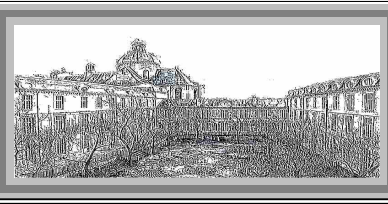
LYCEE CHARLEMAGNE
Lundi 18 décembre
M.P.S.I.2



2023 2024

TD13

◦0◦ $(G,*)$ est un groupe. On enlève un élément, ça reste un groupe. Qui est G ?
$(G,*)$ est un groupe. On enlève deux élément, ça reste un groupe. Qui est G ? (deux solutions)
On pourra utiliser le théorème de Lagrange : le cardinal d'un sous-groupe divise le cardinal du groupe.

On note n le cardinal de G.
On enlève un élément (pas le neutre), et on a encore un groupe, donc un sous-groupe.
Et le cardinal d'un sous-groupe divise le cardinal du groupe. $n-1$ divise n.
n vaut 2.
Par exemple $(\{Id, \overrightarrow{(1\,2)}\}, \circ)$. Et c'est $\overrightarrow{(1\,2)}$ qu'on enlève, et il reste le groupe le plus simple.
Ou alors $\{0,1\}$ pour l'addition modulo 2.

Pour le second, $n-2$ divise n.
n vaut 3 ou 4.
$\{0,\ 1,\ 2\}$ pour l'addition modulo 3 et on enlève 1 et 2.
Ou alors $\{1,\ j,\ j^2\}$ pour la multiplication, et on enlève j et j^2.

$\{0,\ 1,\ 2,\ 3\}$ pour l'addition modulo 4 et on enlève 1 et 3.
Ou alors $\{1,\ -1,\ i,\ -i\}$ pour la multiplication, et on enlève $-i$ et i.

◦1◦ Dans $\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}^{2014}$ quel est le plus grand terme, et que vaut il ? Même question avec $\begin{pmatrix} 5 & 4 \\ -2 & -1 \end{pmatrix}^{2014}$
(évidemment, les deux questions sont liées).

$\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}^{2014} = \begin{pmatrix} 1 & 0 \\ 0 & 3^{2014} \end{pmatrix}$ et le plus grand terme est 3^{2014}. Et de beaucoup !

Sinon, $\begin{pmatrix} 5 & 4 \\ -2 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$ (on trouve le spectre par la méthode habituelle).

On a donc $\begin{pmatrix} 5 & 4 \\ -2 & -1 \end{pmatrix}^{2014} = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 3^{2014} \end{pmatrix} \cdot \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2.3^{2014}-1 & 2.3^{2014}-2 \\ 1-3^{2014} & 2-3^{2014} \end{pmatrix}$

Le plus grand est $\boxed{2.3^{2014}-1}$

◦2◦ Un couple de suites récurrentes vérifie : $u_0 = 1$, v_0 donné et pour tout n $\left\{ \begin{array}{rcll} u_{n+1} & = & u_n & +2.v_n \\ v_{n+1} & = & 6.u_n & +2.v_n \end{array} \right|$. Existe-t-il des valeurs de v_0 pour lesquelles on a $\forall n \in \mathbb{N},\ u_n \geqslant 0$?

La suite $\begin{pmatrix} u_n \\ v_n \end{pmatrix}$ est géométrique de raison à gauche $\begin{pmatrix} 1 & 2 \\ 6 & 2 \end{pmatrix}$.
On diagonalise avec $D = \begin{pmatrix} 5 & 0 \\ 0 & -2 \end{pmatrix}$ et $D = \begin{pmatrix} 1 & 2 \\ 2 & -3 \end{pmatrix}$.

$$\begin{pmatrix} 1 & 2 \\ 6 & 2 \end{pmatrix}^n = \frac{1}{7} \cdot \begin{pmatrix} 3.5^n + 4.(-2)^n & 2.(5^n - (-2))^n \\ 6.5^n - 6.(-2)^n & 4.5^n + 3.(-2)^n \end{pmatrix}$$

On extrait $\boxed{u_n = \dfrac{(3.u_0 + 2.v_0).5^n + (4.u_0 - 2.v_0).(-2)^n}{7}}$
On pouvait y arriver en écrivant des choses « astucieuses » comme

$$\begin{array}{rcll} u_{n+2} & = & u_{n+1} & +2.v_{n+1} \\ u_{n+2} & = & u_{n+1} & +2.(6.u_n \quad +2.v_n) \\ u_{n+2} & = & u_{n+1} & +12.u_n \quad +2.2.v_n \\ u_{n+2} & = & u_{n+1} & +12.u_n \quad +2.(u_{n+1} \quad -u_n) \\ u_{n+2} & = & 3.u_{n+1} & +10.u_n \end{array}$$

Et face à $u_{n+2} = 3.u_{n+1} + 10.u_n$ on calcule le polynôme caractéristique
les valeurs propres 5 et -2
et la forme des solutions $u_n = A.5^n + B.(-2)^n$
Avec $u_n = \dfrac{(3.u_0 + 2.v_0).5^n + (4.u_0 - 2.v_0).(-2)^n}{7}$, exigeons $3.u_0 + 2.v_0 > 0$; et on est sûr d'avoir u_n positif au moins à partir d'un certain rang.
Exigeons même $4.u_0 - 2.v_0 = 0$ et le terme en $(-2)^n$ s'en va. On a alors l'assurance que tous les termes u_n sont positifs.
D'ailleurs, si u_0 et v_0 sont positifs, alors tous les termes des deux suites sont positifs !

◦3◦

♡ La suite $(☻_n)$ est définie par $☻_{n+2} = ☻_{n+1} + 20.☻_n$ avec $☻_0$ et $☻_1$ donnés. Déterminez a et b pour avoir $☻_0 = a + b$ et $☻_1 = 5.a - 4.b$. Montrez alors pour tout n : $☻_n = a.5^n + b.(-4)^n$.
Pouvez vous choisir $☻_0$ et $☻_1$ pour avoir $☻_{2018} = 2018$ et $☻_{2019} = 2019$?

Équation caractéristique : $\lambda^2 = \lambda + 20$.
Spectre : $\{-4, 5\}$.
Forme des suites : $\exists(A, B), \forall n, ☻_n = A.5^n + B.(-4)^n$ avec A et B dépendant des conditions initiales.

Mais l'énoncé semble dire « on ne va pas faire ça, on va le jouer Terminale ».
Ou en tout cas, on va faire de la diagonalisation sans le voir.
$☻_0 = a + b$ et $☻_1 = 5.a - 4.b$ permet de déterminer a et b, par le calcul...
...ou par les matrices : $\begin{pmatrix} ☻_0 \\ ☻_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 5 & -4 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix}$ donc $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 5 & -4 \end{pmatrix}^{-1} \cdot \begin{pmatrix} ☻_0 \\ ☻_1 \end{pmatrix}$.
On la joue vraiment Terminale :
Notons P_n la propriété $☻_n = a.5^n + b.(-4)^n$
Initialisation : P_0 et P_1 sont vraies.
On se donne n quelconque, et on suppose P_n et P_{n+1} vraies.

$$\begin{array}{rcccc} ☻_n & = & a.5^n & + & b.(-4)^n \\ ☻_{n+1} & = & a.5.5^n & + & b.(-4).(-4)^n \end{array}$$

On combine :

$$\begin{array}{rcccc} 20.☻_n + ☻_{n+1} & = & a.(20+5).5^n & + & b.(20-4).(-4)^n \\ ☻_{n+2} & = & a.5^{n+2} & + & b.(-4)^{n+2} \end{array}$$

L'hérédité est établie. la formule est validée pour tout n.

On veut $☻_{2018} = 2018$ et $☻_{2019} = 2019$. Il suffit de bien choisir a et b, donc $☻_0$ et $☻_1$.
Version « je calcule tout »... eh bien je calcule tout.

Version rapide : on veut juste $\begin{pmatrix} 0 & 1 \\ 20 & 1 \end{pmatrix}^{2018} \cdot \begin{pmatrix} ☻_0 \\ ☻_1 \end{pmatrix} = \begin{pmatrix} 2018 \\ 2019 \end{pmatrix}$,
il suffit d'imposer $\begin{pmatrix} ☻_0 \\ ☻_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 20 & 1 \end{pmatrix}^{-2018} \cdot \begin{pmatrix} 2018 \\ 2019 \end{pmatrix}$,
sachant que $\begin{pmatrix} 0 & 1 \\ 20 & 1 \end{pmatrix}^{-2018}$ existe car $\begin{pmatrix} 0 & 1 \\ 20 & 1 \end{pmatrix}$ est inversible.
Si on veut quand même calculer : $\begin{pmatrix} 0 & 1 \\ 20 & 1 \end{pmatrix}^{-2018} = \begin{pmatrix} 1 & 1 \\ -4 & 5 \end{pmatrix} \cdot \begin{pmatrix} (-4)^{-2018} & 0 \\ 0 & 5^{-2018} \end{pmatrix} \cdot \begin{pmatrix} 5 & -1 \\ 4 & 1 \end{pmatrix} \cdot \frac{1}{9}$.
Vous reconnaissez $P = \begin{pmatrix} 1 & 1 \\ -4 & 5 \end{pmatrix}$? Elle a été écrite plus haut quand on a cherché a et b...

◦4◦

Mon fils a eu 6 sur 20 *(en gym, pas en maths)*. La moyenne de classe est à 11. Il me dit : "*j'aurais eu cinq points de plus, j'aurais eu comme la moyenne*". Je lui dis "*non, car la moyenne de la classe aurait alors augmenté*". "*Ah oui, j'aurais du avoir* 11,2 *alors*". Combien y a-t-il d'élèves dans la classe de mon fils ?

Notons N le nombre d'élèves. Notons S la somme des notes tant que mon fils a 6.
On a alors $S = N \times 11$ par définition même de la moyenne.

Faisons gagner cinq points à mon fils et rien qu'à lui. La somme des notes devient $S + 5$.
La moyenne devient $\dfrac{S+5}{N} = \dfrac{S}{N} + \dfrac{5}{N} = 11 + \dfrac{5}{N}$. Comme N n'est pas infini, ceci confirme que la nouvelle moyenne est plus que 11.

Comment avoir égalité alors ? C'est François lui même, en pur matheux, qui le dit : il doit avoir 11,2, c'est à dire 5,2 points de plus.

La nouvelle somme est $S+5,2$ et la nouvelle moyenne est $\frac{S+5,2}{N} = \frac{S}{N} + \frac{5,2}{N} = 11 + \frac{5,2}{N}$.

Mais la nouvelle moyenne est 11,2 puisque mon fils a réussi à atteindre la moyenne. On a donc $11 + \frac{5,2}{N} = 11,2$.

On égalise : $N = \frac{5,2}{0,2} = 26$.

Et pour avoir les points, comme à l'école élémentaire et au collège : « il y a 26 élèves dans la classe ».

∘5∘ Calculez pour tout réel a strictement positif $\int_{x=1/a}^{a} \left(\int_{y=0}^{1} \frac{dy}{x^2+y^2} \right).dx$.

Pour tout x , on calcule $\int_{y=0}^{1} \frac{dy}{x^2+y^2}$ en l'écrivant $\frac{1}{x^2}.\int_{y=0}^{1} \frac{dy}{1+\left(\frac{y}{x}\right)^2}$. Si nécessaire, on change de variable en posant $u = \frac{y}{x}$, en tout cas, on trouve $\left[\frac{Arctan\left(\frac{y}{x}\right)}{x}\right]_0^1$. c'est à dire $\frac{Arctan(1/x)}{x}$.
Il est important dans ce calcul que x soit non nul, et ce sera le cas entre a et $1/a$.

On doit ensuite se donner a et calculer $\int_{1/a}^{a} \frac{Arctan\left(\frac{1}{x}\right)}{x}.dx$.
Pour a égal à 1, c'est facile, mais sinon ?
Mais sinon, l'intégration par parties n'est pas pertinente, elle donne un logarithme qu'on n'apprécie pas trop.

Notons I_a cette intégrale, et effectuons un changement de variable : $u = \frac{1}{t}$ pour voir :

$$I_a = \int_{u=1/a}^{a} \frac{Arctan\left(\frac{1}{x}\right)}{x}.dx = \int_{t=a}^{1/a} t.Arctan(t).\frac{-dt}{t^2} = \int_{1/a}^{a} \frac{Arctan(t)}{t}.dt$$

Elle ressemble à l'autre. On va profiter d'une relation agréable sur l'arctangente en somment $I_a + I_a$:

$I_a + I_a = \int_{1/a}^{a} \frac{Arctan\left(\frac{1}{u}\right) + Arctan(u)}{u}.du$ (variables muettes)

On remplace : $I_a + I_a = \int_{1/a}^{a} \frac{\pi}{2.u}.du = \frac{\pi}{2}.\Big[\ln(u)\Big]_{u=1/a}^{a} = \frac{\pi.2.\ln(a)}{2}$

La valeur est donc $\boxed{I_a = \frac{\pi.\ln(a)}{2}}$

On pouvait aussi nommer F une primitive de $t \longmapsto \frac{Arctan(1/t)}{t}$ et écrire $I_a = F(a) - F\left(\frac{1}{a}\right)$ et dériver $F'(a) + \frac{1}{a^2}.F'\left(\frac{1}{a}\right)$, simplifier, profiter de $I_1 = 0$ et remonter à I_a pour tout a.

∘6∘ Complétez et diagonalisez $\begin{pmatrix} & 7 \\ 1 & \end{pmatrix}$ pour que ses valeurs propres soient 3 et -5 *(s'il y a plusieurs solutions, traitez les toutes)*.
Pouvez vous compléter $\begin{pmatrix} & 7 \\ 1 & \end{pmatrix}$ pour qu'elle ne soit pas diagonalisable sur $\mathbb{R}$.
Pouvez vous compléter $\begin{pmatrix} & 7 \\ 1 & \end{pmatrix}$ pour qu'elle ne soit pas diagonalisable, même sur $\mathbb{C}$.

Pour que $\begin{pmatrix} a & 7 \\ 1 & b \end{pmatrix}$ ait pour spectre $\{-3,\ 5\}$, il faut qu'on la relie à la matrice $\begin{pmatrix} -3 & 0 \\ 0 & 5 \end{pmatrix}$ avec qui elle devra partager trace et déterminant.

On impose donc

trace	déterminant
$a+b = -3+5 = 2$	$a.b - 7 = (-3).5 = -15$

les deux réels a et b sont les deux racines de $X^2 - 2.X - 8 = 0$.
On trouve deux matrices qu'on va d'ailleurs diagonaliser en la même matrice D qu'on connaît déjà : $D = \begin{pmatrix} -3 & 0 \\ 0 & 5 \end{pmatrix}$

$\begin{pmatrix} -2 & 7 \\ 1 & 4 \end{pmatrix}$	$\begin{pmatrix} 4 & 7 \\ 1 & -2 \end{pmatrix}$
$D = \begin{pmatrix} -3 & 0 \\ 0 & 5 \end{pmatrix}$	$D = \begin{pmatrix} -3 & 0 \\ 0 & 5 \end{pmatrix}$
$P = \begin{pmatrix} 1 & 1 \\ -1/7 & 1 \end{pmatrix}$ ou même $P = \begin{pmatrix} -7 & 1 \\ 1 & 1 \end{pmatrix}$	$P = \begin{pmatrix} 1 & 1 \\ -1 & 1/7 \end{pmatrix}$ ou même $P = \begin{pmatrix} 1 & 7 \\ -1 & 1 \end{pmatrix}$

Comment faire pour qu'elle ne soit pas diagonalisable sur $\mathbb{R}$? Qu'elle ne puisse pas être semblable à une matrice diagonale à coefficients réels ?
Imposons que son polynôme caractéristique ait un discriminant négatif :
$\begin{pmatrix} a & 7 \\ 1 & b \end{pmatrix}$ a pour polynôme caractéristique $X^2 - (a+b).X + (a.b - 7)$, de discriminant $(a+b)^2 - 4.a.b + 28$, celui ci vaut $(a-b)^2 + 28$, il est toujours positif.
On a donc toujours au moins une matrice D et on résoudra un petit système bien lourd (mais résoluble).
La matrice $\begin{pmatrix} a & 7 \\ 1 & b \end{pmatrix}$ est toujours diagonalisable.

Et sur $\mathbb{C}$? On va se dire que c'est encore pire. L'équation du second degré a toujours des racines !
Mais si elle n'en a qu'une ?

Je m'explique : si on a une valeur propre double λ, il y a un problème ; la matrice devrait être semblable à $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, or seule $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ est semblable à $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$.
On va donc ici annuler le discriminant $a - b = i.\sqrt{28}$: par exemple $\begin{pmatrix} a & 7 \\ 1 & b \end{pmatrix}$ ne se diagonalise pas :

trace	déterminant	polynôme	spectre	D	P
$i.2.\sqrt{7}$	-7	$X^2 - 2.i.\sqrt{28} - 7$	$\{i.\sqrt{7}\}$ en double	$\begin{pmatrix} i.\sqrt{7} & 0 \\ 0 & i.\sqrt{7} \end{pmatrix}$	jamais inversible

Toutes les matrices P trouvées ont leurs deux colonnes égales ou proportionnelles.

◦7◦

♡ Une suite récurrente u vérifiant $u_{n+2} = 12.u_n - u_{n+1}$ pour tout n reste de signe constant. Montrez que c'est une suite géométrique, et calculez u_{100}/u_5.

Le cours dit • équation caractéristique $\lambda^2 = -\lambda + 12.\lambda$
• spectre $\{-4,\ 3\}$
Les solutions sont de la forme $a.(-4)^n + b.3^n$. Avec a et b à déterminer en fonction des conditions initiales.
Mais si a est non nul, la suite sera du signe de a pour n pair assez grand, puis du signe de $-a$ pour n impair assez grand.
Et ceci contredira « de signe constant ».
Il s'ensuit que a est nul.
La suite est de la forme $(b.3^n)$.
Elle est géométrique de raison 3. Et le quotient $\dfrac{u_{100}}{u_5}$ vaut 3^{95} (raison).

◦8◦

Est il possible de choisir a réel pour que les suites récurrentes "$u_{n+2} = a.u_{n+1} - u_n$ pour tout n" soient toutes périodiques de période 9 ?
Est il possible de choisir a et b rationnels pour que les suites récurrentes "$u_{n+2} = a.u_{n+1} + b.u_n$ pour tout n" soient toutes périodiques de période 12 ?

Est il possible de choisir a et b irrationnels pour que les suites récurrentes "$u_{n+2} = a.u_{n+1} + b.u_n$ pour tout n" soient toutes périodiques de période 12 ?
Est-il possible de choisir a, b, c et d réels pour que dans le couple $(u,\ v)$ de suites vérifiant $\left\{ \begin{array}{rcll} u_{n+1} & = & a.u_n & +b.v_n \\ v_{n+1} & = & c.u_n & +d.v_n \end{array} \right|$ pour tout n, la suite u soit périodique de période 6.
Montrez que si u est périodique, alors v l'est aussi.

Pour l'équation récurrente $u_{n+2} = a.u_{n+1} - u_n$, les solutions sont des combinaisons de suites géométriques. Elles ne seront bornées (car périodiques) que si les deux raisons sont plus petites que 1 en module.
Cas particulier : une racine double, on exige alors que le module soit strictement plus petit que 1 car sinon $(\alpha.n + \beta).r^n$ diverge aussi pour α non nul.
L'équation caractéristique $\lambda^2 - a.\lambda + 1 = 0$ a deux racines dont le produit vaut 1.
Il faut donc que les deux soient de module 1 (sinon, une plus grande, une plus petite et rien n'est périodique).

On va même demander que les deux valeurs propres soient des racines neuvièmes de l'unité.

Il suffit de choisir $a = 2.\cos(2.\pi/9)$, ou même $a = 2.\cos(2.\pi/3)$ et pourquoi pas $a = 2.\cos(2.\pi)$...
Ah, non, pas $a = 2.\cos(2.\pi)$, car on a alors une racine double et des solutions en $(\alpha.n + \beta)$.

Remarque :	Il faut bien sûr ne pas avoir oublié que l'équation dont les racines sont $e^{i.k.\pi/N}$ et son conjugué est $\lambda - 2.\cos(2.k.\pi/N).\lambda + 1 = 0$. Mais si vous avez oublié ça, je ne peux plus rien pour vous...

Avec $u_{n+2} = a.u_{n+1} + b.u_n$ c'est un peu pareil.
On demande que les racines de l'équation caractéristique soient encore des $e^{i.k.\pi/12}$. C'est possible :
$u_{n+2} = 2.\cos(\pi/12).u_{n+1} - u_n$ ou $u_{n+2} = 2.\cos(4.\pi/12).u_{n+1} - u_n$ ou $u_{n+2} = 2.\cos(3.\pi/12).u_{n+1} - u_n$.

Ah, mais on les veut rationnels ! Et ces cosinus ne le sont guère.
Sauf quand même $u_{n+2} = 2.\cos(4.\pi/12).u_{n+1} - u_n$ et $u_{n+2} = 2.\cos(6.\pi/12).u_{n+1} - u_n$.
Les solutions sont périodiques de période 12 (même si 12 n'est pas la plus petite période).

Rappel :	Tant que la question est « pouvez vous choisir... » ou « choisissez... », une réponse est « on propose/on vérifie ». Il n'est pas utile de raisonner par conditions nécessaires ($\Rightarrow$). C'est même idiot si à la fin vous ne vérifiez pas. Il n'y a que pour le cas « on ne peut pas choisir » qu'il faut raisonner par implications, afin d'arriver à une contradiction. C'est parfois ce qu'il manque à certains d'entre vous : déjà lire la question et ne pas se précipiter tout de suite sur des $\Rightarrow$ comme dans un mauvais exercice du bac...

Pour $\left\{ \begin{array}{rcll} u_{n+1} & = & a.u_n & +b.v_n \\ v_{n+1} & = & c.u_n & +d.v_n \end{array} \right.$, c'est cette fois la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ qu'il suffit de bien choisir pour que ses deux valeurs propres soient des racines de l'unité...
On peut même se ramener à des recherches de l'exercice précédent avec $\left\{ \begin{array}{rcll} u_{n+1} & = & a.u_n & +b.v_n \\ v_{n+1} & = & u_n & \end{array} \right.$.

∘9∘

♡ Soit $(E, *)$ une structure interne, dotée d'un neutre et vérifiant :
$\forall (a,\ b,\ c) \in E^3,\ a * (b * c) = (a * c) * b$. Montrez que la loi est commutative et associative.

La commutativité prend juste deux éléments a et b. L'hypothèse a le droit d'en utiliser trois.
On se donne a et b, et on prend « comme par hasard » $c = n$ (le neutre).
L'hypothèse permet d'écrire $a * (b * n) = (a * c) * n$.
Ceci ne nous avance pas.

Mais si on prend b et c quelconques et qu'on choisit $a = n$, on a cette fois $n * (b * c) = (n * c) * b$.
Par neutralité de n, on obtient $b * c = c * b$. Comme ceci est vrai pour tout couple, c'est la définition de la commutativité.

> *Les variables sont muettes, la commutativité c'est $\forall (,\ b) \in E^2,\ a * b = b * a$ mais c'est tout autant $\forall (b,\ c) \in E^2,\ c * b = b * c$.*
> *Ensuite, il y a des élèves qui disent « on ne peut pas prendre $a = n$, c'est un cas particulier.*
> *C'est en effet « prendre un cas particulier dans une hypothèse ». Ceci est tout à fait légitime. C'est convoquer un témoin bien choisi dans l'hypothèse.*
> *Ce qui ne tient pas la route c'est de dire « je dois montrer $\forall a,\ truc$, et j'ai montré truc pour un a particulier, donc c'est bon ».*
> *Non. Il faut le montrer pour tous les a.*
> *Il ne faut pas confondre le statut de l'hypothèse et celui de la conclusion.*

A présent, on se donne a, b et c quelconques, et il faut passer de $(a * b) * c$ à $a * (b * c)$ en utilisant non seulement l'hypothèse, mais aussi la commutativité que l'on vient d'établir :
$a * (b * c) = (a * c) * b$ par hypothèse
$a * (b * c) = a * (c * b)$ (commutativité au sein de la parenthèse)
$a * (b * c) = a * (c * b) = (a * b) * c$ (hypothèse appliquée au triplet $(a,\ c,\ b)$).

◦10◦

♡ Montrez que les matrices de taille 2 sur 2 à déterminant non nul forment un groupe pour la multiplication, non commutatif.
Montrez que l'ensemble des matrices de taille 2 sur 2 à coefficients entiers et à déterminant 1 en forme un sous-groupe.
En est il de même pour les matrices de taille 2 sur 2 à coefficients entiers et à déterminant 1 ou -1.
Montrez que les matrices de la forme $\begin{pmatrix} 2.a & a \\ -2.a & -a \end{pmatrix}$ avec a décrivant $\mathbb{R}^*$ forment un groupe pour la multiplication, mais pas un sous-groupe du groupe précédent...

On note $GL_2(\mathbb{R})$ l'ensemble des matrices carrées de taille 2 sur 2 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de déterminant non nul $a.d - b.c$.

Associativité	Acquise, c'est le produit matriciel : $(A.B).C = A.(B.C)$ que A, B et C soient inversibles ou non.
Neutre	Le neutre est $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Et alors ? Ce n'est pas ça la question. Tu es sûr que tu sais faire des maths ? Le neutre proposé est il dans l'ensemble ?
Stabilité	Si A et B ont un déterminant non nul, alors c'est aussi le cas de AB car $\det(A.B) = \det(A).\det(B)$. Et $A.B$ est évidemment une matrice carrée de taille 2 sur 2.
Symétriques	Si la matrice A (égale à $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$) a un déterminant non nul alors elle a un inverse : $\frac{1}{a.d-b.c}.\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Et alors ? Crétin fini. Tu n'as répondu qu'à la moitié de la question. Tu ne mérites aucun point. Où dis tu que l'invverse est dans l'ensemble ? Nulle part. Tu n'as donc pas compris la question. Que fais tu en salle de maths ?

Pour « non commutative, on donne un contre-exemple.

Les matrices de taille 2 sur 2 à coefficients entiers et de déterminant 1 :
on y trouve la matrice neutre, car son déterminant vaut 1 (et ses coefficients 0 ou 1).
Si A et B sont à coefficients entiers, leur produit est encore à coefficients entier. Et son déterminant vaut 1×1.
Si A est à coefficients entiers et a pour déterminant 1, son inverse est $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, à coefficients entiers, de déterminant $d.a - (-c).(-b)$, ce qui fait 1.

Même démonstration pour déterminant égal à 1 ou -1.

Les matrices de la forme $\begin{pmatrix} 2.a & a \\ -2.a & -a \end{pmatrix}$ sont un exemple intéressant. Leur déterminant est nul. Leur ensemble n'est pas inclus dans le groupe et ne pourra pas en être un sous-groupe. Mais on a quand même

Associativité	Comme toujours.
Neutre	Le neutre est $\begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix}$, et il est dans l'ensemble. Si si : $\begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix}.\begin{pmatrix} 2.a & a \\ -2.a & -a \end{pmatrix} = \begin{pmatrix} 2.a & a \\ -2.a & -a \end{pmatrix}$ et pareil à gauche !
Stabilité	$\begin{pmatrix} 2.a & a \\ -2.a & -a \end{pmatrix}.\begin{pmatrix} 2.b & b \\ -2.b & -b \end{pmatrix} = \begin{pmatrix} 2.a.b & a.b \\ -2.a.b & -a.b \end{pmatrix}$ Elle est de la forme voulue (avec $a.b$ non nul).
Symétriques	$\begin{pmatrix} 2.a & a \\ -2.a & -a \end{pmatrix}$ n'est pas inversible au sens classique du terme $A.A^{-1} = I_2$. Mais il ne s'agit ici d'obtenir le neutre de ce groupe : $\begin{pmatrix} 2.a & a \\ -2.a & -a \end{pmatrix}.quelquechose = \begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix}$. Et ici, on constate $\begin{pmatrix} 2.a & a \\ -2.a & -a \end{pmatrix}.\begin{pmatrix} \frac{2}{a} & \frac{1}{a} \\ -\frac{2}{a} & -\frac{1}{a} \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix}$ (des deux côtés). Et $\frac{1}{a}$ est bien à son tour un réel non nul...

Et ce groupe est commutatif.

Mais ce n'est pas un sous groupe de $(GL_2(\mathbb{R}), \times)$.
Ce n'est pas non plus un sous groupe de $(M_2(\mathbb{R}), \times)$ tout simplement parce que $(M_2(\mathbb{R}), \times)$ n'est même pas un groupe !

∘11∘

N	diviseurs de N	somme des diviseurs non triviaux	somme des carrés des chiffres
125	1, 5, 25, 125	$5+25=30$	$1^2+2^2+5^2=30$
581	1, '7, 83, 581	$7+83=90$	$5^2+8^2+1^2=90$
8 549	1, 83, 103, 8549	$83+103=186$	$8^2+5^2+4^2+9^2=?$
16 999	1, 89, 191	$89+191=?$	$1^2+6^2+9^2+9^2+9^2=280$

Un nombre parfait canadien est un nombre dont la somme des diviseurs propres est la somme des carrés de ses chiffres *(on se demande pourquoi un jour au congrès de la Canadian Mathématical Society à l'Université du Manitoba des gens se sont posé la question dans un couloir entre deux conférences*[a]*)*. Écrivez un programme qui cherche les 7 premiers nombres supercanadiens *(la somme des diviseurs propres est la somme des cubes de ses chiffres)*, et vérifiez à la main que 160 en fait partie.

a. si, pour le plaisir de chercher, c'est ce qui caractérise les mathématiciens et mathématiciennes et fait que les physiciens les regardent avec les yeux surpris du « à quoi ça sert » ?

Pour tester si un nombre n est parfait canadien, on accumule la somme de ses diviseurs propres par un range adéquat avec un test.
On prend aussi la liste de ses chiffres et on en effectue la somme des cubes.

```
def SomCubes(n) :
....SC = 0
....LC = list(str(n))
....for Chif in LC :
........c = int(Chif)
........SC += c*c*c
....return SC
```

```
def SomDiv(n) :
....for d in range(2, n) :
........if n%d == 0 :
............SD += d
....return SD
```

```
Parfaits = [ ]
n = 0
while len(Parfaits)<7 :
....if SomCubes(n) == SomDiv(n) :
........Parfaits.append(n)
........print('et hop : ',n)
........n += 1
print(L)
```

Sinon, pour faire fondre un entier, on a

```
def SomCubes(n) :
....SC, nn = 0, n #copie de sécurité
....while nn > 0 :
........c = nn%10 #on récupère le chiffre des unités
........SC += c*c*c
........nn = nn/10 #on efface le chiffre des unités
....return SC
```

On décompose $160 = 2^5.5$ et on dresse la liste de ses diviseurs :

2	2^2	2^3	2^4	2^5	somme : 63
2.5	$2^2.5$	$2^3.5$	$2^4.5$		somme : 31×5

La somme des diviseurs cherchés vaut 217. Et la somme des cubes des chiffres vaut 1^3+6^3. Pareil.

142	160	1 375	6 127	12 643	51 703	86 833

La syntaxe `while len(Parfaits)<7` est risquée, si on n'en trouve pas 7, la boucle ne s'arrête jamais !

∘11∘

On a posé : $n = 88\,825$ et $p = 7\,267$. Votre voisin a écrit : $192\,171.p - 15\,722.n = 7$. Vous en déduisez : $p.g.c.d.(n,\ p) = 7$.
Vous avez tort. Pourquoi ?

C'est une identité de Bézout ?
Elle dit que 7 est dans $\{a.n + b.p \mid (a,b) \in \mathbb{Z}^2\}$.
Ce qui signifie que 7 est dans « le plus petit sous-groupe de $(\mathbb{Z}, +)$ contenant n et p ».
Mais ce n'est pas forcément un générateur de cet ensemble (plus petit élément non nul).

7 est un multiple du p.g.c.d.
Et ici, le p.g.c.d. vaut 1 : $27\,453.p - 2\,246.n = 1$.
Et on a tout multiplié par 7.

Le cours dit :	si d est le p.g.c.d. alors il existe a et b vérifiant $a.n + b.p = d$.
Et il ajoute	tout nombre de la forme $a.n + b.p$ est un multiple du p.g.c.d. (mais pas forcément « le p.g.c.d. »).

∘12∘

On rappelle que $\{1, 2, \dots 18\}$ est un groupe pour la multiplication modulo 19. Donnez moi quand même pour vérifier la liste des inverses des éléments :

a	1	2	3	4	5	6	7	8	8	10	11	12	13	14	15	16	17	18
a^{-1}																		

Bonus : calculez la somme des éléments de la deuxième ligne.

Dans la deuxième ligne, on retrouve chaque élément de la première une fois et une seule ! (le passage de a à a^{-1} est une bijection de $[1, 18]$ dans lui même).
La somme vaut 171. Ce qui fait 0 modulo 19. On peut d'ailleurs dire que l'on regroupe chaque élément avec son oppose...

Pour les inverses modulo 19, on complète comme on peut. On sait que 1 est son propre inverse, de même que 18 (égal à -1).
On trouve l'inverse de 2 : c'est 10. On en déduit que l'inverse de 10 est 2. Et l'inverse de -2 (connu sous le nom de 17) est -10 (connu sous le nom de 9).

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a^{-1}	1	10							17	2							9	18

L'inverse de 4 est 5. Et vice versa. Et l'inverse de -4 est -5. Et vice versa.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a^{-1}	1	10		5	4				17	2				15	14		9	18

Les suivants doivent s'associer deux à deux. On teste : $3.6 = 18 = -1$. Donc $3.(-6) = 1$. L'inverse de 3 est 13.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a^{-1}	1	10	13	5	4	16			17	2			3	15	14	6	9	18

On teste ce qu'il reste : $7.8 \neq 1$ mais $7.11 = 1$. On peut conclure :

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a^{-1}	1	10	13	5	4	16	11	12	17	2	7	8	3	15	14	6	9	18

Presque sans aucun effort !

Et la somme ? Dans la seconde ligne, on a les mêmes éléments que dans la première, mais dans un ordre différent.
On a donc $\sum_{k=1}^{18} k$ et ceci vaut $\frac{18.19}{2}$ (calculez si vous voulez).

∘13∘

♡ Montrez que $\phi = (a, b) \longmapsto 2^a.(2.b + 1)$ est bijective de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}^*$.
Ecrivez un script Python qui prend en entrée n et retouve son antécédent par ϕ.

$\phi = (a, b) \longmapsto 2^a.(2.b + 1)$ prend eeux entiers et définit un entier.
Elle va de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$.

On n'atteindra jamais 0. $Im(\phi) \subset \mathbb{N}^*$.

Si vous me dite tout de suite $Im(\phi)) = \mathbb{N}^*$, vous n'avez rien compris. Il y a tout le boulot de la surjectivité.

Prenons deux couples (a, b) et (c, d) et supposons qu'ils ont la même image.
On a donc $2^a.(2.b + 1) = 2^c.(2.d + 1)$.
On étudie cette égalalité modulo 2.
Proprement, on suppose $a \neq c$. Par symétrie des rôles, on peut aupposer $a > c$. On divise alors de chaque côté par 2^c : $2^{a-c}.(2.b + 1) = (2.d + 1)$.
Le membre de droite est impair. Celui de gauche est pair. Il y a une contradiction.
On a donc foércément $a = c$.
On reporte : $2^a.(2; b + 1) = 2^a.(2.d + 1)$. On aboutit sans effort à $b = d$.

Du travail « évident ». Mais trop d'élèves se perdent dans les variables, faute de s'être demandé « je démontre quoi ? ».

Pour la surjectivité, il faut trouver un antécédent (a, b) à tout entier naturel N donné.
On se donne N et on le décompose en produit de facteurs premiers : $N = 2^\alpha.3^\beta.5^\gamma \dots$. (produit fini, mais moche à indexer hormis en $\prod_i (p_i)^{\alpha_i}$).

Le produit $3^\beta.5^\gamma \dots$ est impair. On peut l'écrire $2.b + 1$.
Et ona alors $N = 2^\alpha.(2.b + 1)$. On pose $a = \alpha$ et c'est fini.

L'application est donc bien bijective de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}^*$.

Qui sont les crétins qui avec des réflexes de « j'ai des théorèmes, mais pas de vision géométrique » ont essayé à tout prix de sortir un truc du type « application strictement croissante donc injective ». On n'a pas de relation d'ordre sur $\mathbb{N} \times \mathbb{N}$!

Un exemple : 2022 est pair et non multiple de 4, il a pour antécédent $(1, 505)$
2023 est impair, il a pour antécédent $(0, 1012)$
2024 est multiple de 8, il a pour antecedent $(3, 126)$

Démarche : pour N donné, trouver l'exposant de 2 en divisant par 2 tant que c'est possible (e en incrémentant un compteur).
Une fois qu'on a un nombre impair, on l'écrit $2.b + 1$.

```
def Reciproque(N) : #int -> int x int
....n = N #pour ne pas abimer N
....a = 0 #compteur
....while N%2 == 0 : #tant que n est pair
........n = n//2 #on divise par 2
........a += 1
....b = (n-1)//2 #pour n = 2.b+1
....return (a,b)
```

∘14∘

Soient A et B deux ensembles. On définit $A \Subset B$ si il existe une application injective de A dans B.
♡ Montrez que cette relation est transitive et réflexive, mais pas symétrique ni antisymétrique (contre-exemples).

Réflexive | On se donne un ensemble A. Il existe une application injective de A dans A, c'est l'identité.

Transitive | On se donne cette fois A, B et C. On suppose qu'il existe une injection f de A dans B et une injection g de B dans C. Le cours garantit que $g \circ f$ est injective de A dans C.

Non symétrique | Un contre-exemple suffit : il existe une application injective de $\emptyset$ dans $\{0\}$ (ne rien faire), mais il n'existe pas d'application injective de $\{0\}$ dans $\emptyset$.

Non antisymétrique | Prenons $\{0\}$ et $\{1\}$. Il existe une application injective du premier vers le second, et vice versa.
Mais ces deux ensembles ne sont pas égaux. C'est donc un contre-exemple à $\forall (A, B),\ \Big((A \Subset B) \text{ et } (B \Subset A)\Big) \Rightarrow (A = B)$.

En revanche, on va prouver $(A \Subset B)$ et $(B \Subset A)$ implique « il existe une bijection entre A et B ».

♠ 0 ♠

On veut maintenant montrer que si il existe une application injective f de A dans B et une application injective g de B dans A alors il existe au moins une bijection de A dans B.

On rappelle :

pour $X \subset A$	on définit	$f(X) = \{f(x) \mid x \in X\} = \{b \in B \mid \exists a \in A,\ y = f(a)\}$
X partie de A		$f(X)$ partie de B
pour $Y \subset B$	on définit	$f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$
Y partie de B		$f^{-1}(Y)$ partie de A

On rappelle que la notation $f^{-1}(Y)$ ne s'applique qu'à une partie et qu'on ne peut écrire $x = f^{-1}(y)$ que si f est bijective, ou à la rigueur y dans $f(X)$ (ensemble image, y a au moins un antécédent) et f injective (pour qu'il n'y ait pas d'ambigüité sur le choix de x).

Montrer que si $g(B)$ est égal à A alors g est une bijection de B dans A.

Si on suppose que $g(B)$ est égal à A, ceci signifie que tout élément a de A est dans $g(B)$ et s'écrit donc $g(b)$ pour un b de B.
Ceci signifie : tout élément a de A a un antécédent b par g dans B.
C'est la surjectivité de g. Et comme g est déjà injective, la voilà bijective.

Il va de soi qu'on ne peut pas faire des raisonnements sur les cardinaux. Ce serait d'une grande naïveté. On a le droit de travailler sur des ensembles infinis. Tout l'intérêt du théorème est même là.

Il existe une injection de $\mathbb{Q}^+$ *dans* $\mathbb{N}$ *:* $(f = \frac{p}{q} \longmapsto 2^p.3^q)$
il existe aussi une injection de $\mathbb{N}$ *dans* $\mathbb{Q}^+$ *:* $(g = n \longmapsto n)$*,.*
Mais aucune des deux n'est une bijection entre $\mathbb{N}$ *et* $\mathbb{Q}^+$*.*
Pourtant, il doit bien exister des bijections entre $\mathbb{N}$ *et* $\mathbb{Q}^+$*.*
Je vous invite à vérifier que f *est bien clairement définie ci dessus et injective.*
$f\left(\frac{2}{5}\right) = 2^2.3^5$, $f\left(\frac{5}{16}\right) = 2^5.3^{16}$, $f(2) = 2^2.3^1$, $f(0) = 2^0.3^1$
2024 *n'a pas d'antécédent par* f *(car c'est* $2^3.11.23$*).*
2048 *n'a pas d'antécédent car il faudrait avoir* $p = 11$ *et* $q = 0$ *dans le rationnel* $\frac{p}{q}$*.*
1944 *a pour antécédent* $\frac{3}{5}$ *car on a* $1944 = 2^3.3^5$*.*

♠ 1 ♠ On suppose donc $g(B) \neq A$. On pose $X_0 = A - g(B)$ (c'est à dire $X_0 = \{a \in A \mid \forall b \in B,\ g(b) \neq a\}$). Justifiez l'existence de la suite d'ensembles (X_n) définie par $\forall n,\ X_n = g(f(X_n))$. Montrez que chaque X_n est une partie non vide de A non vide, de même que $X = \bigcup_{n\in\mathbb{N}} X_n$.

X_0 est donc formé des éléments de A sans antécédent par g.
C'est une partie de A.
Son image directe par f est une partie de B.
L'image directe par g de cette partie de B est une partie de A.

Proprement, une récurrence déjà initialisée :
On se donne n quelconque. On suppose que $X_n$est une partie de A non vide (disons qu'il y a dedans un élément x_n).
L'ensemble X_{n+1} est alors $\{g(f(x)) \mid x \in X_n\}$.
Il est non vide car on y trouve $g(f(x_n))$.
C'est une partie de A car $g \circ f$ va de A dans A.

Enfin, une réunion de parties non vides est non vide. On a même $X_0 \subset X$.

Si on tente de regarder sur notre exemple

	$f = \frac{p}{q} \longmapsto 2^p.3^q$	
$\mathbb{Q}^+$	$\longrightarrow$ / $\longleftarrow$	$\mathbb{N}$
	$g = n \longmapsto n$	

$g(\mathbb{N})$ *est égal à tous les entiers positifs,*
X_0 *est formé de tous les rationnels positifs sauf les entiers.*
$f(X_0)$ *est donc formé des* $f\left(\frac{p}{q}\right)$ *avec* q *différent de* 1*. Ce sont les* $2^p.3^q$ *avec* $q > 1$*.*
Ce sont donc les entiers ne se décomposant qu'avec que des 2 *et des* 3*, avec au moins deux facteurs* 3*. Le millésime* 1944 *en fait encore partie.*
Facile d'expliciter X_1*, ce sont les mêmes.*
Et ensuite, ça devient horrible.

♠ 2 ♠ On pose enfin $X' = A - X$. Quantifiez $a \in X'$.

Être dans X c'est être dans au moins un des X_n.
Être un des x de X_n (n fixé) c'est vérifier $\exists a \in X_0,\ x = (g \circ f)^n(a)$.
On a donc $X = \{x \in A \mid \exists n \in \mathbb{N},\ \exists a \in X_0,\ (g \circ f)^n(a) = x\}$.

Ne pas y être, c'est donc $\forall n \in \mathbb{N},\ \forall a \in X_0,\ (g \circ f)^n(a) \neq x$.

Et si on y tient

$$\left(x \in X'\right) \Leftrightarrow \left(\forall a \in A,\ \left((\forall b \in B,\ a \neq g(b)) \Rightarrow (\forall n \in \mathbb{N},\ (g \circ f)^n(a) \neq x)\right)\right)$$

♠ 3 ♠ Montrez : $\forall x \in X,\ g(f(x)) \in X$.

Là c'est direct.
On prend x dans X. C'est donc qu'il est dans un des X_n. Il s'écrit $(g \circ f)^n(a)$ pour un a de X_0.
Mais alors $g(f(x)) = (g \circ f)^{n+1}(a)$.
On reconnaît que $g(f(x))$ est dans X_{n+1}. Il est donc dans la réunion X.

♠ 4 ♠ Justifiez $\forall a \in X',\ \exists! b \in B,\ a = g(b)$.

Prenons a dans X' (donc a fortiori dans A).
Il n'est dans aucun des X_n, en particulier : $a \notin X_0$.
Par définition de X_0 vu comme complémentaire, ceci signifie $a \in g(B)$.
Il a donc au moins un antécédent b dans B par g.
Mais par injectivité de g, cet antécédent est unique.

On définit alors φ sur A par $\varphi(a) = f(a)$ si $a \in X$ et $\varphi(a)$ est l'unique antécédent de x par g si a est dans X' (voir question précédente).

♣ 0 ♣ Pour se mettre en situation le temps d'une question : $A = B = \mathbb{N}$ et $f = g = n \longmapsto n+1$ pouvez vous déterminer X, X' et φ ?

C'est quand même plus simple que mon exemple avec des $f\left(\frac{p}{q}\right) = 2^p.3^q$.

Ici, f et g vont bien de $\mathbb{N}$ dans $\mathbb{N}$ (et même de $\mathbb{N}$ dans $\mathbb{N}^*$) et sont injectives.
L'ensemble X_0 est égal à $\mathbb{N} - \mathbb{N}^*$ c'est à dire $X_0 = \{0\}$ (ensemble).

L'application $g \circ f$ n'est autre que $n \longmapsto n+2$.
On a donc $X_1 = \{2\}$, $X_2 = \{4\}$ et ainsi de suite.
Par réunion : $X = 2.\mathbb{N}$ (ensemble des entiers pairs).

Par complémentaire : X' est l'ensemble des entiers impairs.

Comment est alors définie φ ?
$\varphi(x) = f(x) = x+1$ si x est pair.
$\varphi(x) = g^{-1}(x) = x-1$ si x est impair.
Elle a déjà fait l'objet d'exercices dans nos T.D., c'est une bijection de $\mathbb{N}$ dans $\mathbb{N}$ qui échange les couples d'entiers « pair/impair ». Elle est sa propre réciproque.

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	...	$2.p$	$2.p+1$	...	n	...
φ	↓	↓	↓	↓	↓	↓	↓	↓	↓		↓	↓		↓	
$\mathbb{N}$	1	0	3	2	5	4	7	6	9	...	$2.p+1$	$2.p$	...	$n+(-1)^n$	...

♠ 5 ♠ Justifiez : $\varphi(X') = g^{-1}(X')$ et $\varphi(X) = f(X)$.

C'est par définition même.
On prend b dans $\varphi(X')$. On a donc $b = \varphi(a)$ pour un a de X'.
Par définition même, b est l'unique antécédent de a par g. Il est donc dans $g^{-1}(X')$.

Prenons b dans $g^{-1}(X')$. C'est donc que $g(b)$ est dans X'.
C'est donc que $g(b)$ admet un antécédent par g, unique. C'est b.
On a alors $\varphi(g(b)) = b$ par définition de φ avec $g(b)$ dans X'.
On reconnaît $b \in \varphi(X')$.

On prend b dans $\varphi(X)$. Il s'écrit $\varphi(a)$ pour un a de X.
Par définition de φ pour les éléments de X : $\varphi(a) = f(a)$.
b est de la forme $f(a)$ pour un a de X : b est dans $f(X)$.

On prend b dans $f(X)$. Il s'écrit $b = f(a)$ pour un a de X.
Mais comme a est dans X, on a $\varphi(a) = f(a)$.
On a donc $b = \varphi(a)$ pour un a de X. On reconnaît $b \in \varphi(X)$.

♠ 6 ♠ Montrez : $\varphi(X) \cap \varphi(X') = \emptyset$.

On prend b dans $\varphi(X) \cap \varphi(X')$. On va aboutir à une absurdité : un tel b ne pourra donc pas exister.
Il est donc dans $\varphi(X)$ et dans $\varphi(X')$.
Par la question précédente, on a donc $b \in f(X)$ et $b \in g^{-1}(X')$.
On traduit : $\exists a \in X,\ b = f(a)$ et $g(b) \in X'$.
On emboite pour ce a de X : $g(f(a)) \in X'$.
Or, pour a dans X, $g(f(a))$ est dans x (vu plus haut), ce qui contredit $g(f(a)) \in X'$. On la tient notre contradiction.

♠ 7 ♠ Montrez par disjonction de cas $\forall (a, \alpha) \in A^2,\ \varphi(a) = \varphi(\alpha) \Rightarrow a = \alpha$

	$a \in X$	$a \in X'$
$\alpha \in X$		
$\alpha \in X'$		

On prend a et α dans A. On suppose $\varphi(a) = \varphi(\alpha)$ (objectif $a = \alpha$).
Premier cas : a est dans X et α dans X'.
Par définition, $\varphi(a)$ est dans $\varphi(X)$ et $\varphi(\alpha)$ est dans $\varphi(X')$.
Mais comment ce même élément peut il être dans $\varphi(X)$ et $\varphi(X')$ puisque leur intersection est vide (vu juste avant).
Ce cas conduit donc à une impossibilité.

De même, le cas a est dans X' et α dans X par symétrie des rôles.

On a donc éliminé deux cases

	$a \in X$	$a \in X'$
$\alpha \in X$		impossible
$\alpha \in X'$	impossible	

Passons à « a est dans X et α aussi ».
On a alors $\varphi(a) = f(a)$ et $\varphi(\alpha) = f(\alpha)$.
Notre hypothèse devient alors $f(a) = f(\alpha)$ et par injectivité de f (hypothèse du début) : $a = \alpha$.

	$a \in X$	$a \in X'$
$\alpha \in X$	$a = \alpha$ par injectivité de f	impossible car $\varphi(X) \cap \varphi(X') = \emptyset$
$\alpha \in X'$	impossible car $\varphi(X) \cap \varphi(X') = \emptyset$	

On termine avec « a est dans X' et α aussi ».
Par définition : $\varphi(a) = b$ avec $g(b) = a$ et $\varphi(\alpha) = \beta$ avec $g(\beta) = \alpha$ (antécédents par g).
On met bout à bout $\varphi(a) = b$, $\varphi(\alpha) = \beta$ et $\varphi(\alpha) = \varphi(a)$: $b = \beta$.
On applique g : $g(b) = g(\beta)$ et c'est bien $a = \alpha$.

Ça se raconte bien aussi avec des mots sur qui est l'antécédent de qui.

Les quatre cas sont traités, f est injective.

♠ 8 ♠ Montrez par disjonction de cas : $\forall y \in B,\ \exists a \in A,\ \varphi(a) = y$ | $g(y) \in X'$ | $g(y) \in X$ |

On nous donne y, il faut lui construire un antécédent a.
La discussion ne peut donc porter que sur y. Et $g(y)$ existe, et c'est un élément de A.
Par définition d'un ensemble et de son complémentaire, on a deux possibilités en effet | $g(y) \in X'$ | $g(y) \in X$ |
Si $g(y)$ est dans X', on peut calculer comme par hasard $\varphi(g(y))$.
Par définition, c'est l'unique antécédent par g de $g(y)$.
Donc, par unicité/injectivité, c'est b.
On peut donc poser $a = g(y)$.

Si $g(y)$ est dans X, c'est qu'il est dans un des X_n.
Si il est dans X_0, il y a une contradiction. En effet, X_0 est formé des éléments qui ne sont l'mage de personne par g.
Si il est dans un X_n avec n strictement positif, il est donc l'image par $g \circ f$ d'un élément de X_{n-1}.
On s'écrit donc $g(y) = g(f(a))$ pour un a de X_{n-1}.
Mais par injectivité de g ceci donne $y = f(a)$ pour ce a de X_{n-1}.
Gagné, on a un antécédent !

♠ 9 ♠ Concluez.

On a construit une application φ de A dans B.
Elle est injective comme on l'a vu avec la première disjonction de cas.
Elle est surjective sur B comme on l'a vu par la seconde.
Elle est donc bijective.
On a su construire une bijection de A dans B (et sa réciproque de B dans A).

Bilan (théorème de Cantor Bernstein) :
si il existe une application injective de A dans B et une application injective de B dans A alors il existe une bijection de A sur B.

Corolaire :
On définit la relation « avoir le même cardinal que » (ou plus proprement « être équipotent à » par $A \Re b$ si il existe une bijection entre A et B.

On a alors une relation d'équivalence (les classes d'équivalence sont les cardinaux).

Ensuite on définit une relation sur les cardinaux :
$Card(\mathbb{A}) \leqslant card(\mathbb{B})$ si il existe une injection de A dans B (où A est un ensemble de cardinal $\mathbb{A}$ et b un ensemble quelconque de cardinal $\mathbb{B}$).
Le théorème de Cantor Bernstein nous montre que cette relation est antisymétrique.
On la savait aussi réflexive et transitive, c'est donc une relation d'ordre.

∘15∘ ♡ Résolvez $\sum_{k=n+1}^{2.n} k \geqslant 10^5$.
Résolvez $2.\sum_{k=n}^{2.n} k^3 \geqslant 15.\sum_{k=0}^{n^2} k$.

$\sum_{k=n+1}^{2.n} k \geqslant 10^5$ est la somme des termes d'une suite arithmétique.
Il y a n termes, et la moyenne des extrêmes vaut $\frac{2.n+n+1}{2}$.

Si vous préférez : $\sum_{k=n+1}^{2.n} k = \sum_{k=0}^{2.n} k - \sum_{k=0}^{n} k = \frac{2.n.(2.n+1)}{2} - \frac{n.(n+1)}{2}$.
Sinon j'ai aussi : $\sum_{k=n+1}^{2.n} k = \sum_{p=1}^{n} (p+n) = \sum_{p=1}^{n} p + \sum_{p=1}^{n} n = \frac{n.(n+1)}{2} + n.n$.

On résout donc $\frac{n.(3.n+1)}{2} \geqslant 10^5$ soit encore $3.n^2 + n - 2.10^5 \geqslant 0$.
On trouve deux racines de signe opposé. Par cohérence, on va demander d'être plus grand que la racine positive : $n \geqslant \frac{-1+\sqrt{1+24.10^5}}{6}$.
Il faut et suffit que n dépasse 258, *poussieres*. On n'y peut rien : $\boxed{S = [259,\ +\infty[}$

Vérification pythonienne : $\sum_{k=258}^{2.258} k = 99\,975$ *et* $\sum_{k=259}^{2.259} k = 100\,751$.

Pour l'exercice suivant, on utilise encore les formules du cours :

$$2.\sum_{k=n}^{2.n} k^3 \geqslant 15.\sum_{k=0}^{n^2} k \Leftrightarrow 2.\Big(\frac{2.n.(2.n+1)}{2}\Big)^2 - 2.\Big(\frac{n.(n+1)}{2}\Big)^2 \geqslant 15.\frac{n^2.(n^2+1)}{2}$$

On note qu'on a des polynômes de degré 4 de chaque côté. Mais les termes en n^4 se simplifient.

Tous calculs faits : $9.n^3 - 6.n^2 \geqslant 0$.

C'est vrai dès le rang 1 ! Trop fort.

∘16∘ ♡ Montrez que $\Big(2.\sqrt{n} - \sum_{k=1}^{n} \frac{1}{\sqrt{k}}\Big)$ et $\Big(2.\sqrt{n+1} - \sum_{k=1}^{n} \frac{1}{\sqrt{k}}\Big)$ sont adjacentes.
Couple de suites adjacentes : l'une croit, l'autre décroit, celle qui décroit majore celle qui croit, et la différence tend vers 0.

On pose $A_n = 2.\sqrt{n} - \sum_{k=1}^{n} \frac{1}{\sqrt{k}}$ et $B_n = 2.\sqrt{n+1} - \sum_{k=1}^{n} \frac{1}{\sqrt{k}}$.
Il est évident que $B_n$majore A_n.
Les autres calculs sont plus lourds, mais pas tant que ça :

$$A_{n+1} - A_n = 2.\sqrt{n+1} - 2.\sqrt{n} - \frac{1}{\sqrt{n+1}}$$

(le $\frac{1}{\sqrt{n+1}}$ est ce qu'il reste après simplification des sommes. On conjugue :

$$A_{n+1} - A_n = 2.\frac{n+1-n}{\sqrt{n+1}+\sqrt{n}} - \frac{1}{\sqrt{n+1}} = \frac{2}{\sqrt{n+1}+\sqrt{n}} - \frac{2}{\sqrt{n+1}+\sqrt{n+1}}$$

Je suis sûr que là, certains trouvent jolie la transformation de $\frac{1}{\sqrt{n+1}}$ en $\frac{2}{\sqrt{n+1}+\sqrt{n+1}}$. Elle est évidente, mais jolie.
Sous cette forme, $A_{n+1} - A_n$ est positif, puisque le second dénominateur est plus grand que le premier.

Pour B_n on fait de même : $B_{n+1} - B_n = 2.\sqrt{n+2} - 2.\sqrt{n+1} - \frac{1}{\sqrt{n+1}}$ et le travail est du même type. (B_n) est décroissante.

Évidemment aussi, la différence $B_n - A_n$tend vers 0 quand n tend vers l'infini, encore et toujours en écrivant $\sqrt{n+1} - \sqrt{n} = \frac{1}{\sqrt{n+1}+\sqrt{n}}$.

Remarque | *Le programme de mathématiques de première année a cet avantage d'être fait de jolies idées, de petits outils comme la conjugaison. Plus évidemment des définitions.*
En Spé, vous aurez d'avantage de théorèmes.

◦17◦

On note S^+ l'ensemble des matrices symétriques de taille 2 (c'est à dire de la forme $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$) dont la trace et le déterminant sont strictement positifs.
Montrez que S^+ est stable par addition.
Est il stable par multiplication ? Contient il I_2 ? Est il stable par passage à l'inverse ?
On définit la relation $\blacktriangleleft$ par $\forall (A,B) \in (S^+)^2,\ (A \blacktriangleleft B) \Leftrightarrow (B - A \in S^+)$.
Montrez que c'est une relation d'ordre (réflexive antisymétrique et transitive).
Cet ordre est il total (deux matrices prises au hasard sont elles forcément comparables, ou bien peut on n'avoir ni $A \blacktriangleleft B$ ni $B \blacktriangleleft A$) ?
Existe-t-il une matrice de S^+ plus petite que toutes les autres ?
Et si on travaille parmi les matrices de S^+ à coefficients entiers ?

◦18◦

On se place dans $(\mathbb{R}^3, +, .)$ muni de la base canonique orthonormée $(\overrightarrow{i},\ \overrightarrow{j},\ \overrightarrow{k})$.
Pour tout triplet de vecteurs $(\overrightarrow{u_1},\ \overrightarrow{u_2},\ \overrightarrow{u_3})$, on définit la matrice G (dite « matrice de Gram ») de terme général $g_i^k = \overrightarrow{v_i}.\overrightarrow{v_k}$ (produit scalaire des deux vecteurs) : $\begin{pmatrix} ||\overrightarrow{u_1}||^2 & \overrightarrow{u_1}.\overrightarrow{u_2} & \overrightarrow{u_1}.\overrightarrow{u_3} \\ \overrightarrow{u_1}.\overrightarrow{u_2} & ||\overrightarrow{u_2}||^2 & \overrightarrow{u_2}.\overrightarrow{u_3} \\ \overrightarrow{u_1}.\overrightarrow{u_3} & \overrightarrow{u_2}.\overrightarrow{u_3} & ||\overrightarrow{u_3}||^2 \end{pmatrix}$
Montrez : $Tr(G) \geqslant 0$ et $Tr(Com(G)) \geqslant 0$.
Montrez aussi $Tr(Com(G))$ est nulle si et seulement si les trois vecteurs sont colinéaires.

La trace de la matrice de Gram G est la somme $||\overrightarrow{u_1}||^2 + ||\overrightarrow{u_2}||^2 + ||\overrightarrow{u_3}||^2$.
En tant que somme de carrés de normes, elle est positive.

Chaque coefficient de la diagonale de la comatrice est un déterminant de la forme $\begin{vmatrix} ||\overrightarrow{u_1}||^2 & \overrightarrow{u_1}.\overrightarrow{u_2} \\ \overrightarrow{u_1}.\overrightarrow{u_2} & ||\overrightarrow{u_2}||^2 \end{vmatrix}$ (en variant les indices).
Un tel déterminant vaut $(||\overrightarrow{u_1}|| \times ||\overrightarrow{u_2}||)^2 - (\overrightarrow{u_1}.\overrightarrow{u_2})^2$.
Et l'inégalité de Cauchy-Schwarz nous dit : $(\overrightarrow{u_1}.\overrightarrow{u_2})^2 \leqslant ||\overrightarrow{u_1}||^2.||\overrightarrow{u_2}||^2$.
C'est l'inégalité de la forme $(x.x' + y.y' + z.z')^2 \leqslant (x^2 + y^2 + z^2).(x'^2 + y'^2 + z'^2)$.

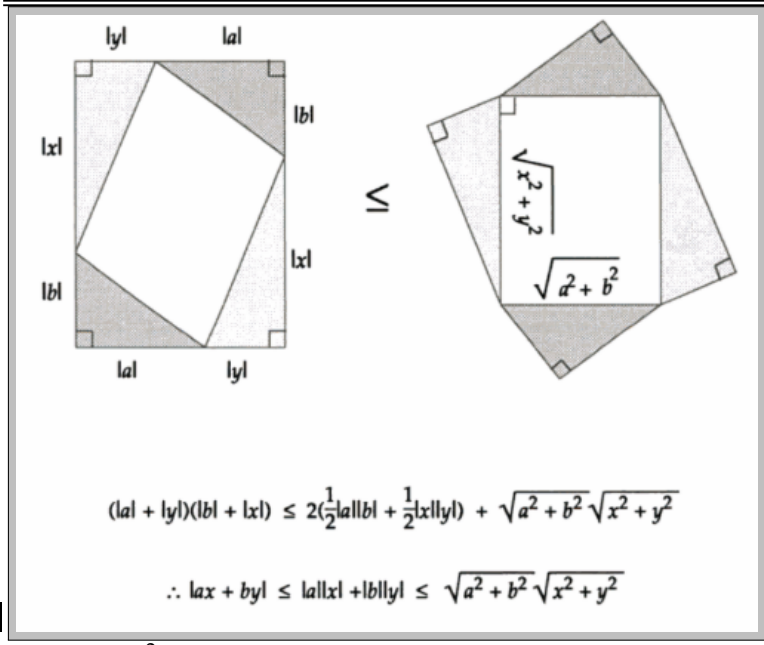
On somme ces trois termes positifs ou nuls, on obtient un réel positif ou nul.
Sinon, il suffit d'écrire $\overrightarrow{u}.\overrightarrow{v} = ||\overrightarrow{u}||.||\overrightarrow{v}||.\cos(angle)$ pour conclure aussi géométriquement.

◦19◦

Un explorateur prétend être allé dans un pays étrange où il y a des chats noirs et des chats blancs. Les chats sont des animaux très propres qui passent leur temps à se laver ou même à laver les autres *(j'ai d'abord voulu raconter ça avec des bonobos, mais je ne savais plus trop ce qu'ils faisaient)*. Chaque chat dispose de la liste des chats qu'il peut laver *(lui même peut ou non en faire partie)*. Quelle que soit la liste à laquelle vous pensez, il y a un chat dont c'est la lave-liste *(pas love-list...)*. Il y a donc un chat "sale" qui ne lave personne. Tiens, existe-t-il un chat qui ne lave que lui même ? Deux chats différents ont des listes différentes. Un chat qui se lave lui même est forcément blanc. Un chat qui ne se lave pas lui même est forcément noir..
De quelle couleur est le chat qui ne lave que les chats noirs ?

Normalement, on aboutit à un paradoxe.

◦20◦ Si f (dérivable) se décompose en $p+i$ avec p paire et i impaire, peut on affirmer que p et i sont dérivables.
Qui est alors la partie paire de f' et qui est sa partie impaire ?



Comparez
$2.\Big(\sum_{i\leqslant n} a_i.b_i\Big)^2 + \sum_{\substack{i\leqslant n\\ j\leqslant n}}(a_i.b_j - a_j.b_i)^2$
et $\Big(\sum_{i\leqslant n}(a_i)^2\Big).\Big(\sum_{j\leqslant n}(b_j)^2\Big)$.
Retrouvez l'inégalité de Cauchy-Schwarz.

◦21◦ Montrez :
$a.\cos(t) + b.\sin(t) \leqslant \sqrt{a^2+b^2}$.

$2.\Big(\sum_{i\leqslant n} a_i.b_i\Big)^2 = 2.\Big(\sum_{i\leqslant n} a_i.b_i\Big).\Big(\sum_{j\leqslant n} a_j.b_j\Big)$

$2.\Big(\sum_{i\leqslant n} a_i.b_i\Big)^2 = 2.\Big(\sum_{\substack{i\leqslant n\\ j\leqslant n}} a_i.b_i.a_j.b_j\Big)$ (chacun rencontre chacun)

de même $\sum_{\substack{i\leqslant n\\ j\leqslant n}}(a_i.b_j - a_j.b_i)^2 = \sum_{\substack{i\leqslant n\\ j\leqslant n}}(a_i.b_j)^2 + \sum_{\substack{i\leqslant n\\ j\leqslant n}}(a_j.b_i)^2 - 2.\sum_{\substack{i\leqslant n\\ j\leqslant n}} a_i.b_j.a_j.b_i$

Le terme $\sum_{\substack{i\leqslant n\\ j\leqslant n}} a_i.b_i.a_j.b_j$ et le terme $\sum_{\substack{i\leqslant n\\ j\leqslant n}} a_i.b_j.a_j.b_i$ sont égaux.

On somme $2.\Big(\sum_{i\leqslant n} a_i.b_i\Big)^2 + \sum_{\substack{i\leqslant n\\ j\leqslant n}}(a_i.b_j - a_j.b_i)^2 = \sum_{\substack{i\leqslant n\\ j\leqslant n}}(a_i.b_j)^2 + \sum_{\substack{i\leqslant n\\ j\leqslant n}}(a_j.b_i)^2$.

Les deux termes de droite sont égaux (variables muettes).

$2.\Big(\sum_{i\leqslant n} a_i.b_i\Big)^2 + \sum_{\substack{i\leqslant n\\ j\leqslant n}}(a_i.b_j - a_j.b_i)^2 = 2.\sum_{\substack{i\leqslant n\\ j\leqslant n}}(a_i.b_j)^2$

De plus, les variables i et j jouent des rôles indépendants : $\sum_{\substack{i\leqslant n\\ j\leqslant n}}(a_i)^2.(b_j)^2 = \Big(\sum_{i\leqslant n}(a_i)^2\Big).\Big(\sum_{j\leqslant n}(b_j)^2\Big)$.

$$2.\Big(\sum_{i\leqslant n} a_i.b_i\Big)^2 + \sum_{\substack{i\leqslant n\\ j\leqslant n}}(a_i.b_j - a_j.b_i)^2 = 2.\Big(\sum_{i\leqslant n}(a_i)^2\Big).\Big(\sum_{j\leqslant n}(b_j)^2\Big)$$

On arrange pour partir en direction de l'inégalité de Cauchy-Schwarz :

$$\frac{1}{2}.\sum_{\substack{i\leqslant n\\ j\leqslant n}}(a_i.b_j - a_j.b_i)^2 = \Big(\sum_{i\leqslant n}(a_i)^2\Big).\Big(\sum_{j\leqslant n}(b_j)^2\Big) - \Big(\sum_{i\leqslant n} a_i.b_i\Big)^2$$

Une somme de carrés de réels, c'est positif :

$$0 \leqslant \Big(\sum_{i\leqslant n}(a_i)^2\Big).\Big(\sum_{j\leqslant n}(b_j)^2\Big) - \Big(\sum_{i\leqslant n} a_i.b_i\Big)^2$$

et donc finalement

$$\Big(\sum_{i\leqslant n} a_i.b_i\Big)^2 \leqslant \Big(\sum_{i\leqslant n}(a_i)^2\Big).\Big(\sum_{j\leqslant n}(b_j)^2\Big)$$

C'est beau, mais c'est moins beau que la méthode avec un discriminant...

$a.\cos(t)+b.\sin(t)\leqslant\sqrt{a^2+b^2}$ provient de la forme $\sqrt{a^2+b^2}.\cos(t-\varphi)$ avec φ bien choisi.
Mais c'est aussi l'inégalité de Cauchy-Schwarz entre les deux vecteurs $\begin{pmatrix} a \\ b \end{pmatrix}$ et $\begin{pmatrix} \cos(t) \\ \sin(t) \end{pmatrix}$ de normes respectives $\sqrt{a^2+b^2}$ et 1.

◦22◦ Soient a, b, c et d quatre réels. Montrez : $(a^5+b^5+c^5+d^5)^2\leqslant(a^4+b^4+c^4+d^4).(a^6+b^6+c^6+d^6)$.

Inégalité de Cauchy Schwarz entre les deux vecteurs $\begin{pmatrix} a^2 \\ b^2 \\ c^2 \\ d^2 \end{pmatrix}$ et $\begin{pmatrix} a^3 \\ b^3 \\ c^3 \\ d^3 \end{pmatrix}$ de normes $\sqrt{a^4+b^4+c^4+d^4}$ et $\sqrt{a^6+b^6+c^6+d^6}$ et de produit scalaire $a^5+b^5+c^5+d^5$.

◦23◦ Montrez : $\int_0^1|\ln(t)|^n.dt=n!$ pour tout entier naturel n. Montrez alors $(n+m)!\leqslant\sqrt{(2.n)!.(2.m)!}$. Pouvez vous le prouver sans passer par les intégrales ?

On ne se préoccupera pas à notre niveau de l'existence de l'intégrale, même si en fait en 0, $\ln(t)$ « explose ».
On peut ensuite calculer la première (puissance 0) : $\int_0^1 1.dt=1$.

Et poursuivre (avec une récurrence sur n) en intégrant $\int_\varepsilon^1|\ln(t)|^{n+1}.dt$ par parties :

$(-\ln(t))^{n+1}$	$\hookrightarrow$	$(n+1).(-\ln(t))^n.\dfrac{-1}{t}$
1	$\hookleftarrow$	t

En effet, sur l'intervalle, $\ln(t)$ est négatif, et on remplace $|\ln(t)|$ directement par $-\ln(t)$ (ou pire par $\ln\left(\frac{1}{t}\right)$ dans certains livres).
On trouve

$$\int_\varepsilon^1|\ln(t)|^{n+1}.dt=\Big[(-1)^{n+1}.t.\ln(t)^{n+1}\Big]_{t=\varepsilon}^{t=1}+(n+1).\int_\varepsilon^1(-\ln(t))^n.dt$$

En 1, le logarithme du crochet $\Big[(-1)^{n+1}.t.\ln(t)^{n+1}\Big]_{t=\varepsilon}^{t=1}$ est nul.
Et quand ε tend vers 0 , la forme indéterminée $t.\ln(t)^{n+1}$ tend vers 0 [1].
Bref, sous réserve d'existence du membre de droite $\int_0^1|\ln(t)|^{n+1}.dt=(n+1).\int_0^1(-\ln(t))^n.dt$.

Dès lors, par récurrence sur n,chaque $\int_0^1(-\ln(t))^n.dt$ existe et vaut $n!$.

Remarque : C'est ce qui permet ensuite de définir par exemple $\left(\frac{1}{2}\right)!$ comme étant $\int_0^1\sqrt{|\ln(t)|}.dt$.

La majoration $(n+m)!\leqslant\sqrt{(2.n)!.(2.m)!}$ c'est l'inégalité de Cauchy-Schwarz. On rappelle :

$$\int_0^1 f(t).g(t).dt\leqslant\sqrt{\int_0^1\Big(f(t)\Big)^2.dt.\int_0^1\Big(g(t)\Big)^2.dt}$$

On prend $f=t\longmapsto|\ln(t)|^n$ et $g=t\longmapsto|\ln(t)|^m$, et c'est réglé.

On peut aussi tenter une preuve directe. On ne restreint pas la généralité en supposant $n\leqslant m$.
On étudie alors $\dfrac{(n+m)!}{(2.n)!}\times\dfrac{(n+m)!}{(2.m)!}$ en simplifiant les termes : $\dfrac{(2.n+1).(2.n+2)\dots(n+m)}{(n+m+1).(n+m+2)\dots(2.m)}$.
On compte qu'il y a autant de termes en haut qu'en bas (en l'occurrence $m-n$), et que chaque terme du haut est plus petit que chaque terme du bas.

Pour saisir : $\dfrac{(5+3)!}{(2.3)!}.\dfrac{(5+3)!}{(2.5)!}=\dfrac{8!}{6!}.\dfrac{8!}{10!}=7.8.\dfrac{1}{9.10}=\dfrac{7.8}{9.10}$.

Remarque : On verra que ceci revient à dire que la factorielle est « logarithmiquement convexe ». Et c'est une des clefs de cette application, qui permet de l'étendre de « $n!$ pour $n\in\mathbb{N}$ » à « $x!$ pour $x\in[0,\ +\infty[$ ».

1. changez de variable avec $T=\dfrac{1}{t}$ et vous retrouvez ce que vous connaissez bien

◦24◦ Montrez pour α et β réels positifs : $\alpha+\beta \geqslant 2.\sqrt{\alpha.\beta}$. Soient $[a_1,\dots a_n]$ et $[b_1,\dots b_n]$ deux listes de réels, on pose $A=\sum_{k=1}^{n}(a_k)^2$, $B=\sum_{k=1}^{n}(b_k)^2$ et $P=\sum_{k=1}^{n}a_k.b_k$ *(supposé non nul)*. Montrez : $\sum_{k=1}^{n}\Big(\frac{(a_k)^2.B}{P^2}+\frac{(b_k)^2}{B}\Big)\geqslant 2.\sum_{k=1}^{n}\frac{a_k.b_k}{P}$. Retrouvez l'inégalité de Cauchy-Schwarz.

La formule $\alpha+\beta\geqslant 2.\sqrt{\alpha.\beta}$ vient de $(\sqrt{\alpha}-\sqrt{\beta})^2\geqslant 0$. C'est direct et rapide.

Lourdeur : *Je suis prêt à parier que je vais voir passer des preuves qui commencent par $(\alpha+\beta)^2\geqslant 4.\alpha.\beta$ et $(\alpha+\beta)^2-4.\alpha.\beta=\dots=(\alpha-\beta)^2\geqslant 0$.*
C'est bon comme démonstration, mais ça tend à prouver que vous avez peur des racines carrées.

La formule $\sum_{k=1}^{n}\Big(\frac{(a_k)^2.B}{P^2}+\frac{(b_k)^2}{B}\Big)\geqslant 2.\sum_{k=1}^{n}\frac{a_k.b_k}{P}$ est juste une application de la question précédente avec $\alpha=\frac{(a_k)^2.B}{P^2}$ et $\beta=\frac{(b_k)^2}{B}$ puis bien sûr

$$\sqrt{\alpha.\beta}=\sqrt{\frac{(a_k)^2.B}{P^2}.\frac{(b_k)^2}{B}}=\sqrt{\frac{(a_k.b_k)^2}{P^2}}=\frac{|a_k.b_k|}{|P|}\geqslant\frac{a_k.b_k}{P}$$

Il ne reste qu'à sommer ces inégalités.

Remarque : *L'argument « nombres positifs » est à citer pour multiplier membre à membre des inégalités.*
Mais pour les sommer, on n'a besoin d'aucun contrôle sur les signes.
D'autre part, si vous écrire une égalité
$\sqrt{\alpha.\beta}=\sqrt{\frac{(a_k)^2.B}{P^2}.\frac{(b_k)^2}{B}}=\frac{a_k.b_k}{P}$*, c'est une erreur.*
Il reste un signe...

A présent, on peut calculer ces sommes *(et seulement seulement maintenant, n'allez pas trop vite en besogne [2]).*

Premier membre :
$$\sum_{k=1}^{n}\Big(\frac{(a_k)^2.B}{P^2}+\frac{(b_k)^2}{B}\Big)=\sum_{k=1}^{n}\frac{(a_k)^2.B}{P^2}+\sum_{k=1}^{n}\frac{(b_k)^2}{B}$$
$$\sum_{k=1}^{n}\Big(\frac{(a_k)^2.B}{P^2}+\frac{(b_k)^2}{B}\Big)=\frac{B}{P^2}.\sum_{k=1}^{n}(a_k)^2+\frac{1}{B}.\sum_{k=1}^{n}(b_k)^2$$
$$\sum_{k=1}^{n}\Big(\frac{(a_k)^2.B}{P^2}+\frac{(b_k)^2}{B}\Big)=\frac{B}{P^2}.A+\frac{1}{B}.B$$
$$\sum_{k=1}^{n}\Big(\frac{(a_k)^2.B}{P^2}+\frac{(b_k)^2}{B}\Big)=\frac{A.B}{P^2}+1$$

Second membre :
$$2.\sum_{k=1}^{n}\frac{a_k.b_k}{P}=\frac{2}{P}.\sum_{k=1}^{n}a_k.b_n$$
$$2.\sum_{k=1}^{n}\frac{a_k.b_k}{P}=\frac{2}{P}.P=2$$

On a donc obtenu : $\frac{A.B}{P^2}+1\geqslant 2$ soit encore $\frac{A.B}{P^2}\geqslant 1$ et $A.B\geqslant P^2$ *(car P^2 est positif)*.
On a donc classiquement

$$\Big(\sum_{k=1}^{n}(a_k)^2\Big)\Big(\sum_{k=1}^{n}(b_k)^2\Big)\geqslant\Big(\sum_{k=1}^{n}a_k.b_k\Big)^2$$

On a effectué cette démonstration en supposant le produit scalaire $P=\sum_{k=1}^{n}a_k.b_k$ non nul.
Mais s'il est nul, la majoration ultime $P^2\leqslant A.B$ est vraie aussi dans le cas $P=0$ puisque A et B sont positifs.

◦25◦ f est de classe C^2, nulle en a et b. Montrez
$\int_a^b(f'(t))^2.dt\Big)^2\leqslant\Big(\int_a^b f(t).f''(t).dt\Big)^2\leqslant\int_a^b(f(t))^2.dt.\int_a^b(f''(t))^2.dt.$

La majoration $\Big(\int_a^b f(t).f''(t).dt\Big)^2\leqslant\int_a^b(f(t))^2.dt.\int_a^b(f''(t))^2.dt$ est une inégalité de Cauchy-Schwarz sur les intégrales.

2. *trouver une inégalité est plus important que de calculer une somme, on est en maths*

Pour la minoration, on intègre $\int_a^b (f'(t))^2.dt$ par parties en intégrant f' dans un sens, et en le dérivant dans l'autre :

$$\int_a^b f(t).f''(t).dt = \Big[f(t).f'(t)\Big]_a^b - \int_a^b f(t).f''(t).dt$$

Or, l'énoncé dit que f est nulle en a et en b. Le crochet est nul.
Et le carré efface le signe moins.

◦26◦ Mettez sous la forme $t \longmapsto A.\cos(t-\varphi)$ la fonction $t \longmapsto a.\cos(t) + \sqrt{1-a^2}).\sin(t)$ sachant que a est un réel de $]-1,\ 1[$.

On pose $a = A.\cos(\varphi)$ et $\sqrt{1-a^2} = A.\sin(\varphi)$ pour pouvoir écrire $a.\cos(t) + \sqrt{1-a^2}).\sin(t) = A.\cos(t-\varphi)$.
On a très vite $A = 1$ et $\varphi = Arccos(a)$ *(à valeurs entre $-\pi/2$ et $\pi/2$, donc avec un sinus positif, c'est bon).*

◦27◦ Calculez $\dfrac{1}{2} + \sum_{k=1}^{n} ch(k.t)$ (noyau de Dir*hyp*chlet ?).

Ceci vaut $\dfrac{1}{2}.\Big(1 + \sum_{k=1}^{n}\Big(e^{k.t} + e^{-k.t}\Big)\Big)$

et on peut écrire $\dfrac{1}{2}.\Big(\sum_{k=0}^{0} e^{k.t} + \sum_{k=1}^{n} e^{k.t} + \sum_{k=-1}^{-n} e^{k.t}\Big)$ *(la première somme vaut 1).*

On replie agréablement en $\sum_{k=-n}^{n} e^{k.t}$.

On reconnaît une série géométrique $\dfrac{1}{2}.\dfrac{e^{-n.t} - e^{(n+1).t}}{1-e^t}$.

On l'écrit $\dfrac{1}{2}.\dfrac{e^{(n+1).t} - e^{-n.t}}{e^t - 1}$ et même $\dfrac{1}{2}.\dfrac{e^{(n+1).t} - e^{-n.t}}{e^t - 1}.\dfrac{e^{-t/2}}{e^{-t/2}}$.

On a finalement $\boxed{\dfrac{sh\Big(\dfrac{2.n+1}{2}.t\Big)}{2.sh\Big(\dfrac{t}{2}\Big)}}$

Le coup de

1	$+e^t$	$+e^{2.t}$	$+e^{3.t}$	$+\ldots$	$+e^{n.t}$
	$+e^{-t}$	$+e^{-2.t}$	$+e^{-3.t}$	$+\ldots$	$+e^{-n.t}$

qui devient

$e^{-n.t}+$	$\ldots$	$+e^{-3.t}$	$+e^{-2.t}$	$+e^{-t}$	$+1$	$+e^t$	$+e^{2.t}$	$+e^{3.t}$	$+\ldots$	$+e^{n.t}$	

est non seulement beau, mais aussi à connaître. Et à comprendre... visuellement.

◦28◦ ♡ On pose $H_n = \sum_{k=1}^{n} \dfrac{1}{k}$. Montrez : $\ln(n+1) \leqslant H_n \leqslant \ln(n) + 1$ par un argument intégral. Déduisez que H_n est équivalent à $\ln(n)$ quand n tend vers l'infini.
Que pouvez vous dire de $H_n = \sum_{k=1}^{n} \dfrac{1}{n}$?

Encadrez $H_{2.n} - H_n$ et montrez que cette quantité tend vers $\ln(2)$ quand n tend vers l'infini.
Quelle est la limite de $H_{3.n} - H_{2.n}$?

L'application $t \longmapsto \dfrac{1}{t}$ est décroissante sur $]0,\ +\infty[$.

Remarque :

- *Vrai :* $t \longmapsto \dfrac{1}{t}$ *est décroissante sur* $]0,\ +\infty[$.
- *Vrai :* $t \longmapsto \dfrac{1}{t}$ *est décroissante sur* $]-\infty,\ 0[$.
- *Vrai :* $t \longmapsto \dfrac{1}{t}$ *est décroissante sur* $]0,\ +\infty[$ *et sur* $]-\infty,\ 0[$.
- *Faux :* $t \longmapsto \dfrac{1}{t}$ *est décroissante sur* $]-\infty,\ 0[\cup]0,\ +\infty[$.

On se donne un entier naturel k.

Pour tout t de $[k-1,\ k]$, on a $\frac{1}{t} \geqslant \frac{1}{k}$. On intègre de $k-1$ à k : $\int_{k-1}^{k} \frac{1}{t}.dt \geqslant \int_{k-1}^{k} \frac{1}{k}.dt = \frac{1}{k}$.	Pour tout t de $[k,\ k+1]$, on a $\frac{1}{t} \leqslant \frac{1}{k}$. On intègre de k à $k+1$: $\int_{k}^{k+1} \frac{1}{t}.dt \leqslant \int_{k-1}^{k} \frac{1}{k}.dt = \frac{1}{k}$.
$\int_{k-1}^{k} \frac{dt}{t} \geqslant \frac{1}{k} \geqslant \int_{k}^{k+1} \frac{dt}{t}$	
$1+\ln(n) = 1+\int_1^n \frac{dt}{t} \geqslant 1+\sum_{k=2}^{n}\int_{k-1}^{k} \frac{dt}{t} \geqslant \sum_{k=2}^{n} \frac{1}{k}$	$\sum_{k=2}^{n} \frac{1}{k} \geqslant \sum_{k=1}^{n}\int_{k}^{k+1} \frac{dt}{t} = \int_1^{n+1} = \ln(n+1)$

Graphiquement, c'est un classique.

Il faut faire attention dans la minoration, de ne pas écrire $\sum_{k=2}^{n} \frac{1}{k} \leqslant \sum_{k=1}^{n}\int_{k-1}^{k} \frac{dt}{t} \leqslant \int_0^n \frac{dt}{t} = \ln(n) - \ln(0)$.

Voyez vous pourquoi ?

On repart de $\ln(n+1) \leqslant H_n \leqslant 1+\ln(n)$ et on divise par $\ln(n)$ (strictement positif) :

$$\frac{\ln(n+1)}{\ln(n)} \leqslant \frac{H_n}{\ln(n)} \leqslant 1+\frac{1}{\ln(n)}$$

et même

$$1+\frac{\ln(n+1)-\ln(n)}{\ln(n)} \leqslant \frac{H_n}{\ln(n)} \leqslant 1+\frac{1}{\ln(n)}$$

Dans le minorant, le terme $\frac{\ln(n+1)-\ln(n)}{\ln(n)}$ tend vers 0 (numérateur de limite nulle, dénominateur de limite infinie).

Par encadrement, $\frac{H_n}{\ln(n)}$ converge vers 1.

C'est la définition des suites équivalentes.

La somme $\sum_{k=1}^{n} \frac{1}{n}$ vaut 1 (nombre de termes tous égaux). Elle est croissante majorée. Elle converge, vers 1.

Première piste ratée :

$$\begin{array}{rccccc} & \ln(2.n+1) & \leqslant & H_{2.n} & \leqslant & 1+\ln(2.n) \\ & \ln(n+1) & \leqslant & H_n & \leqslant & 1+\ln(n) \\ \text{on soustrait} & \ln(2.n+1)-\ln(n) & \leqslant & H_{2.n}-H_n & \leqslant & \ln(2.n)-\ln(n) \end{array}$$

Ca semble bien marcher, le minorant $\ln\left(\frac{2.n+1}{n+1}\right)$ converge vers $\ln(2)$ comme le majorant.

On peut conclure par le théorème des gendarmes.

Et les gendarmes vous foutent en prison pour avir soustrait des inégalités, comme

2	$\leqslant$	3	$\leqslant$	4
1	$\leqslant$	3	$\leqslant$	5
$2-1$	$\leqslant$	$3-3$	$\leqslant$	$4-5$

c'est fou, non ?

Seconde piste ratée quand même aussi :

$$\begin{array}{rccccc} & \ln(2.n+1) & \leqslant & H_{2.n} & \leqslant & 1+\ln(2.n) \\ \text{on renverse} & -1-\ln(n) & \leqslant & -H_n & \leqslant & \ln(n+1) \\ \text{on somme} & \ln(2.n+1)-1-\ln(n) & \leqslant & H_{2.n}-H_n & \leqslant & 1+\ln(2.n)-\ln(n+1) \end{array}$$

Les deux encadrants n'ont pas la même limite. Pas de conclusion.

Et pourtant, combien d'élèves voit on aux concours affirmer :

en combinant $\ln(2.n+1) \leqslant H_{2.n} \leqslant 1+\ln(2.n)$ et $\ln(n+1) \leqslant H_n \leqslant 1+\ln(n)$ on arrive au résultat en question.

Trosième piste réussie. On reprend l'encadrement $\int_{k}^{k+1} \frac{dt}{t} \leqslant \frac{1}{k} \leqslant \int_{k-1}^{k} \frac{dt}{t}$ et on somme de $n+1$ à $2.n$.

On met les intégrales bout à bout par relation de Chasles : $\int_{n+1}^{2.n+1} \frac{dt}{t} \leqslant \sum_{k=n+1}^{2.n} \frac{1}{k} \leqslant \int_{n}^{2.n} \frac{dt}{d}$.

On calcule les intégrales : $\ln\left(\frac{2.n+1}{n+1}\right) \leqslant H_{2.n}-H_n \leqslant \ln(2)$.

Cette fois, le théorème d'encadrement donne l'existence d'une limite, et la limite.

◦29◦

z est un complexe plus petit que 1 en module.

Montrez : $\frac{1}{1-z} = \sum_{k=0}^{+\infty} z^k$. Montrez $\sum_{p=1}^{+\infty} \frac{z^p}{1-z^{2.p}} = \sum_{q=0}^{+\infty} \frac{z^{2.q+1}}{1-z^{2.q+1}}$.

Approche séries : on s'arrête à horizon fini, puis ont fait tendre cet horizon vers l'infini.

$$\sum_{n=0}^{N} z^n = \frac{1-z^{N+1}}{1-z}$$

(puisque z a un module plus petit que 1*, il ne peut pas valoir* 1*).*
Le terme z^{N+1} a pour module $|z|^{N+1}$. Il tend vers 0 quand N tend vers l'infini.
Finalement $1+z+z^2+\ldots+z^N$ tend vers $\frac{1}{1-z}$.
Et abusivement $1+z+z^2+\ldots+z^N+\ldots=\frac{1}{1-z}$.
Et toutes les maths sont dans le deuxième lot de « trois petits points », là où l'infini survient, qui est tout sauf intuitif mais absurde « N grand » ou même « très grand ».

Approche familles sommables.
On considère une somme indexée par $\mathbb{N}$. On prend une partie finie J de $\mathbb{N}$;
On veut majorer $\sum_{n\in J} |z^n|$ *(somme des modules pour raisonner « au pire »).*
On note N le plus grand élément de l'ensemble fini J, alors comme on ne fait que sommer des termes positifs :

$$\sum_{n\in J} |z^n| \leqslant \sum_{n=0}^{N} |z^n| = \sum_{n=0}^{N} |z|^n = \frac{1-|z|^{N+1}}{1-|z|} \leqslant \frac{1}{1-|z|}$$

On a donc $\left\{ \sum_{n\in J} \mid J \textit{ partie finie de } \mathbb{N} \right\}$ qui est majoré. La famille est sommable.
On calcule alors la somme par la méthode « série numérique ».

Si z est de module plus petit que 1 (strictement évidemment), il en est de même de chaque $z^{2.p}$.
On peut remplacer : $\sum_{p=1}^{+\infty} \frac{z^p}{1-z^{2.p}} = \sum_{p=1}^{+\infty} \left(z^p . \sum_{n=1}^{+\infty} (z^{2.p})^n \right)$ *(en prenant bien une variable nouvelle n différente de p).*

On distribue

$$\sum_{p=1}^{+\infty} \frac{z^p}{1-z^{2.p}} = \sum_{p=1}^{+\infty} \left(\sum_{n=0}^{+\infty} z^p . (z^{2.p})^n \right) = \sum_{p=1}^{+\infty} \left(\sum_{n=0}^{+\infty} z^{p.(2;n+1)} \right)$$

Formellement, on permute les sommes *(variables indépendantes, sommation en rectangle et pas en triangle)* :

$$\sum_{p=1}^{+\infty} \frac{z^p}{1-z^{2.p}} = \sum_{p=1}^{+\infty} \left(\sum_{n=0}^{+\infty} z^p . (z^{2.p})^n \right) = \sum_{n=0}^{+\infty} \left(\sum_{p=1}^{+\infty} z^{p.(2.n+1)} \right)$$

Chaque somme $\sum_{p=1}^{+\infty} z^{p.(2;n+1)}$ est une somme de série géométrique du type $\sum_{p=1}^{+\infty} t^p = \frac{t}{1-t}$ *(car on commence à* 1*).*
On a donc

$$\sum_{p=1}^{+\infty} \frac{z^p}{1-z^{2.p}} = \sum_{n=0}^{+\infty} \frac{z^{2;n+1}\Big)}{1-z^{2.n+1}}$$

C'est la formule demandée *(étape purement calculatoire, totalement exigible de tous les élèves de MPSI, même ceux se destinant à PSI).*

Il faut quand même justifier l'interversion des sommes en montrant que la grande famille à double indice est sommable : $\sum_{\substack{1\leqslant p\\ 0\leqslant n}} z^{p.(2.n+1)}$. [3]

La consigne est de regarder « au pire » la somme des modules $\sum_{\substack{1\leqslant p\\ 0\leqslant n}} |z|^{p.(2.n+1)}$.

Il faut majorer $\sum_{(n,p\in J} z^{p.(2.n+1)}$ quand J décrit l'ensemble des parties finies de $\mathbb{N}^* \times \mathbb{N}$.
Mais toute partie finie est incluse dans un rectangle $[1,\ P] \times [0,\ N]$, et comme les termes additionnés sont positifs :

$$\sum_{(n,p\in J} |z|^{p.(2.n+1)} \leqslant \sum_{\substack{1\leqslant p\leqslant P\\ 0\leqslant n\leqslant N}} |z|^{p.(2.n+1)}$$

3. étape exigible des élèves de MPSI se destinant à MP et même à PSI, mais non exigible de leurs futurs profs des matières autres que les maths

On somme par tranche $\sum_{(n,p\in J} |z|^{p.(2.n+1)} \leqslant \sum_{n=0}^{N} \Big(\sum_{p=1}^{P} |z|^{p.(2.n+1)} \Big)$

On effectue : $\sum_{(n,p\in J} |z|^{p.(2.n+1)} \leqslant \sum_{n=0}^{N} \Big(\frac{|z|^{2.n+1} - |z|^{(P+1).(2.n+1)}}{1-|z|^{2.n+1}} \Big)$

On majore : $\sum_{(n,p\in J} |z|^{p.(2.n+1)} \leqslant \sum_{n=0}^{N} \Big(\frac{|z|^{2.n+1}}{1-|z|^{2.n+1}} \Big)$

On majore encore : $\sum_{(n,p\in J} |z|^{p.(2.n+1)} \leqslant \sum_{n=0}^{N} \Big(\frac{|z|^{2.n+1}}{1-|z|} \Big)$ car $|z|^{2.n+1} \leqslant |z| < 1$.

On sort la constante : $\sum_{(n,p\in J} |z|^{p.(2.n+1)} \leqslant \frac{1}{1-|z|} . \sum_{n=0}^{N} |z|^{2.n+1}$.

On calcule la somme : $\sum_{(n,p\in J} |z|^{p.(2.n+1)} \leqslant \frac{1}{1-|z|} . \frac{|z| - |z|^{2.N+3}}{1-|z|^2}$.

On majore encore : $\sum_{(n,p\in J} |z|^{p.(2.n+1)} \leqslant \frac{1}{1-|z|} . \frac{|z|}{1-|z|^2}$.

La majorant ne dépend plus de N ni de P (donc plus de J).

L'ensemble $\Big\{ \sum_{(n,p)\in J} |z^{p.(2.n+1)}| \; | \; J \; partie \; finie \; de \; \mathbb{N}^* \times \mathbb{N} \Big\}$ est majoré.

La famille est sommable.

∘30∘

♡ Guillaume et Clément doivent vider un tonneau de cent litres. Guillaume le vide avec un broc de trois litres et Clément avec un broc de deux litres. Ils l'ont vidé en trente cinq brocs. Combien chacun ?

♣ Guillaume dispose de deux mèches qui brulent chacune en une heure *(mais pas de façon uniforme, on ne peut pas dire "*tiens, le quart a brulé, il s'est écoulé quinze minutes*")*. Quelles sont les durées qu'il peut mesurer avec ces mèches :
une heure en en brulant une, deux heures en en brulant une puis l'autre, une demi heure en en brulant une par les deux bouts. Mais encore ?
Et avec trois mèches ? Et peut on les brûler dans votre camp ?
L'exercice peut être prolongé par la lecture d'un article de Delahaye dans Pour la Science sur les « nombres combustibles ».

Notons G le nombre de brocs vidés par Guillaume et C le nombre de brocs vidés par Clément.

On a alors le simple système $\begin{array}{ccccc} G & + & C & = & 35 \\ 3.G & + & 2.C & = & 100 \end{array}$ qu'on résout.

On trouve heureusement une solution entière.

Solution de matheux	Mais il y a plus simple : s'ils avaient eu chacun un broc de deux litres, en trente cinq brocs ils auraient vidé 70 litres. Comme ils ont vidé trente litres de plus, c'est que Guillaume a fait trente fois « un litre de plus ». Guillaume a donc transvasé 30 brocs. Ce flemmard de Clément 5.Total : $30 \times 3 + 5 \times 2 = 100$. Pour moi, les maths, c'est ça. Sinon, c'est ce que j'appelle de la mauvaise physique, c'est à dire de la mise en équation sans chercher à saisir l'essence des choses. Et pour moi, la vraie physique, c'est le même raisonnement que les maths, sans système.

durée	méthode
une heure	• brûler une mèche
deux heures	• brûler une mèche, puis la suivante
une demi heure	• brûler une mèche mais allumée à chaque bout, elle brûle deux fois plus vite
une heure et demi	• brûler une mèche normalement • allumer ensuite l'autre aux deux bouts
trois quarts d'heure	• allumer une mèche aux deux bouts • mais allumer l'autre en même temps à un de ses bouts quand la première a fini de bruler, il s'est écoulé une demi heure • allumer alors l'autre bout de la mèche à demi consumée elle devait encore brûler une demi heure, elle va se consumer en un quart d'heure

Il y a un article complet de Jean-Paul Delahaye dans Pour la Science sur les nombres dits « combustibles » qui peuvent s'obtenir sous cette forme.

◦31◦ Soit σ une application injective de $\mathbb{N}$ dans $\mathbb{N}$. Montrez par l'absurde que $\{n \in \mathbb{N} \mid \sigma(n) \geqslant n\}$ est infini.
Pouvez vous trouver σ telle que $\{n \in \mathbb{N} \mid \sigma(n) \geqslant n\}$ soit égal à $\mathbb{N}$?
Pouvez vous trouver σ telle que $\{n \in \mathbb{N} \mid \sigma(n) \geqslant n\}$ soit égal à $\mathbb{N}^*$?
Pouvez vous trouver σ telle que $\{n \in \mathbb{N} \mid \sigma(n) \geqslant n\}$ soit égal à $2.\mathbb{N}$?

◦32◦ On va démontrer de plusieurs façons que l'ensemble $\mathbb{P}$ des nombres premiers est infini dans $\mathbb{N}$.

Toutes ces démonstrations vont être un peu sur le même principe :
chaque fois qu'on a des nombres premiers, on en trouve un nouveau.
On va donc en avoir autant qu'on veut, donc une infinité.

Mais le mieux sera à chaque fois de faire un raisonnement par l'absurde :
si il y en a un nombre fini, alors on prend « le plus grand » ou « le plus possible de nombres premiers » ; on en construit un nouyveau, et on a une contradiction.

♡ 0 ♡ On suppose que l'ensemble des nombres premiers est fini, formé de N entiers $\{p_1, \dots p_N\}$. On pose alors $Q = 1 + \prod_{n=1}^{N} p_n$. Montrez que cet entier admet au moins un diviseur premier q. Montrez que q n'est aucun des p_i.

Le nombre Q est un entier (produit et somme d'entiers). Et il est plus grand que 1.
Comme tout entier plus grand que 1, il a au moins un diviseur premier.

Principe : si le nobre est premier, c'est bon. Sinon, par définition de « non premier », il se déceompose en $Q = q_1.q_2$ avec $1 < q_1 < Q$ et $1 < q_1 < Q$.
On recommence avec q_1 qui est soit premier, soit divisible.
Par descente infinie, on s'arrêtera sur un entier qui sera alors un nombre premier.

Variante par récurrence forte.
2 admet un facteur premier.
Supposons pour un n donné que tous les entiers de 2 à n se décomposent.
On considère $n + 1$. Si il est premier, c'est bon, il admet lui même comme facetru premier.
Sinon, il se décompose en deux entiers entre 2 et n qui admettent chacun au moins un facteur premier.

Notons q un diviseur premier de Q.

Si q était l'un des p_i, il diviserait Q mais il diviserait aussi $\prod_{n=1}^{N} p_n$ (en étant un des facteurs du produit).

Mais alors il diviserait la différence $Q - \prod_{n=1}^{N} p_n$.

Et un nombre premier ne peut pas diviser 1.

Le diviseur premier est donc un nouveau nombre premier.

♡ 1 ♡ Concluez.

On suppose par l'absurde qu'il n'y a qu'un nombre fini de nombres premiers. On les prend tous et on en construit

le « produit plus un » appelé Q.
On extrait un facteur premier.
Et on a un nouveau nombre premier, ce qui contredit le fait de les avoir tous pris.

On peut même profiter de cette idée pour construire de proche en proche une liste de nombres premiers.
On part de 2.
On le met dans un produit où il est seul, on ajoute 1. On a 3. C'est un nombre premier.
On prend 2 et 7, on construit $2.3+1$. C'est un nouveau nombre premier.
On regarde alors $2.3.7+1$. C'est 45. Il est premier.
On considère alors $2.3.7.43+1$. Il vaut 1807 et n'est pas premier. Son plus petit facteur premier est 13.
On continue avec $2.3.7.43.13+1$ et ainsi de suite.

Programmation. On crée une procédure qui cherche le plus petit facteur premier d'un entier.

```
def facteur(N) :
....for k in range(2, N+1) : #la dernière possibilité sera Q lui même
........if (N%k) == 0 :
............return k #on a un facteur
```

Cet algorithme cherche le plus petit diviseur de Q. Et comme c'est le premier, il est justement premier.
Cet algorithme termine (par sortie brutale et pas jolie de boucle en cours d'exécution). Si le nombre Q est premier, c'est à la dernière étape qu'on retourne justement Q lui même.

```
L = [2] #car il y a un début à tout
P = 2 #le produit
for loop in range(10) :
....f = facteur (P+1)
....L.append(facteur(P+1))
....P *= f
```

Mais ça devient vite horrible :
[2, 3, 7, 43, 13, 53, 5, 6221671]

◇ 0 ◇ Pour tout n, on pose $F_n = 2^{2^n}+1$ (nombre de Fermat, à comprendre comme $2^{(2^n)}+1$). Calculez F_n pour n de 0 à 3.

0	1	2	3	4
3	5	17	257	65 537

◇ 1 ◇ Montrez pour tout n : $2+\prod_{k=0}^{n} F_k = F_{n+1}$.

On initialise une récurrence avec ce qui est écrit au dessus.

On se donne n et on suppose $2+\prod_{k=0}^{n} F_k = F_{n+1}$ et même

$$\prod_{k=0}^{n} F_k = F_{n+1}-2$$

On multiplie par F_{n+1} :

$$\prod_{k=0}^{n+1} F_k = (F_{n+1})^2 - 2.F_{n+1}$$

On ajoute 2 (et même $1+1$)

$$\prod_{k=0}^{n+1} F_k = (F_{n+1})^2 - 2.F_{n+1}+1+1 = (F_{n+1}-1)^2+1$$

On remplace par la définition

$$\prod_{k=0}^{n+1} F_k = (2^{(2^{n+1})})^2+1 = 2^{(2^{n+1}).2}+1 = 2^{(2^{n+2})}+1 = F_{n+2}$$

L'hérédité est achevée.

Une preuve directe est aussi possible, considérez par exemple $(1+z).(1+z^2).(1+z^4).(1+z^8)$.

$$\begin{array}{lccccc} & (1-z). & (1+z). & (1+z^2). & (1+z^4). & (1+z^8) \\ & = & (1-z^2). & (1+z^2). & (1+z^4). & (1+z^8) \\ \textit{Multipliez par } (1-z)\ : & = & & (1-z^4). & (1+z^4). & (1+z^8) \\ & = & & & (1-z^8). & (1+z^8) \\ & = & & & & (1-z^{16}) \end{array}$$

On a donc $(1+z).(1+z^2).(1+z^4)\dots(1+z^{2^n}) = \dfrac{1-z^{2^{n+1}}}{1-z}$.

Il ne reste plus qu'à prendre $z = 2$.

◇ 2 ◇ Déduisez que le seul diviseur commun de F_k et F_p pour k différent de p est égal à 1.

On se donne deux entiers p et k distincts.
Sans perte de généralité, on va supposer $k < p$.
On cherche alors à vérifier que le seul diviseur commun de F_p et $F_k$est égal à 1.
On prend donc un diviseur commun de F_p et F_k que l'on note d (objectif : $d = 1$.
Comme il divise F_k il divise $\prod_{n=0}^{p-1} F_n$ (c'est le k^{ieme} facteur du produit).
Il divise donc $F_p - 2$ par la formule précédente.
Mais comme il divise aussi F_p il divise la différence
d divise 2. d ne peut donc valoir que 1 ou 2.
Mais 2 n'est pas un diviseur de F_p ni de F_k puisque par construction, F_p et F_k sont premiers.
ne reste donc que la seule solution : $d = 1$.

◇ 3 ◇ Le raisonnement commence alors par « même si les F_i ne sont pas forcément premiers... » et se termine par « ...il y a donc une infinité de nombres premiers ». Complétez le.

Déjà, il y a une infinité de nombres de Fermat.
Et aucun n'a de facteur commun avec les autres.
Si il y avait un nombre fini de nombres premiers p_1 à p_N, il nous suffit de considérer les nombres de Fermat de F_0 à F_n (ça en fait $n+1$).
Chacun d'entre eux a un facteur premier.
On va associer à chacun son plus petit facteur premier : $F_k \longmapsto p_{i_k}$ pour i_k bien choisi.
Mais comme les F_k et F_p n'ont aucun facteur premier en commun, les indices i_k et i_p sont distincts.
On a donc une application injective de l'ensemble $\{F_0,\ F_1, \dots F_n\}$ dans l'ensemble des nombres premiers.
L'ensemble de départ a $n+1$ éléments et l'ensemble d'arrivée n'en a que n. C'est contradictoire avec l'injectivité.

Autre idée sans « par l'absurde » : à chaque F_kj'associe son plus petit facteur premier, je construis ainsi une infinité de nombres premiers.

n	0	1	2	3	4	5	6	
Fermat F_n	3	5	17	257	65 537	4 294 967 297	18 446 744 073 709 551 616	
plus petit facteur premier	3	5	17	257	65 537	641	274 177	

C'est Euler qui a montré que F_5 n'était pas premier.
Fermat avait crû à partir des premiers qu'il avait de quoi engendrer explicitement des nombres premiers.

♯ 0 ♯ Bonus : Écrivez un script qui détermine combien de F_k pour k de 0 à 6 sont premiers.

C'est visible au dessus.
Ensuite, F_7 vaut quand même 340 282 366 920 938 463 463 374 607 431 768 211 456

♠ 10 ♠ Soit p un nombre premier. On pose $N = 2^p - 1$ et on note q un facteur premier de N.

Exemples			
	$p = 5$	$N = 2^5 - 1$ est premier	$q = 2^5 - 1 = 31$
	$p = 7$	$N = 2^7 - 1$ est premier	$q = 2^7 - 1 = 127$
	$p = 11$	$N = 2^{11} - 1$ se factorise	$q = 23$ ou $q = 89$

Montrez : $2^p = 1\ [q]$ et $\forall n \in \mathbb{N},\ (n < p) \Rightarrow (2^n \neq 1\ [q])$ (il faudra penser à écrire une identité de Bézout entre n et p).

Comme q est un facteur de N, il divise N. On a donc $2^p - 1 = 0\ [q]$ et directement $2^p = 1\ [q]$.

Prenons ensuite un entier n et supposons le plus petit que p.
Comme p est premier, n et p sont premiers entre eux. Et l'ami Bézout nous dit qu'il existe deux entiers relatifs a et

b vérifiant $a.n + b.p = 1$.

On montre alors que 2^n ne peut pas valoir 1 modulo q.
Sinon on aurait $2^n = 1\ [q]$ puis $(2^n)^a = 1^a\ [q]$ (compatibilité des puissances avec les congruences [4]).

Comme on a déjà $2^p = 1\ [q]$, on a aussi $(2^p)^b = 1\ [q]$.

Par compatibilité, on multiplie les égalités membre à membre : $(2^n)^a.(2^p)^b = 1\ [q]$.
En développant les puissances, on aboutit à $2^{a.n+b.p} = 1\ [q]$ c'est à dire $2 = 1\ [q]$.
Quitte à pousser le bouchon jusqu'au bout, on a a alors $1 = 0\ [q]$ ce qui est contradictoire (rappelons que q est un facteur premier, il ne vaut pas 1).

♠ 11 ♠ On pose $A = \{1,\ 2, \dots q-1\}$ et on définit sur A la relation $\Re$ par $(a\Re b) \Leftrightarrow (\exists n \in \mathbb{N},\ a = 2^n.b\ [q])$. Montrez que c'est une relation d'équivalence sur A.

Réflexive.
On se donne a et on cherche n vérifiant $a = 2^n.a\ [q]$. Il suffit de prendre $n = 1$.

Symétrique.
On se donne a et b et on suppose que a est en relation avec b (il existe donc un entier n vérifiant $a = 2^n.b\ [q]$).
On cherche alors un (autre) entier m vérifiant $b = 2^m.a\ [q]$.

> *Bien sûr, si on écrit tout de manière formelle sans réfléchir et y voir de logique, on écrit $a.2^{-n} = 2^{-n}.2^n.b\ [q]$ et on dit « c'est bon avec $m = -n$ ». mais ceci n'a pas de sens. m est négatif.*
>
> *Si on garde ses réflexes de Terminable, on met des$+k.q$ partout à la place des congruences et ça devient indigeste.*

Mais on rappelle que l'on a $2^p = 1\ [q]$.
On propose alors $m = p - n$. On a alors $2^{p-n}.a = 2^{p-n}.2^b.b\ [q] = 2^p.b\ [q]$ et c'est fini.
L'idée était de déplacer avec p pour que soit positif (tout repose sur $1 = 2^p\ [q]$).

Ah, mais $p - n$ est peut être encore négatif ?
Bon, proprement, on écrit $n = p.d + r$ avec r entre 0 et $p - 1$ (division euclidienne).
On propose cette fois $m = (d+1).p - n$ et c'est bon, il est positif et les $2^{(d+1).p}$ s'en vont modulo q.

Transitive.
On se donne a, b et c. On suppose $a\Re b$ et aussi $b\Re c$.
On traduit : il existe n et m vérifiant $a = 2^n.b\ [q]$ et $b = 2^m.c\ [q]$.
On reporte : $a = 2^{n+m}.c\ [q]$. Et comme $n + m$ est un entier, on reconnaît $a\Re c$.

> *Comment perdre des points sur ces questions ?*
> *Les élèves qui ont vraiment du mal et regardent les définitions avec les yeux d'une poule qui trouve un couteau [5] écrivent toutes les définitions avec le même n : $a = 2^b.b\ [q]$ et $b = 2^n.c\ [q]$ et ainsi de suite.*
> *Sinon, il y a ceux qui rédigent n'importe comment, avec*
> *$\forall a,\ a\Re a \Leftrightarrow a = 2^0.a\ [q]$*
> *En écrivant ceci, ils disent juste « je connais la définition ». Mais ils ne prouvent pas $\forall a,\ a\Re a$. Ils prouvent une équivalence.*
> *Et cette équivalence pourrait tout aussi bien être $\forall a,\ a \neq a \Leftrightarrow a = e^a$, puisque ce serait ici Faux$\Leftrightarrow$Faux.*
> *Bâtir un raisonnement, ce n'est pas aligner des symboles mathématiques partout. Bien au contraire.*
> *C'est rédiger avec des mots, des idées, et surtout des variables qu'on introduit.*
> *Bref, on écrit sous forme « $\forall,\ \dots \Rightarrow \dots$ » ce qu'on doit prouver.*
> *Mais pour le prouver, on écrit « on prend... on suppose... on montre... ».*

♠ 12 ♠ Explicitez les six classes d'équivalence dans le cas $p = 5$.

p vaut 5, $2^p - 1$ vaut 31 et donc q vaut aussi 31.
On vérifie au passage $2^5 = 32 = 1\ [31]$.
Les puissances de 2 modulo 31 valent donc 1, 2, 4, 8 et 16.
Chaque entier a sera donc en relation avec a, $2.a$, $4.a$, $8.a$ et $16.a$. Et c'est tout.

4. y compris pour les exposants négatifs car q est premier
5. *expression populaire pour dire « sans comprendre »*

On peut donc découper et mettre ensemble 1, 2, 4, 8 et 16.
Ensuite, on prend un élément qu'on a pas encore pris : 3. On met dans sa classe 3, 6, 12, 24 et 48 (égal à 17).
Qui n'a pas encore été pris ? 5. Allez, c'est parti avec 5, 10, 20, 9 et 18.

1	2	4	8	16
3	6	12	24	17
5	10	20	9	18
7	14	28	25	19
11	22	13	26	21
15	30	29	27	23

Chaque élément est dans une classe et une seule. Et ils sont tous là.

♠ 13 ♠ Déterminez les deux classes d'équivalence pour p égal à 11 (avec le choix $q = 23$).

On a choisi $q = 23$ (qui divise bien $2^{11} - 1$.
On n'a que 22 éléments à répartir en classes d'équivalence.
Dans la classe de 1, on a les puissances de 2 (réduites modulo 23) :

1	2	4	8	13	32=9	18	36=13	26=3	6	12

et on a ensuite $2.12 = 24 = 1$, la liste se referme.

Il reste onze éléments à placer dans l'autre classe. On va la commencer par un élément pas encore pris : 5 (mais commencer par 10 ou 7 ne fera que déphaser la liste.

1	2	4	8	13	9	18	13	23	6	12
5	10	20	17	11	22	21	19	15	7	14

♠ 14 ♠ On revient au cas général pour p. Montrez qu'il y a p éléments dans chaque classe d'équivalence.

Dans la classe d'équivalence de l'élément a il y a tous les $2^n.a$ avec n entre 0 et $p - 1$.

♠ 15 ♠ Déduisez que p divise $q - 1$ puis que q est strictement plus grand que p.

On découpe A en classes d'équivalences. C'est une partition de A (chaque élément est dans une classe et une seule).
On dit qu'il y a k classe.
Mais comme chacun est de cardinal p, on déduit au final qu'il y a $k \times p$ éléments dans A.

Mais quel est le cardinal de A ? On commence à 1 et termine à $q - 1$. C'est donc $q - 1$.
On a donc $k \times p = q - 1$.

On note au passage que ceci donne $1 \times q - k \times p = 1$. C'est une identité de Bézout entre p et q.

On a $q = k.p + 1 > p + 1$. Il est donc plus grand que p.

♠ 16 ♠ Déduisez : $\forall p \in \mathbb{P},\ \exists q \in \mathbb{P},\ q > p$. Déduisez que $\mathbb{P}$ est infini.

Pour tout nombre premier p trouvé, il existe un nouveau nombre premier strictement plus grand que p.
On construit ainsi une suite strictement croissante d'entiers premiers (on peut commencer à 2).
Par croissance stricte, on a une infinité d'entiers premiers tous distincts.

Pratiquement, si on part de 2

p	$2^p - 1$	q nouveau nombre premier
2	3	3
3	7	7
7	127	127
127	170 141 183 460 469 231 731 687 303 715 884 105 727	euh...

♣ 1 ♣ Pour tout couple d'entiers relatifs $(a,\ b)$, on pose $N_{a,b} = \{a + n.b \mid n \in \mathbb{Z}\}$. Déterminez $N_{a,,0}$, $N_{a,1}$, $N_{0,2}$ et $N_{1,2}$.
Une partie A de $\mathbb{Z}$ est dite « ouverte » si $\forall a \in A,\ \exists b \in \mathbb{N}^*,\ N_{a,n} \subset A$.
Montrez que ce sont des ensembles ouverts : $\emptyset$ | $\mathbb{Z}$ | $2.\mathbb{Z}$

On mâchouille les définition :

$N_{a,0} = \{a\}$	$N_{a,1} = \mathbb{Z}$	$N_{0,2} = \{2.n \mid n \in \mathbb{Z}\} = 2.\mathbb{Z}$	$N_{1,2} = \{2.n + 1 \mid n \in \mathbb{Z}\} = 2.\mathbb{Z} + 1$

Remarque : $N_{a,1}$ est l'ensemble des $a + n$ et tout entier k s'écrit bien $a + n$ pour n bien choisi.
D'autre part, $N_{0,2} = N_{12,2} = N_{2024,2}$ et ainsi de suite. Le fait de démarrer à 2024 au lieu de 0 ne change rien, puisque n

décrit $\mathbb{Z}$.

L'ensemble vide répond à toute quantification commençant par $\forall a \in \emptyset, \ldots$.

Prenons a quelconque dans $\mathbb{Z}$, l'ensemble $N_{a,1}$ est égal à $\mathbb{Z}$ lui aussi, et est inclus dans $\mathbb{Z}$.

Prenons a dans $2.\mathbb{Z}$. L'ensemble $N_{a,2}$ est égal lui aussi à $2.\mathbb{Z}$. Il existe donc b (égal à 2) vérifiant $N_{a,b} \subset 2.\mathbb{Z}$.

♣ 2 ♣ Montrez que $\mathbb{P}$ n'est pas ouvert (qu'il soit fini ou non, ce n'est pas encore la question).

Être ouvert, c'est vérifier : $\forall a \in A,\ \exists b \in \mathbb{N}^*,\ N_{a,b} \subset A$.

Prouver $\mathbb{P}$ non ouvert, c'est prouver $\exists a \in \mathbb{P},\ \forall b \in \mathbb{N}^*,\ N_{a,b} \not\subset A$.
Et même plus précisément

$$\exists a \in \mathbb{P},\ \forall b \in \mathbb{N}^*,\ \exists n \in \mathbb{Z},\ a + n.b \notin \mathbb{P}$$

A nous de choisir a. Bon, on va prendre 2 car c'est un élément de $\mathbb{P}$ un peu à part (mais peut être que n'importe quel a conviendrait).
Ensuite, b est quelconque. Ce n'est pas à nous de le choisir.
En revanche, n a le droit de dépendre de a et b. Je prends $n = 2$. l'entier $a + 2.b$ est pair, plus grand que 2. Il n'est donc pas premier.

♣ 3 ♣ Montrez que tout ouvert non vide est infini.

On prend un ouvert non vide.
Lequel ? On ne sait pas justement, c'est « montrez que tout ouvert... ».
Quoi qu'il en soit, il contient au moins un élément a.
On applique à cet élément a la définition de « A est ouvert ».
Il existe b non nul tel que l'ensemble $N_{a,b}$ soit inclus dans A.
Mais comme b est non nul, $N_{a,b}$ est infini (faites varier n dans la formule $a + n.b$).
Et comme il est inclus dans A, A est aussi infini.

♣ 4 ♣ Montrez que si A et Ω sont ouverts, alors $A \cup \Omega$ et $A \cap \Omega$ sont ouverts.

On suppose donc deux choses :
• $\forall a \in A,\ \exists b_a \in \mathbb{N}^*,\ \forall n \in \mathbb{Z},\ a + n.b_a \in A$
◦ $\forall \alpha \in \Omega,\ \exists \beta_\alpha \in \mathbb{N}^*,\ \forall n \in \mathbb{Z},\ \alpha + n.\beta_\alpha \in \Omega$

> *Bien choisir les noms de variables c'est important. Mettre des noms différents pour des éléments pris au hasard dans des ensembles différents, c'est plus prudent.*
> *Indiquer qui dépend de qui, c'est aussi capital. Ici, b dépend de a. On l'appelle b_a. En revanche, n ne dépend de personne.*

On a un objectif double.

On commence par la réunion : a-t-on $\forall x \in A \cup \Omega,\ \exists y \in \mathbb{N}^*,\ \forall n \in \mathbb{Z},\ x + n.y \in A \cup \Omega$
On se donne x dans $A \cup \Omega$. On a deux possibilités : il est dans A ou bien il est dans Ω.
Si x est dans A, alors il existe b_x vérifiant $\forall n \in \mathbb{Z},\ x + n.b_x \in A$.
On déduit $\forall n \in \mathbb{Z},\ x + n.b_x \in A \cup \Omega$.

Si x est dans Ω, alors il existe β_x vérifiant $\forall n \in \mathbb{Z},\ a + n.b_x \in \Omega$.
On déduit $\forall n \in \mathbb{Z},\ x + n.\beta_x \in \Omega \cup A$.

Dans les deux cas, un certain $N_{x,b}$ est inclus dans $A \cup \Omega$.

Passons à l'intersection : a-t-on $\forall x \in A \cap \Omega,\ \exists y \in \mathbb{N}^*,\ \forall n \in \mathbb{Z},\ x + n.y \in A \cap \Omega$
On se donne x dans $A \cap \Omega$. Il est à la fois dans A et dans Ω.
Comme x est dans A, alors il existe b_x vérifiant $\forall n \in \mathbb{Z},\ x + n.b_x \in A$.
Comme x est dans Ω, alors il existe β_x vérifiant $\forall m \in \mathbb{Z},\ x + n.\beta_x \in \Omega$.
L'idée est alors de prendre $b_x.\beta_x$ (ou même leur $p; P; c.m.$).
On vérifie pour tout n : $x + n.(b_x.\beta_x) = x + (n.\beta_x).b_x \in A$ et $x + n.(b_x.\beta_x) = x + (n.b_x).\beta_x \in \Omega$
L'ensemble $N_{x,b_x.\beta_x}$ est inclus à la fois dans A et Ω. Il est dans l'intersection $A \cap \Omega$.

La clef était $N_{a,\,b_x.\beta_x} \subset N_{a,\,b_x} \subset A$ et la même ou presque avec Ω.

♣ 5 ♣ Montrez que si les k ensembles A_1 à A_k sont ouverts, alors $\bigcap_{i=1}^{k} A_k$ est encore un ouvert.

On peut faire une récurrence sur le nombre d'ouverts dans l'intersection, en utilisant le résultat précédent « la réunion de deux ouverts est un ouvert ».

♣ 6 ♣ Montrez que si les ensembles A_i (pour i dans I) sont ouverts, alors $\bigcup_{i\in I} A_i$ est encore un ouvert.
Rappel $\bigcup_{i\in I} A_i = \{x \mid \exists i \in I,\ x \in A_i\}$ et $\bigcap_{i\in I} A_i = \{x \mid \forall i \in I,\ x \in A_i\}$.

Attention, ici la réunion peut être une réunion infinie.
On n'aura pas le droit de prendre comme on aurait pu le faire au dessus le produit de tous les p_x.

Mais en fait tout va bien.

On prend un élément a dans la réunion $\bigcup_{i\in I} A_i$. Par définition, il est dans un des A_i qu'on va noter A_{i_0} pour le particulariser.
Mais alors, come A_{i_0}est ouvert et a dans A_{i_0}, il existe un b non nul vérifiant $N_{a,b} \subset A_{i_0}$.
Par définition même de la grande réunion $N_{a,b} \subset A_{i_0} \subset \bigcup_{i\in I} A_i$.
On a bien établi que la réunion était un ouvert.

Le nom « ouvert » et « fer » a été choisi dans cette démonstration car nos démonstrations reprennent les idées de démonstrations que vous croiserez en analyse et topologie, avec le nom d'ouverts et femés.
Sinon , la notion d'intervalle ouvert vous est connue.
Et si $]\alpha,\ \beta[$ est ouvert, on a $\forall a \in]\alpha,\ \beta[,\ \exists b > 0,\ ]a-b,\ a+b[\subset]\alpha,\ \beta[$.

♣ 7 ♣ On dit qu'un ensemble F est fermé si son complémentaire dans $\mathbb{Z}$ est un ouvert.
Montrez que $\{-1,\ 1\}$ est un fermé (mais pas un ouvert).

$\{-1,\ 1\}$ n'est pas ouvert. C'est direct, puisque les ouverts non vides sont de cardinal infini !

Pour montrer maintenant qu'il est fermé, il convient de montrer que $\mathbb{Z} - \{-1,\ 1\}$ est ouvert.

On prend a dans $\mathbb{Z}$ mais différent de -1 et 1.
Il faut trouver b tel que $N_{a,b}$ ne contiennent ni -1 ni 1.
Il s'égit donc de trouver b tel que les $a + b.n$ ne vaillent jamais -1 ou 1.

a faire.

♣ 8 ♣ Montrez que ce sont à la fois des ouverts et des fermés : | $\emptyset$ | $\mathbb{Z}$ | $2.\mathbb{Z}$ |

Pour l'ensemble vide, on a déjà montré qu'il est ouvert. Et son complémentaire est $\mathbb{Z}$. Et $\mathbb{Z}$ est ouvert. C'est bon.

Par symétrie des rôles, $\mathbb{Z}$ est ouvert, et son complémentaire aussi. $\mathbb{Z}$est ouvert et fermé.

On a montré que $2.\mathbb{Z}$ était un ouvert.
Il nous manque que son complémentaire (l'ensemble des entiers impairs) est aussi ouvert.
On prend a quelconque dans $2.\mathbb{Z}+1$ (écrivons le $2.c+1$ avec c entier pour nous simplifier la vie). On considère alors $N_{a,2} = \{(2.c+1) + 2.n \mid n \in \mathbb{Z}\}$. On retrouve l'ensemble des entiers impairs. On a bien $N_{a,2} \subset (2.\mathbb{Z}+1)$.

On note qu'avec « $2.\mathbb{Z}$ et $2.\mathbb{Z}+1$ sont ouverts », on a montré que $2.\mathbb{Z}$ était à la fois ouvert et fermé, mais on a montré aussi que $2.\mathbb{Z}+1$ est à la fois ouvert et fermé.

♣ 9 ♣ Montrez que $\mathbb{N}$ n'est ni ouvert, ni fermé.

Si $\mathbb{N}$ était ouvert, avec le cas particulier $a = 0$ dans la définition, il existerait b non nul vérifiant $N_{0,b} \subset \mathbb{N}$. Or, dans

$N_{0,b}$ il y a $0 + b.(-1)$ qui est négatif.

Si $\mathbb{N}$ était fermé, son complémentaire $\mathbb{Z}^{-*}$ serait ouvert.
On aurait $\forall a < 0,\ \exists b \in \mathbb{N}^*,\ N_{a,b} \subset \mathbb{Z}^{-*}$.
Prenons alors (raisonnement par l'absurde) $a = -1$. il existe un b tel que tous les éléments de la forme $-1 + n.b$ soient strictement négatifs. Or $-1 + b$ est positif. Déjà fini !

♣ 10 ♣ Montrez que chaque $N_{\alpha,\beta}$ est à la fois ouvert et fermé.

On se fixe a et b et on montre que $N_{a,b}$est ouvert.
On y prend un élément quelconque α qu'on écrit $a + n_0.b$ pour un n bien choisi.
Quel β va-t-on prendre ? Pas difficle à construire. Prenons $\beta = b$ et vérifions que $N_{\alpha,\ b}$ est inclus dans $N_{a,b}$.
Mais les éléments de $N_{\alpha,\ b}$ sont de la forme $(a + n_0.b) + n.b$ donc de la forme $a + k.b$ avec k décrivant $\mathbb{Z}$.

On a donc même $N_{\alpha,b} = N_{a,b}$ finalement.

Et son complémentaire est il bien ouvert ? La solution de facilité est de l'écrire

♣ 11 ♣ Montrez que $\bigcup_{p \in \mathbb{P}} N_{0,p}$ est égal à $Z - \{-1,\ 1\}$.

♣ 12 ♣ Concluez que $\mathbb{P}$ ne peut pas être fini.

◦33◦ Une loi $*$ est compatible à droite avec une relation $\blacktriangleleft$ sur un ensemble E si $\forall (a,b,c) \in E^3,\ (a \blacktriangleleft b) \Rightarrow (a * c) \blacktriangleleft (b * c)$.
Parmi ces couples, lesquels sont compatibles, et vérifiez au passage si ce sont des relations d'ordre, d'équivalence :

ensemble	loi	relation	réflexive	symétrique/anti	transitive
$\mathbb{N}^*$	$+$	« est premier avec »			
$P(E)$	$\bigcup$	$\subset$			
$P(E)$	Δ	le cardinal de leur intersection est pair			
$\mathbb{N}^*$	$\times$	« a au moins un diviseur commun avec »			
$\mathbb{R}^+$	puissance	$\leqslant$			
$\mathbb{N}$	puissance	« est premier avec »			
$P(E)$	$\bigcup$	« rencontre »			
$\mathbb{Z}^*$	puissance	$\leqslant$			
$\mathbb{C}[X]$	$\times$	a une racine commune avec			

ensemble	relation	réflexive	symétrique/anti	transitive
$\mathbb{N}^*$	« est premier avec »	oh non !	symétrique	non (1)
$P(E)$	$\subset$	oui	antisymétrique (2)	oui
$P(E)$	le cardinal de leur intersection est pair	oui	symétrique	oui
$\mathbb{N}^*$	« a au moins un diviseur commun avec »	oui	symétrique	oui (3)
$\mathbb{R}^+$	$\leqslant$	oui	antisymétrique	oui
$\mathbb{N}$	« est premier avec »	non		
$P(E)$	« rencontre »	oui quoique (4)	symétrique	non
$\mathbb{Z}^*$	$\leqslant$	oui	symétrique	oui
$\mathbb{C}[X]$	a une racine commune avec	non		

(1) : contre-exemple : 2 est premier avec 3
3 est premier avec 4
2 n'est pas premier avec 4 (diviseur commun non trivial : 2)

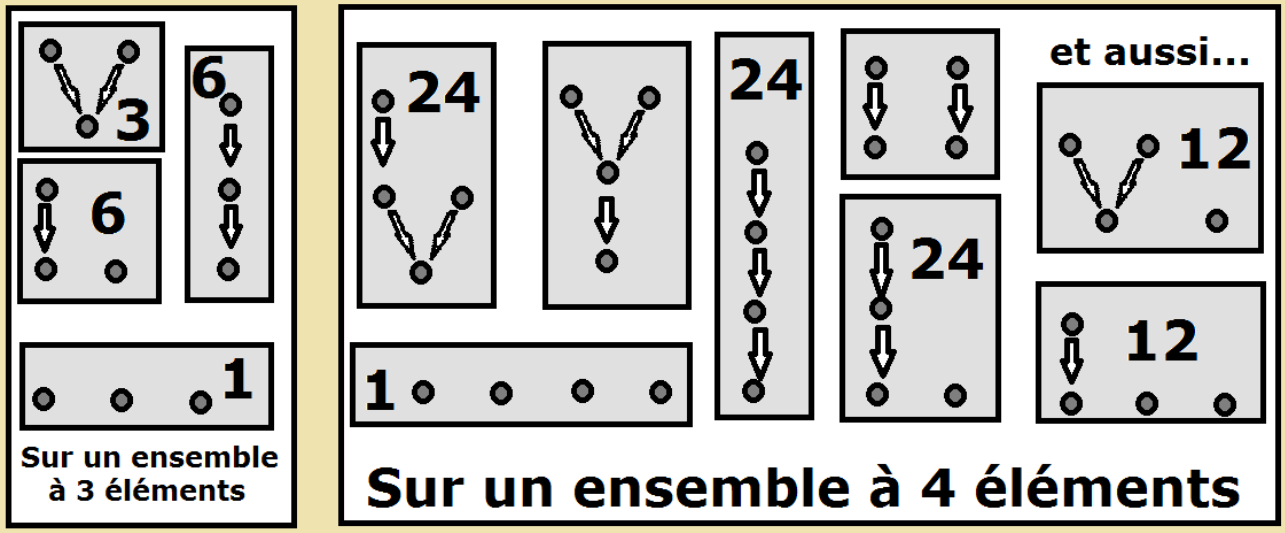
(2) : l'implication $(A \subset B \text{ et } B \subset A) \Rightarrow A = B$ est peut être la définition de $A = B$, non ?
En tout cas, c'est en montrant $A \subset B$ et $B \subset A$ qu'on montre en général $A = B$.

(3) : deux entiers ont toujours au moins un diviseur commun, et c'est 1.

(4) : j'avais envie de dire que tout ensemble se rencontre lui même. mais comment le vide se rencontre-t-il ? $\emptyset \cap \emptyset = \emptyset$, non ?

∘34∘

Montrez que sur un ensemble de cardinal n il y a $n!$ relations d'ordres totaux.
Sur un ensemble à deux éléments a et b il y a trois relations d'ordre :
• un ordre partiel (l'égalité) a et b ne sont pas en relation
• deux ordres totaux : $a \lhd b$ | $a \lhd b$
Montrez que sur un ensemble à trois éléments il y a dix neuf relations d'ordre possibles.
Montrez que sur un ensemble à quatre éléments il y a 219 relations d'ordre possibles.



Ne cherchez pas à expliciter des relations d'ordre par des formules, on fait des maths, pas de la physique qui prétend décrire un monde réel. Ces relations sont caractérisées par leur graphe, et tant pis si vous trouvez absurde ou abscons de dire « $a \blacktriangleleft b \blacktriangleleft d$ et c est à côté sans relation avec eux ».

Normalement, tout est à peu près dit dans l'énoncé avec les dessins.

∘35∘

Montrez $7.\mathbb{Z} + 8.\mathbb{Z} = \mathbb{Z}$.
Montrez $7.\mathbb{Z} + 8.\mathbb{N} = \mathbb{Z}$.
Montrez que tous les entiers à partir de 42 sont dans $7.\mathbb{N} + 8.\mathbb{N}$.

Les inclusions $7.\mathbb{Z} + 8.\mathbb{Z} \subset \mathbb{Z}$ et $7.\mathbb{Z} + 8.\mathbb{N} \subset \mathbb{Z}$ sont des évidences. On combien des entiers, on obtenir des entiers. Ce sont les autres sens qui importent. Mais comme 7 et 8 sont premiers entre eux, une identité de Bézout donne $(-1).7 + 8 = 1$ puis $(-n).7 + n.8 = n$ pour tout entier n.

Maintenant, il faut prouver que tout relatif n s'écrit $a.7 + b.8$ avec a dans $\mathbb{Z}$ et b dans $\mathbb{N}$.
n positif s'écrit $(-n).7 + n.8$, c'est gagné.
Tout entier négatif n avec p positif s'écrit $(-n).7 + n.8$ mais le coefficient de 8 est négatif.
Mais on a aussi $n = (-n + 8.n).7 + (n - 7.n).8$ et cette fois $n - 7.n$ est positif.
Il suffit de jouer sur le fait qu'il y a à chaque fois plusieurs décompositions de Bézout possibles.

---

42 s'écrit par exemple $6 \times 7 + 0 \times 8$. Il est combinaison de 6 et 7 à coefficients tous deux positifs.

On en décompose quelques uns en plus pour avancer :

$42 = 6 \times 7 + 0 \times 8$
$43 = 5 \times 7 + 1 \times 8$
$44 = 4 \times 7 + 2 \times 8$
$45 = 3 \times 7 + 3 \times 8$
$46 = 2 \times 7 + 4 \times 8$
$47 = 1 \times 7 + 5 \times 8$
$48 = 0 \times 7 + 6 \times 8$

Et 49 ? On ne peut pas l'écrire $(-1).7 + 7.8$.
Mais on l'écrit 7.7. Et on recommence.

On peut montrer que 41 n'est pas de la forme indiquée. On teste $0.7 + q.8$, $1.7 + q.8$, $2.7 + q.8$, $3.7 + q.8$, $4.7 + q.8$ et $5.7 + q.8$ avec les premières valeurs de q (ou avec un argument de parité).

Comment montrer qu'ensuite si n plus grand que 48 s'écrit $a.7 + b.8$ avec a et b positif, alors $n + 1$ s'écrit $a'.7 + b'.8$ avec a et b positifs ?

On se donne n, on suppose qu'on peut l'écrire $a.7+b.8$. On a alors

$$n+1=(a.7+b.8)+((-1).7+8)=(a-1).7+b.8$$

Si a valait au moins 1, la nouvelle écrite est bien à coefficients dans $\mathbb{N}\times\mathbb{N}$, et c'est gagné.
Mais si a était nul ? On avait alors $n=0.7+b.8$ avec b valant au moins 6.
On écrit alors $n+1=7.7+(b-6).8$. Et les coefficients sont positif.
Et la récurrence valide les deux cas d'hérédité.

◦36◦

Montrez que ce sont des sous-groupes de $(\mathbb{R},+)$:

$\mathbb{Z}$	$\left\{\frac{a}{7}+\frac{2.b}{5} \mid (a,\,b)\in\mathbb{Z}^2\right\}$	$\left\{\frac{a}{7}+\frac{2.b}{5}+c \mid (a,\,b,\,c)\in\mathbb{Z}^3\right\}$	$\left\{a.\sqrt{4}+b.\sqrt{25} \mid (a,\,b)\in\mathbb{Z}^2\right\}$
$\mathbb{Q}$	$\left\{a+\sqrt{2}.b \mid (a,\,b)\in\mathbb{Z}^2\right\}$	$\left\{a+\sqrt{2}.b+c.\sqrt{3} \mid (a,\,b,\,c)\in\mathbb{Z}^2\right\}$	

Lesquels peuvent s'écrire sous la forme $\{a.p \mid p\in\mathbb{Z}\}$ pour au moins un réel a bien choisi ?

Les inclusions dans $\mathbb{R}$ sont acquises.

Le neutre est présent en prnant $a=b=0$ ou $a=b=c=0$.

La stabilité s'écrit par exemple $\frac{a}{7}+\frac{2.b}{5}+\frac{a'}{7}+\frac{2.b'}{5}=\frac{a+a'}{7}+\frac{2.(b+b')}{5}$.

Le passage au symétrique repose sur le fait qu'on peut passer d'un couple $(a,\,b)$ à un couple $(-a,\,-b)$ tout aussi dans $\mathbb{Z}^2$.

$\mathbb{Z}=1.\mathbb{Z}$	$\left\{\frac{a}{7}+\frac{2.b}{5} \mid (a,\,b)\in\mathbb{Z}^2\right\}=\frac{1}{35}.\mathbb{Z}$	$\left\{\frac{a}{7}+\frac{2.b}{5}+c \mid (a,\,b,\,c)\in\mathbb{Z}^3\right\}=\frac{1}{35}.\mathbb{Z}$	$\left\{a.\sqrt{4}+b.\sqrt{25} \mid (a,\,b)\in\mathbb{Z}^2\right\}=1.\mathbb{Z}$

Comment prouver $\left\{\frac{a}{7}+\frac{2.b}{5} \mid (a,\,b)\in\mathbb{Z}^2\right\}=\frac{1}{35}.\mathbb{Z}$?
Par double inclusion.
Tous les éléments de la forme $\frac{a}{7}+\frac{2.b}{5}$ sont en fait des $\frac{k}{35}$ avec k de la forme $5.a+14.b$.
Tout élément de la forme $\frac{k}{35}$ avec k entier sont de la forme $\frac{5.a+14.b}{35}$ en écrivant $k=5.a+14.b$ avec a et b bien choisis. C'est Bézout qui le dit : $5.\mathbb{Z}+14.\mathbb{Z}=\mathbb{Z}$.

L'ensemble $\left\{\frac{a}{7}+\frac{2.b}{5}+c \mid (a,\,b,\,c)\in\mathbb{Z}^3\right\}$ est inclus dans $\left\{\frac{a}{7}+\frac{2.b}{5} \mid (a,\,b)\in\mathbb{Z}^2\right\}$
En effet, chaque $\frac{a}{7}+\frac{2.b}{5}+c$ s'écrit aussi $\frac{a+7.c}{7}+\frac{2.b}{5}$.

L'ensemble $\left\{\frac{a}{7}+\frac{2.b}{5} \mid (a,\,b)\in\mathbb{Z}^2\right\}$ est inclus dans $\left\{\frac{a}{7}+\frac{2.b}{5}+c \mid (a,\,b,\,c)\in\mathbb{Z}^3\right\}$
En effet, chaque $\frac{a}{7}+\frac{2.b}{5}$ s'écrit aussi $\frac{a+7.c}{7}+\frac{2.b}{5}+0$.

L'ensemble d'écriture étrange $\left\{a.\sqrt{4}+b.\sqrt{25} \mid (a,\,b)\in\mathbb{Z}^2\right\}$ est $2.\mathbb{Z}+5.\mathbb{Z}$. Et c'est $\mathbb{Z}$ puisque 2 et 5 sont premiers entre eux.

$\mathbb{Q}$	$\left\{a+\sqrt{2}.b \mid (a,\,b)\in\mathbb{Z}^2\right\}$	$\left\{a+\sqrt{2}.b+c.\sqrt{3} \mid (a,\,b,\,c)\in\mathbb{Z}^2\right\}$	

Aucun de ces ensembles ne peut s'écrire $\{a.k \mid k\in\mathbb{Z}\}$.
Un ensemble de la forme $a.\mathbb{Z}$ cotient « le premier élément après 0 » (et c'est a).
Or, dans $\mathbb{Q}$ il n'y a pas de plus petit rationnel strictement positif.

Une jolie preuve par l'absurde pour $\left\{a+\sqrt{2}.b \mid (a,\,b)\in\mathbb{Z}^2\right\}$.
Supposons qu'il soit de la forme $\{k.\alpha \mid k\in\mathbb{Z}\}$ pour un α bien choisi (« générateur de l'ensemble).
Alors $1+\sqrt{2}.b$ est dans cet ensemble, et s'écrit donc $p.\alpha$ pour un entier p bien choisi.
De même $0+1.\sqrt{2}$ est dans cet ensemble, et s'écrit donc $q.\alpha$ pour un entier q bien choisi.

On calcule alors $\sqrt{2}=\frac{0+1.\sqrt{2}}{1+0.\sqrt{2}}=\frac{q.\alpha}{p.\alpha}=\frac{q}{p}$.
Le réel $\sqrt{2}$ serait rationnel ! Impossible !

∘37∘ On définit sur $\mathbb{Z}\times\mathbb{Z}^*$ une relation et deux lois :

$(a,\,b)\Re(\alpha,\,\beta)$	$(a,\,b)\oplus(c,\,d)$	$(a,\,b)\otimes(c,\,d)$
si et seulement si	est égal à	est égal à
$a.\beta = b.\alpha$	$(a.d+b.c,\,b.d)$	$(a.c,\,b.d)$

Montrez que ce sont des lois internes sur $\mathbb{Z}\times\mathbb{Z}^*$, commutatives, associatives.
Donnez le neutre de chacune.
Montrez que les deux lois sont compatibles avec $\Re$ $\left.\begin{array}{c}(a,\,b)\Re(\alpha,\,\beta)\\ et\\ (c,\,d)\Re(\gamma,\,\delta)\end{array}\right\}\Rightarrow\left\{\begin{array}{c}((a,\,b)\oplus(c,\,d))\Re((\alpha,\,\beta)\oplus(\gamma,\delta))\\ et\\ ((a,\,b)\otimes(c,\,d))\Re((\alpha,\,\beta)\otimes(\gamma,\delta))\end{array}\right\}$.
Montrez que tout élément de $\mathbb{Z}\times\mathbb{Z}^*$ admet *(modulo $\Re$)* un symétrique pour l'addition *(c'est à dire pour tout q il existe q' vérifiant $q\oplus q'\Re(0,1)$)*.
Montrez que tout élément de $\mathbb{Z}^*\times\mathbb{Z}^*$ admet (modulo $\Re$) un symétrique pour la multiplication *(c'est à dire pour tout q il existe q' vérifiant $q\otimes q'\Re(1,1)$)*.
Est il vrai que la multiplication est directement distributive sur l'addition ?
Montrez que tout élément est en relation par $\Re$ avec un élément irréductible (a,b) avec a et b premiers entre eux et b positif.
Que venez vous de construire ? Était ce passionnant ?

On a construit $(\mathbb{Q},+,.)$ à partir de $(\mathbb{Z},+,.)$.

∘38∘ ♡ La relation « ne pas être inclus dans » est elle réflexive, symétrique, antisymétrique, transitive sur $P(\mathbb{R})$? Est elle compatible avec $\cap$? Est elle compatible avec $\cup$?

On donne des contre-exemple.

propriété	contre-exemple	justification	conclusion
Réflexive.	$A=\emptyset$	0n a $A\subset A$. On n'a donc pas $A\not\subset A$.	raté
Symétrique.	$A=\{1,\,2\}$ et $B=\{1\}$	On a $A\not\subset B$ mais on n'a pas $B\not\subset A$.	raté
Antisymétrique.	$A=\{1\}$ et $B=\{2\}$	On a à la fois $A\not\subset B$ et $B\not\subset A$. Mais on n'a pas $A=B$.	raté
Transitive	$A=\{1]$, $B=\{2\}$, $C=\{1\}$	On a $A\not\subset B$ et $B\not\subset C$ mais on n'a pas $A\not\subset C$	raté

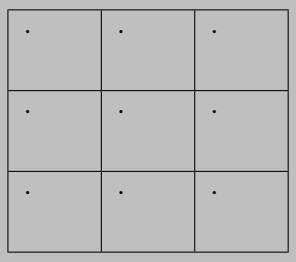
Elle n'a rien pour me plaire.

Peut on passer à coup sûr de $A\not\subset B$ à $A\cap C\not\subset B\cap C$?
Non : $A=\{1\}$, $B=\{2\}$ et $C=\{3\}$.

Peut on passer à coup sûr de $A\not\subset B$ à $A\cap C\not\subset B\cap C$?
Non : $A=\{1\}$, $B=\{2\}$ et $C=\{1,\,2\}$.

Elle me plait de moins en moins.

∘39∘ • Combien de façons de placer deux jetons *Aissata* et *Bintou* dans des cases du tableau ?
• Combien de façons de placer deux jetons *Aissata* et *Bintou* dans des cases distinctes du tableau ?
• Combien de façons de placer deux jetons indistinguables dans deux cases distinctes du tableau ?
• Combien de façons de placer deux jetons indistinguables dans deux cases du tableau, aux symétries, rotations près ?
• Combien de façons de placer deux jetons indistinguables dans deux cases du tableau, sans qu'ils soient sur une même ligne ou une même colonne ?



Aissata et Bintou, c'est juste pour A et B.

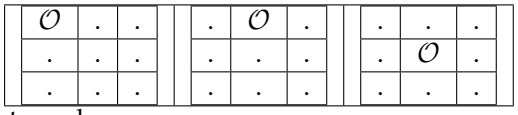
On doit placer deux jetons sur neuf places. Neuf choix pour A, neuf choix pour B. Total : 81 configurations.

Si ils doivent occuper deux cases distinctes, neuf choix pour A et seulement huit pour B : 72 (et si B se place en premier, c'est pareil).

Les deux jetons sont indistinguables. On a deux cas :
• ils sont dans la même case : neuf possibilités.
• ils sont dans deux cases distinctes : $\binom{9}{2}$.
Total : 45.

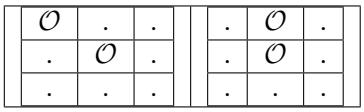
Les deux jetons sont indistinguables, et on peut faire des symétries, rotations.

• ils sont dans la même case :

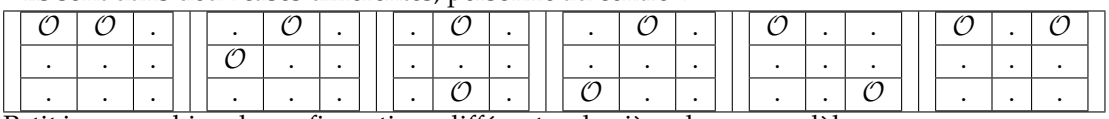


Tout dépend effectivement du type de case.

• ils sont dans deux cases distinctes et l'un occupe la case centrale :



• ils sont dans deux cases différentes, personne au centre :



Petit jeu : combien de configurations différentes derrière chaque modèle.

◦40◦

Combien faut il d'échanges de lettres deux à deux pour passer de "LA_VERITE" à "_RELATIVE" (chaines de caractères de longueur 9).

LA_VERITE	_ALVERITE	_RLVEAITE	...	_RELATIVE

Combien si en plus vous imposez que les lettres échangées soient à chaque fois contigües (on peut commencer par échanger R et I mais pas R et T (mais passez par RI puis IT)) ?

Les TRIPES ont elle des ESPRITS ? Quelles sont les MOEURS des MORUES ? Le PIRATE a-t-il une PARTIE ? Le SPORTIF fait il des PROFITS ? L'ÉTREINTE dure-t-elle une ÉTERNITÉ ?

Associez deux à deux les anagrammes :

La gravitation universelle	tout commença dans l'eau
La vitesse de la lumière	vérité théatrale et loi intersidérale
L'origine de l'univers	un vide noir grésille
La théorie de la relativité restreinte	rien n'est établi
Albert Einstein	limite les rêves au-delà
Le commandant Cousteau	un lot de vestes d'Hérodote
Le Radeau de la Méduse	loi vitale régnant sur la vie
Saint-Germain des Près	matins nègres de Paris
Hôtel des ventes de Drouot	au-delà de la démesure

Ce sont des cadeaux d'Etienne Klein.

Boire l'eau	Gringalet con
Pot au café	Teinte ocre
Testicule	Dure matrone
Note écrite	A cup of tea ?
Gentil garçon	C'est utile
Tendre amour	ou la bière

Ceux là sont de Basile Morin.

Bon, pas grand chose à dire.

Sauf pour l'informatique de seconde période...

◦41◦

♡ Deux matrices carrées A et B de même format sont dites semblables si il existe une matrice inversible P vérifiant $A.P = P.B$.

Montrez que $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$ et $\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$ sont semblables en trouvant une matrice P.

Montrez que $\begin{pmatrix} 2 & 1 \\ -1 & 4 \end{pmatrix}$ et $\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$ ont même trace et même déterminant mais ne sont pas semblables.

Ajustez pour que $\begin{pmatrix} 1 & 1 \\ 1 & \clubsuit \end{pmatrix}$ et $\begin{pmatrix} 4 & \spadesuit \\ 1 & 2 \end{pmatrix}$ soient semblables.

La condition $Tr(A) = Tr(B)$ et $\det(A) = \det(B)$ n'est que nécessaire.

Si on a$Tr(A) \neq Tr(B)$ ou $\det(A) \neq \det(B)$, on peut conclure « pas semblables », c'est direct.

Si on a $Tr(A) = Tr(B) =$ et $\det(A) = \det(B)$, on ne peut a priori pas conclure.

La seule solution à notre niveau est de trouver P.

en voici une, $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$

mais ce n'est pas la seule.

Si une matrice est semblable à $3.I_2$, c'est qu'elle est déjà égale à $3.I_2$ (calculez $P.(3.I_2).P^{-1}$).

La matrice $\begin{pmatrix} 2 & 1 \\ -1 & 4 \end{pmatrix}$ a beau avoir pour trace 6 et déterminant 9, elle n'est pas semblable à $3.I_2$.

On peut quand même la rendre semblable à $\begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}$...

ou à toute matrice $\begin{pmatrix} 3 & a \\ 0 & 3 \end{pmatrix}$ avec a non nul. Mais pas à $\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$.

Pour que $\begin{pmatrix} 1 & 1 \\ 1 & \clubsuit \end{pmatrix}$ et $\begin{pmatrix} 4 & \spadesuit \\ 1 & 2 \end{pmatrix}$ soient semblables, il faut

• qu'elles aient la même trace : $\begin{pmatrix} 1 & 1 \\ 1 & 5 \end{pmatrix}$ et $\begin{pmatrix} 4 & \spadesuit \\ 1 & 2 \end{pmatrix}$

• qu'elles aient le même déterminant : $\begin{pmatrix} 1 & 1 \\ 1 & 5 \end{pmatrix}$ et $\begin{pmatrix} 4 & 4 \\ 1 & 2 \end{pmatrix}$.

Mais maintenant, sont elles bien semblables ? Il faut trouver P.

On résout un système et on propose une solution : $\begin{pmatrix} 1 & 1 \\ 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 & 4 \\ 1 & 2 \end{pmatrix}$.

Il faut écrire quatre équations (et pas juste deux), faire des choix comme $c = 0$ et $d = 1$, et regarder ce que cela donne.

Mais surtout à la fin, il faut vérifier.

◦42◦ Montrez que $\begin{pmatrix} 3 & 9 \\ -1 & -3 \end{pmatrix}$ est semblable à son double *(en donnant P inversible vérifiant donc $A.P = P.(2.A)$)*. Même question avec ses multiples *($\lambda.A$ pour λ non nul)*.

◦43◦ ♡ L'ensemble des suites réelles a vérifiant $\forall n,\ a_{2.n} = 0$ *ou* $a_{2.n+1} = 0$ est il un espace vectoriel ?
Montrez $\{u \in \mathbb{R}^{\mathbb{N}} \mid \forall n,\ u_{2.n} = 0\} \oplus \{u \in \mathbb{R}^{\mathbb{N}} \mid \forall n,\ u_{2.n} = u_{2.n+1}\} = \mathbb{R}^{\mathbb{N}}$ après avoir montré que chaque ensemble est un espace vectoriel. Pourquoi ne pouvez vous pas utiliser les théorèmes sur les dimensions ?

Le ou mathématique étant inclusif, la suite nulle vérifie le critère « au moins un terme sur deux est nul ».

Mais la stabilité additive est en défaut :

$(0,\ 1,\ 0,\ 1,\ 0,\ 1, \ldots)$	$(1,\ 0,\ 1,\ 0,\ 1,\ 0 \ldots)$
$\forall n,\ a_{2.n} = 0$ *ou* $\mathbf{a_{2.n+1} = 0}$	$\forall n,\ a_{2.n+1} = 0$ *ou* $\mathbf{a_{2.n} = 0}$

. Chacune est dans l'ensemble, mais la somme ne l'est pas.

Remarque : *En général une définition avec un « ou » ne conduit pas à un espace vectoriel, car la stabilité additive est vite mise en défaut. C'est d'ailleurs souvent une histoire de réunion de deux sous-espaces vectoriels.*
Rappelons pour les espaces vectoriels que l'union ne fait pas la force. C'est la somme qui fait tout.

$\{u \in \mathbb{R}^{\mathbb{N}} \mid \forall n,\ u_{2.n} = 0\}$ est l'ensemble des suites dont au moins un terme sur deux est nul : les termes d'indices pairs.

La suite nulle en fait partie.
Si (a_n) et (b_n) vérifient $\forall n,\ a_{2.n} = b_{2.n} = 0$ alors on a bien $\forall n,\ a_{2.n} + b_{2.n} = 0$ et aussi $\forall n,\ \lambda.a_{2.n} + \mu.b_{2.n} = 0$.
On a bien un sous-espace vectoriel de $(\mathbb{R}^{\mathbb{N}}, +, .)$ (espace vectoriel des suites réelles sans aucune condition).

Remarque : *On ne cherchera pas à jouer sur les dimensions, on est en dimension infinie.*

Toute suite $(a_0,\ a_1,\ a_2,\ a_3,\ a_4,\ a_5, \ldots)$ se décompose d'une façon unique comme somme :
$(0,\ a_1,\ 0,\ a_3,\ 0,\ a_5, \ldots) + (a_0,\ 0,\ a_2,\ 0,\ a_4,\ 0, \ldots)$.

Remarque : *Pour prouver $E = A \oplus B$, on montre unicité et existence de décomposition par analyse et synthèse.*
Si vous avez fait l'analyse qui prouve l'unicité, ne vous fatiguez pas à prouver $A \cap B = \{\overrightarrow{0}\}$, c'est exactement équivalent à l »unicité de décomposition...

◦44◦ ♡ Donnez une base de l'ensemble E_6 des suites réelles périodiques de période 6 après avoir vérifié qu'il s'agit bien d'un espace vectoriel. Donnez une base de l'ensemble E_8 des suites de période 8. Qui est $E_6 \cap E_8$? Donnez en une base $(a,\ b)$.
Reprenez vos bases de E_6 et E_8 pour qu'elles contiennent a et b.
Montrez que la somme d'une suite de période 6 et d'une suite de période 8 est de période 24.
Montrez qu'il existe des suites de période 24 qui ne sont pas somme d'une suite de période 6 et d'une suite de période 8 *(soit par un argument de dimension, soit en donnant un exemple)*.

Toute suite périodique de période 6 est de la forme $(a, b, c, d, e, f, a, b, c, d, e, f, a, b, c, d, e \ldots)$.
Elle se décompose d'une façon unique à l'aide des six suites suivantes :

$$\begin{array}{cccccccccccccccc}
(1, & 0, & 0, & 0, & 0, & 0, & 1, & 0, & 0, & 0, & 0, & 0, & 1, & 0, & 0, & \ldots) \\
(0, & 1, & 0, & 0, & 0, & 0, & 0, & 1, & 0, & 0, & 0, & 0, & 0, & 1, & 0, & \ldots) \\
(0, & 0, & 1, & 0, & 0, & 0, & 0, & 0, & 1, & 0, & 0, & 0, & 0, & 0, & 1, & \ldots) \\
(0, & 0, & 0, & 1, & 0, & 0, & 0, & 0, & 0, & 1, & 0, & 0, & 0, & 0, & 0, & \ldots) \\
(0, & 0, & 0, & 0, & 1, & 0, & 0, & 0, & 0, & 0, & 1, & 0, & 0, & 0, & 0, & \ldots) \\
(0, & 0, & 0, & 0, & 0, & 1, & 0, & 0, & 0, & 0, & 0, & 1, & 0, & 0, & 0, & \ldots)
\end{array}$$

C'est la définition de « base ».

Pour les suites périodiques de période 8, on fait de même.

$E_6 \cap E_8$ est fait des suites périodiques de période 2.
Toute suite périodique de période 2 est a fortiori périodique de période 6 : $u_{n+6} = u_{n+4} = u_{n+2} = u_n$
périodique de période 8 : $u_{n+8} = u_{n+4.2} = u_n$
Toute suite périodique de périodes 6 et 8 vérifie $a_{n+2} = a_{(n+2)+6} = a_{n+8} = a_n$ pour tout n.
Elle est périodique de période 2.

L'espace des suites $2-$périodiques ont pour base (1) et $((-1)^n)$ par exemple.

Si une suite (a_n) est périodique de période 6 alors $a_{n+24} = a_{n+6.4} = a_n$
(b_n) est périodique de période 8 alors $b_{n+24} = b_{n+8.3} = b_n$ pour tout n
alors la suite $(a_n + b_n)$ est bien périodique de période 24.

Mais les suites de période 24 ne sont pas somme de suites périodiques de périodes 6 et 8.
En effet, la suite $(1, 0, 0, 0 \ldots 0, 1, 0, 0 \ldots)$ avec juste un terme sur 24 égal à 1 ne peut pas être somme de (a_n) et (b_n) de périodes respectives 6 et 8.

Illogicien : *L'élève qui n'a pas le sens de la logique (ou l'a perdu au contact d'individus peu scrupuleux sur le raisonnement) va dire*
« Mais si ! Cette suite est bien une somme $(a_n + b_n)$ avec (a_n) de période 6 et (b_n) de période 8 puisque on a bien
$(u_{n+24} = a_{n+24} + b_{n+24} = a_{n+6.4} + b_{n+8.3} = a_n + b_n = u_n$ ».
Et alors ? Ça ne prouve rien.
Ça montre juste qu'il n'y a pas d'incohérence de ce côté là. Mais il peut y en avoir ailleurs, non ?
Ce qui est nécessaire n'est pas forcément suffisant.
Disons juste que cet argument aurait plutôt servi à invalider « elle est somme d'une suite 7 périodique et d'une suite $5-$périodique ».

Supposons qu'elle soit la somme de (a_n) et (b_n) de périodes respectives 6 et 8.

On a alors $\begin{array}{rrcl} a_0 & +b_0 & = & 1 \\ a_2 & +b_2 & = & 0 \\ a_8 & +b_8 & = & 0 \\ a_{18} & +b_{18} & = & 0 \end{array}$ et donc $\begin{array}{rrcl} a_0 & +b_0 & = & 1 \\ a_2 & +b_2 & = & 0 \\ a_2 & +b_0 & = & 0 \\ a_0 & +b_2 & = & 0 \end{array}$.

Quand on en somme deux, on a $a_0 + b_0 + a_2 + b_2 = 1 + 0$.
Quand on somme les deux autres, on a $a_2 + b_0 + a_0 + b_2 = 0$.
On aboutit à une contradiction.