{pmatrix}$ de longueur $n - j + 1$ donc de signature $(-1)^{n-j}$.
Puis un deuxième sur les lignes $\begin{pmatrix} L_n & L_{n-1} & \cdots & L_{i+1} & L_i \end{pmatrix}$ de longueur $n-i+1$ donc de signature $(-1)^{n-i}$, la signature totale vaut $(-1)^{n-j+n-i} = (-1)^{-(j+i)} = (-1)^{j+i}$ On se retrouve alors avec e_i en position (n, n) et des zéros sur le reste de C_n et L_n alors

$$D_C = (-1)^{i+j} \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1(j-1)} & a_{1(j+1)} & \cdots & a_{1n} & 0 \\ a_{21} & a_{22} & \cdots & a_{2(j-1)} & a_{2(j+1)} & \cdots & a_{2n} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{(i-1)1} & a_{(i-1)2} & \cdots & a_{(i-1)(j-1)} & a_{(i-1)(j+1)} & \cdots & a_{(i-1)n} & 0 \\ a_{(i+1)1} & a_{(i+1)2} & \cdots & a_{(i+1)(j-1)} & a_{(i+1)(j+1)} & \cdots & a_{(i+1)n} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{n(j-1)} & a_{n(j+1)} & \cdots & a_{nn} & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 \end{vmatrix} = (-1)^{i+j} D'_C$$

Avec D'_C le nouveau déterminant on calcul $D'_C = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{p=1}^{n} a_{\sigma(p),p}$

Or vu la n-ième ligne ou colonne $a_{\sigma(n),n} = 0$ si $\sigma(n) \neq n$ et $a_{\sigma(n),n} = 1$ si $\sigma(n) = n$.

Propriété 5 (Suite)

Or il existe un bijection de $\{\sigma \in \mathfrak{S}_n \text{ tel que } \sigma(n) = n\}$ dans $\mathfrak{S}_{n-1}$:

$$\varphi : \{\sigma \in \mathfrak{S}_n \mid \sigma(n) = n\} \to \mathfrak{S}_{n-1}$$

$$\sigma \mapsto \begin{pmatrix} \mathbb{N}_{n-1} \to \mathbb{N}_{n-1} \\ i \mapsto \sigma(i) \end{pmatrix}$$

Alors pour tout $\sigma \in \mathfrak{S}_n$ tel que $\sigma(n) = n$ il existe la permutation $\varphi(\sigma) \in \mathfrak{S}_{n-1}$ de décomposition en produit de cycles à support disjoint identique à σ, alors $\varepsilon(\sigma) = \varepsilon(\varphi(\sigma))$. De plus pour tout $\sigma \in \mathfrak{S}_{n-1}$ on peut associé la permutation $\varphi^{-1}(\sigma) \in \mathfrak{S}_n$ en posant pour $k \in \mathbb{N}_{n-1}$, $\varphi^{-1}(\sigma(k)) = \sigma(k)$ et $\varphi^{-1}(\sigma(n)) = n$, et $\varepsilon(\sigma) = \varepsilon(\varphi^-1(\sigma))$.

$$D'_C = \sum_{\sigma \in \mathfrak{S}_{n-1}} \varepsilon(\sigma) \prod_{p=1}^{n-1} a_{\sigma(p),p}$$

Théorème 3 (Développement suivant une ligne ou une colonne)

Toujours pour une matrice $A \in \mathcal{M}_n(\mathbb{K})$, $n \geq 2$ de terme général a_{ij} de déterminant $\Delta = \det A$, en utilisant les notations des définitions précédentes :
Pour tout $i \in \mathbb{N}_n$, on dit que l'on développe le déterminant suivant la i-ème ligne avec $\det A = \sum_{j=1}^{n} (-1)^{i+j} \Delta_{ij} a_{ij} = \sum_{j=1}^{n} \gamma_{ij} a_{ij}$.
Et pour tout $j \in \mathbb{N}_n$, on dit que l'on développe le déterminant suivant la j-ème colonne avec $\det A = \sum_{i=1}^{n} (-1)^{i+j} \Delta_{ij} a_{ij} = \sum_{j=1}^{n} \gamma_{ij} a_{ij}$.

Suivant une ligne i ; soit $e = \{e_1, \dots, e_n\}$ une base canonique de $\mathbb{K}^n$.

$\det A = \det_e(L_1, \dots, L_{i-1}, L_i, L_{i+1}, \dots, L_n)$ avec $L_i = \sum_{j=1}^{n} a_{ij} e_j$ donc

$\det A = \det_e(L_1, \dots, L_{i-1}, \sum_{j=1}^{n} a_{ij} e_j, L_{i+1}, \dots, L_n)$ et par n-linéarité $\det A = \sum_{j=1}^{n} a_{ij} \det_e(L_1, \dots, L_{i-1}, e_j, L_{i+1}, \dots, L_n) = \sum_{j=1}^{n} a_{ij} \gamma_{ij}$.

Références

[1] Marc Schaul. « La Bible ».

[2] Thomas Arocena et Constance Sarrazin. Les auteurs de ces lignes. Ce qui est signalé par cette référence doit être accueilli avec la plus grande méfiance, puisque c'est un travail original de gens pas très futés.

[3] Patrick Dehornoy. *Théorie des ensembles*. Calvage & Mounet, 2017.