Promenade Mathématique

Quatre pas vers l'Algèbre

Quang-Thai Ngo, Août 2002

Table des matières

Alphabet grec

Il est utile de connaître l'alphabet grec. Grâce aux " équivalences " avec l'alphabet romain, on mémorisera plus facilement. On utilisera aussi en mathématique quelques lettres hébraïques comme $\aleph$ (lire aleph).

Equivalent alphabet romain	Nom	Minuscule	Majuscule
a	alpha	α	A
b	bêta	β	B
c	chi	χ	X
d	delta	δ	Δ
e	epsilon	ε	E
f	phi	ϕ	Φ
g	gamma	γ	Γ
h	êta	η	H
i	iota	ι	I
j	phi (autre)	φ	/
k	kappa	κ	K
l	lambda	λ	Λ
m	mu	μ	M
n	nu	ν	N
o	omicron	o	O
p	pi	π	Π
q	thêta	θ	Θ
r	rho	ρ	P
s	sigma	σ	Σ
t	tau	τ	T
u	upsilon	υ	Υ
v	/	/	/
w	oméga	ω	Ω
x	xi	ξ	Ξ
y	psi	ψ	Ψ
z	zêta	ζ	Z

Logique et mathématiques

Il y a une différence essentielle entre les mathématiques et les sciences expérimentales : la véracité d'une relation mathématique vient de ce qu'on la démontre à partir des règles du jeu que l'on s'est données, et non pas parce qu'elle est vérifiée expérimentalement.

La logique étant l'étude de la construction des propriétés et de leurs propriétés d'emploi, les différents éléments de cette science sont à la base de tous les raisonnements mathématiques. Ceux que nous allons considérés sont très particuliers, ils constituent ce que l'on appelle le calcul propositionnel. Ils établissent les règles du raisonnement correct, en excluant les processus psychologiques. Justifier une proposition c'est la rattacher à d'autres propositions déjà admises, la déduire de ces propositions. Bien que le raisonnement mathématique ne se limite pas à des propositions élémentaires d'inclusion son principe est un peu près le même : identifier une proposition nouvelle à des propositions déjà admises, faire apparaître des tautologies (rappelons que autolegein signifie en grec «dire la même chose»). Démontrer une proposition c'est la rendre évidente à autrui.

L'étude des règles de la logique remonte au moins à Aristote (384 - 322 AC), l'étude mathématique du calcul propositionnel à Augustes De Morgan (1806 - 1871) et à George Boole (1815 - 1864). Elle est donc bien antérieure à la théorie des ensembles et d'une portée à priori plus vaste.

I) Le calcul propositionnel

Le calcul propositionnel permet d'exprimer les termes, les propositions, les relations par des symboles simples, et de ramener les opérations logiques à des calculs s'effectuant selon des règles précises.

A) Variables propositionnels et connecteurs logiques

Définition

☐ On appellera proposition ou assertion toute énoncé dont on peut dire qu'elle est vraie ou fausse. Par exemple, les assertions «6 est un nombre premier» est une proposition. Au contraire, «fermer la porte !», «quel âge avez-vous» n'en sont pas. On peut représenter les propositions par des lettres A, B, ..., A. Ces lettres sont des variables propositionnels. On utilise les parenthèses pour séparer les propositions.

☐ Les connecteurs logiques sont des opérations permettant de créer de nouvelles propositions à partir d'assertions existantes p et q. Voici les différents connecteurs logiques :

Négation $\neg$ (non) :

l'assertion $\neg p$ (non p) est vraie quand p est fausse, et fausse quand p est vraie.

Disjonction $\vee$ (ou) :

$p \vee q$ (p ou q) est vraie quand l'un au moins des deux assertions p, q est vraie.

Conjonction $\wedge$ (et) :

$p \wedge q$ est vraie quand les deux assertions p, q sont vraies à la fois.

Implication $\Rightarrow$ (flèche) :

$p \Rightarrow q$ est vraie quand p est fausse (le faux implique n'importe quoi) ou quand p, q sont vraies.

Equivalence $\Leftrightarrow$ (double flèche) :

$p \Leftrightarrow q$ est vraie si p, q sont toutes les deux vraies ou toutes les deux fausses.

☐ Un assemblage ou un mot est une suite finie de symbole : $\Rightarrow)\neg \vee (pq \Leftrightarrow$.

☐ On appelle forme propositionnel tout assemblage φ pour lequel il existe une suite finie φ_1, φ_2, ..., $\varphi_n = \varphi$ d'assemblages, vérifiant pour tout $i < n$ l'une des conditions :

φ est une variable propositionnel.

1°) $j < i$ tel que $\varphi_i = \neg(\varphi_j)$

2°) Il existe j, $j' < i$ tels que $\varphi_1 = (\varphi_j)\perp(\varphi_{j'})$ où $\perp$ représente un des connecteurs logiques.

☐ Un raisonnement est un procédé indirect de justification, soumis par là aux règles de la logique. On dit qu'une proposition mathématique est démontrée lorsqu'on montre qu'elle découle logiquement et nécessairement d'autres propositions déjà admises.

Remarque

1°) Tout énoncé a une et une seule des formes :
- A où A est une variable propositionnelle
- $\neg(\varphi)$ où φ est un énoncé
- $(\varphi)\perp(\varphi')$ où φ, φ' sont des énoncés.

2°)$\varphi(\neg(C)) \vee ((A)) \Rightarrow (B))$ est un énoncé car on peut poser

$\varphi_1 = A$ $\quad$ $\varphi_4 = \neg(C)$
$\varphi_2 = B$ $\quad$ $\varphi_5 = (A) \Rightarrow (B)$
$\varphi_3 = C$ $\quad$ $\varphi_6 = (A(C)) \vee ((A) \Rightarrow (B))$.

3°) On peut supprimer certaines parenthèses :

$\neg(A) \Rightarrow \neg A$
$((A) \vee (B)) \Rightarrow (C) \Rightarrow A \vee B \Rightarrow C$
$((A) \vee (B)) \wedge (C) \Rightarrow (A \vee B) \wedge C$.

Mais attention à

$((A) \vee (B)) \wedge (C) \Rightarrow (A \vee B) \wedge C$.

B) Tableaux de vérité

Définition

☐ Sur $\{0, 1\}$, 0 représente le faux et 1 le vrai. On introduit ainsi une loi binaire notée $\perp$.

☐ La définition d'une loi binaire $\perp$ peut être résumée en des tableaux indiquant quand cette loi est vraie et quand elle est fausse. Ces tableaux sont appelés tableaux de vérité.

☐ Deux assertions $P(A, B, C, ...)$ et $Q(A, B, C, ...)$ sont dites synonymes (et on note $P \equiv Q$) si elles ont le même tableau de vérité.

Représentons les lois $\neg$, $\vee$, $\wedge$, $\Rightarrow$ et $\Leftrightarrow$ par des tableaux de vérités :

Négation

☐ La négation s'exprime parfois par un trait au dessus du symbole propositionnel (il existe d'autre façon d'exprimer la négation, par exemple $\neg A$). L'expression $\overline{A}$ (lire non A ou A barre) signifie la négation de la proposition A.

Règle

Si A est vraie, $\overline{A}$ est fausse. Si $\overline{A}$ est fausse, A est vraie. Si la valeur vrai est exprimée par la lettre V et la valeur faux par la lettre F, on peut établir la table de vérité :

A	$\overline{A}$
V	F
F	V

Conjonction

☐ Une proposition complexe telle que (A et B) est constituée par la conjonction de deux propositions élémentaires A, B. On exprime la conjonction par le signe $\wedge$.

Règle

(A et B) est vraie si et seulement les deux assertions A, B sont vraies à la fois. Voici la table de vérité :

A	B	$A \wedge B$
V	V	V
V	F	F
F	V	F
F	F	F

Disjonction

☐ Considérons maintenant la proposition (A ou B), en donnant au mot ou un sens inclusif. C'est la disjonction exprimées par le signe $\vee$.

Règle

(A ou B) est fausse si et seulement si A, B sont fausses toutes les deux

A	B	$A \vee B$
V	V	V
V	F	V
F	V	V
F	F	F

Conjonction et disjonction sont des opérateurs logiques.

Théorème (de De Morgan)

Soient A et B deux propositions élémentaires. On aura

$$\overline{A \wedge B} = \overline{A} \vee \overline{B} \text{ et } \overline{A \vee B} = \overline{A} \wedge \overline{B}.$$

Preuve

On peut vérifier très facilement ces deux lois en utilisant les tables de vérités :

A	B	$A \wedge B$	$\overline{A \wedge B}$	$\overline{A}$	$\overline{B}$	$\overline{A} \vee \overline{B}$
V	V	V	F	F	F	F
V	F	F	V	F	V	V
F	V	F	V	V	F	V
F	F	F	V	V	V	V

Ainsi on voit bien que $\overline{A \wedge B} = \overline{A} \vee \overline{B}$. De même, le lecteur vérifiera facilement que $\overline{A \vee B} = \overline{A} \wedge \overline{B}$.

Implication

☐ Considérons maintenant la proposition "si A alors B". La proposition A est dite impliquer la proposition B. Le signe de l'implication est $\Rightarrow$. La règle ci-dessous nous permet de donner une équivalence de «$A \Rightarrow B$» qui signifie en fait «non A ou B».

Règle

Il suffit d'un seul cas sans B (c'est-à-dire que B est fausse) pour que l'implication soit fausse.

A	B	$A \Rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

En écrivant la table de vérité de la proposition ($\overline{A}$ ou B), on voit bien que la disjonction ($\overline{A}$ ou B) est une implication :

A	$\overline{A}$	B	$\overline{A} \vee B$
V	F	V	V
V	F	F	F
F	V	V	V
F	V	F	V

Théorème

> Les propositions $(A \Rightarrow B)$ et $(\overline{B} \Rightarrow \overline{A})$ sont équivalentes. Souvent, pour démontrer un théorème on peut démontrer sa négation.

Preuve

II suffit d'écrire les tables de vérités pour s'en rendre compte.

A	$\overline{A}$	B	$\overline{B}$	$A \Rightarrow B$	$\overline{B} \Rightarrow \overline{A}$
V	F	V	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	V	F	V	V	V

Les propositions A et B de l'implication $A \Rightarrow B$ sont appelées respectivement antécédent et conséquent. Soit B une proposition A impliquant B s'appelle condition suffisante de B. Toute proposition A résultant de B s'appelle condition nécessaire de B.

Cette technique s'appelle la contraposition des cas.

Exemple

☐ Soient les propositions :

- A : «le nombre x est nul»
- B : «le produit xy est nul»

La proposition A est une condition suffisante de B. En effet, pour que le produit xy soit nul, il suffit que x le soit. Pour que x soit nul, il est nécessaire que le produit xy soit nul. Mais B n'est pas une condition suffisante de A : la nullité du produit xy n'entraîne pas nécessairement celle de x.

☐ Dans la vie quotidienne, chacun applique le règle de De Morgan sans jamais avoir seulement entendu prononcer ce nom. Considérons les propositions suivantes :

A : cette chemise est en nylon

B : elle est impassable.

Formons les phrases $(A \wedge B)$ et $(\overline{A} \vee \overline{B})$:

$A \wedge B$: cette chemise est en nylon et elle est impassable.

$\overline{A} \vee \overline{B}$: cette chemise n'est pas en nylon ou elle n'est pas impassable.

Equivalence

☐ Deux propositions A, B sont dites équivalentes si et seulement les deux implications $A \Rightarrow B$ et $B \Rightarrow A$ sont vraies. On note alors $B \Leftrightarrow A$. On dit des propositions A et B qu'elles sont chacune une condition nécessaire et suffisante de l'autre. Ceci peut encore s'énoncer :

- pour que A soit vraie, il est nécessaire et suffisante que B le soit
- A a lieu si et seulement si B a lieu
- A est vraie si et seulement si B l'est.

Règle

A	B	$A \Leftrightarrow B$
V	V	V
V	F	F
F	V	F
F	F	V

Remarque

S'il y a n variables propositionnels, il y a 2^n lignes dans la table de vérité. Cela pose un problème lorsque l'on veut étudier beaucoup de variables. Par exemple si il y a 64 variables, on ne peut même pas faire écrire par un ordinateur la liste des lignes. Le nombre 2^{64} est trop grand : supposons qu'on en écrive un million par seconde, combien de temps pour écrire toutes les lignes ? Et bien $2^{64}/10^6$ secondes, ce qui correspond un peu près à 500000 ans ! On ne sait pas s'il existe un algorithme polynomial, en la taille des données, qui résout ce problème.

Le fait que 2^{64} est un grand nombre est à la base d'une histoire concernant le jeu d'échec(né en Inde) : l'inventeur aurait demandé comme récompense du riz, correspondant à 1 grain sur la $1^{ère}$ case, 2 grains sur la $2^{ième}$, 4 sur la $3^{ième}$, 8 sur la $4^{ième}$ etc ..., soit $1+2+4+\ldots+2^{64}$ puisqu'il y a 64 cases sur l'échiquier. Cela fait $2^{64}-1$ grains, quantité excédant largement les ressources planétaires.

II) Le calcul des prédicats.

Le langage en termes de proposition est très restreint. La plupart des phrases mathématiques ne s'expriment que dans un langage plus évolué, pensez par exemple à la phrase «pour tout réel $\varepsilon > 0$, il existe ...».

A) Prédicats et quantificateurs

Définition

☐ Un prédicat est un énoncé A contenant une ou plusieurs variables x, y, ... qu'on peut remplacer par des éléments de tel ou tel ensemble, produisant ainsi des assertions $A(x, y, \cdots)$ valides.

☐ Dans un premier temps, on ne considère que des prédicats à une variable x, x pouvant être remplacé par les éléments d'un ensemble E, appelé le référentiel du prédicat.

☐ Si pour un élément x de E, l'assertion $A(x)$ est vraie, on dit que x vérifie la propriété A, et on écrit simplement "$A(x)$" plutôt que "$A(x)$ est vraie".

☐ Soit $\Re(x)$ une assertion dépendant de l'objet variable x, on écrit $\exists x \,|\Re\,(x)$ pour exprimer qu'il existe au moins un des objets x pour lequel $\Re(x)$ est vrai. $\exists$ est appelé quantificateur existentiel.

☐ On écrit $\forall x \,|\Re\,(x)$ pour dire quelque soit x, $\Re(x)$ est vrai ou pour tout x, $\Re(x)$ est vrai. $\forall$ est appelé quantificateur universel.

Théorème

La négation d'une propriété contenant un certain nombre de fois les quantificateurs $\forall$, $\exists$, et ensuite l'énoncé d'un propriété P, s'obtient en remplaçant chaque quantificateur $\forall$ par le quantificateur $\exists$ et vice versa, et la propriété P par sa négation $\overline{P}$.

Preuve

Supposons qu'il n'y ait qu'un seul quantificateur, par exemple $\forall$. Notre propriété a donc la forme :

$$(\forall x \text{ vérifiant } S) : P.$$

Sa négation est évidemment : il existe un x vérifiant S qui cependant ne vérifie pas P, ou

$$(\exists x \text{ vérifiant } S) : \overline{P}.$$

Le théorème est ainsi démontré dans ce cas, et aussi, de manière analogue, s'il n'y a qu'un quantificateur $\forall$.
Il suffit alors de faire une récurrence sur le nombre de quantificateurs. Supposons le théorème démontré lorsqu'il y a $(n-1)$ quantificateurs, montrons le lorsqu'il y en a n. Alors la propriété s'écrit, par exemple :

$$(\forall x \text{ vérifiant } S) : L.$$

où L est une propriété contenant $(n-1)$ quantificateurs. Sa négation est donc

$$(\exists x \text{ vérifiant } S) : \overline{L},$$

en vertu de ce qui a été vu pour un seul quantificateur ; mais $\overline{L}$ s'obtient en appliquant le théorème, puisque L ne contient que $(n-1)$ quantificateurs, et alors le théorème est encore vrai dans ce cas ; il en est de même si le premier quantificateur est $\exists$, et le théorème est vrai dans le cas général.

La logique qu'on vient de voir est bivalente (deux valeurs) : il y a deux qualifications vrai ou faux. A cote de cette logique, on peut construire des logiques plurivalentes. En réalité, ces logiques répondent à certaines exigences des sciences modernes. Par exemple, Heyting propose une logique à trois valeurs : le vrai. le faux et l'indécidable. Cette logique répond aux besoins de la mathématique intuitionniste de Brouwer qui distingue le vrai, le faux et l'absurde.

B) Applications au raisonnement mathématique.

Définition

☐ Les définitions mathématiques paraissent s'opposer radicalement aux définitions empiriques. Les définitions empiriques sont de simples descriptions, c'est-à-dire des copies de la nature. En mathématique, les définitions sont d'une autre nature. Elles ne sont pas descriptives, mais créatrices. Définir un objet mathématique c'est le construire et le créer. Le rapport du mathématicien aux êtres mathématiques est celui d'un Dieu à ses créatures. Dans cette perspective, on peut dire que la définition mathématique est un modèle.

☐ Les postulats sont des propositions indémontrables que le mathématicien demande (postulare) à son auditeur d'accorder. Le mathématicien fait appel à la bonne volonté de l'auditeur. Mais depuis l'invention de la géométrie non-euclidienne, les postulats apparaissent comme des définitions déguisées (Poincaré).

☐ Les axiomes sont des exigences purement logiques, des conventions opératoires identiques aux codes de la route. Les axiomes ne sont ainsi ni vrais, ni faux. Ils s'imposent dans toutes les branches de la mathématique. C'est ce mot qu'on utilise aujourd'hui à la place des postulats car depuis l'invention de la géométrie non-euclidienne on s'est aperçu qu'il n'existe pas de vérité absolue.

☐ Les théorèmes sont des expressions d'un système formel démontrables à l'intérieur de ce système. Les lemmes sont des propositions préliminaires dont la démonstration facilite celle d'un théorème subséquent. Les corollaires sont des conséquences nécessaires et évidentes des théorèmes.

☐ Démontrer une proposition par l'absurde consiste à partir non pas de cette proposition supposée vraie, mais de sa contradiction et de remonter ainsi à des propositions qui seront en contradiction avec des propositions précédemment établies.

Remarque

En mathématique, la justification de la fausseté d'un énoncé est la donnée d'un contre exemple.

Exemple

☐ Montrons que la phrase «f strictement croissante sur $I \Leftrightarrow \forall x \in I,\ f'(x) > 0$» est fausse.
Pour cela, on étudie l'exemple $f : x \mapsto x^3$ sur $[-1, 1]$. f est strictement croissant sur $[-1, 1]$, mais $f'(0) = 0$.

☐ L'oiseau se définira comme un vertébré ovipare qui a des ailes et des plumes. Cette définitions est purement biologique. Le biologiste ne crée pas l'oiseau, il le découvre. En mathématique, un cercle C de centre O et de rayon R est l'ensemble de points à distant du point O. On vient de construire un objet qui n'existe pas dans la nature.

☐ En arithmétique, on ne peut pas diviser par 0. Pourquoi ? Eh bien, raisonnons par l'absurde. Supposons qu'on peut diviser par 0. Soient a et b deux nombres égaux différent de 0, on peut écrire $a = b$. Multiplions par a membre à membre, on obtient :

$$a^2 = ab$$

On soustrait ensuite par b^2 membre à membre, on a :

$$a^2 - b^2 = ab - b^2.$$

On factorise, on obtient :

$$(a + b)(a - b) = b(a - b)$$

Si on divise par 0, on obtient

$$a + b = b.$$

Comme $a = b$, on a : $a = \dfrac{a}{2}$. En divisant par a dans chaque membre, il vient $1 = \dfrac{1}{2}$, ce qui est contradictoire avec les règles de l'arithmétique. Donc on ne peut pas diviser par 0.

☐ Euclide pour démontrer sa vingt-neuvième proposition demande qu'on veuille bien lui accorder que par un point pris hors d'une droite dans un plan on ne peut mener qu'une seule parallèle.

☐ Euclide postule que le tout est plus grand que la partie. Or si on considère l'ensemble des entiers naturels $\mathbb{N}$ et l'ensembles des entiers naturels pairs $2\mathbb{N}$, on constate qu'il existe une bijection de $\mathbb{N}$ dans $2\mathbb{N}$. D'après un théorème en algèbre, s'il existe une bijection entre deux ensembles, ces deux ensembles ont même cardinal. Donc de façon imagée il y a autant d'entiers pairs que d'entiers naturels. L'axiome d'Euclide n'est donc pas compatible avec notre système formel.

☐ Soit (x_n) une suite réelle. On dit que $\ell \in \mathbb{R}$ est limite de (x_n) lorsque

$$\forall \varepsilon > 0,\ \exists p \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geq p \Rightarrow |x_n - \ell| \leq \varepsilon.$$

La phrase logique exprimant qu'un réel ℓ n'est pas limite de (x_n) est :

$$\exists \varepsilon > 0,\ \forall p \in \mathbb{N},\ \exists n \in \mathbb{N},\ n \geq p \text{ et } |x_n - \ell| > \varepsilon.$$

☐ On dit qu'une suite (x_n) de réels est une suite de Cauchy lorsque

$$\forall \varepsilon > 0,\ \exists p \in \mathbb{N},\ \forall (m, n) \in \mathbb{N}^2,\ m,\ n \geq p \Rightarrow |x_m - x_n| \leq \varepsilon.$$

La phrase logique exprimant qu'une suite (x_n) n'est pas de Cauchy est :

$$\exists \varepsilon > 0,\ \forall p \in \mathbb{N},\ \exists (m, n) \in \mathbb{N}^2,\ m,\ n \geq p \Rightarrow |x_m - x_n| > \varepsilon.$$

☐ Une application f de $\mathbb{R}$ dans $\mathbb{R}$ est continue en $a \in \mathbb{R}$ lorsque

$$\forall \varepsilon > 0,\ \exists \eta \in \mathbb{R}_+^*,\ \forall x \in \mathbb{R},\ |x - a| < \eta \Rightarrow |f(x) - f(a)| \leq \varepsilon.$$

La phrase logique exprimant que f n'est pas continue en a est :

$$\exists \varepsilon > 0,\ \forall \eta > 0,\ \exists x \in \mathbb{R},\ |x-a| < \eta \text{ et } |f(x)-f(a)| > \varepsilon.$$

□ Une application f de $\mathbb{R}$ dans $\mathbb{R}$ est uniformément continue sur un intervalle I de $\mathbb{R}$ lorsque

$$\forall \varepsilon > 0,\ \exists \alpha \in \mathbb{R}_+^*,\ \forall (x,y) \in \mathbb{R}^2,\ |x-y| < \eta \Rightarrow |f(x)-f(y)| \leq \varepsilon.$$

La phrase logique exprimant que f n'est pas uniformément continue sur I est :

$$\exists \varepsilon > 0,\ \forall \eta > 0,\ \exists (x,y) \in \mathbb{R}^2,\ |x-y| < \eta \text{ et } |f(x)-f(y)| > \varepsilon.$$

□ Considérons deux propositions

A : l'ensemble des nombres premier est infini.

B : tout entier supérieur ou égal à 2 possède un diviseur premier.

On suppose que B est un théorème et on veut monter A par l'absurde. On suppose $\overline{A}$ vrai. Si A est fini, on écrire l'ensemble des nombres premiers sous la forme

$$\{1, \ldots, p_k\}.$$

Posons $q = p_1 \ldots p_k + 1$. Aucun p_i ne divise q, donc B est faux.

□ On suppose que

$$u_n = 1 + \ldots + \frac{1}{n!} < e < u_n + \frac{1}{n!}.$$

Montrons que e n'est pas rationnel. Soit A la proposition suivante :

$$A : e \notin \mathbb{Q}.$$

Le raisonnement par absurde s'impose lorsqu'il est plus simple de montrer $\overline{A}$. Supposons que e soit rationnel, il existe alors p et q des entiers tels que : $e = \dfrac{p}{q}$. Il vient donc

$$u_n < \frac{p}{q} < u_n + \frac{1}{n!} \Rightarrow q!u_q < p(q-1)! < u_q q! + 1.$$

Posons $n = q!u_q$, on obtient : $n < p(q-1)! < n+1$.

Comme $p(q-1)!$ est un entier, on obtient une absurdité.

□ Donnons nous un exemple de raisonnement par contraposition. Nous voulons montrer la propriété suivante

C : si pour toute suite (x_n) telle que $\lim\limits_{n\to+\infty} x_n = x_0$, on a $\lim\limits_{n\to+\infty} f(x_n) = \ell$, alors $\lim\limits_{x\to x_0} f(x_0) = \ell$.

Soit A et B des propositions, et posons

A : $\forall (x_n),\ \lim\limits_{n\to+\infty} x_n = x_0 \Rightarrow \lim\limits_{n\to+\infty} f(x_n) = \ell$

B : $\lim\limits_{x\to x_0} f(x_0) = \ell$

On peut vérifier $\overline{B}$.

Comment exprimer $\overline{A}$? D'après les règles sur l'implication, on sait que les propositions suivantes : ($\overline{C}$ ou D) et ($C \Rightarrow D$) sont synonymes. Donc A est synonyme de

$$\forall (x_n),\ \text{non } (\lim_{n\to+\infty} x_n = x_0) \text{ ou } \lim_{n\to+\infty} f(x_n) = \ell.$$

Exprimons $\overline{A}$:

$\overline{A}$: non ($\forall x_0$, non ($\lim\limits_{n\to+\infty} x_n = x_0$) ou $\lim\limits_{n\to+\infty} f(x_n) = \ell$)

$\Rightarrow \overline{A}$: $\exists (x_n)$, ($\lim\limits_{n\to+\infty} x_n = x_0$) et non ($\lim\limits_{n\to+\infty} f(x_n) = \ell$).

Autrement dit, il existe une suite (x_n) tel que $\lim\limits_{n\to+\infty} x_n = x_0$ et $f(x_n)$ ne tend pas vers ℓ.

Exprimons $\overline{B}$:

$$\exists \varepsilon > 0,\ \forall \eta > 0,\ \exists x / |x-x_0| < \eta \text{ et } |f(x)-\ell| \geq \varepsilon.$$

En particulier, on a :

$$\exists \varepsilon > 0,\ \forall n > 0,\ \exists x / |x - x_0| < \frac{1}{n} \text{ et } |f(x) - \ell| \geq \varepsilon,$$

qui est la proposition $\overline{A}$.

Remarque

Les exemples ci-dessus montrent que le mathématicien n'est pas un automate ou une machine à déduire. II faut qu'il fasse preuve d'intuitions ingénieuses pour faire surgir des tautologies ou des contradictions. C'est un art. Pascal invitait le mathématicien à tourner les propositions à tout sens et Evariste Galois disait que le mathématicien ne déduit pas mais combine, compare et ne parvient à faire des découvertes qu'en heurtant de coté et d'autre.

Raisonnement par récurrence

☐ Une proposition vraie dans certain cas particulier peut-elle être vraie en général ? La réponse peut être donnée par le raisonnement par récurrence. Dans le cours sur les entiers naturels, nous verrons la démonstration de ce théorème :

soit $\Re(n)$ une relation dépendant d'un entier naturel n et telle que $\Re(1)$ soit vraie. Si pour tout entier naturel n, $\Re(n)$ implique $\Re(n+1)$, alors $\Re(n)$ est vraie pour tout entier naturel n.

Exemple

☐ Etablissons l'inégalité de Jean Bernoulli :

$$\text{si } h > -1, \text{ alors } (1+h)^n \geq 1 + nh \text{ pour tout } n \in \mathbb{N}.$$

En effet, l'inégalité de Bernoulli est vraie pour $n = 1$.

Supposons qu'elle est vraie pour $n = m > 1$, c'est-à-dire

$$(1+h)^m \geq 1 + mh.$$

Alors multiplions les deux membres de cette inégalité par $(1+h) > 0$:

$$(1+h)^{m+1} \geq (1+mh) \cdot (1+h) = 1 + (m+1)\,h + mh^2.$$

En éliminant le terme positif mh^2, on obtient $(1+h)^{m+1} \geq 1 + (m+1)\,h$, c'est-à-dire l'inégalité est valable pour $n = m+1$, donc elle l'est pour tout entier naturel n.

☐ On vous laisse le soin de vérifier par récurrence que la somme des n premiers entiers vaut $\frac{n(n+1)}{2}$.

Raisonnement par analyse synthèse

☐ Lorsqu'on raisonne par analyse-synthèse, on procède en deux étapes :

– l'analyse ou recherche des conditions nécessaires : on suppose qu'il existe une solution vérifiant les conditions ($\exists x \in E | x$ vérifie une propriété P). On raisonne alors par déduction, pour dresser un portrait assez précis de cette solution.

– la synthèse consiste à retenir les éléments (de l'ensemble des suspects correspondant à la description) obtenue à la fin de l'analyse). Il s'agit donc d'une vérification sur un nombre fini de cas.

Exemple

☐ Montrons par analyse-synthèse que pour toute fonction f de $\mathbb{R}$ dans $\mathbb{R}$, il existe un et un seul couple de fonction (g, h) chacune de $\mathbb{R}$ dans $\mathbb{R}$ telles que $f = g + h$ avec g paire et h impaire.

Analyse : supposons trouvées g et h deux fonctions de $\mathbb{R}$ dans $\mathbb{R}$ telles que $f = g + h$ avec g paire et h impaire. Soit $x \in \mathbb{R}$, $f(x) = g(x) + h(x)$ et $f(-x) = g(-x) + h(-x) = g(x) - h(x)$. On obtient rapidement

$$g(x) = \frac{1}{2}[f(x) + f(-x)] \text{ et } h(x) = \frac{1}{2}[f(x) - f(-x)].$$

On a donc l'existence et l'unicité du couple (g, h).
Synthèse : soit g et h les fonctions définies sur $\mathbb{R}$, respectivement par

$$\forall x \in \mathbb{R},\ g(x) = \frac{1}{2}[f(x) + f(-x)] \text{ et } h(x) = \frac{1}{2}[f(x) - f(-x)].$$

Alors on a bien $f = g + h$. On vérifie facilement que $g(-x) = g(x)$ et $h(-x) = -h(x)$. Le couple (g, h) ainsi construit vérifie donc les conditions imposées.

Conclusion : il existe un et un seul couple de fonctions vérifiant les conditions requises.

☐ Cherchons l'ensemble des $(x, y) \in \mathbb{R}^2$ tels que $xy = 55$ et $x^2 + y^2 = 146$.

Analyse : supposons qu'il existe $(x, y) \in \mathbb{R}^2$ vérifiant les conditions requises. Posons $p = xy = 55$ et $s = x + y$. Alors $s^2 - 2p = x^2 + y^2 = 146$, donc $s^2 = 146 + 2 \times 55 = 256$. On en déduit $s = \pm 16$. Or reconnaissant le produit et la somme de deux réels, on peut en déduire ces réels, d'où quatre possibilités : $(5, 11)$, $(11, 5)$, $(-5, -11)$ et $(-11, -5)$.

Synthèse : on vérifie que ces quatre solutions vérifient effectivement les conditions imposées.

Conclusion : l'ensemble des solutions est $\{(5, 11), (11, 5), (-5, -11), (-11, -5)\}$.

C) Algorithmes

Le mot algorithme provient du mathématicien arabe Al Khwarizmi, né durant le IXième siècle en Perse. Chacun de nous applique les algorithmes appris depuis l'école primaire lorsqu'il calcule la somme de deux nombres.

Définition

☐ Un algorithme est une suite finie d'instructions d'une méthode de résolution d'un problème.

☐ Prouver un algorithme, c'est montrer qu'il parvient bien au résultat attendu, et en un nombre fini d'étapes. Tout algorithme doit être prouvé, comme un théorème en maths.

☐ La complexité d'un algorithme est l'estimation du temps de calcul en fonction de la taille des données. Le plus souvent, on associe à chaque donnée un nombre n directement lié à la complexité du problème. Pour chaque algorithme, on évalue le nombre d'instructions effectuées en fonction de n. Seul l'ordre de grandeur de cette quantité nous intéresse. On se contente en général d'évaluer le nombre d'itérations réalisées.

☐ Un algorithme est dit de complexité exponentielle lorsque le temps de calcul s'exprime comme une fonction exponentielle.

☐ Un algorithme est dit de complexité linéaire si ce temps est une fonction linéaire.

☐ Un algorithme est dit de complexité en n^2 si le temps de calcul est un trinôme. Les algorithmes de complexité linéaire, en $n \log n$ ou en n^2 sont des algorithmes rapides.

☐ Un algorithme est dit récursif lorsqu'il intervient lui-même dans sa propre description. Un algorithme récursif est lié à une situation du type : «si, pour une taille de données (notion à préciser) fixée, je sais résoudre le problème pour une taille inférieure de données, alors je sais résoudre le problème pour la taille fixée».

Les algorithmes, aussi complexes soient ils, sont construits à partir d'actions élémentaires, essentiellement au nombre de trois.

Définition

☐ Les affectations de variables qui permettent d'attribuer des valeurs à des variables ou de changer ces valeurs. On le symbolise par le symbole « :=». Par exemple, l'affectation $a := b$ stocke dans l'espace-mémore symbolisé par a la valeur b.

☐ Les instructions conditionnelles qui permettent de choisir une ou plusieurs alternatives en fonction du résultat d'un test. Nous écrirons cette instruction :

si < *Condition* > *alors* < *Alternatif* 1 >
sinon < *Alternatif* 2 >.
En Maple, ces instructions sont codées
if < *Condition* > *then* < *Alternatif* 1 > *else* < *Alternatif* 2 > *fi*.

☐ Les instructions itératives qui permettent d'automatiser l'exécution d'une séquence d'instructions en une boucle. Il est nécessaire de veiller à l'arrêt de la boucle. Ceci peut se faire de deux manières :

– Si le nombre N d'itérations est connu à l'avance, on écrira

$$pour\ i = 1\ à\ N\ faire < Instruction >.$$

En Maple : *for i from* 1 *to* N *do* < *Instructions* > *od*.

– Si le nombre d'itérations est inconnu et dépend de la réalisation d'une condition, on écrira :

$$tant\ que < Condition > faire < Instructions\ ¿.$$

En Maple : *while* < *Condition* > *do* < *Instructions* > *od*.

☐ A cela, il faut ajouter les instructions de lecture des données et de sortie des résultats.

Exemple

☐ *La dichotomie*

On souhaite déterminer des valeurs approchées des solutions d'une équation du type $f(x) = 0$, où f est une fonction continue. Une étude de la fonction f permet en général de définir des intervalles $I = [a, b]$ sur lesquels f est strictement monotone et change de signe entre a et b. Le théorème des valeurs intermédiaires assure alors l'existence d'une solution unique à l'équation, sur l'intervalle I. Nous supposerons donc ces conditions réalisées. On calcule

$$c = \frac{a+b}{2} \text{ et } f(c).$$

Si $f(a)$ et $f(c)$ sont de même signe, alors la solution cherchée est entre c et b, et on recommence la même méthode sur l'intervalle $[c, b]$.

Si $f(a)$ et $f(c)$ sont de signe contraire, alors la solution cherchée est entre a et c, et on recommence la même méthode sur l'intervalle $[a, c]$. On divise ainsi l'intervalle de recherche par 2 jusqu'à obtenir un encadrement de la précision ε voulue. Voici l'algorithme et le listing en Maple :

Lire a	> dichotomie := proc(f, a, b, epsilon)
Lire b	> local sup,inf,milieu ;
Lire ε	> if a < b then inf :=a ; sup :=b
sup := b	> else inf :=b ; sup :=a fi ;
inf := a	> while sup - inf > epsilon do
$Precision := \varepsilon$	> milieu := (inf + sup) / 2 ;
tant que sup − inf > $Precision$, faire	> if f(milieu)*f(inf) > 0 then inf := milieu
$Milieu := \frac{\sup + \inf}{2}$	> else sup := milieu fi ;
si $f(Milieu)f(\inf) > 0$, alors inf := $Milieu$	> od ;
sinon sup := $Milieu$	> evalf(milieu) ;
Fin tant que Ecrire Milieu	> end ;

En voici la preuve.

Soit n le nombre d'itérations dans la boucle tant que. On considère la propriété

$$P(n) : \text{soit } c \text{ la racine exacte de l'équation } f(x) = 0, \text{ alors on a : } c \in [\inf, \sup].$$

On va montrer que $P(n)$ est vraie en permanence lors de l'instruction itérative tant que. Il est clair que $P(1)$ est vraie, puisqu'on a supposé l'existence d'une racine unique dans l'intervalle

[inf := a, sup := b]. Supposons qu'au bout d'un nombre n quelconque d'itérations, $P(n)$ est vraie. Montrons que $P(n+1)$ reste encore valable. Plusieurs cas se présentent :

i) Si $f(Milieu) \times f(\text{inf}) > 0$, alors f change signe sur $[Milieu, \text{sup}]$ qui doit devenir notre nouvel intervalle d'étude, d'où l'instruction inf := $Milieu$.

ii) Si $f(Milieu) \times f(\text{inf}) < 0$, alors f change de signe sur $[\text{inf}, Milieu]$ qui doit devenir notre nouvel intervalle d'étude, d'où l'instruction sup := $Milieu$.

iii) Si $f(Milieu) = 0$ ou $f(\text{inf}) = 0$, alors c appartient évidemment à l'intervalle $[\text{inf}, Milieu]$ et l'affectation sup := $Milieu$ permet d'affirmer qu'on aura, après cette itération c dans l'intervalle [inf, sup].

L'instruction itérative doit devenir fausse au bout d'un nombre fini d'itérations. Si Precision est strictement positif, c'est effectivement le cas car

$$\text{sup} - \text{inf} = \frac{L}{2^n}$$

où L est la longueur initiale de l'intervalle et n le nombre d'itérations (on divise l'intervalle par 2 à chaque itération). Cette quantité devient inférieure à Precision pour

$$n > \frac{\ln(L/Precsion)}{\ln 2}.$$

Le nombre d'itérations est donc fini. Si Précision = $10^{(-n)}$, alors le nombre d'itérations est de l'ordre de n. La complexité de l'algorithme est dite de l'ordre de n. Pratiquement, cela signifie que le temps d'exécution de l'algorithme est proportionnel au nombre de décimales souhaitées.

□ *Suite de Fibonacci* définie par

$$\begin{cases} u_0 = u_1 = 1 \\ u_{n+1} = u_{n+1} + u_n \end{cases}$$

Voici les algorithmes :

Version récursive	> Fibo :=proc(n) # option remember
si $n \leq 1$, alors $Fibo(n) := 1$	> if n=0 or n=1 then 1
sinon $Fibo(n) := F(n-1) + F(n-2)$	> else Fibo(n - 1) + Fibo(n - 2)
	> fi ;
Version itérative	> end ;
$a := 1$ # $Fibo(0)$	
$b := 1$ # $Fibo(1)$	> Fibo2 :=proc(n)
Pour $i := 1$ à $(n-1)$ faire	> local i, u ;
$c := b$ # $c := Fibo(i) := b$, $a = Fibo(i-1)$	> u[0] :=1 ;
$b := a + b$ # $b := Fibo(i+1)$	> u[1] :=1 ;
$a := c$ # $a := Fibo(i)$	> for i from 2 to n do u[i] :=u[i-1]+u[i-2] od ;
$F(n) := b$	> End ;

Le calcul de chaque Fibo(n) nécessite le calcul de toutes les branches qui suivent. En particulier, Fibo(2) est calculé 3 fois. Le calcul final revient donc à sommer $1 + 1 + 1 + ... + 1$, Fibo(n) fois, qui croît exponentiellement. Pour $n = 100$, il y a en effet environ 800.000.000.000.000.000.000 sommes à faire, alors que 100 suffisent.

Remarque

□ Pour permuter le contenu de deux variables x et y, il est nécessaire d'introduire une variable temporaire par exemple $temp$: $temp := x$; $x := y$; $y := temp$.

□ Soit (u_n) une suite numérique. On veut calculer la somme $S = \sum_{i=1}^{n} u_i$ avec la convention $S := 0$ lorsque $n := 0$. On procède par récurrence :

$$S_0 = 0,\ S_1 = S_0 + u_1,\ ...,\ S_n = S_{n-1} + u_n,$$

d'où

$S := 0$
Pour $k := 1$ à n faire
$S := S + u[k]$
fin pour.

Maintenant, si $S = \sum_{i=1}^{p} \sum_{j=1}^{q} u_{i,j}$ est une somme double, il suffit d'utiliser deux boucles «pour » :

$S := 0$
Pour $i := 1$ à n faire
Pour $j := 1$ à n faire
$S := S + u[i, j]$
fin pour
fin pour.

Si on est dans le cas $S = \sum_{0 \leq i \leq n, i \neq k} u_i$, on peut faire :

$S := 0$
Pour $i := 1$ à n faire
si $i \neq k$, alors $S := S + u[i]$ fin si
fin pour.

Si on veut augmenter la vitesse, il suffit de faire moins de «test». On peut par exemple calculer les sous-sommes correspondant aux intervalles $[\![0, k-1]\!]$ et $[\![k+1, n]\!]$:

$S := 0$
si $[(0 \leq k)$ et $(k \leq n)]$,
alors
pour $i := 0$ à $(k-1)$ faire $S := S + u[i]$ fin pour
pour $i := (k+1)$ à n faire $S := S + u[i]$ fin pour
sinon
pour $i := 0$ à n faire $S := S + u[i]$ fin pour
fin si.

□ Soit u_1, u_2, ..., u_n des nombres réels et P une propriété dépendant de u_i. Pour trouver le maximum tel que P soit vraie, on peut faire :

$max := 0$
pour $i := 1$ à n faire
si $[x[i] > max)$ et $P(x[i])]$, alors
$max := x[i]$
$place\_max := i$
fin si
fin pour.

D) Rédaction d'une démonstration

Nous avons vu ici quelques principes de démonstration. Au chapitre suivant, nous allons étudier quelques règles de base du langage mathématique. Bien que ce langage présente l'avantage de produire des phrases mathématiques concises et comprises directement par les mathématiciens, son usage systématique pour rédiger une preuve n'est pas très commode. On fait un compromis entre le langage courant et formalisme mathématique. Le français est réduit à sa plus simple expression : soit, si, alors, d'où, supposons que, c'est-à-dire, etc...

1. On annonce le type de raisonnement
   Dès le début sauf s'il s'agit d'un raisonnement déductif, on annonce le type de raisonnement utilisé. Par exemple, écrivez : «je vais montrer, par l'absurde, que...», «montrons, par récurrence, que ...».
2. On annonce la technique ou le théorème utilisée si ils ont un nom
3. Définition des variables
   Si on utilise une variable non encore définie, deux cas se présentent :
   – cette variable n'est liée à aucune variable déjà définie, dans ce cas, on écrit «soit $x \in E$ ... »
   – cette variable est fonction d'une ou plusieurs variables déjà définies, dans ce cas on utilise «posons $z = x + y$ », «soit g la fonction définie en fonction de f par... » etc.
4. Utilisation d'un résultat
   Si dans un calcul on utilise un résultat démontré auparavant, on peut
   – soit numéroter ce résultat à un endroit du texte et rappeler le numéro quand vous l'utilisez : «d'après la formule (4)».
   – soit citer le numéro de la question : «d'après la propriété démontrée ou donnée au I)1)c-.
5. Si on utilise un résultat du cours portant un nom, on rappèle ce nom et vérifie que les hypothèses d'utilisation de ce résultat sont satisfaites dans le cas où on l'utilise : «d'après le théorème des valeurs intermédiaires, f étant continue sur $[0, 1]$, ... », «d'après la formule de la somme géométrique, z étant différent de 1, on a ... ».
6. Quand on utilise plusieurs fois le même résultat du cours. C'est le seul cas où l'on peut se permettre d'utiliser une abréviation. Au début du texte, on récapitule les abréviation utilisées par la suite : «T.A.F : théorème des accroissements finis».

Exemple

☐ Montrons l'égalité

$$\{x \in \mathbb{R} \mid \lim_{n\to+\infty} x^n = 0 \text{ ou } \lim_{n\to+\infty} x^n = 1\} =]-1, 1]$$

par double inclusion.

– Soit $x \in \mathbb{R}$ tel que $\lim_{n\to+\infty} x^n = 0$ ou $\lim_{n\to+\infty} x^n = 1$, montrons que $x \in]-1, 1]$. On raisonne par l'absurde. Supposons que $x \notin]-1, 1]$, nous avons alors deux cas : soit $x \leq -1$ et la suite $(x^n)_n$ n'a pas de limite ; soit $x > 1$ et $\lim_{n\to+\infty} x^n = +\infty$. Dans les deux cas, il y a contradiction avec la limite finie de $(x^n)_n$. Ainsi $x \in]-1, 1]$.

– Soit $x \in]-1, 1]$. On a deux cas : soit $x = 1$ et alors $\lim_{n\to+\infty} x^n = 1$; soit $x \in]-1, 1]$ et alors $\lim_{n\to+\infty} x^n = 0$. Donc x est élément de l'ensemble $\{x \in \mathbb{R} \mid \lim_{n\to+\infty} x^n = 0 \text{ ou } \lim_{n\to+\infty} x^n = 1\}$.

Finalement, on peut écrire $\{x \in \mathbb{R} \mid \lim_{n\to+\infty} x^n = 0 \text{ ou } \lim_{n\to+\infty} x^n = 1\} =]-1, 1]$.

Quelques bons conseils

Dans le raisonnement logique, la syntaxe est primordiale. Elle va de pair avec la clarté du style. Quelques bonnes habitudes doivent être prises :

☐ Indiquer clairement les hypothèses de la démonstration, et quel résultat on veut obtenir.

☐ Mettre en évidence les liens logiques entre les phases successives de la démonstration. Le symbole " $\Rightarrow$ " n'est pas innocent. Son emploi doit être justifié.

☐ Ne pas mélanger les symboles " $\Rightarrow$ " et " $\Leftrightarrow$ ".

☐ Dans une proposition "à tiroirs ", utiliser des parenthèses pour lever toute ambiguïté. Ainsi la proposition

$$(A \Rightarrow B) \Rightarrow C$$

n'est pas synonyme de

$$A \Rightarrow (B \Rightarrow C).$$

☐ Eviter d'utiliser exclusivement le langage de la logique formelle (propositions, quantificateurs) là où on peut s'exprimer "en français". En particulier, on ne mélangera pas les deux styles. On évitera d'écrire, par exemple : "pour tout $x \in E$,...").

☐ Varier le style, pour éviter toute sécheresse. Le mot "donc", par exemple, possède plusieurs synonymes : "on en déduit", "il s'ensuit", "par conséquent", etc.

☐ On peut construire des assertions avec plusieurs quantificateurs, notamment sur des prédicats $A(x, y, \cdots)$ à plusieurs variables. Dans ce cas, on prendra garde à l'ordre de ces quantificateurs. Par exemple :

"$\forall x \in E,\ \exists y \in F,\ A(x, y)$" n'est pas synonyme de " $\exists y \in F,\ \forall x \in E,\ A(x, y)$".

On le vérifie avec les assertions :

"$\forall x \in \mathbb{N},\ \exists y \in \mathbb{N},\ x \leq y$" et " $\exists y \in \mathbb{N},\ \forall x \in \mathbb{N},\ x \leq y$".

☐ Dès que l'on vous demande de démontrer une propriété «pour tout entier n», vous pouvez essayez d'appliquer une récurrence :il y a grandes chances que cela fonctionne à merveille. Plus précisément, on pensera aux cas suivants :

– suites et séries (monotonie, encadrements, etc...

– fonctions (propriétés sur les dérivées successives).

– intégration (formule de récurrence par intégration par parties).

– polynômes (récurrence sur le degré, passage de n à $(n + 1)$ par intégration)...

– ensemble (récurrence sur le cardinal)

– espaces vectoriels et matrices (dimension, etc...)

☐ Raisonner par l'absurde pour démontrer

$$A \Rightarrow B$$

consiste à supposer A et non B et à chercher ensuite une contradiction.

☐ Raisonner par contraposition

$$A \Rightarrow B$$

consiste à montrer

$$\text{non } B \Rightarrow \text{non } A.$$

☐ Lorsque l'on veut prouver que deux propositions sont équivalentes, il est généralement dangereux de prouver directement cette équivalence. Mieux vaut prouver séparément les deux implications séparément, d'autant que généralement l'une des deux est plus simple que l'autre. Commencez par raisonner par implication, en regardant ce qu'entraînent vos hypothèses. Si vous ne parvenez pas à remonter aux hypothèses initiales, c'est que les propriétés que vous avez trouvée sont trop faibles (nécessaires, mais pas suffisantes).

Supposons que l'on vous demande d'établir l'équivalence entre

$$\text{(i)} \Leftrightarrow \text{(ii)} \Leftrightarrow \text{(iii)} \Leftrightarrow \text{(iv)}$$

Il est hors question de démontrer toutes les équivalences. La bonne méthode est de partir d'un bout, et d'essayer d'y parvenir en passant par toute les propositions. Par exemple, il est suffisant de montrer

$$\text{(i)} \Rightarrow \text{(iv)} \Rightarrow \text{(iii)} \Rightarrow \text{(ii)} \Rightarrow \text{(i)}$$

Chercher le chemin le plus court.

□ Lorsque l'on vous demande de trouver une caractérisation, on ne vous demande en fait rien d'autre que des conditions nécessaires et suffisantes de E (c'est ce que l'on appelle raisonner par analyse-synthèse).

□ Prouver que les éléments de E sont **exactement** les fonctions telles que ... Il y a là deux choses à démontrer, à savoir une double inclusion.

– Les éléments de E sont des fonctions telles que...

– Les fonctions telles que ... sont effectivement des éléments de E.

Chercher le chemin le plus court.

□ La preuve d'un algorithme peut se décomposer en :

– la description verbeuse du résultat d'une séquence d'instructions.

– la preuve d'une boucle inconditionnelle : montrer par récurrence le résultat de la boucle.

– la preuve d'une boucle conditionnelle : montrer en plus que la condition d'arrêt finit nécessairement par être remplie.

– la preuve de chacun des sous-algorithmes auxquels l'algorithme fait appel.

– la démonstration d'un algorithme récursif se fera en utilisant la récurrence sur la taille).

□ Lorsque l'on vous demande de prouver l'existence et l'unicité, il y a deux règles à respecter si vous voulez parvenir au but sans encombres :

– séparer la preuve de l'existence de celle de l'unicité.

– commencer par prouver la non-multiplicité, c'est souvent le plus simple et ça peut donner une idée pour l'existence.

L'unicité se prouve en utilisant certains théorèmes, en raisonnant sur la monotonie, par l'absurde etc... L'existence se prouve en appliquant certains théorèmes de vos cours qui garantissent l'existence d'un objet. Sinon, elle se prouve par construction, il s'agit d'expliciter un élément satisfaisant aux conditions requises. Il arrive fréquemment que l'unicité soit assez lié à l'existence, c'est-à-dire que la vérification de l'unicité peut vous donner une idée assez précise pour l'existence.

Langage des ensembles

Le célèbre mathématicien Georg Cantor[1] (1845-1918) a introduit le langage des ensembles vers 1870, à fin de préciser certaines questions de l'analyse. Ce langage permet d'unifier la présentation de questions très diverses et apporte à l'exposé du mathématicien des qualités indispensables de clarté et de rigueur. La justification des règles posées par Georg Cantor fait l'objet de la théorie des ensembles, c'est là une affaire de spécialistes, lesquels sont des logiciens et non nécessairement des mathématiciens.

Dans ce chapitre, nous allons présenter les concepts ensemblistes de base : ensemble, appartenance, fonction, relation... C'est à partir de ces concepts que les mathématiques sont formalisées aujourd'hui. On peut faire des mathématiques en dehors de ce cadre puisqu'on a fait ainsi pendant des millénaires. On peut même penser que dans le futur on trouvera d'autres cadres. Mais en ce moment de notre histoire, les ensembles constituent par leur portée, leur précision et leur concision le meilleur cadre que l'on a.

Les objets étudiés plus tard dans ce cours pourraient être présentés sans recours aux ensembles. Une fois le problème étudié, on peut se débarrasser de cet intermédiaire et retourner à un mode d'expression plus simple puisque la plupart des objets mathématiques sont apparus bien avant l'invention des ensembles. Mais l'expérience montre qu'il est très commode de disposer d'un moyen précis et opérationnel de s'exprimer. C'est ce qui fournit le langage des ensembles pour manipuler les différents êtres mathématiques, pour prouver quelque chose, surtout si l'on n'est pas expert. La forme ne se sépare pas si facilement du contenu : l'étude des ensembles a eu des retombées significatives sur les mathématiques. Mais ceci ne nous concerne nullement dans ce chapitre...

I) Notion d'ensembles et de relations.

Il n'existe aucune définition possible des ensembles. Mais, nous allons quand même proposer une pseudo-définition pour notre commodité.

A) Ensembles et éléments

Définition

☐ Intuitivement, un ensemble est une collection d'objets. Les objets d'un ensemble sont appelés éléments de cet ensemble.

☐ Soit E un ensemble constitué d'éléments. Si l'on admet que x est un élément de l'ensemble E, on dit que x appartient à l'ensemble E et on note $x \in E$ (lire x appartient à E). Lorsque x n'est pas élément de E, on note $x \notin E$ (lire x n'appartient pas à E).

[1] **Georg Cantor** : Mathématicien allemand né en 1845 et mort en 1918. Il naît à Saint-Pétersbourg. Il enseigne à l'université de Halle et y devient professeur à partir de 1872. Ses premiers travaux sur les séries de Fourier le mènent au développement d'une théorie des nombres irrationnels. Cantor formule également la théorie des ensembles, sur laquelle l'analyse mathématique moderne est fondée. Cette théorie étend le concept de nombre en y introduisant l'idée de l'infini ou, comme Cantor lui-même les a appelés, les nombres transfinis. Les travaux de Cantor seront alors le fondement de la critique logique des mathématiques.

☐ Soient E et F deux ensembles. On dit que E est inclus dans F et on note $E \subset F$ (lire E inclus dans F) si et seulement si la relation d'appartenance à E implique la relation d'appartenance à F, ce qu'on note

$$\forall x \in E \Rightarrow x \in F \text{ (lire quelque soit } x \text{ appartient à } E \text{ implique } x \text{ appartient à } F).$$

☐ Soient E et F deux ensembles. On dit que E et F sont égaux si et seulement si la relation d'appartenance à E est équivalence à celle de F, c'est-à-dire : $E = F \Leftrightarrow E \subset F$ et $F \subset E$.

☐ Soit E un ensemble. Si un ensemble A est contenu dans E, on dit que A est une partie ou un sous-ensemble de E. Les éléments de E n'appartenant pas à l'ensemble A constituent une nouvelle partie de E, appelée complémentaire de A dans E et notée ${}^cA$ ou $E - A$. Formellement, $E - A = \{x \in E \mid x \notin A\}$.

☐ Les parties de l'ensemble E constitue un nouvel ensemble, appelé ensemble des partie de E et noté $\mathcal{P}(E)$.

☐ Pour tout x de E, on appelle singleton de x l'ensemble $\{x\}$ définie par

$$\forall t \in \{x\},\ t = x.$$

☐ On définit $(a, b) = \{\{a\}, \{a, b\}\}$, puis de pas en pas $(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$.

Vous pouvez vous amuser à définir d'autres ensembles, par exemple l'ensemble pair $\{x, y\}$ de x et y est définie par $\{x, y\}$. On résume ces différentes définitions sous forme d'axiomes :

Axiomes d'extensionnalité et du vide

1°) Tout ensemble E est inclus dans lui-même, c'est la réflexivité de l'inclusion : $E \subset E$.

2°) Soient E et F des ensembles. Si $E \subset F$ et $F \subset E$, alors $E = F$, c'est l'antisymétrie de la relation d'inclusion.

3°) Soient E, F et G des ensembles. Si $E \subset F$ et $F \subset G$, alors $E \subset G$, c'est la transitivité de l'inclusion.

4°) Il existe un ensemble contenant aucun élément, appelé ensemble vide et noté $\emptyset$, qui possède une propriété étonnante :

$$\text{pour toute propriété } P(x),\ \forall x \in \emptyset,\ P(x).$$

Lemme

Soit M un sous ensemble de E. Alors ${}^c({}^cM) = M$.

Preuve

On a :

$$x \in {}^c({}^cM) \Leftrightarrow x \in E \text{ et } x \notin {}^cM \Leftrightarrow x \in E \text{ et non } (x \notin M) \Leftrightarrow x \in E \text{ et } x \in M,$$

donc ${}^c({}^cM) = M$.

Propriété

1°) Soient M et N des parties d'un ensemble E, alors les relations suivantes sont équivalentes

i- $M \subset N$

ii- $E - N \subset E - M$.

2°) L'ensemble vide est inclut dans tous les ensembles.

3°) L'ensemble vide est unique.

Preuve

1°) Montrons i) ⇒ ii). Si $M \subset N \subset E$, alors

$$x \in {}^cN \Leftrightarrow x \in E \text{ et } x \notin N \Rightarrow x \notin M \Rightarrow x \in {}^cM$$

puisque par hypothèse M est inclus dans N. D'où l'implication i) $\Rightarrow$ ii).

Montrons finalement ii) $\Rightarrow$ i). Supposons

$$^cN \subset {}^cM.$$

L'implication que l'on vient de justifier entraîne

$$^c(^cM) \subset {}^c(^cN),$$

soit $M \subset N$; et on a bien l'équivalence entre i) et ii).

2°) Soit E un ensemble, alors l'implication suivante est vraie

$$(\forall x \in \emptyset) \ \Rightarrow \ (x \in E).$$

Donc $\emptyset \subset E$.

3°) Supposons l'existence de deux ensembles vides $\emptyset$ et $\emptyset'$, alors d'après 2°) on a

$$\emptyset \subset \emptyset' \text{ et } \emptyset' \subset \emptyset.$$

Donc $\emptyset = \emptyset'$.

Propriété

On a :

$$(a, b) = (a', b') \ \Rightarrow \ a = a' \text{ et } b = b'.$$

Preuve

Si $(a, b) = (a', b')$, alors

$$\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}.$$

On a plusieurs cas :

- si $\{a\} = \{a'\}$ et $\{a, b\} = \{a', b'\}$, alors
$$(a = a') \text{ et } (b = a' \text{ ou } b = b').$$
Cela donne ou bien $a = a'$ et $b = b'$, ou bien $b = a = a'$. Dans le dernier cas, on a :
$$\{a, b\} = \{a\} = \{a', b'\}.$$
Donc $\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$.
- si $\{a\} = \{a'\}$ et $\{a, b\} = \{a\prime\}$, alors $a = b = a' = b'$.
- si $\{a\} = \{a'\}$ et $\{a, b\} = \{a'\}$, alors $a = b = a' = b'$.
- si $\{a\} = \{a', b'\}$ et $\{a, b\} = \{a', b'\}$, alors $a = a' = b' = b$.

Finalement, on a bien : $a = a'$ et $b = b'$.

Exemple

□ Soit un ensemble $A = \{a, b, c\}$. L'ensemble des parties $\mathcal{P}(A)$ de A est la famille de tous les sous ensembles de A. On a alors $P(A) = \{A, \{a, b\}, \{a, c\}, \{b, c\}, \{a\}, \{b\}, \{c\}, \emptyset\}$.

Remarque

Si $A' \in P(A)$, alors $A' \subset A$.

On démontrera que si Card $(A) = n$, alors Card $\mathcal{P}(A) = 2^n$.

B) Opérations sur les ensembles

Nous allons nous intéresser aux opérations élémentaires sur les ensembles, la réunion et l'intersection. Vous pouvez faire des dessins, appelés diagramme de Venn[2], pour se donner une idée.

[2] **John Venn** : (1834 - 1923)

Définition

☐ Soient E et F deux ensembles. Les éléments appartenant à l'un au moins des ensembles E et F constituent un nouvel ensemble, appelé réunion de E et de F et noté $E \cup F$ (lire E union de F) :

$$E \cup F = \{x, x \in E \text{ ou } x \in F\}.$$

☐ Soient E et F deux ensembles. Les éléments appartenant à la fois à E et à F constituent un nouvel ensemble, appelé intersection de E et de F et noté $E \cap F$ (lire E inter F) :

$$E \cap F = \{x, x \in E \text{ et } x \in F\}.$$

Si l'intersection de E et de F est vide, on dit que E et F sont disjoints, ce qu'on écrit $E \cap F = \emptyset$.

☐ On appelle différence de A et B la partie notée $A - B$ (ou $A \backslash B$) définie par

$$\{x \in E | x \in A \text{ et } x \notin B\}.$$

On a

$$A \backslash B = A \cap \overline{B}.$$

☐ La différence symétrique de A et B est : $A \Delta B = (A \backslash B) \cup (B \backslash A)$.

Propriété

i) Idempotence $E \cup E = E$, commutativité $E \cup F = F \cup E$, associativité$(E \cup F) \cup G = E \cup (F \cup G)$.

ii) Idempotence $E \cap E = E$, associativité $(E \cap F) \cap G = E \cap (F \cap G)$, commutativité $E \cap F = F \cap E$.

Propriété

i) Idempotence $E \cup E = E$, commutativité $E \cup F = F \cup E$, associativité $(E \cup F) \cup G = E \cup (F \cup G)$.

ii) Idempotence $E \cap E = E$, associativité $(E \cap F) \cap G = E \cap (F \cap G)$, commutativité $E \cap F = F \cap E$.

iii) Soient E, F et G des ensembles. Si $E \subset F$, alors $E \cup G \subset F \cup G$.
On dit que la réunion est compatible avec la relation d'égalité.

iv) Soient E, F et G des ensembles. Si $E \subset F$, alors $E \cap G \subset F \cap G$.
On dit que l'intersection est compatible avec la relation d'inclusion.

Preuve

i) Soit x un élément de $E \cup G$. Si x appartient à G, x appartient évidemment à $F \cup G$. Si x n'appartient pas à G, x appartient nécessairement à E, par suite x appartient à F et donc à $F \cup G$. On a bien prouver l'assertion suivante : $\forall x \in E \cup G \Rightarrow x \in F \cup G$, donc $E \cup G \subset F \cup G$.

ii) Soit x un élément de $E \cap G$, c'est-à-dire un élément commun à E et G. Comme E est inclus dans F, x appartient à la fois à F et à G.

Propriété : (Lois de De Morgan)

Soient A et B deux parties d'un ensemble E. On a :

i) ${}^c(A \cup B) = {}^cA \cap {}^cB$

ii) ${}^c(A \cap B) = {}^cA \cup {}^cB$.

Preuve

i) On a :

$$x \in {}^c(A \cup B) \Leftrightarrow x \notin A \cup B \Leftrightarrow x \notin A \text{ et } x \notin B \Leftrightarrow x \in {}^cA \text{ et } x \in {}^cB.$$

Cela est équivalent à $x \in {}^cA \cap {}^cB$, d'où ${}^c(A \cup B) = {}^cA \cap {}^cB$.

ii) Posons $A' = {}^cA$ et $B' = {}^cB$. D'après i), on a

$${}^c(A' \cup B') = {}^cA' \cap {}^cB'.$$

Mais ${}^cA' = A$ et ${}^cB' = B$, donc ${}^c(A' \cup B') = A \cap B$. En prenant en particulier le complémentaire de chaque membre, on a :

$$^c(^c(A' \cup B')) = \ ^c(A \cap B).$$

On obtient

$$A' \cup B' = \ ^c(A \cap B), \text{ d'où } ^cA \cup \ ^cB = \ ^c(A \cap B).$$

Propriété : (distributivité)

Soient E, F et G trois ensembles. On a alors
i) $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$.
ii) $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$.

Preuve

i) Soit x un élément tel que $x \in E$ et $x \in F \cup G$. Si $x \in F$, alors

$$x \in (E \cap F).$$

Si $x \in G$, alors

$$x \in (E \cup G),$$

donc

$$x \in (E \cap F) \cup (E \cap G).$$

En résumé, $x \in E \cap (F \cap G) \Leftrightarrow x \in (E \cap F) \cup (E \cap G)$.

ii) De i), on peut déduire que $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$. En effet, posons

$$H = E \cup F \cup G,\ E\prime = \ ^cE,\ F' = \ ^cF \text{ et } G' = \ ^cG \text{ (complémentaire dans } H).$$

On a alors

$$^c(E' \cap (F' \cup G')) = E \cup \ ^c(F' \cup G')$$

et

$$^c(F' \cup G') = F \cap G.$$

De même

$$^c(E' \cap F') = (^cE') \cup (^cF') = E \cup F$$
$$^c(E' \cap G') = \ ^cE' \cup \ ^cG' = E \cup G.$$

Or

$$E' \cap (F' \cup G') = (E' \cap F') \cup (E' \cap G').$$

Par passage à la complémentarité, on obtient la relation

$$E \cup (F \cap G) = (E \cup F) \cap (E \cup G).$$

Définition

☐ Soient E et F deux ensembles. Les couples (x, y) dont la première projection x appartient à E et dont la seconde projection y appartient à F constituent un ensemble, appelé produit des ensembles E et F, et noté $E \times F$ (lire E croix F). Si $E = F$, on note cet ensemble E^2. Comme $\{\{x\}, \{x, y\}\} \in \mathcal{P}(\mathcal{P}(E \cup F))$, on peut définir

$$E \times F = \{(x, y) \in \mathcal{P}(\mathcal{P}(E \cup F)) \mid x \in E \text{ et } y \in F\}.$$

☐ On peut généraliser cette notion de produit d'ensembles. Soit p un entier naturel. A la donnée de tout système a_1, a_2, ..., a_p de p objets pris dans cet ordre, est associé un élément $(a_1, a_2, ..., a_p)$ tel que $(\forall a_1)(\forall a_2)...(\forall b_1)...(\forall b_p)$ on ait

$$(a_1, ..., a_p) = (b_1, ..., b_p) \Leftrightarrow a_1 = b_1,\ ...,\ a_p = b_p.$$

L'élément $(a_1, a_2, ..., a_p)$ est appelé p-uple. Soit

$$a = (a_1, a_2, ..., a_p),\ a_i = p_n(a),\ \forall i \in K = \{i, 1 \leq i \leq p\},$$

a_i est appelé la i-ème projection de a.

Propriété

i) Pour que $E \times F$ soit vide, il faut et il suffit que l'un au moins des ensembles E et F le soit.

ii) $E \times F \subset E' \times F' \Leftrightarrow E \subset E'$ et $F \subset F'$.

iii) Le produit est distributif par rapport à la réunion et à l'intersection

$$E \times (F \cup G) = (E \times F) \cup (E \times G)$$

et

$$E \times (F \cap G) = (E \times F) \cap (E \times G).$$

Exercice

Soit $E = \{a, b\}$ et $F = \{1, 2, 3\}$. Alors

$$E \times F = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$$

C) Relations binaires dans un ensemble

Nous allons examiner le cas des relations binaires dans un ensemble, c'est-à-dire des relations binaires entre éléments d'un même ensemble E.

Définition

☐ Soient E et F deux ensembles. Les parties de l'ensemble produit $E \times F$ sont appelées graphes. Un graphe est un ensemble dont les éléments sont des couples.

☐ Soient E et F deux ensembles. On appelle correspondance γ de E vers F tout triplet (G, E, F) où G est une partie de $E \times F$. Les ensembles G, E et F sont respectivement appelés graphe, ensemble de départ et ensemble d'arrivée de la correspondance γ.

☐ Soit E un ensemble. Une relation binaire sur E associe à chaque couple de $E \times E$ une et une seule des assertions suivantes :

«x est lié à y», notée $x \Re y$
«x n'est pas lié à y»

On représente les relations binaires dans un ensemble de manière sagittale, c'est-à-dire à l'aide de flèches.

☐ On peut confondre les relations binaires et les graphes. En effet, considérons une relation $\Re$ portant sur les élément de $E \times F$, c'est-à-dire sur les couples (x, y) où $x \in E$ et $y \in F$, c'est ce qu'on appelle relation binaire. Les couples (x, y) tels que la relation $\Re(x, y)$ soit vraie constituent une partie de $E \times F$, appelée graphe de la relation $\Re$. Inversement, toute partie G de $E \times F$ peut être considérée comme un graphe.

☐ Le domaine d'une relation binaire $\Re$ est défini par $\{x, (x, y) \in \Re\}$, son image par $\{y, (x, y) \in \Re\}$, sa relation réciproque par $\Re^{-1} = \{(y, x), (x, y) \in \Re\}$ et sa relation identité ou diagonal par $\Delta = \{(x, x), x \in E\}$.

Exemple

☐ Voici quelques exemples de relations :

Ensemble	**Relation** $\Re$	$x \Re y$
a) E	la différence	$x \neq y$
b) {droites}	le parallélisme	$D // D'$
c) E	l'égalité	$x = y$
d) $\mathbb{R}$	l'infériorité	$x \leq y$
e) $\mathcal{P}(E)$	l'inclusion	$A \subset B$
f) $\mathbb{Z}$	la congruence	$x \equiv y[p]$
g) $\mathbb{N}^*$	la divisibilité	$n \mid p$
h) $\mathbb{Z} \times \mathbb{Z}^*$		$(a, b) \Re (a', b') \Leftrightarrow ab' = ba'$

☐ Soit $E = \{1, 2, 3\}$ et $F = \{a, b, c\}$. On considère les relations suivantes : $2\Re a$, $2\Re c$ et $3\Re a$. Le graphe de $\Re$ est $G = \{(2, a), (2, c), (3, c)\}$.

Soit $\Re$ une relation binaire sur E. La relation $\Re$ peut avoir des propriétés remarquables.

Définition

☐ On dit que $\Re$ est réflexive si $\forall x \in E$, $x\Re x$. C'est le cas de la relation définie par les couples de personnes ayant les mêmes parents.

☐ On dit que $\Re$ est symétrique si $\forall (x, y) \in E$, $x\Re y \Rightarrow y\Re x$. C'est le cas de la relation dans un ensemble de filles définie par les couples (x, y) tels que x ait pour sœur y.

☐ On dit que $\Re$ est antisymétrique si $\forall (x, y) \in E$, $(x\Re y)$ et $(y\Re x) \Rightarrow x = y$.

☐ On dit que $\Re$ est transitive si, pour tout triplet $(x, y, z) \in E$, on a $(x\Re y)$ et $(y\Re z) \Rightarrow x\Re z$.

☐ Soient $\Re'$ une relation de E dans F et $\Re$" une relation de F dans G. La relation $\Re$ de E dans G formée de tous les couples $(x, w) \in E \times G$ tels qu'il existe un élément $y \in F$ vérifiant $(x, y) \in \Re'$ et $(y, w) \in \Re$" se nomme la composée de la relation $\Re'$ par la relation $\Re$" et se note $\Re" \circ \Re'$.

Propriété

Soient $\Re$ une relation dans A, c'est-à-dire $\Re \subset A \times A$. Alors :

i) $\Re$ est réflexive si et seulement si $\Delta \subset \Re$.

ii) $\Re$ est symétrique si et seulement si $\Re = \Re^{-1}$.

iii) $\Re$ est transitive si et seulement si $\Re \circ \Re \subset \Re$.

Preuve

i) Rappelons la définition de la diagonale $\Delta = \{(x, x), x \in E\}$. Cela étant, $\Re$ est réflexive si et seulement si pour tout $x \in E$, $(x, y) \in \Re$; c'est-à-dire $\Delta \subset \Re$.

ii) Cette proposition est une conséquence immédiate des définitions de $\Re^{-1}$ et de la symétrie d'une relation.

iii) Soit $(x, w) \in \Re \circ \Re$, alors $y \in E$ tel que $(x, y) \in \Re$ et $(y, w) \in \Re$. Par transitivité (x, y), $(y, w) \in \Re$ entraîne $(x, w) \in \Re$. Par conséquent, $\Re \circ \Re \subset \Re$.

Réciproquement, supposons $\Re \circ \Re \subset \Re$. Si $(x, y), (y, w) \in \Re \circ \Re \subset \Re$. Autrement dit, $\Re$ est transitive.

Définition

☐ Soit E un ensemble. Une relation binaire $\Re$ sur E est une relation d'ordre si elle est :

- réflexive
- antisymétrique
- transitive

☐ Une relation binaire $\Re$ est une relation d'équivalence si elle est

- réflexive
- Symétrique
- transitive.

Remarque

1°) La relation d'égalité est à la fois une relation d'ordre et une relation d'équivalence.

2°) Si on définit une relation d'ordre $\leq$ dans $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$, il n'en est pas de même dans $\mathbb{C}$. Pourquoi ? Les relations définies sur les ensembles de nombres présentent une certaine compatibilité avec les lois $+$ et $\times$définies sur ces ensembles. En particulier, on a

$$a \geq 0 \text{ et } b \geq 0 \Rightarrow a + b \geq 0 \text{ et } ab \geq 0.$$

Si l'on avait, sur $\mathbb{C}$, une relation du type $i \geq 0$, alors, en effectuant le produit, on obtiendrait $-1 \geq 0$.

De même si $-i \geq 0$. Cela ne veut pas dire qu'il est impossible de définir une relation d'ordre sur $\mathbb{C}$, mais que cette relation ne présentera aucun caractère de compatibilité avec les lois $+$ et $\times$.

Exemple

Voici quelques exemples de relation d'ordre et d'équivalence.

☐ L'infériorité $x \leq y$ sur $\mathbb{R}$ est une relation d'ordre.

L'inclusion $A \subset B$ dans $\mathcal{P}(E)$: considérons la relation d'inclusion $\subset$. Pour tout ensemble A, on a $A \subset A$. D'autre part, si $A \subset B$ et $B \subset C$, alors $A \subset C$. Donc $\subset$ est à la fois réflexive et transitive. Mais $A \subset B$ et $A \neq B$ implique $B \not\subset A$. Par conséquent, $\subset$ n'est pas symétrique et n'est donc pas une relation d'équivalence.

☐ En géométrie euclidienne, la similitude des triangles est une relation d'équivalence. En effet, soient α, β et γ des triangles quelconques. Il est claire que α est semblable à lui-même. Si α est semblable à β, alors β est semblable à α. Enfin, si α est semblable à β et β est semblable à γ, alors α est semblable à γ.

☐ Soit la relation $\Re = \{(1,1),(2,3),(3,2)\}$ définie dans $A = \{1,2,3\}$. Alors $\Re$ n'est pas réflexive puisque $2 \in A$ et $(2,2) \notin \Re$. Comme $\Re^{-1} = \Re$, la relation $\Re$ est symétrique. Enfin, $\Re$ n'est pas transitive car $(3,2) \in \Re$ et $(2,3) \in \Re$, mais $(3,3) \notin \Re$.

☐ Il est facile de vérifier que les relations suivantes sont des relations d'équivalence :

Relation	**Propriété définie par $\Re$**
a) le parallélisme	avoir même direction
c) l'égalité	être identique
f) la congruence modulo p	avoir même reste dans la division par p
h) $ab' = ba'$	représenter le même rationnel $\frac{a}{b}$.

D) Ensemble ordonné

Comme son nom l'indique, une relation d'ordre sert à établir une hiérarchie parmi les éléments de E.

Définition

☐ Un ensemble E muni d'une relation d'ordre est appelé ensemble ordonné. On note usuellement une relation d'ordre par $\leq$.

☐ Des éléments x et y de E tels que l'une au moins des relations $\Re(x,y)$ et $\Re(y,x)$ soient vraies sont dites comparables.

☐ Si deux éléments quelconques de E sont comparables, on dit que $\Re$ est une relation d'ordre total, ou encore que l'ensemble E est totalement ordonné.

☐ On dit qu'une relation binaire est d'ordre strict si et seulement si cette relation est transitive et non nécessairement réflexive et symétrique.

☐ Une relation d'ordre au sens large est à la fois réflexive, antisymétrique et transitive.

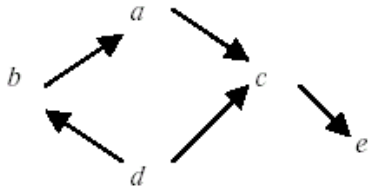
☐ Lorsque deux éléments de E ne sont pas nécessairement comparables par $\Re$, cette relation est dite d'ordre partiel de l'ensemble E. Dans ce cas, l'ensemble E est dite partiellement ordonné. On note souvent les relations d'ordre par $\leq$. Formellement, cela se traduit par :

$$\exists x \in E,\ \exists y \in E,\ [\text{non } (x \Re y) \text{ et non } (y \Re x)].$$

Exemple

☐ Dans $\mathbb{N}$ des entiers naturels, la relation $\Re$ qui exprime que a est un diviseur de b est une relation d'ordre au sens large qui permet de classer 3, 6, 24 ... ou 1, 7, 21, 42 ... mais qui ne peut comparer 3, 7 et 25. Ce n'est qu'une relation d'ordre partiel.

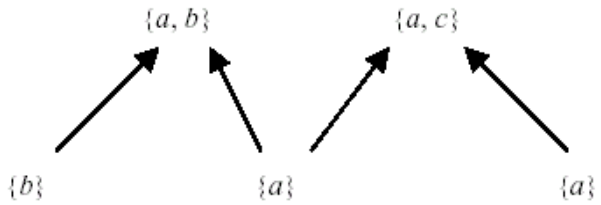
☐ Soit $X = \{a, b, c, d, e\}$. Le diagramme ci-dessous



permet de définir de la manière suivante une relation d'ordre sur X :

$x \leq y \Leftrightarrow x = y$ ou si l'on peut aller de x à y sur le diagramme dans le sens des flèches.

☐ Soit $A = \{a, b, c\}$. Les sous-ensembles de A totalement ordonnés sont $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$. La relation d'inclusion est représenté de la façon suivante :



☐ Soit $A = \{2, 3, 4, \ldots\} = \mathbb{N} - \{1\}$, ordonnons A par la relation

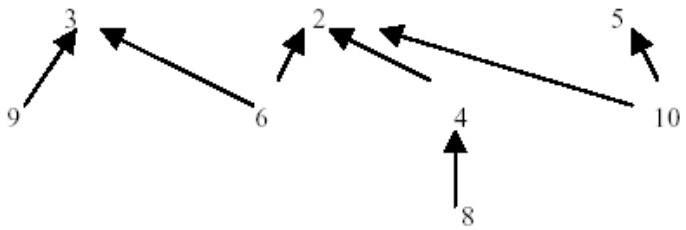
$$x \Re y \Leftrightarrow x \text{ divise } y.$$

Déterminons les éléments minimaux de A. Si $p \in A$ est un nombre premier, le seul diviseur de p est p (car $1 \notin A$). Donc tous les nombres premiers sont des éléments minimaux. En outre, si $a \in A$ n'est pas premier, il existe $b \in A$ tel que b divise a c'est-à-dire $b \Re a$; et donc a n'est pas minimal. Autrement dit, l'ensemble des éléments minimaux est identique à l'ensemble des nombres premiers. En revanche, il n'y a pas d'ensemble d'éléments maximaux car par exemple pour tout $a \in A$, a divise $2a$.

☐ Soit $B = \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$ muni de la relation d'ordre

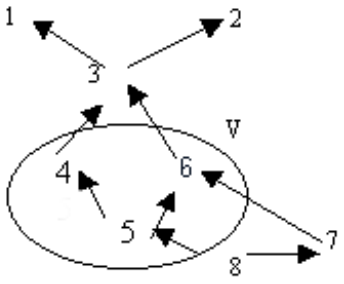
$$x \Re y \Leftrightarrow x \text{ est un multiple de } y.$$

On obtient le diagramme suivant



Ainsi les éléments maximaux sont 2, 3 et 5. Les éléments minimaux sont 6, 8, 9 et 10.

☐ Soit $W = \{1, 2, \ldots, 7, 8\}$ ordonné comme suit



et $V = \{4, 5, 6\}$ est un sous-ensemble de W.

Cherchons les majorants de V. Chaque élément de l'ensemble $\{1, 2, 3\}$, et seulement ces éléments, majore les éléments de V. Les majorants de V sont donc 1, 2 et 3.

Cherchons les minorants de V. Les éléments 6 et 8 sont les seuls minorants de V, donc {6, 8} est l'ensemble des minorants de V. Puisque 3 est le plus petit élément de l'ensemble des majorants de V, $\sup V = 3$. On remarquera que $3 \notin V$.

Puisque 6 est le plus grand élément de l'ensemble des minorants de V, $\inf V = 6$. On notera que $6 \in V$.

Définition

Soit E un ensemble muni d'une relation d'ordre $\leq$ et P une partie de E.

☐ On dit qu'un élément b de E majore P, ou est un majorant de P, si tout élément de P est inférieur à b. On dit encore que la partie P est majorée par b.

☐ On dit de même qu'un élément a de E est un minorant de P s'il est inférieur à tout élément de P.

☐ On dit qu'une partie P d'un ensemble E est majorée si l'ensemble de ses majorants est non vide, qu'elle est minorée si l'ensemble de ses minorants est non vide, et qu'elle est bornée si elle est à la fois majorée et minorée.

☐ On dit que P admet un minimum m si :

$$m \in P \text{ et } \forall x \in P,\ m \leq x.$$

m est dont un minorant de P, lui-même élément de P.

☐ On dit que P admet un maximum M si :

$$M \in P \text{ et } \forall x \in P,\ x \leq M.$$

M est donc un majorant de P, lui-même élément de P.

☐ Le plus petit des majorants, s'il existe, s'appelle la borne supérieure de P et se note : $S = \sup_{x \in P} x$.

De même, la borne inférieure de P, notée $I = \inf_{x \in P} x$ est le plus grand des minorants. Cela signifie :

$$\forall x \in P,\ x \leq S \text{ et } \forall \varepsilon > 0,\ \exists \in P,\ x > S - \varepsilon$$
$$\forall x \in P,\ x \geq I \text{ et } \forall \varepsilon > 0,\ \exists x \in P,\ x < I + \varepsilon.$$

Propriété

i) Il existe au plus un majorant de P appartenant à P.

ii) Un tel majorant s'appelle le plus grand élément de P.

iii) De même, le plus petit élément de P, s'il existe est l'unique de P appartenant à P.

Preuve

i) Soient b et b' des majorants de P appartenant à P. Puisque b appartient à P et que b' est un majorant de P, on a : $b \leq b'$. De même : $b' \leq b$.

Or la relation d'ordre est antisymétrique, on obtient bien : $b = b$.

ii) On raisonne de la même façon.

Remarque

Une partie, admettant un plus grand élément b, admet une borne supérieure, à savoir b, une partie admettant une borne supérieure est majorée. En général, les réciproques sont fausses car l'existence des majorants n'implique pas l'existence d'une borne supérieure, et l'existence d'une borne supérieure n'implique pas celle d'un plus grand élément.

Les parties remarquables des ensembles ordonnées sont les parties qui, dès qu'elles contiennent deux éléments, contiennent tous les éléments intermédiaires, ce qui nous amène à définir la notion d'intervalle.

Définition

☐ On dit qu'une partie I d'un ensemble ordonné E est un intervalle de E si : $\forall (y,z) \in I^2,\ y \leq z$, tout élément x satisfaisant à la relation $y \leq x \leq z$ appartient à I.

☐ Un ensemble ordonné E est dit inductif si tout partie C, totalement ordonné, de E admet au moins un majorant.

☐ On appelle bon ordre sur un ensemble E, toute relation d'ordre sur E telle que toute partie non vide de E admet un plus petit élément. Il est à remarquer qu'un bon ordre est forcément total, car pour une paire $\{a,b\}$ de E, comme il y a un plus petit élément, si c'est a, alors $a \leq b$, et si c'est b on aura $b \leq a$. Dans les deux cas, a et b sont comparables.

Axiome de Zorn, de Zermelo, du choix

- Tout ensemble ordonné, non vide, inductif admet au moins un élément maximal.
- Tout ensemble E non vide, peut être bien ordonné.
- Pour tout ensemble non vide E, il existe au moins une application f de $\mathcal{P}(E)$ dans E telle que $\forall A \subset B$, avec $A \neq \emptyset$, $f(A) \in A$. On dit que f est une fonction de choix. En fait, l'axiome de choix formalise la phrase de bon sens suivante «soit a dans A», avec A partie non vide de E.

Théorème

On admet le théorème suivant (difficile à démontrer) : les axiomes de Zorn, de Zermelo et du choix sont équivalents. Le lemme de Zorn est un des outils les plus importants des mathématiques.

Regardons quelques exemples de minimum et de maximum :

Exemple

☐ 0 est le minimum de $[0,1]$ (avec la relation usuelle) et 1 est son maximum.

☐ $]0,1]$ n'admet pas de minimum, mais admet 1 comme maximum.

☐ $]0,1[$ n'admet ni maximum ni minimum.

☐ $\emptyset$ est le minimum de $\mathcal{P}(E)$ pour la relation d'inclusion $\subset$. E est le maximum.

☐ Si A est l'ensemble de tous les singletons de E, A n'admet ni de minimum, ni de maximum.

☐ Pour la relation de divisibilité de $\mathbb{N}$, 1 est le minimum, il n'y a pas de maximum.

☐ $]0,1[$ admet pour borne inférieure 0, et pour borne supérieure 1.

☐ Soit X un ensemble ordonné. Nous allons montrer à l'aide du lemme de Zorn qu'il existe un sous-ensemble totalement ordonné de X qui n'est strictement inclus dans aucun autre sous-ensemble totalement ordonné de X. En effet, soit A la famille de tous les sous-ensembles totalement ordonné de X. Ordonnons A par inclusion. Supposons que $B = \{B_i \ / \ i \in I\}$ soit une sous-famille totalement ordonné de A. Posons

$$A = \bigcup \{B_i \ / \ i \in I\}.$$

Observons que $B_i \subset X$ pour tout $B_i \in B$ implique $A \subset X$. Montrons maintenant que A est totalement ordonné. Soient a, $b \in A$, alors $\exists B_j$, $B_k \in B$ tels que : $a \in B_j$, $G \in B_k$.

Or B est totalement ordonné par la relation d'inclusion entre ensemble ; donc par exemple $B_j \subset B_l$. Par conséquent a, $b \in B_k$. Puisque les sous-ensembles B_k de X est totalement ordonné on a :

$$\text{ou } a \leq b \text{ ou } b \leq a.$$

Ainsi le sous-ensemble A est totalement ordonné et donc $A \in A$.

Or si $B_i \subset A$ pour tout $B_i \in B$; et donc A est un majorant de B. Puisque tout sous-ensemble totalement ordonné de A possède un élément maximal, c'est-à-dire un sous-ensemble totalement ordonné de X qui n'est strictement inclus dans aucun autre sous-ensemble totalement ordonné de X.

E) Ensembles quotients

Considérons une relation d'équivalence $\Re$ dans un ensemble E.

Définition

☐ Pour tout élément x de E, on pose

$$\overline{x} \quad = \{y \in E, x \Re y\} = \{y \in E, (x, y) \in \Re\}.$$

L'ensemble $\overline{x}$ est appelé la classe d'équivalence de x modulo $\Re$, c'est l'ensemble des éléments de E qui sont équivalents à x modulo $\Re$.

☐ L'ensemble des classes d'équivalence constitue un nouvel ensemble, appelé ensemble quotient de E par $\Re$ et noté $E/\Re = \{\overline{x}, x \in E\}$.

☐ L'application φ de E dans $E/\Re$ qui à tout élément x de E associe sa classe d'équivalence $\overline{x}$ est appelé application canonique de E sur $E/\Re$.

☐ Une partition d'un ensemble E est une famille $(A_i)_{i \in I}$ vérifiant :

- $\forall i$, $A_i \neq \emptyset$
- $\forall i$, $\forall j$, $i \neq j \Rightarrow A_i \cap A_j = \emptyset$
- $\bigcup_{i \in I} A_i = E$.

Exemple

☐ Les quatre symboles trèfle, carreau, cœur et pique déterminent une partition de l'ensemble des cartes d'un jeu en quatre sous-ensemble disjoints appelés couleurs.

☐ $\mathbb{R}_+^*$ et $\mathbb{R}_-^*$ ne constituent pas une partition de $\mathbb{R}$.

☐ $\mathbb{R}_+^*$, $\mathbb{R}_-^*$ et $\{0\}$ constituent une partition de $\mathbb{R}$.

Propriété

i) Pour tout élément x de E, $x \in \overline{x}$. Donc $\overline{x} \neq \emptyset$.

ii) $\overline{a} = \overline{b}$ si et seulement si $(a, b) \in \Re$.

En particulier, deux classes d'équivalence qui ont un élément commun sont confondues.

iii) Si $\overline{a} \neq \overline{b}$, alors $\overline{a}$ et $\overline{b}$ sont disjoints, c'est-à-dire qu'ils ne possèdent aucun point commun.

iv) Soit $\Re$ une relation d'équivalence sur E, alors l'ensemble quotient $E/\Re$ est une partition de E.

Autrement dit, tout élément de E appartient à une classe d'équivalence et à une seule. Toute partition de

$$A \subset E$$

peut s'obtenir ainsi comme quotient par une (unique) relation d'équivalence de E.

Preuve

i) Une relation d'équivalence est réflexive. Donc : $(x,x) \in \Re \Rightarrow x \in \overline{x}$ et $\overline{x} \neq \emptyset$.

ii) Supposons $(a,b) \in \Re$. Nous voulons montrer que $\overline{a} = \overline{b}$, Soit $x \in \overline{b}$, alors $(b,x) \in \Re$. Par hypothèse, on a $(a,b) \in \Re$. De plus, la transitivitéde $\Re$ implique $(a,x) \in \Re$. Par conséquent, $(a,x) \in \Re$ et $x \in \overline{a}$, c'est-à-dire $\overline{b} \subset \overline{a}$. Pour démontrer que $\overline{a} \subset \overline{b}$, remarquons que $(a,b) \in \Re$ entraîne $(b,a) \in \Re$, puisque la relation $\Re$ est symétrique. Un raisonnement semblable au précédent nous permet donc d'écrire $\overline{a} \subset \overline{b}$. Finalement $\overline{a} = \overline{b}$.

Réciproquement, si $\overline{a} = \overline{b}$, alors la réflexivité de $\Re$ entraîne $b \in \overline{b}$, c'est-à-dire $(a,b) \in \Re$.

En particulier, si $x \in \overline{a}$ et $x \in \overline{b}$, les relations $(a,x) \in \Re$ et $(b,x) \in \Re$ entraînent par symétries et transitivité $(a,b) \in \Re$, soit $\overline{a} = \overline{b}$.

iii) Nous allons montrer que la proposition contraposée est vraie. La proposition contraposée de :

$$\text{«si } \overline{a} \neq \overline{b}\text{, alors } \overline{a} \text{ et } \overline{b}\text{»}$$

est

$$\text{«si } \overline{a} \cap \overline{b} \neq \emptyset\text{, alors } \overline{a} = \overline{b}\text{»}.$$

Supposons donc que $\overline{a} \cap \overline{b} \neq \emptyset$. Alors il existe un élément $x \in E$ tel que $x \in \overline{a} \cap \overline{b}$. Par suite,

$$(a,b) \in \Re \text{ et } (b,x) \in \Re.$$

Puisque $\Re$ est symétrique, $(x,b) \in \Re$ et puisque $\Re$ est transitive $(a,b) \in \Re$. L'assertion ii) permet alors de conclure que $\overline{a} = \overline{b}$.

iv) Rappelons que

$$E/\Re = \{\overline{x}, x \in E\} \text{ et } \overline{x} = \{y \in E, x\Re y\}.$$

Il est clair que

$$\bigcup_{x \in E} \overline{x} = \bigcup_{x \in E} \{y \in E, x\Re y\} = E.$$

D'après ii), les classes d'équivalence sont disjoints. Ainsi $E/\Re$ est une partition de E.

Exemple

☐ Soit E l'ensemble des droites de l'espace et soit $\Re$ la relation d'équivalence exprimant que deux droites de même direction qu'une droite donnée D_1 constituent la classe d'équivalence C_1 définie par D_1. Si D_1 et D_2 n'ont pas même direction, elles définissent deux classes disjoints, C_1 et C_2 ne possédant aucun élément commun. L'ensemble des classes d'équivalence C_1, C_2, C_3 ... est l'ensemble quotient $E/\Re$ qui n'est autre que l'ensemble des directions de l'espace.

☐ Soit n un entier positif. Si m et m' sont des entiers relatifs, on dit que m est congru à m' modulo n et on écrit

$$m \equiv m'[n] \text{ (lire } m \text{ congru à } m' \text{ modulo } n)$$

s'il existe un entier r tel que $m - m' = nr$. La congruence ainsi définie est une relation d'équivalence :

i) C'est une relation réflexive, car $m - m = 0$. Donc il existe un entier relatif r tel que $m - m = 0r$. Donc m est congru à lui-même modulo 0.

ii) C'est une relation symétrique. Montrons que

$$(m,m') \in \Re \Rightarrow (m',m) \in \Re.$$

Supposons que : $m - m' = nr$, alors

$$m' - m = -nr.$$

Posons : $r' = -r$, on obtient bien

$$m' - m = nr'.$$

Donc

$$(m, m') \in \Re \ \Rightarrow \ (m', m) \in \Re.$$

iii) C'est une relation transitive. Supposons que l'on ait

$$m \text{ - } m\prime = nr \text{ et } m\prime \text{ - } m\prime\prime = nr\prime.$$

Alors, on a

$$m - m'' = m - m' + nr' = nr + nr' = n(r + r').$$

Posons $r'' = r + r'$, on obtient $m - m'' = nr''$.

☐ Soit $\Re_5$ la relation définie sur l'ensemble $\mathbb{Z}$ des entiers par $x \equiv y$ [mod 5] dont le sens est

$$\text{«}(x - y) \text{ est divisible par 5»}.$$

Alors $\Re_5$ est une relation d'équivalence dans $\mathbb{Z}$. Il existe exactement cinq classes d'équivalence distinctes dans $\mathbb{Z}/\Re_5$:

$$\begin{aligned} E_0 &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} = \overline{5} \\ E_1 &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} = \overline{1} \\ E_2 &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} = \overline{2} \\ E_3 &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} = \overline{3} \\ E_4 &= \{\ldots, -6, -1, 4, 9, 14, \ldots\} = \overline{4}. \end{aligned}$$

Notons que les classes d'équivalence sont deux à deux disjointes et que $\mathbb{Z} = E_0 \cup E_1 \cup E_2 \cup E_3 \cup E_4$.

II) Correspondances et applications

Nous allons continuer l'étude des relations binaires remarquables et examiner certaines graphes d'une importance fondamentale. Commençons par donner quelques définitions.

A) Applications, équations, injections, surjections et bijections

Définition

☐ Soient E et F deux ensembles et Γ une partie de $E \times F$. Supposons que, pour tout x de E, il existe un élément y de F tel que (x, y) appartienne à Γ. Le triplet (Γ, E, F) s'appelle application de E dans F. On le représente par les symboles $E \to F$ ou $f : E \to F$. E est l'ensemble de départ ou de source et F l'ensemble d'arrivée ou de but. La correspondance entre x et $f(x)$ se note $f : x \mapsto f(x)$ (lire x flèche f de x).

☐ On appelle équation définie par f et par y la relation suivante : $f(x) = y$.

L'élément x s'appelle inconnue. Tout élément x_0 vérifiant la relation précédente, c'est-à-dire : $f(x_0) = y$, s'appelle solution de l'équation.

L'étude des équations conduit à poser les définitions suivantes :

☐ On dit que f est injective (one to one en anglais) si, pour tout élément y de F, l'équation : $f(x) = y$ a au plus une solution. Une condition suffisante et nécessaire pour que f soit injective est que :

$$\forall (x, x') \in E \times E, \ f(x') = f(x) \Rightarrow x = x'$$

ou encore par contraposition

$$\forall (x, x') \in E \times E, \ x \neq x' \Rightarrow f(x) \neq f(x').$$

☐ On dit que f est surjective (onto) si, pour tout élément y de F, l'équation : $f(x) = y$ a au moins une solution. Formellement, une fonction est (onto) si :

$$\forall y \in F, \ \exists x \in E, \ y = f(x).$$

Autrement dit l'ensemble des valeurs prises par f est égal à l'ensemble F tout entier : $f(E) = F$.

☐ On dit que f est bijective si, pour tout élément y de F, l'équation : $f(x) = y$ a une solution et une seule. Autrement dit, f est à la fois injective et surjective.

☐ Les bijections d'un ensemble E sur lui-même sont appelées permutation de E.

☐ Soit B une partie de F. L'image réciproque de B par f est l'ensemble noté $f^{-1}(B)$ défini par :

$$f^{-1}(B) = x \in E \backslash f(x) \in B\}.$$

Autrement dit :

$$x \in f^{-1}(B) \Leftrightarrow f(x) \in B$$

$f^{-1}(B)$ est l'ensemble des antécédents des éléments de B.

☐ Soit E un ensemble, l'application f de E vers E définie par $f(x) = x$ pour tout élément x de E est appelée l'application identique de E. L'application identique de E est notée Id_E.

Remarque

1°) En analyse, les applications prennent le nom traditionnel de fonctions. On distinguera les deux flèches $\rightarrow$ et $\mapsto$, mais aussi l'application f et sa valeur $f(x)$ prise sur un élément x de E. L'application f est le triplet (Γ, E, F), tandis que $f(x)$ est un élément de l'ensemble F.

Quelle est la différence entre la notion de fonction et celle d'application ? Une application f de E vers F fait correspondre à tout élément $x \in E$ un élément unique $y \in F$, tandis qu'une fonction fait correspondre au plus un élément de F. Soit $f : x \mapsto \dfrac{1}{x}$. C'est une application de $\mathbb{R}^*$ dans $\mathbb{R}$, c'est une fonction de $\mathbb{R}$ dans $\mathbb{R}$. A part ça, ces deux notions se ressemblent beaucoup.

2°) On emploi aussi le mot famille. Soit I un ensemble (ensemble d'indice) et X un autre ensemble. On appellera famille à valeurs dans X indexée par I une application $f : I \rightarrow X$, $i \mapsto x_i$.

Cette famille est noté $(x_i)_{i \in I}$. Lorsque $I = \mathbb{N}$, on parle de suite. L'ensemble X peut être aussi l'ensemble des partie d'un ensemble E.

3°) On prendra garde que $f^{-1}(B)$ est définie même si f n'est pas bijective, que $f^{-1}(\{y\})$ est l'ensemble (éventuellement vide ou constitué de plus d'un élément) des antécédents de y, et que la notation $f^{-1}(y)$, elle, n'est tolérée que si f est bijective ; on désigne ainsi l'antécédent unique de y.

4°) L'ensemble de toutes les applications d'un ensemble E vers un ensemble F est noté F^E. Lorsque E et F sont finis avec respectivement m et n éléments, F^E possède alors n^m éléments. Pas question ici d'en donner une "démonstration" formelle, mais on peut l'expliquer assez bien : on a n choix dans F pour l'image d'un premier élément x_1 de E, puis encore n choix pour l'image d'un deuxième élément x_2, ces choix se faisant indépendamment : on a donc $n \times n = n^2$ choix pour les images de ces deux éléments. Puis on a n choix pour l'image de x_3, donc n^3 choix pour l'image des trois premiers éléments, et ainsi de suite. Cette propriété explique le choix de la notation F^E.

5°) Soit $f : E \rightarrow F$ une application. Pour montrer que f est surjective, on prend un $y \in F$ et on cherche un $x \in E$ tel que $y = f(x)$. Pour montrer que f est non surjective, on montre le proposition suivante

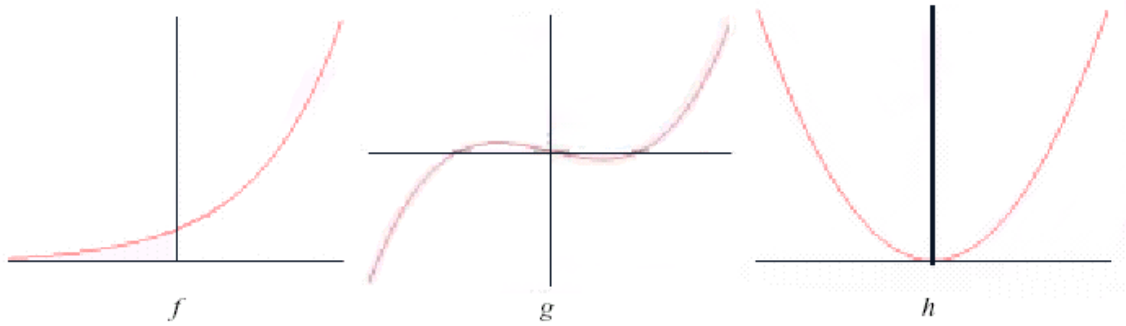
$$(\exists y \in F)(\forall x \in E)(f(x) \neq y).$$

Exemple

☐ Soient $f : \mathbb{R} \rightarrow \mathbb{R}$, $g : \mathbb{R} \rightarrow \mathbb{R}$ et $h : \mathbb{R} \rightarrow \mathbb{R}$ trois applications définies par

$$f(x) = e^x,\ g(x) = x^3 - x \text{ et } h(x) = x^2.$$

Géométriquement, une application est injective si toute droite horizontale contient un point de cette application au plus. Une application est surjective si toute droite horizontale contient au moins un point de cette application. Reprenons les graphes de f, g et h :

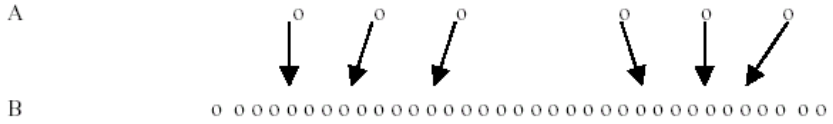


On voit que f est injective et g surjective. Par contre h n'est ni injective ni surjective. En effet, on a

$$h(2) = h(-2) = 4$$

et $h(\mathbb{R})$ est un sous-ensemble de $\mathbb{R}$ distinct de $\mathbb{R}$, par exemple $-16 \notin h(\mathbb{R})$.

☐ Exemple d'injection



Exemple de surjections

☐ Montrons que l'application $f : x \mapsto x^3$ de $\mathbb{Q}$ dans $\mathbb{Q}$ n'est pas surjective. Soit $y = 2$. Alors $x^3 = 2$ n'admet pas de solution dans $\mathbb{Q}$. En effet s'il existait une solution $x = \frac{p}{q}$ avec p et q premiers ente eux telle que $x^3 = 2$, alors

$$p^3 = 2q^3.$$

Si p est impair, alors p^3 est impair. Par contraposition si p^3 est pair, alors p est pair. Donc il existe p' tel que $p = 2p'$. En remplaçant cette relation dans $p^3 = 2q^3$, on voit que q^3 est pair, donc q pair. Il y a contradiction avec le fait que p et q sont premiers entre eux. Donc il existe $y \in \mathbb{Q}$ tel que $\forall x \in \mathbb{Q}$, $f(x) \neq y$. f est alors non surjective. Montrons maintenant que f est injective. Soit x et x' dans $\mathbb{Q}$ tels que $f(x) = f(x')$. Alors on a

$$\begin{aligned}
& x^3 - x\prime^3 = 0 \\
\Rightarrow \quad & (x - x')(x^2 + xx' + x'^2) = 0 \\
\Rightarrow \quad & (x - x')[(x + \tfrac{x'}{2})^2 + \tfrac{3}{4}x'^2] = 0 \\
\Rightarrow \quad & x = x' \text{ ou } (x + \tfrac{x'}{2})^2 + \tfrac{3}{4}x'^2 = 0 \\
\Rightarrow \quad & x = x' \text{ ou } (x + \tfrac{x}{2} = 0 \text{ et } x' = 0) \\
\Rightarrow \quad & x = x' \text{ ou } x = x = 0 \\
\Rightarrow \quad & x = x'.
\end{aligned}$$

Donc

$$(\forall x \in Q)(\forall x' \in Q)(f(x) = f(x') \Rightarrow x = x').$$

En revanche, c'est une bijection si on remplace $\mathbb{Q}$ par $\mathbb{R}$.

☐ L'application $f : \mathbb{N} \to 2\mathbb{N}$ définie par $f(x) = 2x$ est bijective. C'est injective car :

$$f(x) = f(x') \Rightarrow 2x = 2x' \Rightarrow 2(x - x') = 0 \Rightarrow x = x'.$$

C'est surjective car si on prend $y \in 2\mathbb{N}$, alors par définition il existe x tel que $y = 2x = f(x)$.

Définition

Soient E, F des ensembles ordonnés et f une application de E dans F.

□ On dit que f est croissante si l'on a

$$f(x) \leq f(y)$$

dès que $x \leq y$. L'application f est strictement croissante

$$f(x) < f(y)$$

dès que $x < y$.

□ On dit que f est décroissante si l'on a

$$f(x) \leq f(y)$$

dès que $x \geq y$. L'application f est strictement décroissante

$$f(x) < f(y)$$

dès que $x > y$.

□ On dit que f est monotone si elle est croissante ou décroissante et qu'elle est strictement monotone si elle est strictement croissante ou strictement décroissante.

On a la propriété suivante :

Propriété

i) Si une application monotone est injective, elle est strictement monotone.
ii) Toute application monotone strictement monotone d'un ensemble ordonné totalement ordonné dans un ensemble totalement ordonné est injective.

Propriété

Soit $f : E \to F$. Alors, quels que soient les sous ensembles A et B de E, on a :

i) $A \subset B \Rightarrow f(A) \subset f(B)$
ii) $f(A \cup B) = f(A) \cup f(B)$.
iii) $f(A \cap B) \subset f(A) \cap f(B)$ (l'égalité a lieu si f est injective).

Preuve

i) On a : $\forall y \in f(A)$, $\exists x \in A$, $y = f(x)$. Puisque $A \subset B$, on a : $\exists x \in B$, $y = f(x)$ et $y \in f(B)$. Donc $f(A) \subset f(B)$.

ii) Montrons tout d'abord que $f(A \cup B) \subset f(A) \cup f(B)$. Soit $y \in f(A \cup B)$. Il existe $x \in A \cup B$ tel que $f(x) = y$. Donc ou $x \in A$ ou $x \in B$. Or

$$x \in A \text{ implique} f(x) = y \in f(A)$$
$$x \in B \text{ implique } f(x) = y \in f(B).$$

Dans tous les cas, on a $y \in f(A) \cup f(B)$.

Démontrons maintenant l'inclusion inverse, c'est-à-dire $f(A) \cup f(B) \subset f(A \cup B)$. Soit

$$y \in f(A) \cup f(B).$$

Alors $y \in f(A)$ ou $y \in f(B)$. Or

$$y \in f(A) \text{ implique, } \exists x \in A \text{ tel que } f(x) = y$$
$$\text{et } y \in f(B) \text{ implique, } \exists x \in B \text{ tel que } f(x) = y.$$

iii) Montrons que

$$y \in f(A \cap B) \Rightarrow y \in f(A) \cap f(B).$$

Si $y \in f(A \cap B)$, alors $\exists x \in A \cap B$ tel que $f(x) = y$. Or

$$x \in A \cap B \Rightarrow x \in A \text{ et } x \in B.$$

Ainsi, $y = f(x) \in f(A)$ et $y \in f(B) \Rightarrow y \in f(A) \cap f(B)$.

Pour montrer que $f(A) \cap f(B) \not\subset f(A \cap B)$, il suffit de prendre un exemple. Soit $A = \{a, b\}$, $B = \{b, c\}$ et f l'application de $A \cup B$ dans $F = \{1, 2\}$ définie par $f(a) = f(c) = 2$ et $f(b) = 1$. On a :

$$f(A \cap B) = \{1\} \text{ et } f(A) \cap f(B) = \{2, 1\} \cap \{1, 2\} = \{1, 2\}.$$

Donc $f(A) \cap f(B) \not\subset f(A \cap B)$ en général.

Supposons maintenant f injective. On a déjà : $f(A \cap B) \subset f(A) \cap f(B)$. Pour montrer l'égalité, il suffit de vérifier l'inclusion dans l'autre sens. Pour tout $y \in f(A) \cap f(B)$, alors il existe $a \in A$ tel que $y = f(a)$. De même, il existe aussi $b \in B$ tel que $y = f(b)$. Il vient alors : $f(a) = f(b)$. Mais comme f est injective, on obtient : $a = b \in A \cap B$. Donc $y \in f(A \cap B)$. C'est gagné et on est content.

L'application identique de E est notée Id_E.

Remarque

Si f n'est pas injective, on n'a seulement une inclusion dans un seul sens : $f(A \cap B) \subset f(A) \cap f(B)$. Par exemple l'application $f : x \mapsto x^2$ de $\mathbb{R}$ dans $\mathbb{R}$ n'est pas injective. Prenons $A = [0, 1]$ et $B = [-1, 0]$. On a alors : $A \cap B = \{0\}$, donc $f(A \cap B) = \{0\}$. Mais $f(A) \cap f(B) = [0, 1]$.

B) Composition des applications

Définition

☐ Soient E, F et G trois ensembles, f une application de E dans F et g une application de F dans G.

☐ L'application de E dans G qui à tout élément x de E associe l'élément $g[f(x)]$, c'est-à-dire la valeur prise par g sur $f(x)$, s'appelle composée des applications f et g, et se note $g \circ f$ (lire g rond f).

Propriété

i) Soient H un quatrième ensemble et h une application de G dans H. Alors $h \circ (g \circ f) = (h \circ g) \circ f$.

ii) Si f et g sont injectives, il en est de même de $g \circ f$.

iii) Si f et g sont surjectives, il en est de même de $g \circ f$.

iv) Si f et g sont bijectives, il en est de même de $g \circ f$.

Preuve

i) Les deux membres associent à tout élément x de E le même élément de H, à savoir $h(g(f(x)))$. La valeur commune des deux membres se note plus simplement$h \circ g \circ f$.

ii) Supposons que f et g sont surjectives, et considérons un couple (x, x') d'éléments de E tel que

$$(g \circ f)(x) = (g \circ f)(x'),$$

c'est-à-dire que $g[f(x)] = g[f(x')]$. Or g est injective, on a $f(x) = f(x')$. De plus, f est injective, on a donc : $x = x'$, ce qui montrer que $g \circ f$ est injective.

iii) Maintenant, si f et g sont surjectives, considérons un élément z de G. Puisque g est surjective, il existe un élément y de F tel que $g(y) = z$; puisque f est surjective, il existe un élément x de E tel que $f(x) = y$. Par suite, l'élément x est tel que $(g \circ f)(x) = z$, ce qui montre que $g \circ f$ est surjective.

iv) Le cas des applications bijectives se résultent aussitôt des deux précédents.

Propriété

Soient $f : X \to Y$ et $g : Y \to Z$ deux applications.

i) Si $g \circ f$ est injective, alors f est injective.

ii) Si $g \circ f$ est surjective, alors g est surjective.

Preuve

i) On suppose $g \circ f$ injective, on veut prouver que f est injective. Soient donc x' et x'' de X tels que

$$f(x') = f(x''),$$

on veut prouver que $x' = x''$. On utilise l'injectivité de $g \circ f$. On prend les images par g, on a

$$g(f(x')) = g(f(x''))$$

soit

$$(g \circ f)(x') = (g \circ f)(x'')$$

et comme $g \circ f$ est injective, on conclut que $x' = x''$, d'où f injective.

ii) Dans le deuxième cas, on suppose $g \circ f$ surjective. On veut prouver que $g : Y \to Z$ est surjective, c'est-à-dire, partant de $z \in Z$, trouver un antécédent par g. Soit $z \in Z$, comme $g \circ f$ est surjective, il existe x dans X tel que $(g \circ f)(x) = z$, soit encore tel que $g(f(x)) = z$.

En posant $y = f(x)$, on a trouvé y dans Y tel que $g(y) = z$, donc g est injective.

Exemple

☐ On va voir comment on peut appliquer ces propriétés. Comme exercice, on peut montrer :

$$(g \circ f \text{ injective et } f \text{ surjective}) \Rightarrow g \text{ injective.}$$

Si $g \circ f$ est injective, alors f est injective. Donc f est bijective. Dans ce cas, f^{-1} existe et est bijective, donc aussi injective. $(g \circ f) \circ f^{-1} = g$ est alors injective comme composée de deux injections.

☐ Montrons maintenant :

$$(h \circ g \circ f \text{ injective, } g \circ f \circ h \text{ injective et } f \circ h \circ g \text{ surjective}) \Rightarrow f,\ g,\ h \text{ bijective.}$$

Si $(h \circ g) \circ f$ est injective, alors f est injective. Si $f \circ (h \circ g)$ est surjective, alors f est surjective. Donc f est bijective et f^{-1} existe et est bijective aussi, donc surjective.

On a alors : $h \circ g = f^{-1} \circ (f \circ h \circ g)$ surjective. Il vient alors h surjective. Comme $(g \circ f) \circ h$ est injective, h est injective. Donc h est une bijection. h^{-1} existe.

On a : $g = h^{-1} \circ (h \circ g \circ f) \circ f^{-1}$ injective.

On a aussi : $g = (h^{-1} \circ f^{-1}) \circ (f \circ h \circ g)$ surjective.

C) Applications inversibles

Définition

☐ Soient E et F deux ensembles et f une application de E dans F. On dit que l'application f est inversible s'il existe g de F dans E telle que $g \circ f = Id_E$ et $f \circ g = Id_F$ (Id représente l'application identité).

☐ g s'appelle application réciproque de f et on la note f^{-1}.

Lemme

Soit $f : E \to F$ et $g : F \to E$ deux applications. Si on a : $g \circ f = Id_E$, alors f est injective et g surjective.

Preuve

Soit avec x et x' des éléments de E quelconques. Si $f(x) = f(x')$, alors on a par composition de g :

$$g[f(x)] = g[f(x')] \Rightarrow (g \circ f)(x) = (g \circ f)(x') \Rightarrow Id_E(x) = Id_E(x') \Rightarrow x = x'.$$

Donc f est injective.

Pour la surjectivité de g, prenons $z \in E$. Posons $y = f(z)$. Alors

$$g(y) = (g \circ f)(z) = Id_E(z) = z.$$

Donc g est surjective.

Exemple

□ Soit $E = \mathbb{R}$ et $F = \mathbb{R}^2$. On définit $f : E \to F$ par $f : x \mapsto (x, 2x)$. Si $g : F \to E$ est définie par $g : (x, y) \mapsto x$, alors on a : $g \circ f = Id_E$. L'application f est donc injective et g surjective.

Théorème (caractérisation d'applications bijectives)

i) Soit f une application d'un ensemble E vers un ensemble F. f est une bijection si et seulement s'il existe une application g de F vers E telle que $g \circ f = Id_E$ et $f \circ g = Id_F$.

ii) Lorsque f est une bijection, l'application réciproque f^{-1} de f, est unique.

Preuve

i) Prouvons d'abord l'implication "⇒", en supposant que f est une bijection. Par conséquent, tout élément y de F possède un et un seul antécédent par f. Choisissons donc d'appeler $g(y)$ cet unique antécédent. Il faut vérifier que le g ainsi construit vérifie les deux identités réclamées.
Vérifions d'abord que $g \circ f = Id_E$. Soit x un élément de E. L'antécédent de $f(x)$ par f est évidemment x, ce qui s'écrit :

$$g[f(x)] = x$$

en revenant à la définition de g. Cette identité étant vraie pour tout x, on a bien prouvé l'égalité entre applications :

$$g \circ f = Id_E.$$

Prouvons l'autre identité, en vérifiant que $f \circ g = Id_F$. Soit y un élément de F. Puisque $g(y)$ est par définition un antécédent de y, ceci signifie que

$$f[g(y)] = y.$$

Cette identité étant vraie pour tout y, on a bien prouvé l'égalité entre applications :

$$f \circ g = Id_F.$$

On a donc bien réussi à construire le g que l'on souhaitait. Et ceci prouve l'implication "⇒".
L'implication "⇐" est immédiate avec le lemme en haut.

ii) Soit deux applications g et h vérifiant à elles deux les quatre identités :

$$g \circ f = Id_E,\ f \circ g = Id_F,\ h \circ f = Id_E \text{ et } f \circ h = Id_F.$$

On a alors

$$g = g \circ (f \circ h) = (g \circ f) \circ h = h.$$

On obtient bien $g = h$, d'où l'unicité de f^{-1}.

Remarque

Ce théorème nous donne un moyen élégant pour prouver qu'une application $f : E \to F$ est bijective. Il suffit en effet d'exhiber g telle que $g \circ f = Id_E$ et $f \circ g = Id_F$.

Propriété

i) Pour qu'une application f de E dans F soit inversible, il faut et il suffit que f soit bijective. Dans ces conditions, l'application f^{-1} n'est autre que l'application qui à tout élément y de F associe l'unique solution de l'équation $f(x) = y$.

ii) Si $f : E \to F$ et $g : F \to G$ sont des applications bijectives, alors $(g \circ f)^{-1} : G \to E$ existe et est égale à

$$f^{-1} \circ g^{-1} : G \to E.$$

Démonstration

i) Tout d'abord, supposons que f est inversible, et considérons l'unique application g telle que

$$g \circ f = Id_E \text{ et } f \circ g = Id_F.$$

Soit (x, x') un couple d'éléments de E tels que $f(x) = f(x')$. En calculant la valeur prise par g sur les deux membres, on voit que

$$(g \circ f)(x) = (g \circ f)(x\prime)$$

c'est-à-dire $Id_E(x) = Id_E(x')$, ou encore $x = x'$. L'application f est donc injective.

Ensuite, l'équation $f(x) = y'$ a une solution évident, à savoir $x' = g(y')$. L'application f est donc surjective, et, par suite bijective.

Réciproquement, si f est bijective, considérons l'application g qui à tout élément y de F associe l'unique solution de l'équation $f(x) = y$. Il est clair que, pour tout élément x de E,

$$(g \circ f)(x) = g(y) = x$$

et que, pour tout élément y de F,

$$(f \circ g)(y) = f(x) = y.$$

Ainsi, $g \circ f = Id_E$ et $f \circ g = Id_F$, ce qui montre que f est inversible et que $f^{-1} = g$. L'application g^{-1} est elle-même inversible et $g^{-1} = f$.

ii) Il est clair que $(g \circ f)^{-1}$existe car $g \circ f$ est bijective. Il est facile de vérifier que

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Exemple

□ Soit f une application d'un ensemble E vers un ensemble F, soit E_1 une partie de E et F_1 une partie de F telles que

$$f(E_1) \subset F_1.$$

On définit sans nom ni notation bien clairement fixée une notion de "restriction" de f de E_1 vers F_1 encore définie par

$$f(x) = g(x) \text{ pour } x \text{ dans } E_1.$$

Une des utilités de cette technique est de permettre de retaper avec assez peu de travaux une application qui n'est pas injective ou pas surjective - ou ni l'un ni l'autre - et d'en faire une nouvelle application ayant de bien meilleures propriétés.

- Soit f l'application de $\mathbb{R}$ vers $\mathbb{R}$ définie par $f(x) = \ln|x|$ pour tout x réel non nul. Cette application est surjective, mais pas injective. Si nous considérons plutôt la restriction $f_{|\mathbb{R}_+}$ ... , il s'agit alors d'une bijection.

- Toujours plus fort, soit g l'application de $\mathbb{R}$ vers $\mathbb{R}$ définie par

$$h(x) = x^2 \text{ pour tout } x \text{ réel.}$$

Cette application n'est pas injective (les réels strictement positifs ont deux antécédents), ni surjective (les réels strictement négatifs n'en ont aucun). Mais on remarque que $h(\mathbb{R}) = \mathbb{R}^+$ et donc a fortiori $h(\mathbb{R}^+) \subset \mathbb{R}^+$. Il est donc possible de restreindre h en une application de $\mathbb{R}^+$ vers $\mathbb{R}^+$. Et on obtient alors une bijection (on le prouvera rigoureusement plus tard). La fonction racine carrée peut alors être définie comme l'inverse de cette bijection.

- De même la fonction sin n'a rien d'une bijection vue comme fonction de $\mathbb{R}$ vers $\mathbb{R}$, mais en devient une si on la restreint en une application de $[-\frac{\pi}{2}, \frac{\pi}{2}]$ vers$[-1, 1]$. Ceci permet encore de

définir sa réciproque, une nouvelle fonction nommée arcsin.

☐ Soit E et F deux ensembles. On suppose que A soit une partie de E. On considère deux application $f : E \to F$ et $g : A \to F$.

On dit que g est la restriction de f à l'ensemble A et l'on note $g = f_{|A}$ lorsqu'on a : $\forall x \in A$, $g(x) = f(x)$.

On dit que f est le prolongement de g à E lorsque : $\forall x \in A$, $g(x) = f(x)$. Par exemple, on peut prendre

$$g : \begin{cases} \mathbb{R}^* \to \mathbb{R} \\ x \mapsto \frac{\sin x}{x} \end{cases} \quad \text{et } f : \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto \frac{\sin x}{x} \\ 0 \mapsto 1 \end{cases}$$

g est la restriction de f à $\mathbb{R}^*$ et f est le prolongement de f à $\mathbb{R}$.

D) Décomposition canonique d'une application

La notion d'ensemble quotient permet de décomposer toute application en une injection, une bijection et une surjection.

Définition

☐ Soient E et F des ensembles, f une application de E dans F, et $\Re$ est une relation d'équivalence sur E. On dit que f est compatible avec $\Re$ si, pour tous x, $y \in E$ tels que $x\Re y$, on a $f(x) = f(y)$.

☐ Soit $\Re$ une relation d'équivalence sur un ensemble non vide E et

$$\overline{x} = \{y \in E, x\Re y\} = \{y \in E, (x, y) \in \Re\}$$

la classe d'équivalence modulo $\Re$ de $x \in E$. Rappelons que l'ensemble quotient de E par $\Re$, noté $E/\Re$ est l'ensemble des classes d'équivalence. L'application de E sur $E/\Re$ définie par $i : x \mapsto \overline{x}$ s'appelle l'application canonique.

Théorème

Soient E et F deux ensembles, f une application de E dans F et $\Re$ la relation d'équivalence dans E associé à f. Il existe une application g et une seule de $E/\Re$ dans E telle que, pour tout élément x de E, on ait

$$(g \circ \varphi)(x) = f(x)$$

où φ est l'application canonique de E sur $E/\Re$. Cette application g est bijective et $f = i \circ g \circ \varphi$ où i est l'injection canonique de $f(E)$ dans F. Cette relation est appelée décomposition canonique de l'application f.

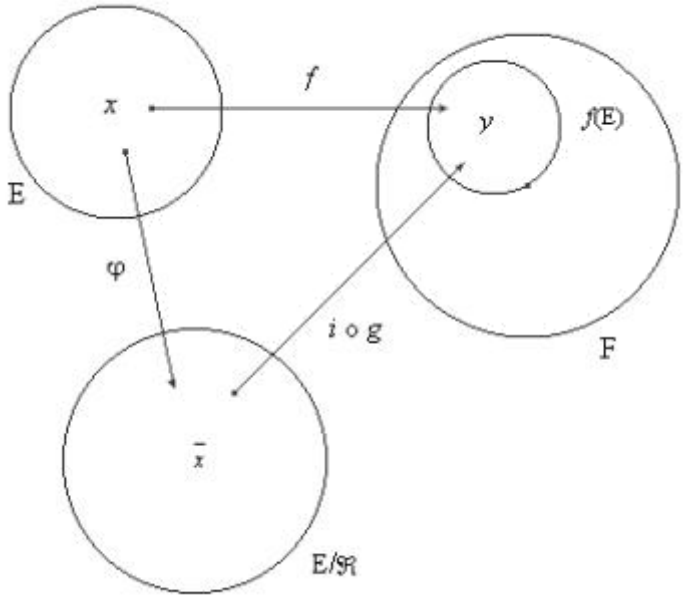
Preuve

Soit $\overline{x}$ un élément de l'ensemble quotient $E/\Re$. L'image de $\overline{x}$ par g est nécessairement donnée par la formule

$$g(\overline{x}) = f(\overline{x}).$$

Soit x un représentant de $\overline{x}$. Puisque $f(x)$ ne dépend pas du représentant choisi, la formule précédent définit effectivement une application g de $E/\Re$ dans $f(E)$. Montrons que cette application est surjective. Puisque, pour tout élément y de $f(E)$, il existe un élément x de E tel que $f(x) = y$. Ainsi, y est l'image par g de sa classe x.

Enfin, l'application g injective. En effet, la relation $g(\overline{x}) = g(\overline{x}')$ implique que, pour tout élément de $\overline{x}$ et pour tout représentant x' de $\overline{x}'$, $f(x) = f(x')$, c'est-à-dire $(x, x') \in \Re$, ou encore $\overline{x} = \overline{x}'$.


f
x
y
f(E)
E
φ
i o g
F
x̄
E/ℜ

Les ensembles usuels de nombres

Nous pouvons nous demander combien il y a de moutons dans un troupeau. Dans la vie courante, nous cherchons toujours le nombre d'objets, le nombre de situations, le nombre de ... Ainsi il semblerait que le fait de compter est une action vieille comme le monde. Ainsi, nous énonçons :

un mouton, deux moutons, trois moutons, ..., dix moutons.

Le troupeau contient dix moutons, dix est un entier et mouton est un objet du troupeau. Onze, douze etc. sont des entiers qui ont été déterminés par la répétition de l'objet mouton. Les entiers naturels se présentent à l'intuition sous ces aspects et permettent d'exprimer la quantité d'objets que comporte une collection. Au début de l'humanité, compter c'était mettre en correspondance les objets à compter des éléments de référence : doigts, entailles sur des bâtons, jetons en terre, etc. , puis de façon plus abstraites, avec des signes gravés sur des tablettes d'argile. En formalisant ce cheminement, nous allons construire une théorie axiomatique des entiers naturels en utilisant le langage des ensembles.

I) Construction de l'ensemble des entiers naturels

Les axiomes de Péano permettent une construction des entiers naturels.

A) Axiomes de Péano

Définition

☐ Péano postule l'existence d'un triplet $(0, \mathbb{N}, S)$, où $\mathbb{N}$ est un ensemble, 0 un élément particulier de $\mathbb{N}$, et $S : \mathbb{N} \to \mathbb{N}$ une application qui vérifient les axiomes suivants :

– Pour tout $n \in \mathbb{N}$, il existe un unique n^* (parfois noté aussi n' ou $\overset{\bullet}{n}$) appelé successeur tel que $n^* = S(n)$. Donc, S est injective, c'est-à-dire pour tout couple $(m, n) \in \mathbb{N}^2$, on a

$$m^* = n^* \text{ implique } m = n.$$

– Pour tout $n \in \mathbb{N}$, $S(n) \neq 0$. L'image de S est $\mathbb{N}^*$.

– Axiome de récurrence : si A contient 0 et telle que $n \in A$ entraîne $S(n) \in A$, alors on a : $\mathbb{N} = A$.

☐ L'ensemble $\mathbb{N}$ s'appelle ensemble des entiers naturels. L'élément 0 s'appelle zéro. L'application $S : \mathbb{N} \to \mathbb{N}$ s'appelle application successeur. Par définition, cette application est injective. Pour$n^* \in \mathbb{N}$, l'élément n s'appelle le prédécesseur de n^*. Zéro est l'unique élément n'ayant pas de prédécesseur. On note

$S(0) = 1$, $S(1) = 2$, $S(2) = 3$, $S(3) = 4$, $S(4) = 5$, $S(6) = 7$, $S(7) = 8$, $S(8) = 9$, $S(9) = 10$...

Théorème

Si $P(n)$ est une propriété dépendant du nombre entier naturel n telle que les deux assertions suivantes soient vérifiées :

i- $P(0)$ est vrai ;

ii- Si $P(n)$ est vrai, alors $P(S(n))$ est vrai.

Alors $P(n)$ est vrai pour tout entier naturel n.

Preuve

Soit A l'ensemble de tous les entiers naturels n tels que $P(n)$ soit vrai. Alors 0 est élément de A en vertu de l'hypothèse i- et si $n \in A$, alors $n^* \in A$ en vertu de l'hypothèse ii-. Puisque A est un ensemble vérifiant les axiomes de Péano, on a : $\mathbb{N} = A$. Cela signifie bien que pour un entier naturel n quelconque $P(n)$ est vrai.

Théorème

i) Soit $x \in \mathbb{N}$. Pour tout $y \in \mathbb{N}$, il existe une application unique $\varphi_x : \mathbb{N} \to \mathbb{N}$ vérifiant

- $\varphi_x(0) = x$
- $\forall y \in \mathbb{N}$, $\varphi_x(S(y)) = S(\varphi_x(y))$.

ii) Soit $x \in \mathbb{N}$. Pour tout $y \in \mathbb{N}$, il existe une application unique $p : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ vérifiant

- $p(x, 0) = 0$.
- $\forall y \in \mathbb{N}$, $p(x, S(y)) = \varphi_{p(x,y)}(x)$.

iii) Il existe une et une seule application, notée $+$, de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$ vérifiant

$$\begin{cases} \forall n \in \mathbb{N}, n + 0 = n \\ \forall p \in \mathbb{N}, \forall q \in \mathbb{N}, p + S(q) = S(p + q) \\ \forall n \in \mathbb{N}, S(n) = n + 1. \end{cases}$$

iv) Il existe une unique application, notée $\times$, ou ., ou sans symbole, de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$ vérifiant

$$\begin{cases} \forall n \in \mathbb{N}, n \times 0 = 0 \\ \forall p \in \mathbb{N}, \forall q \in \mathbb{N}, p \times (q + 1) = p \times q + p. \end{cases}$$

Preuve

i) **Unicité**

Pour x fixé quelconque dans $\mathbb{N}$, considérons deux application $\varphi_x : \mathbb{N} \to \mathbb{N}$ et $\varphi_{x\prime} : \mathbb{N} \to \mathbb{N}$ deux applications vérifiant

- $\varphi_x(0) = \varphi_{x\prime}(0) = 0$.
- $\forall y \in \mathbb{N}$, $\varphi_x(S(y)) = S(\varphi_x(y))$ et $\varphi_{x\prime}(S(y)) = S(\varphi_{x\prime}(y))$.

Supposons par récurrence que $\varphi_x(n) = \varphi_{x\prime}(n) = c$, alors

$$\varphi_x(S(n)) = S(\varphi_x(n)) \Rightarrow \varphi_x(n^*) = S(\varphi_x(n)) = d.$$

De même,

$$\varphi_{x\prime}(S(n)) = S(\varphi_{x\prime}(n)) \Rightarrow \varphi_{x\prime}(n^*) = S(\varphi_{x\prime}(n)).$$

Comme $\varphi_x(n) = \varphi_{x\prime}(n) = c$ et par injectivité de S, on a

$$S(\varphi_x(n)) = S(\varphi_{x\prime}(n)) = d \Rightarrow \varphi_x(n^*) = \varphi_{x\prime}(n^*).$$

Par application du théorème de récurrence, on a

$$\varphi_x(n) = \varphi_{x\prime}(n)$$

pour tout n, donc $\varphi_x = \varphi_{x\prime}$.

Existence

Pour montrer l'existence d'une telle application φ_x, on peut montrer l'existence d'un élément $\varphi_x(y) \in \mathbb{N}$ pour tout $y \in \mathbb{N}$. Posons

$$A = \{y \in \mathbb{N} \ / \ \varphi_x(y) \text{ existe et } \varphi_x(S(y)) = S(\varphi_x(y))\}.$$

Il est clair que $0, 1 \in A$ puisque $\varphi_x(0) = x$ existe et

$$\varphi_x(S(0)) = \varphi_x(1) = S(\varphi_x(0)) = S(x) = x^*.$$

Supposons que $n \in A$ et montrons que $n^* \in A$. Pour cela, il suffit de vérifier que $\varphi_x(n^*)$ existe. Par définition

$$\varphi_x(n^*) = \varphi_x(S(n)).$$

Or on a

$$\varphi_x(S(n)) = S(\varphi_x(n))$$

par récurrence. Comme $\varphi_x(n) \in \mathbb{N}$, il existe un unique $\varphi_x(n)^* \in \mathbb{N}$ tel que $S(\varphi_x(n)) = \varphi_x(n)^*$. On en déduit de là l'existence de $\varphi_x(n^*)$. Donc $n^* \in A$. L'axiome de récurrence montre que $A = \mathbb{N}$.

ii) **Unicité**

Pour x fixé quelconque dans $\mathbb{N}$, considérons deux application $p : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ et $p' : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ deux applications vérifiant

- $p(x, 0) = p'(x, 0) = 0$.
- $\forall y \in \mathbb{N}$, $p(x, S(y)) = \varphi_{p(x,y)}(x)$ et $p'(x, S(y)) = \varphi_{p\prime(x,y)}(x)$.

Supposons par récurrence que : $p(x, n) = p'(x, n) = c$, alors

$$p(x, S(n)) = \varphi_{p(x,n)}(x) \Rightarrow p(x, n^*) = \varphi_{p(x,n)}(x).$$

De même,

$$p'(x, S(n)) = \varphi_{p\prime(x,y)}(x) \Rightarrow p\prime(x, n^*) = \varphi_{p\prime(x,y)}(x).$$

Comme $p(x, n) = p'(x, n)$, on obtient

$$\varphi_{p(x,n)}(x) = \varphi_{p\prime(x,y)}(x) \Rightarrow p(x, n^*) = p'(x, n^*).$$

Par application du théorème de récurrence, on a : $p(x, n) = p'(x, n)$ pour tout n, donc $p = p'$.

Existence

Pour montrer l'existence d'une telle application φ_x, on peut montrer l'existence d'un élément $p(x, S(y)) \in \mathbb{N}$ pour tout $y \in \mathbb{N}$. Posons

$$A = \{y \in \mathbb{N} \ / \ p(x, S(y)) \text{ existe et } p(x, S(y)) = \varphi_{p(x,y)}(x)\}.$$

Il est clair que $0, 1 \in A$ puisque $p(x, 0) = 0$ existe et

$$p(x, S(0)) = p(x, 1) = \varphi_{p(x,0)}(x) = \varphi_0(x) \in \mathbb{N}.$$

Supposons que $n \in A$ et montrons que $n^* \in A$. Pour cela, il suffit de vérifier que $p(x, n^*)$ existe. Par définition

$$p(x, n^*) = p(x, S(n)).$$

Or on a

$$p(x, S(n)) = \varphi_{p(x,n)}(x).$$

par récurrence. Comme $p(x, n) \in \mathbb{N}$, il existe un unique $\varphi_{p(x,n)}(x) \in \mathbb{N}$. On en déduit l'existence de $p(x, n^*)$. Donc $n^* \in A$. L'axiome de récurrence montre que $A = \mathbb{N}$.

iii) Définissons l'application $(x, y) \mapsto x + y = \varphi_x(y)$ de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$. C'est bien une loi de composition interne. On a par ailleurs

- $\forall n \in \mathbb{N}$, $n + 0 = \varphi_n(0) = n$.
- $\forall p \in \mathbb{N}$, $\forall q \in \mathbb{N}$, $p + S(q) = \varphi_p(S(q)) = S(\varphi_p(q)) = S(p + q)$.
- Avec $S(0) = 1$, il vient

$$n + 1 = n + S(0) = \varphi_n(S(0)) = S(\varphi_n(0)) = S(n).$$

iv) De même, définissons l'application $(x, y) \mapsto xy = p(x, y)$ de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$. C'est bien une loi de composition interne. On a aussi

- $\forall n \in \mathbb{N}$, $n0 = p(n, 0) = 0$
- $\forall m, n \in \mathbb{N}$, $m(n + 1) = mS(n) = p(m, S(n)) = \varphi_{p(m,n)}(m) = p(m, n) + m) = mn + m$.

B) L'addition, la multiplication et propriétés subséquentes

Définition

☐ L'application $\mathbb{N}\times\mathbb{N} \to \mathbb{N}$, $(p,q) \mapsto p+q$ est une loi interne sur $\mathbb{N}$ appelé addition. Si $(p,q) \in \mathbb{N}\times\mathbb{N}$, $p+q$ est appelé somme de p et de q.

☐ L'application $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(p,q) \mapsto p \times q$ est une loi interne sur $\mathbb{N}$ appelé multiplication. Si $(p,q) \in \mathbb{N} \times \mathbb{N}$, $p \times q$ est appelé produit de p et de q.

☐ On peut définir la puissance n-ième d'un entier naturel n. On définit par récurrence

$$m^0 = 1 \text{ et } m^{n+1} = m^n m.$$

On verra que l'application ainsi définie $(m,n) \mapsto m^n$ est une loi de composition interne.

Théorème (Forme définitive du théorème de récurrence)

Comme $S(n) = n+1$, on peut écrire $P(S(n)) = P(n+1)$. Avec cette notation additif, on obtient la forme définitive du théorème de récurrence. Si $P(n)$ est une propriété dépendant du nombre entier naturel n telle que

i- On suppose $P(0)$.

ii- On suppose également que pour tout n : $P(n) \Rightarrow P(n+1)$.

Alors pour tout entier n, $P(n)$.

Il y a plusieurs formes de ce théorème. Nous allons les énumérer car dans certains cas, nous aurons besoin de ces variantes :

Corollaire

Soit n_0 un entier naturel.

i- Soit $P(n_0)$.

ii- Si, pour $n \geq n_0$, $P(n) \Rightarrow P(n+1)$.

Alors pour tout entier $n \leq n_0$, $P(n)$.

La récurrence double est donnée par le corollaire suivant :

Corollaire

Soit n_0 un entier naturel.

i- Soit $P(n_0)$ et $P(n_0+1)$

ii- Si, pour tout $n \geq n_0$, $P(n)$ et $P(n+1) \Rightarrow P(n+2)$.

Alors, $\forall n \geq n_0$, $P(n)$.

Donnons enfin la version de récurrence la plus puissante, c'est la récurrence forte :

Corollaire

Soit n_0 un entier naturel.

i- Soit n_0 un entier, on suppose $P(n_0)$.

ii- On suppose aussi que : $(\forall n \geq n_0, (P(n_0), P(n_0+1), \ldots, P(n))) \Rightarrow P(n+1)$.

Alors, $\forall n \geq n_0$, $P(n)$.

Propriété

i) L'addition entre entiers possède les propriétés suivantes :

- Associativité : $\forall (p,q,r) \in \mathbb{N}^3$, $(p+q)+r = p+(q+r)$.
- Elément neutre : $0+n = n+0 = n$.
- Commutativité : $\forall (p,q) \in N^2$, $p+q = q+p$.
- Régularité : $\forall (p,q,r) \in \mathbb{N}^3$, $(p+r) = (q+r) \Rightarrow p = q$.
- Etant donné p et q dans $\mathbb{N}$, on a : $p+q = 0 \Rightarrow p = q = 0$.

ii) La multiplication entre entiers possède les propriétés suivantes :

- Distributivité du produit par rapport à l'addition :
$$\forall (p,q,r) \in \mathbb{N}^3,\ p(q+r) = pq + pr \text{ et } (p+q)r = pr + qr.$$
- $\forall p \in \mathbb{N},\ 0p = p0 = 0$.
- Associativité : $\forall (p,q,r) \in \mathbb{N}^3,\ (p \times q) \times r = p \times (q \times r)$.
- Commutativité : $\forall (p,q) \in \mathbb{N}^2,\ p \times q = q \times p$.
- Elément neutre : $\forall p \in \mathbb{N},\ p \times 1 = 1 \times p$.
- Régularité : $\forall (p,q,r) \in \mathbb{N}^3,\ p \times r = q \times r \Rightarrow p = q$.
- Etant donné p et q deux entiers, alors on a les deux implications suivantes
$$pq = 0 \Rightarrow p = 0 \text{ ou } q = 0$$
$$pq = 1 \Rightarrow p = q = 1.$$

Preuve

i) **A**ssociativité

Considérons la propriété $P(n) : (p+q) + n = p + (q+n)$ pour tout $p,\ q \in \mathbb{N}$ fixés. $P(0)$ est vraie car 0 est neutre à droite par définition. On supposons que $P(n)$ soit vraie. Vérifions que$P(n+1)$ est également vraie. On a
$$P(n+1) : (p+q) + n + 1 = p + (q+n) + 1.$$
Par hypothèse de récurrence, il vient
$$(q+n) + 1 = q + (n+1) = (q+n+1),$$
d'où :
$$P(n+1) : (p+q) + n + 1 = p + (q+n+1).$$
Donc $P(n)$ est vraie $\forall n \in \mathbb{N}$.

– **Elément neutre**

Par définition, 0 est neutre à droite. Considérons la propriété $P(n) : 0 + n = n$.

$P(0)$ est vraie puisque $0 + 0 = 0$. Supposons que $P(n)$ soit vraie et vérifions que $P(n+1)$ est encore vraie. On a
$$P(n+1) : 0 + n + 1 = (0+n) + 1 = n + 1.$$
Donc $P(n)$ est vraie $\forall n \in \mathbb{N}$.

– **Commutativité**

Considérons la propriété
$$P(n) : p + n = n + p \text{ pour tout } p \in \mathbb{N} \text{ fixé.}$$
La propriété $P(0)$ est vraie puisque 0 est élément neutre. Supposons que $P(n)$ soit réalisé et observons
$$\begin{aligned} P(n+1) : p + n + 1 &= (p+n) + 1 \\ &= (n+p) + 1 \\ &= n + (p+1) \\ &= n + (1+p) \\ &= n + 1 + p. \end{aligned}$$
Donc $P(n)$ est vraie $\forall n \in \mathbb{N}$.

– **Régularité**

Considérons la propriété
$$P(n) : p + n = q + n \Rightarrow p = q.$$

Il est clair que $P(0)$ est vraie car 0 est élément neutre. Supposons que $P(n)$ soit vraie et

$$p+n+1=q+n+1.$$

Alors

$$S(p+n)=S(q+n).$$

Par injectivité de S, il vient

$$p+n=q+n.$$

Par hypothèse de récurrence, on obtient

$$p+n+1=q+n+1\Rightarrow p=q.$$

Donc $P(n+1)$ est réalisé $\forall n\in\mathbb{N}$.

− Raisonnons par l'absurde en supposant que $q\neq 0$ et $p+q=0$. Le prédécesseur q^- de q vérifie

$$p+(q^-+1)=(p+q^-)+1=0\Rightarrow S(p+q^-)=0.$$

C'est absurde puisque pour tout entier n, $S(n)$ est non nul. Donc

$$p+q=0\Rightarrow p=q=0.$$

ii) **Distributivité**

Soit la propriété dépendant de n :

$$P(n):p(q+n)=pq+pn \text{ et } (p+q)n=pn+qn.$$

Comme $\forall p\in\mathbb{N}$, $p0=0$, $P(0)$ est vraie. Supposons que $P(n)$ soit réalisée et calculons :

$$\begin{aligned} p(q+n+1) &= p((q+n)+1)\\ &= p(q+n)+p\\ &= pq+pn+p. \end{aligned}$$

Or $pn+p=p(n+1)$, donc

$$p(q+n+1)=pq+p(n+1).$$

Par ailleurs,

$$\begin{aligned} (p+q)(n+1) &= (p+q)n+(p+q)\\ &= pn+qn+p+q\\ &= pn+p+qn+q\\ &= p(n+1)+q(n+1). \end{aligned}$$

Donc $P(n)$ est vraie $\forall n\in\mathbb{N}$.

− Par définition, on a : $p0=0$, $\forall p\in\mathbb{N}$. Comme la multiplication est distributive par rapport à l'addition et par ailleurs $0+0=0$, il vient

$$(0+0)n=0.n\Rightarrow 0.n=0.n+0.n\Rightarrow 0.n=0.$$

Donc, on a : $0p=p0=0$, $\forall p\in\mathbb{N}$.

− **Associativité**

Considérons la propriété

$$P(n):(pq)n=p(qn) \text{ pour } p,\ q \text{ fixés.}$$

Il est évident que $P(0)$ est vraie. Supposons que $P(n)$ soit vraie à l'ordre n. Calculons

$$\begin{aligned} (pq)(n+1) &= (pq)n+pq\\ &= p(qn)+pq\\ &= p(qn+q)\\ &= p(q(n+1)). \end{aligned}$$

Donc $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

– Commutativité

La commutativité se démontre aussi par récurrence. Considérons en effet la propriété $P(n)$: $pn = np$ pour p fixé.

Il est évident que $P(0)$ est vraie. Supposons que $P(n)$ est vraie. Calculons

$$\begin{aligned} p(n+1) &= pn + p \\ &= np + p \\ &= (n+1)p. \end{aligned}$$

Donc $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

– Elément neutre

Considérons

$$P(n) : 1n = n1 = n.$$

Il est évident que $P(0)$ est vraie. Supposons que $P(n)$ soit vraie et calculons :

$$1(n+1) = 1n + 1 = n + 1.$$

De l'autre côté, on a

$$(n+1)1 = n1 + 1 = n + 1.$$

Donc la propriété $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

– Régularité

Se démontre aisément par récurrence.

– On raisonne par l'absurde en supposant que $p \neq 0$ et $q \neq 0$. Les prédécesseur p^- et q^- de p et q respectivement vérifient

$$pq = 0 \Rightarrow (p^- + 1)(q^- + 1) = p^-q^- + p^- + q^- + 1$$

et $p^-q^- + p^- + q^-$ aurait pour successeur 0. C'est impossible et donc $p = 0$ et $q = 0$.

Supposons maintenant que $pq = 1$ avec $p \neq 0$ et $q \neq 0$. Calculons

$$\begin{aligned} & pq &= (p^- + 1)(q^- + 1) = p^-q^- + p^- + q^- + 1 = 1 \\ \Rightarrow \quad & p^-q^- + p^- + q^- &= 0 \\ \Rightarrow \quad & p^- &= 0 \text{ et } q^- = 0. \\ \Rightarrow \quad & p &= q = 1. \end{aligned}$$

Théorème

i) L'application $m \mapsto m^n$ est un morphisme de $\mathbb{N}$ muni de l'addition dans $\mathbb{N}^*$ muni de la multiplication :

$$m^{n+n'} = m^n m^{n'}.$$

ii) Pour tout triplet d'entiers naturels, on a : $(m^n)^p = m^{np}$.

Preuve

i) On peut raisonner par récurrence. Considérons la relation $P(n)$: $m^{a+n} = m^a m^n$ avec $a \in \mathbb{N}$. La propriété est vraie pour $n = 0$, en effet $(m.m')^0 = 1$ et $m^0 m'^0 = 1$, donc : $(m.m')^0 = m^0 m'^0$. Supposons que la propriété est vraie pour n. Et examinons $P(n+1)$. On a alors :

$$(m.m')^{n+1} = (m.m')^n.(m.m') \text{ par définition.}$$

Or par hypothèse de récurrence, on sait que $(m.m')^n = m^n m'^n$, donc :

$$(m.m')^{n+1} = m^n.m'^n.m.m' = m^n.m.m'^n.m'$$

car la multiplication est commutative. On a finalement $(m.m')^{n+1} = m^{n+1}.m'^{n+1}$.

ii) On démontre par récurrence, en considérant la propriété $P(n)$:

– $P(0)$ est vraie car : $(m^a)^0 = 1$ et $m^{a\cdot 0} = 1$

– Supposons $P(n)$ vraie, et calculons $P(n+1)$. On a alors

$$(m^a)^{n+1} = (m^a)^n \cdot m^a = m^{an} \cdot m^a = m^{an+a} = m^{a(n+1)},$$

ce qui achève la démonstration.

C) Relation d'ordre dans l'ensemble des entiers naturels, unicité de $\mathbb{N}$

Il existe une relation d'ordre total privilégiée dans $\mathbb{N}$, on l'appelle l'ordre canonique de $\mathbb{N}$.

Définition

☐ Soient a, b et n des entiers naturels. Si $a = b + n$, on dit que a est supérieur ou égal à b et que b est inférieur ou égal à a. On écrit

$$a = b + n \Leftrightarrow a \geq b \text{ ou } b \leq a.$$

☐ Si $n \neq 0$, alors $a \neq b$. On dit alors que a est strictement supérieur à b et que b est strictement inférieur à a, et on écrit

$$a = b + n \text{ (avec } n \neq 0) \Leftrightarrow a > b \text{ ou } b < a.$$

☐ On dit qu'un nombre n est positif lorsque $n \geq 0$. Il est alors clair que tout entier naturel n est positif puisque $n = 0 + n$.

☐ Soient E et F des ensembles ordonnés. On appelle morphisme des ensembles ordonnés E et F une application croissante.

Propriété

i) La relation d'inégalité ($\geq$ ou $\leq$) définit dans l'ensemble $\mathbb{N}$, une relation d'ordre total au sens large.

ii) Tout couple d'entier (a, b) vérifie soit $a \geq b$ soit $a \leq b$.

iii) Lorsqu'un entier naturel a est supérieur à un entier b, il est au moins égal à son suivant $b^* = b + 1$, ce qu'on écrit aussi : $a > b \Rightarrow a \geq b + 1$.

iv) Si a et b sont deux entiers naturels tels que $a \geq b$, il existe un entier naturel x unique tel que $a = b + x$, appelé différence des entiers a et b pris dans cet ordre (ou excès de a sur b). On écrit :

$$a = b + x \Leftrightarrow x = a - b.$$

vi) Soit n un entier naturel. Il n'y a pas de nombre entier naturel x tel que : $n < x < n + 1$.

vii) L'exponentiation est compatible avec la relation d'ordre, c'est-à-dire :

$$\begin{cases} a = b \Leftrightarrow a^m = b^m \\ a < b \Leftrightarrow a^m < b^m. \end{cases}$$

Preuve

i) Elle est réflexive car $a = a + 0 \Rightarrow a \geq a$.

Elle est antisymétrique car les égalités

$$a = b + x$$

et

$$b = a + y$$

entraînent

$$a + b = b + a + x + y.$$

Donc $x + y = 0$, soit $x = y$ et $a = b$, donc $a \geq b$ et $b \geq a \Rightarrow a = b$.

Elle est transitive, car les égalités

$$a = b + x$$

et

$$b = c + y$$

entraînent

$$a = (c + y) + x = c + (x + y).$$

Donc $a \geq b$ et $b \geq c \Rightarrow a \geq c$.

ii) Donnons nous l'entier a et montrons que l'entier b se compare à a. Cela est vraie pour $b = 0$ car

$$a = 0 + a \Rightarrow a \geq 0.$$

Supposons n classé par rapport à a, il vérifie soit $n \geq a$, soit $n < a$. Montrons que $b = n^*$ se compare à a. Si $n \geq a$, on a

$$n = a + x \text{ et } n^* = a + x^* \Rightarrow n^* > a.$$

Si $n < a$, on a

$$a = n + x^* = x + n^* \Rightarrow n^* \leq a.$$

Donc tout entier b est comparable à a.

iii) Comme $a > b$, on peut écrire par définition $a = b + m^*$, ce qui est équivalent

$$a = b^* + m = (b + 1) + m,$$

donc

$$a \geq b + 1.$$

iv) La relation $a \geq b$ suppose l'existence de x tel que $a = b + x$. Cet entier x est unique car s'il en existait un second x', cela impliquerait $a = b + x = b + x'$ soit $x = x'$.

v) On montre par récurrence la propriété $P(n)$. Il n'y a pas d'entier naturel x tel que $n < x < n+1$. $P(0)$ est vrai puisque, sinon, on aurait un entier x tel que $0 < x < 1$. Dans ce cas, $x \neq 0$ et donc,

$$(x - 1) \in \mathbb{N}.$$

Mais, on aurait aussi $x - 1 < 0$, ce qui est absurde. Si maintenant, on suppose que $P(n)$ est vrai, alors $P(n + 1)$ ne peut être fausse, sinon on aurait un $x \in \mathbb{N}$ tel que $n + 1 < x < n + 2$ et donc un entier

$$x - 1 \in \mathbb{N}$$

tel que $n < x - 1 < n + 1$, ce qui est impossible par hypothèse de récurrence.

vi) Montrons $a = b \Leftrightarrow a^m = b^m$. Vraie pour $m = 0$ car $a^0 = b^0 = 1$. Supposons que

$$a^m = b^m \Leftrightarrow a = b,$$

on a alors

$$a^m a = b^m b,$$

donc

$$a^{m+1} = b^{m+1}.$$

On montre $a < b \Leftrightarrow a^m < b^m$ également par récurrence.

Remarque

1°) On pouvait montrer d'une autre manière que entre n et $(n+1)$, il n'y a pas d'entiers. Notons $\overset{\bullet}{n}$ l'élément suivant de n. Alors $1 = \overset{\bullet}{0}$ et $n+1 = n+\overset{\bullet}{0} = \overbrace{n+0}^{\bullet} = \overset{\bullet}{n}$.

2°) Si $a < b$, la différence $a - b$ n'existe pas car

$$a = b + x \Rightarrow a \geq b,$$

ce qui est incompatible avec $a < b$. Ainsi la soustraction n'est pas une loi de composition interne définie pour tout couple ordonné d'entiers naturels (a, b).

3°) Les deux définitions suivantes sont de bon sens, mais les avoir en tête permet de trouver la bonne idée pour débuter une démonstration.

– Soit A une partie de $\mathbb{N}$ et n un élément de A. On dit que n est le plus grand élément de A lorsque pour tout k de A, $k \leq n$.

– Soit A une partie de $\mathbb{N}$ et n un élément de A. On dit que n est le plus petit élément de A lorsque pour tout k de A, $n \leq k$.

Théorème

i) Tout partie non vide de $\mathbb{N}$ admet un plus petit élément.

ii) Tout partie non vide de $\mathbb{N}$ qui est majoré par un certain entier naturel admet un plus grand élément.

iii) Pour tout naturel non nul a et pour tout entier naturel b, il existe $n \in \mathbb{N}$ tel que $na > b$. On dit aussi que l'ensemble $\mathbb{N}$ est archimédien.

iv) Pour tout entier naturel non nul p et pour tout entier naturel n, on a (inégalité de Bernouilli)

$$p^n \geq 1 + n(p-1).$$

v) Toute suite strictement décroissante de $\mathbb{N}$ est finie (principe de descendante infinie de Fermat).

Preuve

i) Raisonnons par l'absurde et considérons une partie E non vide de $\mathbb{N}$ qui n'a pas de plus petit élément. On va montrer par récurrence la propriété $P(n) : \forall x \in E,\ n \leq x$.

La propriété $P(0)$ est vrai car tout élément de E est un entier naturel positif. Si la propriété $P(n)$ est vrai, montrons que $P(n+1)$ est vrai. S'il en était autrement, il existerait un x de E tel que $x < n+1$. Puisque $P(n)$ est supposée vrai, on a alors l'encadrement $n \leq x \leq n+1$ ce qui entraîne $n = x$, et donc $n \in E$; ceci montre que n est le plus petit élément de E, contrairement à notre hypothèse. Donc $P(n+1)$ ne peut être que vraie. Ceci achève de montrer la propriété $P(n)$ pour tout entier naturel n. Prenons maintenant $x \in E$ et $n = x+1$, on obtient grace à $P(n)$ à la relation

$$n + 1 \leq n$$

qui est absurde, à moins que E soit vide, ce qui est aussi absurde.

ii) Soit E une partie non vide majorée de $\mathbb{N}$. L'ensemble M de ses majorants est donc non vide. M étant non vide admet un plus petit élément m.

– si $m = 0$, alors nécessairement $E = \{0\}$ et 0 est le plus grand élément de E.

– si $m > 0$, alors $m-1$ n'appartient pas à M, (puisque m est le plus petit élément de M), donc $(m-1)$ ne majore pas E. Il existe donc un élément x de E tel que :

$$m - 1 < x \leq m.$$

Donc $x = m$, et comme m majore E, x est bien le plus grand élément de E.

iii) L'ensemble des multiples de a n'est pas majorée, c'est ce que le théorème d'Archimède exprime. Pour démontrer qu'il existe $n \in \mathbb{N}$ tel que $na > b$, il suffit de prendre $n = b+1$, car

$$\begin{array}{rcl}(b+1)a & = & ba+a=b+a+b(a-1)\\ & \geq & b+a\\ & \geq & b+1\\ & \geq & b.\end{array}$$

iv) Nous allons démontrer par récurrence sur l'entier n. Si $n=0$, $p^n=1$ et $1+n(p-1)=1$, l'inégalité est donc vérifiée. Supposons la propriété vraie pour l'entier n, alors

$$\left\{\begin{array}{ll}p^{n+1} & =pp^n\geq[1+(p-1)]\cdot[1+n\,(p-1)]\\ & =1+(n+1)\cdot(p-1)+n\,(p-1)^2\end{array}\right.$$

ce qui implique $p^{n+1}\geq 1+(n+1)\cdot(p-1)$.

v) Prendre comme partie E l'ensemble des termes de la suite. Le fait que E admette un plus petit élément x_n et que la suite soit décroissante entraîne que x_n est nécessairement le dernier élément de la suite.

On peut aussi raisonner par l'absurde. Si (x_n) était une telle suite, on aurait $x_{n+1}<x_n$ pour tout n entier naturel, donc $x_{n+1}\leq x_n-1$. En appliquant ceci à $n=0$, 1, 2, ..., on trouve successivement :

$$x_1\leq x_0-1,\ x_2\leq x_1\ -1,\text{ etc.}$$

On en déduit :

$$x_2\leq x_0-2,\ x_3\leq x_0-3,\ ...,\ x_n\leq x_0-n.$$

En prenant $n=\ x_0\ +1$, on obtient $x_n<-1$, ce qui contredit le fait que la suite x_n est composée d'entiers naturels.

Cette propriété est utilisée par Fermat sous la forme suivante : Pour montrer qu'une propriété P est vraie pour tout n, Fermat montre que si P est fausse pour un entier, alors elle est fausse pour un entier strictement plus petit. Ce qui est impossible, car en itérant le procédé, on construirait une suite strictement décroissante d'entiers.

Nous allons maintenant démontrer un théorème qui nous permet d'identifier tous les ensembles naturels à $\mathbb{N}$.

Théorème

Soient E et F des ensembles naturels vérifiant les axiomes de Péano. Il existe un et un seul isomorphisme d'ensembles ordonnées de E et F.

Si on applique ce résultat, on peut identifier tous les ensembles naturels à $\mathbb{N}$. Par conséquent $\mathbb{N}$ est unique à un isomorphisme près.

Démonstration

Notons m, n les plus petits éléments de E et F respectivement. Pour $a\in E$, notons par a' l'élément suivant de a et par $'a$ le précédent de a.

Unicité

Soient f, g des isomorphismes de E sur F. Pour $a\in E$, on a : $m\leq a\Rightarrow f(m)\leq f(a)$.

Alors $f(m)=n$ puisque f est surjective. De même $g(m)=n$. Prouvons que $f(a')=(f(a))'$. On a : $a<a'\Rightarrow f(a)<f(a')$.

Supposons qu'il existe : $y\in[\![f(a),f(a')]\!]$.

Soit $x\in E$ tel que $y=f(x)$. Comme f est un isomorphisme, il vient $a<x<a'$. C'est absurde. On a donc

$$f(a')=(f(a))'.$$

On prouve de même que $g(a') = (g(a))'$. Soit $X = \{x \in E; f(x) = g(x)\}$. D'après ce qui précède, il vient $X = E$. D'où $f = g$.

Existence

Soit S l'ensemble des éléments a pour lesquels existe $f_a : [\![m, a]\!] \to F$ vérifiant $f_a(m) = n$ et $f_a(x') = (f_a(x))'$ si

$$m \leq x < a.$$

On a $m \in S$ et, posant

$$f_{m'}(m) = n,\ f_{m'}(m') = n',$$

on voit que $m' \in S$.

Si $a \in S$, $a' \notin [\![m, a]\!]$ par définition de a', et $[\![m, a']\!] = [\![m, a]\!] \cup \{a'\}$. Définissant $f_{a'}$ par

$$f_{a'} \big|_{[\![m,a]\!]} = f_a\ ,$$

on obtient $a' \in S$. Donc $S = E$.

Soient a, $b \in E^*$ tels que $a \leq b$. Alors

$$'a \in [\![m, b]\!] \text{ et } f_b(a) = f_b(('a)') = (f_b('a))'.$$

Par suite,

$$f_b(a) \in E^* \text{ et } f_b('a) = '(f_b(a)).$$

Soient a, $b \in E$ tels que $a \leq b$. Prouvons que

$$f_b \big|_{[\![m,a]\!]} = f_a$$

(ce qui montrera en particulier que les f_x sont uniquement déterminés). l'ensemble

$$Y = \{x \in [\![m, a]\!]; f_a(x) \neq f_b(x)\}$$

possède un plus petit élément c. Par définition des f_x, on a $c > m$. Alors

$$f_a('c) = '(f_a(c)),\ f_b('c) = '(f_b(c)).$$

Il en résulte que $f_a('c) \neq f_b('c)$, soit $'c \in Y$. Il y a contradiction.

D'après ce qui précède, il existe une unique application de E dans F telle que

$$f \big|_{[\![m,a]\!]} = f_a$$

pour tout $a \in E$. On a aussi $f(m) = n$, et $f(x') = (f(x))'$ pour tout $x \in E$. Soient $a \in E$, et

$$Z = \{x \in]\, a, \infty\, [; f\,(x) \leq f\,(a)\}\,.$$

Supposons $Z \neq \emptyset$. Soit b le plus petit élément de Z. Alors $b > m$, et $f(b) \leq f(a)$. Comme $f(a') = (f(a))'$, on obtient $b \neq a'$, donc $'b > a$. D'autre part, on sait que $f('b) = '(f(b)) < f(b) \leq f(a)$. Par conséquent, $'b \in Z$. Contradiction. On donc montré que f est strictement croissante.

Soit $T = F \backslash f(E)$. Supposons $T \neq \emptyset$, et soit d son plus petit élément. Par construction de f, on a $d > m$. Alors $'d$ existe, ainsi que $u \in E$ tel que $'d = f(u)$. D'où $d = ('d)' = (f(u))' = f(u')$. Autrement dit, $d \in f(E)$. C'est absurde. L'application f est donc surjective.

Donc f est un morphisme bijectif. Soient g la bijection croissante réciproque de f, et x, $y \in E$, avec $x \leq y$. Comme f est strictement croissante, si $g(y) < g(x)$, on a $y = f(g(y)) < f(g(x)) = x$. Contradiction. Par suite, f est un isomorphisme de E sur F.

On a montré ainsi qu'un ensemble $\mathbb{N}'$ quelconque, vérifiant les axiomes de Péano, est pourvu d'une structure isomorphe avec $\mathbb{N}$. Du point de vue mathématique, ces deux ensembles sont indiscernables. D'où l'unicité de $\mathbb{N}$ à un isomorphisme près.

Sur $\mathbb{N}$, seul zéro admet un opposé. Ainsi $\mathbb{N}$ n'est pas un groupe. L'équation $a+x=b$ n'admet pas de solution si $b<a$. Donc, l'application $(a,b)\mapsto b-a$ n'étant pas définie sur $\mathbb{N}\times\mathbb{N}$ tout entier, n'est pas une loi composition. Il convient donc de chercher un groupe G, noté additivement, tel que $\mathbb{N}$ soit une partie stable de G et que la loi de composition induite par celle de G ne soit autre que l'addition sur $\mathbb{N}$. Pour cela, nous allons symétriser pour l'addition, l'ensemble $\mathbb{N}$ des entiers naturels, c'est-à-dire à partir de $\mathbb{N}$, un nouvel ensemble $\mathbb{Z}$ où tout élément aura un opposé et dans lequel nous pourrons inclure $\mathbb{N}$. On parvient à ce but en étendant aux différents couples d'entiers naturels (a,b) les propriétés (égalité, somme, produit) des différences d'entiers naturels $(a-b)$. $(\mathbb{Z},+,\times)$ est alors un anneau. $\mathbb{Q}$ est construit de façon que tout élément non nul de $\mathbb{Z}$ possède un inverse pour $\times$. $(\mathbb{Q},+,\times)$ est alors un corps.

II) Construction de $\mathbb{Z}$

La soustraction dans $\mathbb{N}$ n'est pas toujours possible : l'équation $x+a=b$ n'admet pas dans $\mathbb{N}$ de solution pour $a\leq b$, mais la différence $b-a$ existe et on a

$$b-a=(b+m)-(a+m),\ \forall m\in\mathbb{N}.$$

En posant $(a',b')=(a+m,b+m)$, on peut dire que les couples (a,b) et (a',b') sont équivalents. Cette considération nous amène à étudier la relation $\Re$ définie sur $\mathbb{N}^2$ entre (a,b) et (a',b') par l'égalité

$$a+b'=a'+b.$$

A) Structures algébriques de $\mathbb{N}^2/\Re$

Donnons tout d'abord la définition de groupe et d'anneau.

Définition

☐ Un ensemble G muni d'une loi de composition interne notée additivement $+$ est un groupe s'il satisfait aux trois conditions suivantes :

i) La loi $+$ est associative

ii) Il existe un élément neutre noté 0 pour la loi $+$

iii) Tout élément de G est symétrisable.

Un groupe G est dit abélien ou commutatif lorsque sa loi de composition $+$ est commutative.

Une partie E d'un groupe $(G,+)$ est un sous-groupe si $(E,+)$ est un groupe.

☐ Un anneau est un ensemble A muni de deux lois de composition internes (l'addition $+$ et la multiplication $\times$) tel que

i) A est un groupe commutatif par rapport à l'addition ;

ii) la multiplication est associative et possède un élément neutre 1 (unité) ;

iii) la multiplication est distributive par rapport à l'addition.

☐ Un anneau A est dit commutatif lorsque sa loi $\times$ est commutative.

☐ Une partie E de $(A,+,\times)$ est un sous-anneau si $(E,+,\times)$ est un anneau.

☐ Une application d'un anneau A dans un anneau B est un morphisme si : $\forall(x,y)\in A$

$$f(x+y)=f(x)+f(y)$$
$$f(xy)=f(x)f(y)$$
$$f(1_A)=1_B.$$

☐ On note $\ker f$ l'image réciproque de $\{0\}$ par f. On a une propriété remarquable :

$$f \text{ injective} \Leftrightarrow \ker f=\{0\}.$$

Propriété

1°) Définissons l'addition et la multiplication sur $\mathbb{N}^2$:

$$\forall (a,a',b,b') \in \mathbb{N}^4,\ (a,b)+(a',b') = (a+a', b+b\prime)$$
$$\forall (a,a',b,b') \in \mathbb{N}^4,\ (a,b)\times(a',b') = (aa'+bb', ab'+ba').$$

Ces deux opérations sont commutatives et associatives.

2°) La relation $\Re$ définie par :

$$(a,b)\Re(a',b') \Leftrightarrow a+b' = b+a'$$

est une relation d'équivalence compatible avec l'addition et la multiplication sur $\mathbb{N}^2$.

3°) Le quotient $\mathbb{N}^2/\Re$ muni des opérations quotients

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)} \text{ et } \overline{(a,b)(c,d)} = \overline{(ac+bd, ad+bc)}$$

est un anneau commutatif.

4°) Considérons l'application $\varphi : \mathbb{N} \to \mathbb{N}^2/\Re$ définie par $\varphi : a \mapsto \overline{(a,0)}$. Cette application est injective.

Preuve

1°) A partir des propriétés des opérations dans $\mathbb{N}$, on montre facilement l'associativité et la commutativité de l'addition :

Associativité :

$[(a,b)+(a',b')]+(a'',b'')$ et $(a,b)+[(a',b')+(a'',b'')]$ sont égales à $(a+a'+a'', b+b'+b'')$.

Commutativité :

$$(a+a', b+b') = (a'+a, b'+b) \Rightarrow (a,b)+(a',b') = (a',b')+(a,b).$$

Elément neutre :

$$(0,0)+(a,b) = (a,b)+(0,0) = (a,b).$$

Pour la multiplication, les choses sont plus pénible, mais rien de difficile. Il suffit d'écrire :

$$\begin{aligned}
[(a,b)(c,d)](e,f) &= (ac+bd, ad+bc)(e,f) \\
&= [(ac+bd)e + (ad+bc)f, (ac+bd)f + (ad+bc)e] \\
&= [a(ce+df)+b(cf+de), a(cf+de)+b(ce+df)] \\
&= (a,b)[(c,d)(e,f)].
\end{aligned}$$

2°) **R**éflexive car : $a+b = b+a \Rightarrow (a,b)\Re(a,b)$.

Symétrique car $a+b' = b+a' \Rightarrow a'+b = b'+a$, soit $(a,b)\Re(a',b') \Rightarrow (a',b')\Re(a,b)$.

Transitive car supposons que $a+b' = a'+b$ et que $a'+b'' = a''+b'$, alors

$$(a+b')+b'' = (a'+b)+b''$$

et

$$(a''+b')+b = (a'+b'')+b.$$

Or, l'addition dans $\mathbb{N}$ étant associative et commutative, on a :

$$a+b''+b' = a''+b+b'.$$

L'entier naturel b' étant régulier, $a+b'' = a''+b$. Ce qui montre que la relation $\Re$ est transitive.

Montrons que la relation d'équivalence $\Re$ est compatible avec les deux lois internes de $\mathbb{N}^2$. Pour l'addition, calculons :

$$(a,b)\Re(a',b') \text{ s'écrit } a+b' = b+a'$$
$$(c,d)\Re(c',d') \text{ s'écrit } c+d' = d+c'.$$

Par addition, nous obtenons :

$$a+c+b'+d'=b+d+a'+c'$$

c'est-à-dire

$$(a+c,b+d)\Re(a'+c',b'+d').$$

Pour la multiplication, nous passons par la différence dans $\mathbb{N}$, en supposant que $a\leq b$ et $d\leq c$. Nous pouvons donc écrire les deux relations $(a,b)\Re(a',b')$ et $(c,d)\Re(c',d')$ sous la forme :

$$b-a=b'-a'$$

et

$$c-d=c'-d'.$$

En multipliant membre à membre, il vient

$$(b-a)(c-d)=(b'-a')(c'-d')$$

soit

$$ad+bc-ac-bd=a'd'+b'c'-a'c'-b'd'\Rightarrow(a'c'+b'd')+(ad+bc)+(a'd'+b'c')$$

c'est-à-dire

$$(ac+bd,ad+bc)\Re(a'c'+b'd',a'd'+b'c').$$

La compatibilité signifie que si l'on remplace (a,b) et (c,d) par des couples équivalents (a',b') et (c',d'), le couple $(a'+c',b'+d')$ est équivalent au couple $(a+c,b+d)$. Autrement dit, la classe de $(a+c,b+d)$ ne dépend que des classes de $\overline{(a,b)}$ et de $\overline{(c,d)}$.
L'égalité

$$a+(b+k)=b+(a+k)$$

montre que $(a,b)=(a+k,b+k)$ et par suite $(a,b)=(a-k,b-k)$ lorsque les deux différences $a-k$ et $b-k$ sont possibles en entiers naturels.

3°) Montrons tout d'abord que $\mathbb{N}^2/\Re$ est un groupe commutatif pour l'addition. La commutativité et l'associativité de l'addition sont facile à vérifier. Le neutre pour l'addition est la classe de $(0,0)$ ou (a,a) (ils sont équivalents pour $\Re$) car

$$\overline{(a,b)}+\overline{(0,0)}=\overline{(0,0)}+\overline{(a,b)}=\overline{(a,b)}.$$

D'autre part, tout élément $\overline{(a,b)}\in\mathbb{N}^2/\Re$ admet $\overline{(b,a)}$ pour symétrique :

$$\overline{(a,b)}+\overline{(b,a)}=\overline{(a+b,b+a)}=\overline{(0,0)}.$$

Donc $(\mathbb{N}^2/\Re,+)$ est un groupe est un groupe commutatif.
Montrons maintenant que $(\mathbb{N}^2/\Re,+,\times)$ est un anneau commutatif. L'associativité et la commutativité de la multiplication sont évident. Le neutre de la multiplication est $\overline{(1,0)}$ ou $\overline{(a+1,a)}$ car :

$$\overline{(a,b)}$$

Il ne nous reste plus qu'à montrer la distributivité de la multiplication par rapport à l'addition :

$$\begin{aligned}\overline{(m,n)}[\overline{(a,b)}+\overline{(a',b')}] &= \overline{(m(a+a')+n\,(b+b')\,,m\,(b+b')+n\,(a+a'))}\\ &= \overline{((ma+nb)+(md+nb')\,,(mb+na)+(nb'+na'))}\\ &= \overline{(ma+nb,nb+na)}+\overline{(na'+nb',mb+nd)}\\ &= \overline{(m,n)(a,b)}+\overline{(m,n)(a',b')}\end{aligned}$$

Ainsi $(\mathbb{N}^2/\Re, +, \times)$ est un anneau commutatif.

4°) On a :

$$\varphi(a) = \varphi(b) \Leftrightarrow \overline{(a,0)} = \overline{(b,0)} \Leftrightarrow (a,0)\Re(b,0) \Leftrightarrow a+0 = b+0 \Leftrightarrow a = b.$$

B) L'anneau $\mathbb{Z}$ et propriétés premières

Définition

☐ On définit l'ensemble $\mathbb{Z}$ (du mot allemand Zahl pour nombre) des entiers relatifs comme l'ensemble quotient $(\mathbb{N}\times\mathbb{N})/\Re$. On appelle entier relatif, la classe d'équivalence $\overline{(a,b)}$ des éléments de $\mathbb{N}^2$ équivalents au couple (a,b) modulo $\Re$.

☐ Si $a > b$, on a

$$a - b = n.$$

Dans ce cas, on peut écrire $\overline{(a,b)} = \overline{(a-b, b-b)} = \overline{(n,0)}$. L'entier $\overline{(n,0)}$ est dit positif et s'écrire n.

☐ Si $a < b$, alors $b - a = n$, dans ce cas , on peut écrire $\overline{(a,b)} = \overline{(a-a, b-a)} = \overline{(0,n)}$. L'entier $\overline{(0,n)}$ est dit négatif et s'écrit -n. Avec ces définitions, on voit que $\overline{(0,0)}$ est à la fois positif et négatif.

Propriété

1°) La somme de deux entiers positifs est un entier positif. La somme de deux entiers négatifs est un entier négatifs.

2°) Si m et n sont positifs, alors mn est positif. Si m et n sont négatifs, alors mn est positif.

Si l'un des deux nombres m et n est positif et l'autre négatif, alors mn est négatif.

Preuve

1°) On a

$$a + b = \overline{(a,0)} + \overline{(b,0)} = \overline{(a+b,0)} = a + b.$$
$$(-a) + (-b) = \overline{(0,a)} + \overline{(0,b)} = \overline{(0,a+b)} = -(a+b)$$

Par ailleurs, on a :

$$a + (-b) = \overline{(a,0)} + \overline{(0,b)} = \overline{(a,b)}.$$

Là on a deux cas :

$\overline{(a,b)}$ est égal à $\overline{(a-b,0)}$ pour $a > b$.

$\overline{(a,b)}$ est égal à $\overline{(0,b-a)}$ pour $b > a$.

2°) Il est clair que

$$\overline{(a,0)(b,0)} = \overline{(ab,0)} = ab$$
$$\overline{(a,0)(0,b)} = \overline{(0,ab)} = -ab$$
$$\overline{(0,a)(0,b)} = \overline{(ab,0)} = ab$$

Avec les notations usuelles abrégée, on écrit :

$$a(-b) = -ab \text{ et } (-a)(-b) = ab.$$

Définition

☐ Etant donné deux entiers a et b, il existe un entier unique $n = a+(-b)$ tel que $a = b+n$, appelé différence de a et b qu'on note $a - b$:

$$n = a - b \Leftrightarrow a = b + n \Leftrightarrow n = a + (-b).$$

☐ Une somme algébrique est le résultat d'une suite d'additions et de soustraction à effectuer dans l'ordre des termes.

☐ Si $a = bn$, on dit que l'entier relatif n est le quotient exact de a par b. On note $a : b = n$ ou $\frac{a}{b} = n$.

☐ On définit $(a)^p = a^p$ et

$$(-a)^p = (-1)^p a^p = \begin{cases} a^p \text{ si } p \text{ pair} \\ -a^p \text{ si } p \text{ impair} \end{cases}.$$

Propriété

1°) La soustraction est une loi de composition interne dans $\mathbb{Z}$ définie pour tout couple ordonné d'entiers relatifs (a, b). Cette loi de composition n'est ni commutative ni associative et n'admet pas d'élément neutre.

2°) On a

$$\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = ba'$$

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + ba'}{bb'}$$

$$\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}.$$

On ne peut pas diviser par 0.

Preuve

1°) La soustraction n'est pas commutative :

$$3 - 5 = -2 \neq 5 - 3 = 2.$$

ni associative :

$$3 - (5 - 1) = -1 \neq (3 - 5) - 1 = -3.$$

Par ailleurs, pour tout $(n, p) \in \mathbb{Z}^2$, on a :

$$n - p \neq p - n.$$

Il est donc impossible que n soit neutre pour la soustraction.

2°) Si $x = \frac{a}{b}$ et $y = \frac{a'}{b'}$, on peut écrire $a = bx$ et $a' = b'y$. Alors on a :

$-$ $ab'y = a'bx$ donc $y = x$ ou $\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = ba'$

$-$ $ab' + a'b = b'bx + bb'y = bb'(x + y)$ donc $x + y = \frac{a}{b} + \frac{a'}{b'} = \frac{a'b + ba'}{bb'}$

$-$ $aa' = bb'xy$ donc $xy = \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$.

Notons que $a = 1.a \Rightarrow \frac{a}{a} = 1$ et $\frac{a}{1} = a$.

Pour $a \neq 0$, $0 = a.0 \Rightarrow \frac{0}{a} = 0$. Par contre $\frac{a}{0}$ est impossible car $0 \times q = 0 \neq a$.

Théorème

1°) $\mathbb{Z}^+$ et $\mathbb{N}$ sont isomorphe.

2°) $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$.

Preuve

1°) A tout entier positif ou nul $\overline{(m,0)} \in \mathbb{Z}^+$, faisons correspondre l'entier $m \in \mathbb{N}$. Cette correspondance est bijective car tout élément de chacun des ensembles $\mathbb{Z}^+$ et $\mathbb{N}$ est ainsi associé à un élément unique de l'autre. C'est pourquoi, on identifie ces deux ensembles, et on écrit $\mathbb{N} = \mathbb{Z}^+$ et on a $\mathbb{N} \subset \mathbb{Z}$.

2°) Soient n un entier relatif et $\overline{(a,b)}$ un représentant de n.

− si $a > b$, alors $n = a - b \in \mathbb{N}^*$

− si $a < b$, alors $n = -(b-a) \in -\mathbb{N}^*$

− si $a = b$, alors $n = 0$.

Maintenant que nous avons vu la division, nous pouvons donner un exemple de descente infinie :

Exemple

□ On se donne une propriété P qu'on doit prouver qu'elle n'est vérifiée par aucun entier. Le principe de descendente infinie de Fermat consiste à supposer qu'il existe un entier vérifiant P, et à montrer ensuite qu'il existe un entier strictement plus petit vérifiant P. On extrait de là une suite infinie strictement décroissante d'entiers vérifiant P, or cela n'est pas possible dans $\mathbb{N}$, donc absurde.

Par exemple si on avait $x^2 + y^2 = z^2$ et $\frac{1}{2}xy$ carré, on construit un autre triangle $a^2 + b^2 = c^2$ et $\frac{1}{2}ab$ carré, avec $c < z$.
De là, on en déduit que l'aire d'un triangle rectangle à coefficients entiers ne peut être un carré.

□ Cette propriété permet de montrer l'impossibilité de solutions entières non nulles à l'équation

$$x^4 + y^4 = z^4.$$

Il suffit de poser $a = y^4$, $b = 2x^2z^2$, $c = z^4 + x^4$ et $d = y^2xz$. On a alors :

$$a^2 + b^2 = y^8 + 4x^4z^4 = (z^4 - x^4)^2 + 4x^4z^4 = (z^4 + x^4)^2 = c^2$$
$$\frac{1}{2}ab = x^2y^4z^2 = d^2$$

ce qui donne un triangle rectangle à coefficients entiers d'aire un carré.

□ On peut démonstrer directement qu'il n'existe pas de triplets d'entiers strictement positifs tels que :

$$a^4 + b^4 = c^2.$$

Supposons a et b premiers entre eux, par exemple avec a impair et b pair. Dans ce cas, (a^2, b^2, c) forme alors un triplets pythagoricien, et on a :

$$a^2 = p^2 - q^2$$
$$b^2 = 2pq$$
$$c = p^2 + q^2$$

p ou q étant impair, l'autre étant pair. On ne peut avoir p est pair et q impair, car alors

$$p^2 = a^2 + q^2$$

avec $p^2 \equiv 0 \bmod 4$ alors que $a^2 + q^2 \equiv 2 \bmod 4$. Donc p est impair, et q pair. p et $2q$ sont alors deux entiers premiers entre eux dont le produit est un carré. Ils sont donc eux-mêmes des carrés, $2q$ étant par ailleurs le carré d'un nombre pair. Donc $p = u^2$, $2q = (2v)^2$. On a ainsi :

$$p^2 = u^4 = a^2 + (2v^2)^2$$

d'où à nouveau :

$$a = w^2 - z^2$$
$$2v^2 = 2wz$$
$$u^2 = w^2 + z^2$$

w et z sont premiers entre eux et leur produit est un carré. Ils sont donc eux-même des carrés, à savoir $w = r^2$ et $z = s^2$. On obtient alors :

$$u^2 = r^4 + s^4.$$

On vérifie que $u < c$.

C) Relation d'inégalité dans $\mathbb{Z}$

Définition

☐ Un élément non nul a d'un anneau $(A, +, \times)$ est dit diviseur de zéro s'il existe $b \in A$ tel que

$$ab = 0 \text{ ou } ba = 0.$$

Un anneau sans diviseur de zéro est dit intègre.

☐ Un anneau A ordonné est un anneau commutatif muni d'une relation d'ordre compatible avec l'addition telle que :

i) l'élément unité est positif

ii) $\forall (x, y, z) \in A^2 \times A^+$, $x \leq y \Rightarrow xz \leq yz$.

☐ On dit qu'un anneau ordonné A est archimédien si, pour tout élément $(a, b) \in A^+ \times A^{+*}$, il existe $n \in \mathbb{N}$ tel que $a \leq nb$. $\mathbb{Z}$ est archimédien car $\mathbb{N}$ est archimédien.

☐ Etant donné deux entiers relatifs distincts a et b, on dit que a est supérieur à b ou que b est inférieur à a si la différence $a - b$ est positive. On note :

$$a - b = (n, 0) \Leftrightarrow a > b \text{ ou } b < a \text{ au sens strict.}$$

En particulier, la relation

$$a - 0 = \alpha$$

montre que tout entier positif est supérieur à 0 et tout entier négatif est inférieur à 0.

☐ Soit a et b deux éléments de $\mathbb{Z}$. On définit de même les inégalités au sens large :

$$a \geq b \Leftrightarrow a - b \geq 0 \Leftrightarrow a - b \in \mathbb{Z}^+ \text{ ou } b - a \in \mathbb{Z}^-.$$

☐ La valeur absolue est l'application $\mathbb{Z} \to \mathbb{N}$, $a \mapsto |a| = \sup\{a, -a\}$.

☐ Nous allons voir que tout couple d'entiers (n, a), on peut écrire de façon unique :

$$n = \ d_0 + d_1 a + d_2 a^2 + ... + d_k \ a^k, \text{ avec } 0 \leq d_i \ < a.$$

Le nombre entier a défini s'appelle base.

On a l'habitude de noter les nombres à l'aide la base 10. En fait, le nombre 10 est arbitraire, et l'on aurait pu choisir n'importe quel entier a supérieur ou égal à 2. Les bases les plus courantes sont :

− la base 10 (nombres décimaux).

− la base 2, avec les chiffres 0 et 1 (nombres binaires).

− la base 16, avec les chiffres 0, 1, ..., 9, A, B, C, D, E, F (nombres hexadécimaux).

Propriété

i) La relation d'inégalité ($\geq$ ou $\leq$) est une relation d'ordre total au sens large dans l'ensemble $\mathbb{Z}$ des entiers relatifs.

ii) De ce qui précède, il est immédiat que $\mathbb{Z}$ est un anneau totalement ordonné.

iii) Tout entier positif est supérieur à tout entier négatif.

iv) Deux entiers négatifs sont dans l'ordre inverse de leurs valeurs absolues.

v) Les inégalités $a > b$ et $a + n > b + n$ sont équivalentes. On peut transposer un terme d'un membre dans l'autre et changer son signe.

vi) On peut ajouter membre à membre des inégalités de même sens.

vii) L'inégalité $a > b$ est équivalente à $na > nb$ si n est positif, à $na < nb$ si n est négatif.

viii) On peut multiplier membre à membre des inégalités de même sens dont les deux membres sont positifs.

Preuve

i) **R**éflexive : $a \geq a$ puisque $a = a$.

Antisymétrique : $a \geq b$ et $b \geq a \Rightarrow a - b \in \mathbb{Z}^+$ ou $b - a \in \mathbb{Z}^-$, donc soit $a - b = 0$ et $a = b$.

La **T**ransitivité est évident.

iii) On a

$$\overline{(a,0)} - \overline{(0,b)} = \overline{(a,0)} + \overline{(b,0)} = \overline{(a+b,0)}.$$

iv) Il est clair que

$$\overline{(0,a)} - \overline{(0,b)} = \overline{(0,a)} + \overline{(b,0)} = \overline{(b,a)}$$

est positif ou négatif suivant que a est inférieur ou supérieur à b.

v) Les différences

$$a - b \text{ et } (a+n) - (b+n)$$

sont égales, donc de même signe.

Par ailleurs,

$$a + b > n \Leftrightarrow a + b + (-b) > n + (-b) \Leftrightarrow a > n - b.$$

On peut donc transposer un terme d'un membre dans l'autre et changer son signe.

vi) Soit $a \geq b$ et $c \geq d$. Alors on a :

$$a - b \geq 0 \text{ et } c - d \geq 0,$$

donc

$$(a - b) + (c - d) \geq 0,$$

soit

$$(a + c) - (b + d) \geq 0 \text{ et } a + c \geq b + d.$$

vii) Si $n > 0$, alors

$$a - b > 0 \Leftrightarrow n(a - b) > 0 \Leftrightarrow na - nb > 0,$$

donc

$$a > b \Leftrightarrow na > nb.$$

Si $n < 0$, alors

$$a - b > 0 \Leftrightarrow n(a - b) < 0 \Leftrightarrow na - nb < 0,$$

donc

$$a > b \Leftrightarrow na < nb.$$

viii) En particulier, si a et b sont des entiers positifs non nuls,

$$a < b \Leftrightarrow a^n < b^n.$$

Supposons $0 < a < b$ et $0 < c < d$, alors

$$0 < ac < bc \text{ et } 0 < bc < bd,$$

donc

$$0 < ac < bd.$$

Théorème

1°) Soient a un entier rationnel et b un entier naturel non nul. Il existe alors un couple (q, r) d'entiers rationnels et un seul tel que

$$a = bq + r \text{ avec } 0 \leq r < b.$$

Les entiers rationnels q et r s'appellent encore quotient et reste de la division euclidienne de a par b.

2°) Un sous-ensemble H de $\mathbb{Z}$ est un sous-groupe additif de $(\mathbb{Z}, +)$ si et seulement s'il existe un entier positif n tel que $H = nZ$.

En particulier, le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même.

Preuve

1°)

− Montrons l'unicité du couple (q, r). Soit (q', r') un couple satisfaisant aux mêmes conditions

$$a = bq' + r' \text{ où } r' < b.$$

Supposons par exemple $q' \geq q$. Alors $r' \leq r$ et on a

$$b(q' - q) = r - r'.$$

Si $q' > q$, le premier membre est supérieur à b, tandis que le second membre est strictement inférieur à b. Il est donc contradictoire de supposer que $q' > q$. Finalement, $q' = q$ et par suite $r' = r$.

− Montrons l'existence. Supposons que a soit positif. Considérons la partie $P = \{q \in \mathbb{N} \ / \ bq \leq a\}$ de $\mathbb{N}$ constitué des éléments q tels que

$$bq \leq a.$$

Il est clair que P est non vide, car 0 appartient à P. En outre, P est majorée par a. Par suite, P admet un plus grand élément q_0. Par définition même du plus grand élément, on a

$$a \geq bq_0 \text{ et } a < b(q_0 + 1).$$

Autrement dit, l'entier naturel $r_0 = a - bq_0$ est strictement inférieur à b. Le couple (q_0, r_0) ainsi construit convient donc.

Lorsque a est négatif, alors $(-a)$ est positif, il existe donc un couple (q', r') d'entiers naturels tel que

$$-a = bq' + r' \text{ avec } 0 \leq r' < b.$$

2°)

− Soit n un élément de $\mathbb{N}$. Montrons que $n\mathbb{Z}$ est un sous groupe de $(\mathbb{Z}, +)$. Si $n = 0$ ou $n = 1$, c'est évident. Supposons que $n \geq 2$. Alors $n\mathbb{Z}$ est non vide car $0 \in n\mathbb{Z}$.

Soit $(p, p') \in (n\mathbb{Z})^2$ il existe $(k, k') \in \mathbb{Z}^2$ tels que $p = kn$ et $p' = k'n$. Ainsi

$$p + p' = (k + k')n \Rightarrow p + p' \in nZ.$$

D'autre part, la loi induite est associative ; 0 est l'élément neutre ; tout élément de $n\mathbb{Z}$ admet un symétrique.

– Réciproquement, soit H un sous-groupe additif de $(\mathbb{Z}, +)$. Montrons qu'il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Si $H = \{0\}$, alors $n = 0$ convient et $H = 0\mathbb{Z}$.

Si $H \neq \{0\}$, alors H contient un élément strictement positif de H car tout élément de H a son opposé dans H. Soit n le plus petit élément strictement positif de H. Pour tout $p \in n\mathbb{Z}$, il existe $k \in \mathbb{Z}$ tel que $p = nk$. Comme p peut s'écrire comme la somme $p = n + \ldots + n$ (k fois), p appartient à H car n est un élément du sous-groupe H. Par conséquent

$$n\mathbb{Z} \subset H.$$

Soit $m \in H$. Il existe q et r tels que $m = nq + r$ avec $0 \leq r < n$. Comme $m \in H$ et $nq \in H$, on a

$$r = m - nq \in H$$

car H est un sous-groupe. Comme n est le plus petit élément strictement positif de H, on a $r = 0$ et $m = nq$, donc $H \subset n\mathbb{Z}$. Finalement, $H = n\mathbb{Z}$.

– Un sous-anneau A de $(\mathbb{Z}, +, \times)$ doit contenir 1, de là on en déduit que A est un sous-groupe de $(\mathbb{Z}, +)$ contenant 1. Mais les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z}$. Pour que $1 \in n\mathbb{Z}$, il suffit que $n = 1$. Donc $A = \mathbb{Z}$.

Propriété

1°) Pour tout $(a, b) \in \mathbb{Z}^2$, on a :

$$|a + b| \leq |a| + |b|$$
$$||a| - |b|| \leq |a - b|$$

et $|ab| = |a||b|$.

2°) $(\mathbb{Z}, +, \times)$ est un anneau intègre.

Les seuls éléments inversibles de $\mathbb{Z}$ sont 1 et -1. Autrement dit, le groupe multiplicatif de $\mathbb{Z}$ est $\{-1, 1\}$.

La division n'est pas une loi de composition interne dans $\mathbb{Z}$.

Preuve

1°) L'inégalité triangulaire est vérifié en effectuant une distinction de quatre cas :

– si a et b sont positifs, alors $|a + b| = a + b$ et $|a| = a$, $|b| = b$, et on a bien $|a + b| = |a| + |b|$.

– de même si a et b sont négatifs, on a aussi $|a + b| = |a| + |b|$.

– si a est strictement positif et b strictement négatif, alors

$$|a + b| = \sup\{a + b, -a - p\}.$$

Mais $\sup\{a + b, -a - p\} < \sup\{a, -p\} = \sup\{|a|, |b|\} < |a| + |b|$.

– le cas où a est strictement négatif et b strictement positif se traite de la même manière que le précédent.

De l'inégalité triangulaire, nous pouvons écrire :

$$|a| = |b + (a - b)| \leq |b| + |a - b| \text{ et } |b| = |a + (b - a)| \leq |a| + |b - a|.$$

Comme $|b - a| = |a - b|$, on obtient bien :

$$||a| - |b|| \leq |a - b|.$$

L'égalité

$$|ab| = |a||b|.$$

découle de la règle des signes.

2°)

– Soit a et b deux entiers relatifs tels que $ab = 0$. Alors

$$|n||p| = |np| = 0.$$

Puisque $|a|$ et $|b|$ sont des entiers naturels, nous en déduisons que l'un au moins de ces entiers naturels est nul. Finalement, l'un au moins de ces entiers relatifs a et b est nul, ce qui montre qu'il n'y a pas de diviseur de 0 dans $\mathbb{Z}$.

– Par ailleurs, si $ab = 1$, alors $|a||b| = 1$. Puisque $|a|$ et $|b|$ sont des entiers naturels, il en découle que

$$|a| = |b| = 1,$$

c'est-à-dire que a et b appartient à $\{-1, 1\}$.

– La division n'est pas une loi de composition interne définie dans $\mathbb{Z}$ pour tout couple d'entier a et b. Pour cela, montrons que la division n'est pas toujours possible. Soit r tel que $0 < r < b$. Quelque soit q, on obtient

$$bq < bq + r < b(q + 1).$$

Or si l'entier $a = bq + r$ était divisible par b, on aurait $a = bq + r = bx$. Ce qui donnerait

$$bq < bx < b(q + 1)$$

soit

$$q < x < q + 1,$$

relation impossible en entier.

Propriété

L'ensemble $\mathbb{Z}$ des entiers rationnels est dénombrable, c'est-à-dire qu'il existe une bijection entre $\mathbb{Z}$ et $\mathbb{N}$.

Preuve

Définissons deux applications $f : \mathbb{N} \to \mathbb{Z}$ et $g : \mathbb{Z} \to \mathbb{N}$ par les formules respectives suivantes :

$$\text{pour tout } n \in \mathbb{N},\ f(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ est pair} \\ \frac{n+1}{2} & \text{si } n \text{ est impair} \end{cases}$$

et

$$\text{pour tout } m \in \mathbb{Z},\ g(m) = \begin{cases} -2m & \text{si } m \leq 0 \\ 2m - 1 & \text{si } r > 1 \end{cases}.$$

Il convient tout d'abord de vérifier que f et g sont "bien des applications" au sens suivant : il n'est pas tout à fait clair que les formules qui les définissent fournissent un résultat situé dans l'ensemble d'arrivée demandé.

– Vérifions que f définit bien une application : si n est pair, $\dfrac{n}{2}$ (qui est a priori seulement une fraction) est bien lui-même un entier ; si n est impair, $n + 1$ est pair et donc $\frac{n+1}{2}$ est lui aussi entier. La formule proposée pour $f(n)$ définit donc bien un élément de $\mathbb{Z}$.

– Vérifions que g définit bien une application : si m est négatif, $-2m$ est positif, donc bien dans $\mathbb{N}$; si m est strictement positif, ($2m$ vaut au moins 2 et donc$2m - 1$ est aussi dans $\mathbb{N}$ (et est même strictement positif).

Vérifions maintenant que $g \circ f$ est bien l'application identique. Prenons un n dans $\mathbb{N}$.

– Si n est pair, $f(n) = -\dfrac{n}{2}$ est négatif : on calcule donc $g[f(n)] = g[\dfrac{n}{2}]$ par la première formule pour g et on trouve :

$$g[f(n)] = -2(-\frac{n}{2}) = n.$$

– Si n est impair, $f(n) = \frac{n+1}{2}$ est strictement positif : on calcule donc $g[f(n)] = g[\frac{n+1}{2}]$ par la deuxième formule pour g et on trouve :

$$g[f(n)] = 2(\frac{n+1}{2}) - 1 = n.$$

La conjonction des deux cas prouve bien que $g \circ f = Id_{\mathbb{N}}$.

– si m est négatif, $g(m) = -2m$ est pair : on calcule donc $f[g(m)] = f[-2m]$ par la première formule pour f et on trouve :

$$f[g(r)] = -[-2m/2] = m.$$

– si m est strictement positif, $g(m) = 2m - 1$ est impair : on calcule donc $f[g(m)] = f[2m-1]$ par la première formule pour f et on trouve :

$$f[g(m)] = \frac{(2m-1)+1}{2} = m.$$

Il est clair que l'application $g : \mathbb{N} \to \mathbb{Z}$ ainsi définie est la fonction réciproque de f, donc f est bijectif et on a

$$\text{Card } \mathbb{N} = \text{Card } \mathbb{Z}.$$

Voyons maintenant une conséquence fondamentalde la division euclidienne :

Propriété

Tout entier n s'écrit de manière unique sous la forme :

$$n = \ d_0 + d_1 a + d_2 a^2 + ... + d_k \ a^k, \text{ avec } 0 \leq d_i \ < a.$$

Preuve

Existence

Montrons l'existence par récurrence. On a :

– $0 = 0$.

– si $n < a$ alors, on pose $n = d_0$.

Supposons la propriété vraie jusqu'à $n-1$. Montrons-là pour n. On effectue la division euclidienne de n par a. On a

$$n = aq + d_0 \text{ avec } d_0 < a.$$

Par ailleurs, $a \geq 2 \Rightarrow q < n$ donc on peut appliquer l'hypothèse de récurrence sur q en posant

$$q = d_1 + d_2 \ a^2 + ... + d_k \ a^{k-1}.$$

Unicité

Montrons d'abord l'unicité de la décomposition. Supposons qu'il existe deux décompositions distinctes de n dans la base a :

$$\begin{cases} n = d_0 + d_1 a + d_2 a^2 + \cdots + d_q a^q + \cdots \\ n = d'_0 + d'_1 a + d'_2 a^2 + \cdots + d'_q a^q + \cdots \end{cases}$$

Désignons par m_1 et par m_2 le plus grand et le plus petit des entiers naturels q tel que $d'_q \neq d_q$. Supposons par exemple $d'_{m_2} > d_{m_2}$, alors :

$$\left(d'_{m_2} - d_{m_2}\right) p^{m_2} = \sum_{q=m_2+1}^{m_1} \left(d_q - d'_q\right) p^q.$$

Simplifions les deux membres par p^{m_2} :

$$\left(d'_{m_2} - d_{m_2}\right) = \sum_{q=m_2+1}^{m_1} \left(d_q - d'_q\right) p^{q-m_2}.$$

Nous arrivons à une contradiction, car le second membre est divisible par p, tandis que le second ne l'est pas puisque

$$0 < d'_{m_2} - d_{m_2} < p.$$

Exemple

Pour déterminer le développement d'un entier dans une base a donnée, il suffit d'appliquer successivement des divisions par a, d_0 étant le premier reste. Les algorithmes de calculs dans une base a sont identiques aux algorithmes décimaux, mais les retenues se font à partir de a et non de 10. En prenant une valeur élevée de a, on obtient ainsi des algorithmes de calculs de grands entiers.

☐ Convertir en base 16 l'entier décimal 1457 :

$$\begin{aligned} 1457 &= 16 \times 91 + 1 \\ &= 16 \times (16 \times 5 + 11) + 1 \\ &= 5B1_h. \end{aligned}$$

☐ Convertir en base 2 l'entier donné en base 7 par 2456 :

$$\begin{aligned} 2455_7 &= 1226.2 \\ &= (446.2 + 1).2 \\ &= 223.2^3 + 2 \\ &= (111.2 + 1).2^3 + 2 \\ &= (40.2 + 1).2^4 + 2^3 + 2 \\ &= 20.2^6 + 2^4 + 2^3 + 2 \\ &= 10.2^7 + 2^4 + 2^3 + 2 \\ &= (3.2 + 1).2^7 + 2^4 + 2^3 + 2 \\ &= (2 + 1).2^8 + 2^7 + 2^4 + 2^3 + 2 \\ &= 2^9 + 2^8 + 2^7 + 2^4 + 2^3 + 2 \\ &= 1110011010_b. \end{aligned}$$

☐ Convertir en base 2 ou 16 l'entier décimal 125624 :

$$\begin{aligned} 125624_d &= 2^2.31406 = 2^3.15703 \\ &= 2^3 + 2^3.15702 = 2^3 + 2^4.7851 \\ &= 2^3 + 2^4 + 2^4.7850 = 2^3 + 2^4 + 2^5.3925 \\ &= 2^3 + 2^4 + 2^5 + 2^5.3924 = 2^3 + 2^4 + 2^5 + 2^7.981 \\ &= 2^3 + 2^4 + 2^5 + 2^7 + 2^7.980 = 2^3 + 2^4 + 2^5 + 2^7 + 2^9.245 \\ &= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^9.244 \\ &= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11}.61 \\ &= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{11}.60 \\ &= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{13}.15 \\ &= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{13} + 2^{13}.14 \\ &= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{13} + 2^{14}.7 \\ &= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{13} + 2^{14} + 2^{14}.6 \\ &= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{13} + 2^{14} + 2^{15}.3 \\ &= 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{11} + 2^{13} + 2^{14} + 2^{15} + 2^{16} \\ &= 11110101010111000_b \\ &= 1EAB8_h. \end{aligned}$$

Voici maintenant un exemple d'opération :

$$\begin{array}{r} 14\mathrm{ED}_h \\ +\ 27\mathrm{F}_h \\ \hline = 176\mathrm{C}_h \end{array}$$

Avec un peu d'entraînement, on peut aussi effectuer des multiplications et des divisions.

III) Construction de $\mathbb{Q}$

On utilise pour la construction des outils d'arithmétique qui ne seront étudiés que dans le prochain chapitre.

Les seuls éléments inversibles de l'anneau $\mathbb{Z}$ sont 1 et -1. Nous allons construire un corps commutatif qui contient un sous-anneau isomorphe à $\mathbb{Z}$. Pour cela nous allons symétriser, pour la multiplication, l'anneau $\mathbb{Z}$ des entiers relatifs, c'est-à-dire construire, à partir de $\mathbb{Z}$, un nouvel ensemble $\mathbb{Q}$ où tout élément aura un inverse et dans lequel nous pourrons inclure $\mathbb{Z}$. On y parvient en étendant aux différents couples d'entiers relatifs (a, b) tels que $b \neq 0$ les propriétés des rapports entiers. Les deux relations suivantes :

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + ba'}{bb'}$$

$$\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}.$$

nous amènent à munir $\mathbb{Z} \times \mathbb{Z}^*$ de lois suivantes :

$$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^*,\ \forall (a',b') \in \mathbb{Z} \times \mathbb{Z}^*,\ (a,b) + (a',b') = (ab' + a'b, bb')$$
$$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^*,\ \forall (a',b') \in \mathbb{Z} \times \mathbb{Z}^*,\ (a,b) \times (a',b') = (aa', bb').$$

A) Structures algébriques de $\mathbb{Z}^2/\Re$

Donnons tout d'abord la définition de corps.

Définition

☐ Un corps est un anneau dans lequel tout élément non nul est inversible et $1 \neq 0$.

☐ On dit qu'une partie d'un sous-corps si elle est stable pour les deux lois de compositions et si, muni des lois induites par celles du corps, elle est encore un corps.

☐ On appelle morphisme de corps tout morphisme des anneaux sous-jacents.

Propriété

1°) Définissons l'addition et la multiplication sur $\mathbb{Z} \times \mathbb{Z}^*$:

$$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^*,\ \forall (a',b') \in \mathbb{Z} \times \mathbb{Z}^*,\ (a,b) + (a',b') = (ab' + a'b, bb')$$
$$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^*,\ \forall (a',b') \in \mathbb{Z} \times \mathbb{Z}^*,\ (a,b) \times (a',b') = (aa', bb')$$

Ces deux opérations sont des lois de composition interne, commutatives et associatives.

2°) Dans l'ensemble $\mathbb{Z} \times \mathbb{Z}^*$, la relation $\Re$ définie par :

$$(a,b)\Re(a',b') \Leftrightarrow ab' = ba'$$

est une relation d'équivalence compatible avec l'addition et la multiplication sur $\mathbb{Z} \times \mathbb{Z}^*$.

3°) Le quotient $\mathbb{Z}^2/\Re$ muni des opérations quotients

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad + bc, b + d)} \text{ et } \overline{(a,b)(c,d)} = \overline{(ac, bd)}$$

est un corps commutatif.

4°) Considérons l'application $\varphi : \mathbb{Z} \to \mathbb{Z}^2/\Re$ définie par $\varphi : a \mapsto \overline{(a,1)}$. Cette application est injective.

Preuve

1°) Ce sont bien des lois de composition interne car $(\mathbb{Z}, +, \times)$ est un anneau intègre, donc pour $(b, b') \in \mathbb{Z} \times \mathbb{Z}^*$, on a $bb' \in \mathbb{Z}^*$ et bien sûr $ab' + a'b \in \mathbb{Z}$ et $aa' \in \mathbb{Z}$.

Il est facile de vérifier que l'addition est commutative, associative, d'élément neutre (0, 1) et que le produit est commutatif, associatif, d'élément neutre (1, 1).

2°) **R**éflexive car

$$ab = ba \Rightarrow (a, b)\Re(a, b)$$

Symétrique car

$$ab' = ba' \Rightarrow a'b = b'a.$$

Donc

$$(a, b)\Re(a', b') \Rightarrow (a', b')\Re(a, b).$$

Transitive car

$$ab' = ba' et a'b'' = b'a'' \Rightarrow ab'a'b'' = ba'b'a''$$

c'est-à-dire, tout au moins si $a' \neq 0$:

$$ab'' = ba''.$$

Donc

$$(a, b)\Re(a', b') \text{ et } (a', b')\Re(a'', b'') \Rightarrow (a, b)\Re(a'', b'').$$

Pour $a' = 0$, la propriété reste vraie car on a alors

$$a = a' = a'' = 0.$$

Montrons que la relation d'équivalence $\Re$ est compatible avec les deux lois internes de $\mathbb{Z} \times \mathbb{Z}^*$. Pour l'addition, calculons :

$$(a, b)\Re(a', b') \text{ s'écrit } ab' = ba' \ (1)$$
$$(c, d)\Re(c', d') \text{ s'écrit } cd' = dc' \ (2)$$

Multiplions la première relation par dd' et la deuxième relation par bb' :

$$adb'd' = bda'd' \text{ et } bcb'd' = bdb'c'$$

En ajoutons les relations, on a :

$$(ad + bc)b'd' = (a'd' + b'c')bd$$

c'est-à-dire

$$(ad + bc, bd)\Re(a'd' + b'c', b'd').$$

Pour la multiplication, il suffit de faire un produit de (1) et de (2) :

$$acb'd' = bda'c'.$$

De là, on voit que la multiplication et $\Re$ sont compatibles.

3°) Les propriétés de l'addition et de la multiplication sur $\mathbb{Z} \times \mathbb{Z}^*$ se transmettent au quotient. L'addition sur $(\mathbb{Z} \times \mathbb{Z}^*)/\Re$ est donc commutative, associative, d'élément neutre $\overline{(0, 1)}$ la classe de $(0, 1)$. Tout élément $\overline{(p, q)}$ de $(\mathbb{Z} \times \mathbb{Z}^*)/\Re$ admet $\overline{(-p, q)}$ pour opposé. Ainsi, l'addition fait de $(\mathbb{Z} \times \mathbb{Z}^*)/\Re$ un groupe commutatif.

Dans $(\mathbb{Z} \times \mathbb{Z}^*)/\Re$, le produit distribue l'addition car les quantités

$$[\overline{(p, q)} + \overline{(p', q')}]\overline{(p'', q'')} \text{ et } \overline{(p, q)(p'', q'')} + \overline{(p', q')(p'', q'')}$$

sont égaux. L'élément neutre pour le produit est $\overline{(1, 1)}$. Ainsi $(\mathbb{Z}\times\mathbb{Z}^*)/\Re$ est un anneau commutatif. Montrons qu'elle est intègre :

$$\text{si } \overline{(p, q)(p', q')} = \overline{(pp', qq')} = \overline{(0, 1)}, \text{ alors } pp' = 0$$

ce qui implique ou $p = 0$ ou $p' = 0$ car $\mathbb{Z}$ est intègre.
Par ailleurs, tout élément $\overline{(p,q)} \in (\mathbb{Z} \times \mathbb{Z}^*)/\Re$ admet $\overline{(q,p)}$ pour inverse car :

$$\overline{(p,q)(q,p)} = \overline{(pq,pq)} = \overline{(1,1)}.$$

Ainsi $((\mathbb{Z} \times \mathbb{Z}^*)/\Re, +, \times)$ est un corps commutatif.

4°) On a :

$$\varphi(a) = 0 \Leftrightarrow (a,1)\Re(0,1) \Leftrightarrow a = 0.$$

On vérifie facilement que φ est un morphisme d'anneau, donc φ est injective. Par conséquent $\mathbb{Z} \subset (\mathbb{Z} \times \mathbb{Z}^*)/\Re$.

B) Le corps $\mathbb{Q}$ et propriétés premières

Définition

□ L'ensemble quotient $(\mathbb{Z} \times \mathbb{Z}^*)/\Re$ s'appelle ensemble des nombres rationnels et se note $\mathbb{Q}$ (pour quotient). Les éléments de $\mathbb{Q}$ s'appellent des nombres rationnels (du latin ration, signifiant rapport).

□ Nous allons voir que tout élément $r \in \mathbb{Q}$ peut s'écrire sous forme fractionnaire $\frac{a}{b}$. L'élément a est appelé le numérateur et b le dénominateur.

Une notation proche de celle utilisée quand on écrit 22/7 a été utilisée par les mathématiciens indiens et ce sont les arabes qui ont introduit la barre horizontale comme $\frac{22}{7}$.

Théorème

1°) Soit $\mathbb{K}$ un corps. Si f est un homomorphisme injectif de $\mathbb{Z}$ dans $\mathbb{K}$, alors il existe un homomorphisme g de $\mathbb{Q}$ dans $\mathbb{K}$ tel que

$$f = g \circ \varphi \text{ avec } \varphi : \mathbb{Z} \to \mathbb{Q},\ a \mapsto \overline{(a,1)}.$$

2°) Le seul sous-corps de $\mathbb{Q}$ contenant $\mathbb{Z}$ est $\mathbb{Q}$ lui-même. On dit que $\mathbb{Q}$ est un corps premier.

3°) Tout élément de $r \in \mathbb{Q}$ se présente comme le produit d'un élément $p \in \mathbb{Z}$ par l'inverse d'un élément non nul q de $\mathbb{Z}$.

4°) Tout rationnel non nul s'écrit sous forme $\frac{p}{q}$ unique avec $q > 0$ et p et q premiers entre eux.

Preuve

1°) Soit f un homomorphisme de $\mathbb{Z}$ dans $\mathbb{K}$. Soit (a,b) et (c,d) deux éléments de $\mathbb{Z} \times \mathbb{Z}^*$. Il est clair que :

$$(a,b)\Re(c,d) \text{ s'écrit } ad = bc.$$

L'application f étant injective, on a alors $f(b) \neq 0$ et $f(d) \neq 0$. En appliquant f à l'égalité ci-haut, il vient :

$$f(af(d) = f(b)f(c) \Rightarrow f(a)f(b)^{-1} = f(c)f(d)^{-1}.$$

Il en résulte que $f(a)f(b)^{-1}$ ne dépend que de la classe (a,b) modulo $\Re$. On peut ainsi définir une application g de $\mathbb{Q}$ dans $\mathbb{K}$ par :

$$g : \overline{(a,b)} \mapsto f(a)f(b)^{-1}.$$

On vérifie facilement que g est un homomorphisme d'anneaux. Montrons maintenant que g est injective. Si $g(\overline{(a,b)}) = 0$, alors

$$f(a)f(b)^{-1} = 0 \Rightarrow f(a) = 0 \Rightarrow a = 0$$

car $\mathbb{K}$ est un corps. Ainsi $\ker g = \{\overline{(0,b)}\}$. Comme $\overline{(0,b)}$ est l'élément neutre de l'addition de $\mathbb{Q}$, l'homomorphisme g est injectif.

Par ailleurs, pour tout $a \in \mathbb{Z}$, on a :

$$g(\varphi(a)) = g(\overline{(a,1)}) = f(a)f(1)^{-1} = f(a).$$

et donc $f = g \circ \varphi$.

2°) Soit $\mathbb{K}$ un sous-corps de $\mathbb{Q}$ contenant $\mathbb{Z}$. L'application $f : x \mapsto x$ de $\mathbb{Z}$ dans $\mathbb{K}$ est un homomorphisme injectif. Comme $\mathbb{K}$ est un corps, il existe un homomorphisme g de $\mathbb{Q}$ dans $\mathbb{K}$ par application de 1°). Donc $g(\mathbb{Q}) \subset \mathbb{K}$. Mais $\mathbb{K}$ est un sous-corps de $\mathbb{Q}$, donc $g(\mathbb{Q}) \subset \mathbb{Q}$. L'application g étant un homomorphisme injectif de $\mathbb{Q}$ dans $\mathbb{Q}$, on a bien $g(\mathbb{Q}) = \mathbb{Q}$ et donc $g(\mathbb{Q}) \subset K$. Finalement, $\mathbb{Q} = \mathbb{K}$ par identification.

3°) Grâce au morphisme injectif $\varphi : p \mapsto \overline{(p,1)}$ de $\mathbb{Z}$ dans $\mathbb{Q}$, on peut considérer $\mathbb{Z}$ comme un sous-anneau de $\mathbb{Q}$. Ceci nous permet d'écrire $\overline{(p,1)}$ sous la forme p. Puisque $\mathbb{Q}$ est un corps, tout élément non nul q de $\mathbb{Z}$ est inversible dans $\mathbb{Z}$ et son inverse est $\overline{(1,q)}$. Le produit pq^{-1}, c'est-à-dire $\overline{(p,1)(1,q)}$, se note encore $\frac{p}{q}$. Avec les notations ci-haut, on peut écrire$\overline{(1,q)}$ sous la forme $\dfrac{1}{q}$.

Posons maintenant $E = \{\dfrac{p}{q} \ / \ (p,q) \in \mathbb{Z} \times \mathbb{Z}^*\}$. E n'est pas vide puisque $1 \in E$. Par ailleurs, E contient $\mathbb{Z}$ car E contient les éléments $\dfrac{p}{1} = p$. On montre facilement que E est un sous-corps de $\mathbb{Q}$ contenant $\mathbb{Z}$. Donc $E = \mathbb{Q}$.

4°) Nous venons de voir que tout nombre rationnel r s'écrit sous la forme d'une fraction $\dfrac{p}{q}$. Une telle écriture peut se faire d'une infinité de manières. Mais lorsque p et q sont premiers cette écriture est unique.

Montrons d'abord l'unicité d'une telle écriture. Supposons que

$$r = \frac{p_1}{q_1} = \frac{p_2}{q_2} \text{ avec } p_1,\, p_2 \in \mathbb{Z} \text{ et } q_1,\, q_2 \in \mathbb{N}^*.$$

$\Rightarrow p_1 q_2 = p_2 q_1$.

Puisque q_2 divise le premier membre, q_2 divise le second membre. D'après le théorème de Gauss, puisque q_2 est premier avec p_2, q_2 divise q_1, ce qui implique $q_2 \leq q_1$. De même, q_1 divise q_2 et donc $q_1 \leq q_2$. Finalement, $q_1 = q_2$. L'anneau $\mathbb{Z}$ étant intègre, il vient $p_1 = p_2$. D'où l'unicité de l'écriture.

Montrons maintenant l'existence. Nous savons que r peut s'écrire sous la forme $r = \dfrac{p'}{q'}$. Si $q' < 0$, alors

$$r = \frac{-p'}{-q'},$$

ce qui nous permet de se ramener au cas où $q' > 0$. Dans ces conditions, posons $d =$pgcd (p', q'). Alors

$$p' = dp \text{ et } q' = dq$$

où p et q sont premiers entre eux. Le couple (p,q) convient visiblement.

C) Relation d'ordre dans le corps $\mathbb{Q}$.

Définition

□ Soit $r = \dfrac{a}{b}$ un rationnel. On dit que r est positif si a et b sont de même signe et négatif si a et b sont de signe contraire. On note $\mathbb{Q}^+$ l'ensemble des rationnels positifs.

□ Soit $r = \frac{a}{b}$ et $r' = \frac{c}{d}$ deux rationnels. On dit que r' est supérieur à r si $\frac{bc-ad}{bd}$ est positif. On note :

$$\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow \frac{bc-ad}{bd} \in \mathbb{Q}^+.$$

Théorème

La relation $\leq$ est une relation d'ordre sur $\mathbb{Q}$ qui prolonge l'ordre usuelle de $\mathbb{Z}$ et qui fait de ce corps un corps ordonné.

Propriété en vrac

1°) Il n'y a pas dans le corps $\mathbb{Q}$ d'élément maximal supérieur à tous les autres.

Le corps $\mathbb{Q}$ des rationnels est un ensemble totalement ordonné, illimité dans les deux sens car tout rationnel r admet des rationnels supérieurs $r + \lambda$ et des rationnels inférieurs $r - \lambda$, ceci quelque soit le rationnel positif λ.

2°) Entre deux rationnels distincts r et r', on peut intercaler une infinité de rationnels. On dit que l'ensemble $\mathbb{Q}$ est partout dense.

Si $r < r'$, alors tout λ tel que

$$0 < \lambda < r' - a$$

donne

$$r < r + \lambda < r'.$$

En particulier entre $r - \varepsilon$ et $r + \varepsilon$ s'intercale tout rationnel $r \pm \frac{\varepsilon}{k}$ pour $k > 1$.

3°) Quel que soit le rationnel r, il existe un entier relatif unique n tel que $n \leq \alpha < n + 1$.

On peut toujours supposer que r est le quotient $\frac{a}{b}$ de deux entiers relatifs a et b tels que $|b| > 1$, ce qui entraîne $|r| < |a| \Rightarrow -|a| < r < |a|$. Il y a donc des entiers relatifs supérieurs à r, des entiers relatifs inférieurs ou égaux à r et n est l'élément maximal de ces derniers. L'ensemble $\mathbb{Q}$ **est dit archimédien**.

4°) $\mathbb{Q}$ a les propriétés différentes de $\mathbb{N}$ et $\mathbb{Z}$. Chaque élément de $\mathbb{Q}$ n'a ni successeur, ni prédécesseur.

Soit $y > x$. On a $\frac{x+y}{2} - x = \frac{y-x}{2} > 0$ et $y - \frac{x+y}{2} = \frac{y-x}{2} > 0$, donc $x < \frac{x+y}{2} < y$.

IV) Les nombres décimaux et les nombres réels

Nous savons que l'origine des nombres rationnels a été liée à des problèmes de mesure géométrique. On doit aux mathématiciens grecs Pythagore (VI-ème siècle avant J.C) et Euclide (III-ème siècle avant J.C) la découverte des quantités les nombres irrationnels et une première présentation axiomatique des nombres réels positifs considérés comme des longueurs.

Cette présentation fut suffisante jusqu'à la découverte au XIXème siècle de phénomènes "pathologiques" (fonctions continues dé rivables nulle part, ...) ou difficiles à préciser. On doit à Bolzano, Cauchy, Cantor, Dedekind et Weierstrass différentes constructions de R, qui levèrent ces difficultés. Parmi les nombres rationnels, les nombres de la forme

$$a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n} \ (a_i \text{ entiers})$$

sont d'une importance fondamentale et permettent une construction de $\mathbb{R}$. Ces nombres sont des nombres décimaux.

A) L'anneau des nombres décimaux

Définition

☐ On dit qu'un nombre rationnel d est décimal s'il existe un entier naturel m tel que le nombre $10^m d$ soit un entier relatif.

☐ Le plus petit entier m tel que $10^m d$ soit un entier relatif est appelé l'ordre du décimal d.

☐ On représente l'ensemble des nombres décimaux par la lettre $\mathbb{D}$.

Propriété

1°) Tout entier relatif est un nombre décimal. Tout nombre décimal est un nombre rationnel.

2°) Soit $r = \dfrac{p}{q}$ un nombre rationnel sous forme irréductible. Pour que r soit un nombre décimal, il faut et il suffit que le dénominateur q ne comporte aucun facteur premier autre que 2 et 5, autrement dit, il faut et il suffit que

$$q = 2^m 5^n.$$

Ainsi, il est parfois plus agréable de représenter l'écriture d'un nombre décimal sous la forme $\dfrac{p}{2^m 5^n}$ avec pgcd $(p, 2) =$ pgcd $(p, 5) = 1$.

Preuve

1°) Soit a un entier relatif, alors $10^0 a = a$ appartient à $\mathbb{Z}$. Donc tout entier relatif est un nombre décimal.

Soit d un nombre décimal, alors il existe un couple $(n, a) \in \mathbb{N} \times \mathbb{Z}$ tel que $10^n d = a$. On peut donc écrire

$$d = \frac{a}{10^n}$$

qui est un nombre rationnel.

2°) Supposons tout d'abord que r soit décimal. Si r appartient à $\mathbb{Z}$, alors r peut s'écrire sous forme

$$d = \frac{d}{2^0 5^0}.$$

Si d n'appartient pas à $\mathbb{Z}$, nous pouvons l'écrire

$$r = \frac{p}{q} = \frac{n}{10^m}$$

où n est un entier relatif et m un entier naturel. Par suite :

$$10^m p = nq.$$

Comme q divise le second membre, q divise le premier membre. D'après le lemme de Gauss, puisque q est premier avec p, q divise 10^m. Or

$$10^m = 2^m 5^m.$$

Il en découle que 2 et 5 sont les seuls facteurs premiers pouvant figurer dans la décomposition de q.

Réciproquement, si d est de la forme

$$\frac{p}{2^m 5^n},$$

prenons $a = \max\{m, n\}$, et il vientque $10^a d$ appartient à $\mathbb{Z}$.

Exemple

□ $\frac{5}{7}$ n'est pas un nombre décimal. En revanche, le nombre $\frac{11}{80}$ est un nombre décimal car $80 = 2^4 \times 5$.

Théorème

1°) L'ensemble $\mathbb{D}$ des nombres décimaux est un sous-anneaux intègre du corps de $\mathbb{Q}$.

2°) Un élément de $\mathbb{D}$ est inversible si et seulement si il est de la forme $\varepsilon 2^m 5^n$ avec $(m, n) \in \mathbb{Z}^2$ et $\varepsilon = \pm 1$. Ainsi $\mathbb{D}$ n'est pas un sous-corps de $\mathbb{Q}$.

Preuve

1°) Il est clair que l'ensemble $\mathbb{D}$ est non vide puisque tout élément de $\mathbb{Z}$ appartient à $\mathbb{D}$. Pour montrer que $\mathbb{D}$ est un sous-anneau de $\mathbb{Q}$, il suffit de montrer que, pour tout couples (d, d') de nombres décimaux, $d - d'$ et dd' sont encore des nombres décimaux.

− Par hypothèse, il existe deux entiers naturels n et n' tels que

$$10^n d \in \mathbb{Z} \text{ et } 10^{n'} d' \in \mathbb{Z}.$$

Il en résulte que

$$10^{n+n'} dd' \in \mathbb{Z},$$

ce qui prouve que dd' est décimal.

− D'autre part, on a

$$10^N (d - d') \in \mathbb{Z},$$

où l'on posé $N = \max\{n, n'\}$. Ainsi, $d - d'$ est décimal.

Ce qui montre que $\mathbb{D}$ est un sous-anneau de $\mathbb{Q}$. Il est unitaire car $1 \in \mathbb{D}$ et donc intègre. Par la même occasion, précisons que $\mathbb{Z}$ est un sous-anneau de $\mathbb{D}$ et que $\mathbb{D}$, étant une partie du corps totalement ordonné $\mathbb{Q}$, est un anneau totalement ordonné par l'ordre induit.

On peut aussi montrer que $\mathbb{D}$ est engendré par $\{\frac{1}{10}\}$ car si un sous-anneau de $\mathbb{Q}$ contient $\frac{1}{10}$, alors il contient tous les entiers car $1 = \frac{1}{10} + \ldots + \frac{1}{10}$ et il contient donc tous les rationnels de la forme $\frac{n}{10^m}$, avec $n \in \mathbb{Z}$ et $m \in \mathbb{Z}$. Il contient donc tous les nombres décimaux.

$\mathbb{D}$ n'est pas un idéal de $\mathbb{Q}$, car $\mathbb{Q}$ étant un corps, ses seuls idéaux sont $\{0\}$ et $\mathbb{Q}$.

2°) On sait que 3 est un nombre décimal, mais son inverse $\frac{1}{3}$ n'est pas un nombre décimal, ce qui prouve que $\mathbb{D}$ n'est pas un sous-corps $\mathbb{Q}$ du corps $\mathbb{Q}$ des nombres relatifs.

Par ailleurs, tout élément $\varepsilon 2^m 5^n$ appartient à $\mathbb{D}$ et, comme

$$\varepsilon 2^m 5^{n\varepsilon} 2^{-m} 5^{-n} = \varepsilon^2 = 1.$$

Ainsi, tous les nombres de ce type sont inversibles.

Réciproquement, considérons deux nombres décimaux

$$d_1 = \frac{p_1}{2^{m_1} 5^{n_1}} \text{ et } d_2 = \frac{p_2}{2^{m_2} 5^{n_2}}.$$

Si $d_1 d_2 = 1$, alors

$$p_1 p_2 = 2^{m_1+m_2} 5^{n_1+n_2} \Rightarrow 2^{m_1+m_2} 5^{n_1+n_2} \in \mathbb{N}.$$

Cela implique

$$m_1 + m_2 \geq 0 \text{ et } n_1 + n_2 \geq 0$$

car 2 ne divise pas 5 et 5 ne divise pas 2. Par le théorème de Gauss, on a

$$p_i = \pm 1.$$

Théorème

1°) L'anneau des nombres décimaux est un anneau principal euclidien, plus précisément

$$\forall (a,b) \in \mathbb{D} \times (\mathbb{D} - \{0\}),\ \exists (q,r) \in \mathbb{D}^2 \ /\ a = bq + r,\ \varphi(r) < \varphi(b).$$

L'application φ est définie par

$$\varphi : d = p2^m5^n \mapsto |p|.$$

2°) Pour tout idéal I de $\mathbb{D}$, distinct de $\{0\}$, il existe un unique entier n tel que $I = n\mathbb{D}$ avec

$$\text{pgcd } (n,2) = \text{pgcd } (n,5) = 1.$$

Preuve

1°) On sait que les anneaux euclidiens sont toujours des anneaux principaux. Montrons que $\mathbb{D}$ est euclidien, donc principal.

Si $a = 0$, alors $(q,r) = (0,0)$ convient.

Supposons $a \neq 0$ et considérons les écritures canoniques de a et b :

$$a = \frac{m}{2^k5^\ell} \text{ et } b = \frac{n}{2^k5^\ell}.$$

Par la division euclidienne dans $\mathbb{Z}$, il existe $(u,v) \in \mathbb{Z}^2$ tels que

$$m = nu + v \text{ avec } 0 \leq v < |n|.$$

On obtient

$$a = \frac{nu+v}{2^k5^\ell} = \frac{n}{2^s5^t}\frac{u}{2^{k-s}5^{\ell-t}} + \frac{v}{2^k5^\ell}.$$

Soit $v\prime = 2^x5^yv$ avec pgcd $(2,v') = $ pgcd $(5,v') = 1$. Posons

$$q = \frac{u}{2^{k-\ell}5^{\ell-t}} \text{ et } r = \tfrac{v}{2^k5^\ell}.$$

On a bien

$$a = bq + r.$$

Si $r \neq 0$, alors

$$v \neq 0 \text{ et } \varphi = |v'| < |n| = \varphi(b).$$

2°) Si $d = \dfrac{p}{2^m5^n}$ est un élément non nul de I, alors $|p| = \pm d2^m5^n$ est encore dans I et I contient donc des entiers strictement positifs. Soit n le plus petit d'entre eux. Si $n = 2^p5^qn'$, avec $n' \in \mathbb{N}$, alors on a $p = q = 0$ car sinon $n' \in I$, et $0 < n' < n$. On a donc pgcd $(n,2) = $ pgcd $(n,5) = 1$, $n > 0$ et $n\mathbb{D} \subset I$.

Exemple

1°) En utilisant la division euclidienne dans $\mathbb{D}$, on peut montrer que tout idéal de $\mathbb{D}$ est principal par une preuve semblable à celle que l'on fait dans le cas de $\mathbb{Z}$.

2°) Si $I = nD$, $n \geq 0$, est un idéal de $\mathbb{D}$, alors $I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$.

Mais tout idéal de $\mathbb{Z}$ n'est pas l'intersection d'un idéal de $\mathbb{D}$ avec $\mathbb{Z}$ et si c'est le cas, les générateurs peuvent être distincts (penser à $2\mathbb{Z}$, $15\mathbb{Z}$, $15\mathbb{D} \cap \mathbb{Z} = 3\mathbb{Z}$, ...).

3°) On a

$$n\mathbb{D} \subset m\mathbb{D} \Leftrightarrow m \text{ divise } n.$$

Donc les idéaux maximaux de $\mathbb{D}$ sont de la forme $p\mathbb{Z}$ avec p premier différent de 2 et 5.

4°) L'anneau $\mathbb{D}$ étant principal, on peut, comme dans $\mathbb{Z}$, définir le pgcd et le ppcm de deux éléments et décomposer tout élément non nul en un produit de facteurs premiers.

Propriété

| Pour tout nombre premier p, distinct de 2 et 5, le corps $\mathbb{D}/p\mathbb{D}$ est isomorphe au corps $\mathbb{Z}/p\mathbb{Z}$.

Preuve

Considérons deux nombres décimaux d_1 et d_2 écrits sous la forme

$$d_i = \frac{n_i}{10^{m_i}}$$

avec $n_i \in \mathbb{Z}$ et $m_i \geq 0$.

Si $d_1 = d_2$, alors

$$n_1 10^{m_2} = n_2 10^{m_1}$$

et donc, dans $\mathbb{Z}/p\mathbb{Z}$,

$$\overline{n_1}\left(\overline{10}\right)^{m_2} = \overline{n_2}\left(\overline{10}\right)^{m_1}.$$

L'entier p étant premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps et, après avoir noté que 10 et p sont premiers entre eux, l'égalité précédente peut s'écrire

$$\overline{n_1}\left(\overline{10}^{-1}\right)^{m_1} = \overline{n_2}\left(\overline{10}^{-1}\right)^{m_2}.$$

On peut donc définir une application f de $\mathbb{D}$ dans $\mathbb{Z}/p\mathbb{Z}$, en posant

$$f(\frac{n}{10^m}) = \overline{n}\left(\overline{10}^{-1}\right)^{m}.$$

Cette application est un morphisme d'anneaucar :

$$\begin{aligned} f\left(\frac{n_1}{10^{m_1}} + \frac{n_2}{10^{m_2}}\right) &= f\left(\frac{n_1 10^{m_2} + n_2 10^{m_1}}{10^{m_1+m_2}}\right) \\ &= \left(\overline{n_1}\,\overline{10}^{m_2} + \overline{n_2}\,\overline{10}^{m_1}\right)\left(\overline{10}^{-1}\right)^{m_1+m_2} \\ &= \overline{n_1}\left(\overline{10}^{-1}\right)^{m_2} + \overline{n_2}\left(\overline{10}^{-1}\right)^{m_1} \\ &= f\left(\tfrac{n_1}{10^{m_1}}\right) + f\left(\tfrac{n_2}{10^{m_2}}\right) \end{aligned}$$

et

$$f\left(\frac{n_1}{10^{m_1}}\frac{n_2}{10^{m_2}}\right) = f\left(\frac{n_1}{10^{m_1}}\right) f\left(\frac{n_2}{10^{m_2}}\right).$$

Il est clair que l'application f est surjective car $f(n) = \overline{n}$.

Par ailleurs,

$$f(\frac{n}{10^m}) = \overline{n}\left(\overline{10}^{-1}\right)^{m} = 0 \Leftrightarrow \overline{n} = 0,$$

ce qui équivaut encore à

$$\tfrac{n}{10^m} = p\tfrac{\lambda}{10^m} \text{ avec } \lambda \in \mathbb{Z}.$$

Il en résulte que

$$\ker f = pD,$$

d'où finalement l'isomorphisme de $\mathbb{D}/p\mathbb{D}$ et $\mathbb{Z}/p\mathbb{Z}$.

B) Représentation décimale illimitée

Définition

☐ On appelle chiffre tout nombre entier compris entre 0 et 9 et suite décimale toute suite de chiffres (a_n).

☐ On appelle développement décimal illimité une écriture $a_0, a_1 ... a_n .....$ où (a_n) est une suite décimale :

$$a_0, a_1 ... a_n ..... = \sum_{q=0}^{+\infty} \frac{a_q}{10^q},\ a_q \in [[0, 9]].$$

☐ On verra que tout nombre décimal r peut s'écrire d'une manière unique sous forme :

$$r = \sum_{q=m_2}^{m_1} d_q 10^q,\ m_1 \geq m_2,\ d_q \in [[0, 9]] \text{ et } (d_{m_1}, d_{m_2}) \neq (0, 0).$$

On appelle partie entière de r le plus grand entier naturel inférieur à r.

La partie décimale de r est la différence entre r et sa partie entière.

On représente un nombre décimal positif en séparant la partie entière et la partie décimale par une virgule.

Théorème

Tout nombre décimal strictement positif r s'écrit d'une manière et d'une seule sous la forme

$$r = \sum_{q=m_2}^{m_1} d_q 10^q,\ m_1 \geq m_2,\ d_q \in [[0, 9]] \text{ et } (d_{m_1}, d_{m_2}) \neq (0, 0).$$

− Si m_2 est positif, la partie décimale de r est nulle.

− Si m_1 est strictement négatif, la partie décimale de r est nulle.

Preuve

Comme r est un nombre décimale positif, écrivons r sous forme canonique

$$r = a10^p \text{ où } a \in \mathbb{N}.$$

Par ailleurs, on peut écrire a sous forme

$$a = \sum_{q=q_2}^{q_1} d_q 10^q.$$

En multipliant les deux membres par 10^p, nous obtenons une décomposition de la forme annoncée avec

$$m_1 = q_1 + p \text{ et } m_2 = q_2 + p.$$

L'unicité de cette écriture découle de l'écriture décimale de a.

Théorème

Il y a équivalence entre :

i) x est rationnel

ii) Le développement décimale illimité de $x = a_0, a_1 \ldots ..$ est périodique à partir d'un certain rang, c'est-à-dire qu'il existe des entiers naturels non nuls h et k tels que, pour tout entier naturel n strictement supérieur à k :

$$a_{n+h}(x) = a_n(x).$$

Démonstration

Supposons tout d'abord que la suite (a_n) des décimales de x est périodique à partir du rang k, et montrons que le nombre x est rationnel. En effet :

$$x = 0, a_1 a_2 \cdots a_{k-1} + \left(\frac{a_k}{10^k} + \frac{a_{k+1}}{10^{k+1}} + \cdots + \frac{a_{k+h-1}}{10^{k+h-1}} \right) + \ldots.$$

Posons

$$a = 0, a_1 a_2 \cdots a_{k-1} \text{ et } b = \frac{a_k}{10^k} + \frac{a_{k+1}}{10^{k+1}} + \cdots + \frac{a_{k+h-1}}{10^{k+h-1}}.$$

Alors $(x - a)$ est la somme des termes d'une suite géométrique de premier terme b et de raison 10^{-h}. Donc

$$x = a + b\frac{1}{1 - 10^{-h}}.$$

Puisque les nombres a et b sont rationnels, il en est de même de x.

Réciproquement, écrivons x sous la forme $x = \frac{p}{q}$. Si x est décimal, nous verrons que les deux représentations décimales illimitées de x ne comportent l'une que des 0, l'autre que des 9, à partir d'un certain rang. Par ailleurs, il est possible d'écrire

$$q = 2^a 5^b c \text{ et } p = a_0 q + r_0 \text{ et } 0 \leq r_0 < q.$$

Par conséquent, on peut supposer q premier avec $2, 5$ et $0 < p < q$, alors dans ce cas q est premier avec 10. Il existe par le théorème de Bézout u et v tels que

$$uq + 10v = 1.$$

Ainsi 10 est un élément inversible de $\mathbb{Z}/q\mathbb{Z}$. Il existe donc t et k tels que

$$10^t = kq + 1 \Rightarrow 10^t - 1 = kq.$$

Or on peut écrire

$$x = \frac{p}{q} = \frac{kp}{kq} = \frac{kp}{10^t - 1}.$$

Ecrivons kp en base 10

$$kp = b_N 10^N + b_{N-1} 10^{N-1} + ... + b_0.$$

Comme $0 < p < q = 10^t - 1$, on a l'inégalité suivante :

$$N < t.$$

On s'aperçoit que

$$1 = (10^t - 1) \times 0,00 \ldots 010 \ldots 01 \Rightarrow \frac{1}{10^t - 1} = 0,00 \ldots 010 \ldots 010 \ldots ((t-1) \text{ zéros entre les } 1).$$

En multipliant cette égalité par kp qui s'écrit $b_N b_{N-1} \ldots b_0$, on obtient

$$x = \frac{kp}{10^t - 1} = 0,00 \ldots \ b_N b_{N-1} \ldots b_0 00 \ldots 00 \ b_N b_{N-1} \ldots b_0 00 ... \ ((t - N - 1) \text{ zéros entre les suites } b_i.$$

On a maintenant deux cas.

1^{er} cas : $N = t - 1$

On a alors

$$\sum_{k=0}^{n} \frac{1}{10^{tk}} \left(\frac{b_{t-1}}{10} + \frac{b_{t-2}}{10^2} + ... + \frac{b_0}{10^t} \right) = \left(\frac{b_{t-1} 10^{t-1} + ... + b_0}{10^t} \right) \sum_{k=0}^{n} \frac{1}{10^{tk}} = \left(\frac{kp}{10^t} \right) \sum_{k=0}^{n} \left(\frac{1}{10^t} \right)^k.$$

On sait $\sum_{k=0}^{n}\left(\frac{1}{10^t}\right)^k$ converge vers $\frac{1}{1-10^{-t}}$ et donc

$$\left(\frac{kp}{10^t}\right)\frac{1}{1-10^{-t}}=\frac{kp}{10^t-1}=\frac{p}{q}=x.$$

$2^{ème}$ cas : $N<t-1$

Si N est strictement plus petit que $t-1$, c'est la même chose à ceci près que des zéros apparaissent effectivement et alourdissent la rédaction.

C) Application à la construction de $\mathbb{R}$

Le modèle des développements décimaux illimités" est un modèle idéal qui permettra de traiter tous les réels, aussi loufoques qu'ils soient. Dans une mémoire d'ordinateur, même très performant, on ne saurait stocker une suite de chiffres (on peut à la rigueur stocker la formule qui la produit, si cette formule existe...). Un ordinateur ne stockera que des flottants limités, c'est-à-dire des nombres décimaux.

Définition

☐ Un développement décimal illimité est dit impropre si à partir d'un certain rang n_0 tous les chiffres a_n sont égaux à 9. Par exemple, $12,1257999.....$ en est un.

☐ On dit qu'un développement décimal illimité est propre dans le cas contraire, c'est-à-dire si ses chiffres ne sont pas tous égaux à 9 à partir d'un certain rang.

☐ On appelle nombre réel positif tout développement décimal illimité propre et on désigne par $\mathbb{R}$ leur ensemble.

☐ On appelle représentation décimale de $x\in\mathbb{R}$, toute suite décimale (a_n) telle que

$$x=\lim_{n\to+\infty}\sum_{k=0}^{n}\frac{a_k}{10^k}.$$

☐ Soit $x\in R$ et (a_n) la suite décimale propre qui représente x. Le nombre décimale $d_n=\sum_{k=0}^{n}\frac{a_k}{10^k}$ est appelé l'approximation décimale par défaut à 10^{-n} près de x et le nombre décimal $d_n+\frac{1}{10^n}$ l'approximation décimale par excès à 10^{-n} près de x.

☐ On appellera flottant illimité un couple $((a_n),e)$ où (a_n) est une suite de chiffres vérifiant $a_0\neq 0$ et e un entier relatif. Pour comprendre ce que signifie cette obscure définition, donnons un exemple de flottant illimité :

$((3,1,4,1,5,9,\ldots),2)$ a vocation à représenter le réel $0,314159\ldots\times 10^2$, c'est-à-dire 10π.

Théorème

Soit $r=a_0,a_1a_2a_3.....$ et $s=b_0,b_1b_2b_3.....$ deux nombres réels. La relation binaire $\leq$ sur $\mathbb{R}$, définie par

$$(r\leq s\Leftrightarrow r=s)\text{ ou }(\exists n\in N\ /\ a_n<b_n\text{ et }a_k=b_k\text{ si }k<n)$$

est une relation d'ordre total sur $\mathbb{R}$, pour laquelle toute partie non vide de $\mathbb{R}$ majorée possède une borne supérieure.

Preuve

Il est facile de vérifier que $\leq$ est une relation d'ordre total.

Soit X une partie non vide de $\mathbb{R}$, majorée par $m = (m_n)$. On définit la borne supérieure (s_n) de X par récurrence sur n.

− L'ensemble des premiers termes des éléments de X est majorée par m_0. Cet ensemble d'entiers possède donc un plus grand élément s_0.

− On suppose s_0, ..., s_n définis et tels que, pour $1 \leq k \leq n$, s_k est le plus grand $(k+1)$-ième terme des éléments de X commençant par s_0, ..., s_{k-1}. Le terme s_{n+1} est alors défini comme étant le plus grand $(n+2)$-ième terme des éléments de X commençant par s_0, ..., s_n.

Théorème

1°) Toute suite de nombres réels positifs croissante et majorée est convergente.

2°) Toute suite décimale est la représentation décimale d'un nombre réel.

Démonstration

1°) La démonstration repose sur l'utilisation répétée du résultat suivant :

− soit une suite croissante $(x_n)_n$ de nombres d'entiers dont l'ensemble X des valeurs est fini, alors cette suite est stationnaire, plus précisément constante et égale au plus grand élément de X à partir d'un certain rang.

Soit $(u_n)_n$ une suite croissante et majorée de réels. Alors pour chaque n, on peut écrire u_n à l'aide d'un développement illimité. La démonstration consiste à regarder ce qui se passe colonne par colonne.

$$\begin{array}{lll} u_1 & = & a_{10}, a_{11}a_{12}a_{13}...a_{1k}..... \\ u_2 & = & a_{20}, a_{21}a_{22}a_{23}...a_{2k}..... \\ u_3 & = & a_{30}, a_{31}a_{32}a_{33}...a_{3k}..... \\ u_4 & = & a_{40}, a_{41}a_{42}a_{43}...a_{4k}..... \\ .... & ... & ..... \\ u_n & = & a_{n0}, a_{n1}a_{n2}a_{n3}...a_{nk}..... \end{array}$$

Montrons que la suite d'entiers $(a_{n0})_n$ converge dans $\mathbb{N}$ vers un entier a_0. Soit M un majorant de $(u_n)_n$. L'ensemble

$$A = \{E_n[u_n],\ n \text{ entier}\}$$

des parties entières des termes de la suite $(u_n)_n$ est un ensemble d'entiers naturels majorés par la partie entière de M. Comme A est une partie de $\mathbb{N}$, A admet un plus grand élément a_0. il existe k_0 tel que tout $n \geq k_0$ entraîne

$$E_n[u_n] = a_0.$$

Vérifions maintenant que la suite $(a_{n1})_n$ est croissante pour $n \geq k_0$ et déduisons qu'il existe a_1 et k_1 tels que

$$a_{n1} = a_1 \text{ pour tout } n \geq k_1.$$

La suite $(a_{n1})_{n \geq k_0}$ est la suite d'entiers obtenue en prenant les premiers termes des développements décimaux des u_n pour $n \geq n_0$; comme suite extraite de la suite $(a_{n1})_n$, elle prend ses valeurs dans l'ensemble fini

$$\{0, 1, ..., 9\}.$$

Par ailleurs, la suite $(u_n)_{n \geq k_0}$ est la suite extraite de la suite $(u_n)_n$ dont tous les termes ont même partie entière a_0. Elle est en plus croissante. Puisque $(u_n)_{n \geq k_0}$ est une suite croissante de nombres réels dont toutes les parties entières sont égales à a_0 alors la suite $(a_{n1})_{n \geq k_0}$ est croissante et donc constante à partir d'un certain rang, c'est à dire qu'il existe $a_1 \in \{0, 1, ..., 9\}$et un entier $k_1 \geq k_0$ tel que

$$a_{n1} = a_1 \text{ pour tout } n \geq k_1.$$

Montrons par récurrence sur $h \geq 1$ que la suite $(a_{nh})_n$ est croissante - pour n suffisamment grand - et qu'il existe a_h et k_h tels que $a_{nh} = a_n$ pour tout $n \geq k_h$. On fait l'hypothèse de récurrence suivante :

soit m un entier quelconque strictement supérieur à 0 ; pour tout entier $h \leq m$, la suite a_{nh} est stationnaire et plus précisément il existe un entier k_h tel que $k_{h-1} \leq k_h$ $(1 \leq h \leq m)$, un entier $a_h \in \{0, 1, ..., 9\}$ tel que pour tout $n \geq k_h$, $a_{nh} = a_h$.

La suite $(u_n)_{n \geq k_m}$ est extraite de la suite $(u_n)_n$ comme suite extraite de suite extraite, à ce titre elle est croissante et par définition tous ses termes ont un développement décimal commençant par $a_0, a_1 a_2 .... a_m$. On s'intéresse alors à la suite $(a_{n,m+1})_{n \geq m+1}$ des $(m+1)$-èmes décimales et en raisonnant comme pour le cas 1, on montre l'existence de a_{m+1} et d'un entier k_{m+1} tel que pour $n \geq k_{m+1}$ on ait

$$a_{n,m+1} = a_{m+1}.$$

Maintenant deux cas peuvent se produire :

1^{er} cas : $a_0, a_1 a_2 ..... a_n ....$ est un développement propre

Montrons que

$$u = a_0, a_1 a_2 ..... a_n ....$$

est la limite de la suite $(u_n)_n$. Soit a et b tels que

$$a < u < b.$$

Soit $\varepsilon = \min\{u - a, b - u\}$. Si $\varepsilon \geq 1$, alors pour $n \geq k_0$ on a

$$u_n = u$$

et donc

$$a < u_n < b.$$

Si $\varepsilon < 1$, soit h le plus grand entier tel que

$$10^{-h} < \varepsilon$$

alors pour $n \geq k_h$ on a

$$a < u_n < b.$$

On a donc bien trouvé le $N(\varepsilon)$ de la définition.

$2^{ème}$ cas : $a_0, a_1 a_2 ..... a_n ....$ est un développement impropre

Ceci veut dire qu'il existe un entier M tel que $n > M$ entraîne $a_n = 9$. Soit M le plus petit entier satisfaisant cette propriété, c'est à dire qu'on a

$$a_0, a_1 .... a_M 999...999..... \text{ et } a_M = 9.$$

Soit le nombre décimal

$$u = a_0, a_1 ... a_{M-1},$$

obtenu à partir du développement précédent en gardant les $(M-1)$ premiers chiffres après la virgule et en ajoutant 1 au M-ième. En raisonnant comme ci-dessus on montre que u est la limite de $(u_n)_n$.

2°) C'est une conséquence de 1°), puisque la suite (d_n) définie par

$$d_n = \sum_{k=0}^{n} \frac{a_k}{10^k}$$

est croissante. Il reste à montrer qu'elle est majorée :

$$\text{pour } n \geq 1,\ d_n \leq a_0 + 9 \sum_{k=1}^{n} \frac{1}{10^k} = a_0 + 1 - \frac{1}{10^n} < a_0 + 1.$$

La suite (d_n) croissante et majorée converge vers un réel x tel que

$$d_n \leq x \leq d_n + \frac{1}{10^n},\ n \in \mathbb{N}.$$

Théorème

1°) Toute partie majorée non vide de $\mathbb{R}_+$ admet une borne supérieure.

2°) Si (A, B) forme une partition de $\mathbb{R}$ de façon que :

$$\forall a \in A,\ \forall b \in B,\ a < b$$

alors il existe un élément x_0 de $\mathbb{R}$ tel que :

ou bien

$$A = \{a \in \mathbb{R} \ / \ a \leq x_0\} \text{ et } B = \{b \in \mathbb{R} \ / \ b > x_0\}$$

ou bien

$$A = \{a \in \mathbb{R} \ / \ a < x_0\} \text{ et } B = \{b \in \mathbb{R} \ / \ b \geq x_0\}.$$

Preuve

1°) Soit A une partie majorée non vide de $\mathbb{R}_+$. Soit a_0 le plus grand entier i tel que

$$A \cap [\![i, i+1]\!] \neq \emptyset$$

et pour tout n soit a_{n+1} le plus grand des entiers $k \in \{0, ..., 9\}$ tels que

$$A \cap [a_0, a_1...a_n k; a_0, a_1...a_{n(k+1)}[\neq \emptyset$$

Si $k = 9$, on prend

$$a_0, a_1...a_{nk} + \frac{1}{10^{n+1}}$$

comme extrémité droite de l'intervalle. La suite

$$u_n = a_0, a_1...a_n$$

est croissante et majorée donc elle converge vers

$$u = a_0, a_1...a_n.....$$

Montrons que u est un majorant de A en raisonnant par l'absurde : si $x \in A$ est tel que $x > u$, alors, si x est le développement illimité $x_0, x_1...x_n...$, soit m tel que

$$x_m > a_m$$

et

$$x_i = a_i \text{ pour tout } i = 0, ..., m-1,$$

alors

$$x \in [a_0, a_1...a_{m-1}k, a_0, a_1...a_{m-1(k+1)}[\text{ pour} k \geq a_{m+1},$$

ce qui contredit la construction de a_m.

Montrons que u est le plus petit majorant de A. Soit $v < u$ avec $v = v_0, v_1...v_n...$ Soit m le plus petit entier tel que $v_m < a_m$ et $a_i = v_i$ pour $0 \leq i < m$. Par définition de a_m il existe $x \in A$ tel que

$$x \geq a_0, a_1...a_m.$$

Par suite on a $x > v$, donc v n'est pas un majorant de A.

2°) Montrons 1°) $\Rightarrow$ 2°). En fait, on peut même montrer l'équivalence de 1°) et 2°) (voir cours sur les réels).

Soit E une partie non vide, majorée par m. Appelons B l'ensemble des majorants de E et $A = \mathbb{R} - B$.

Alors :

$-$ B est non vide, car m appartient à B.

$-$ A est non vide, car il existe un élément x dans E, et $x - 1$ ne majorant pas x se trouve donc dans A.

Par ailleurs, on a

$$\forall a \in A,\ \forall b \in B,\ a < b.$$

En effet, $a \in A$ signifie que a ne majore pas E, et donc qu'il existe x élément de E tel que $a < x$. $b \in B$ signifie que b majore E et donc que $x \leq b$. Donc $a < b$.

$\{A, B\}$ forme une partition de $\mathbb{R}$. C'est évident puisque $A = \mathbb{R} - B$.

Les hypothèses de 2°) sont vérifiées. Il existe donc m_0 élément de R tel que :

(a) ou bien $A = \{a \in \mathbb{R} \ / \ a \leq m_0\}$ et $B = \{b \in \mathbb{R} \ / \ b > m_0\}$

(b) ou bien $A = \{a \in \mathbb{R} \ / \ a < m_0\}$ et $B = \{b \in \mathbb{R} \ / \ b \geq m_0\}$.

Dans le cas (b), m_0 est le plus petit élément de B. m_0 est donc le plus petit majorant de E. La borne supérieure de E existe donc.

Montrons que le cas (a) est impossible. Dans le cas (a), m_0 est élément de A et ne majore donc pas E. Il existe x élément de E tel que :

$$m_0 < x.$$

On a alors

$$m_0 < \frac{m_0 + x}{2} < x.$$

$\frac{m_0 + x}{2}$ étant supérieur à m_0 est élément de B, donc majore E. Il est cependant inférieur à x élément de E. La contradiction est ainsi prouvée.

Théorème

1°) Soit (r_n) et (s_n) deux réels, définissons

$$(r_n) + (s_n) = \sup\{r_n + s_n \ / \ n \in \mathbb{N}\}$$
$$r_n s_n = \sup\{r_n s_n \ / \ n \in \mathbb{N}\}.$$

Alors, $(\mathbb{R}, +, \times)$ est un corps commutatif totalement ordonné et possédant la propriété de la borne supérieure.

2°) Si (a_n) est une suite décimale et si $u_n = \sum_{k=0}^{n} \frac{a_k}{10^k}$, alors la suite (u_n) converge vers un réel $s(a)$ tel que, pour tout $n \in \mathbb{N}$,

$$u_n \leq s(a) \leq u_n + \frac{1}{10^n}.$$

Preuve

1°) On l'admet car techniquement difficile.

2°) La suite (u_n) est croissante car

$$u_{n+1} - u_n = \tfrac{a_{n+1}}{10^{n+1}} \geq 0.$$

Par ailleurs, pour tout $n \geq 1$,

$$u_n \leq a_0 + 9\sum_{k=1}^{n} \frac{1}{10^k} = a_0 + 1 - \frac{1}{10^n} < a_0 + 1.$$

La suite (u_n), croissante et majorée, converge vers un réel $s(a)$ avec, pour tout $n \in \mathbb{N}$,

$$u_n \leq s(a).$$

Pour $p \geq n+1$, on a :

$$u_p = u_n + \sum_{k=n+1}^{p} \frac{a_k}{10^k} \leq u_n + 9\sum_{k=n+1}^{p} \frac{1}{10^k} = u_n + \frac{1}{10^n} - \frac{1}{10^p},$$

d'où

$$s(a) \leq u_n + \frac{1}{10^n}.$$

Propriété

1°) Tout réel strictement positif non décimal admet exactement une représentation décimale illimitée.

2°) Tout réel strictement positif décimal en admet exactement deux, l'une se terminant par des chiffres 0, l'autre par des chiffres 9.

Preuve

1°) Soit x un réel strictement positif possédant au moins deux représentations décimales illimitées, et soit (a_n) et (b_n) deux telles représentations distinctes. On notera (u_n) la suite de nombres décimaux associée à (a_n) et (v_n). Soit x un réel strictement positif possédant au moins deux représentations décimales illimitées, et soit $((a_n), e)$ et $((b_n); f)$ deux telles représentations distinctes. On notera (u_n) la suite de nombres décimaux associée à $((a_n), e)$ et (v_n) celle associée à $((b_n), f)$:

$$u_n = 10^e \sum_{k=0}^{n} \frac{a_k}{10^k} \text{ et } v_n = 10^f \sum_{k=0}^{n} \frac{b_k}{10^k}.$$

Etudions le cas où $e \neq f$, quitte à échanger les deux flottants, on peut supposer $e < f$. Comme v_0 minore x, on voit que

$$10^{f-1} \leq x.$$

Par ailleurs, on a

$$x \leq 10^e.$$

On en conclut que

$$10^{f-1} \leq 10^e$$

donc que

$$f - 1 \leq e.$$

Ceci conjoint à l'inégalité

$$e < f$$

assure que

$$f = e + 1,$$

et que

$$x = 10^{f-1} = 10^e.$$

Le nombre x qui avait deux écritures est donc un nombre décimal - et même beaucoup mieux, une puissance positive ou négative de 10.

Etudions maintenant le cas où

$$e = f.$$

C'est donc que les suites (a_n) et (b_n) sont distinctes. Soit $N \geq 0$ le plus petit indice tel que $a_N \neq b_N$. Comme plus haut pour e et f, on peut supposer $a_N < b_N$. On en déduit que $u_N < v_N$. Comme $v_N \leq x$, on en déduit que $u_N < x$. Si tous les chiffres dans (a_N) après le N-ème étaient nuls, on aurait $u_N = x$; c'est donc qu'un au moins des chiffres du flottant $((a_n); e)$ après le N-ème est non nul ; soit $M \geq 1$ le plus petit entier tel que a_{N+M} ne soit pas nul.

Considérons alors les flottants $((a_{N+M}, a_{N+M+1}, \ldots), e - N - M)$ et $((b_N - a_N, b_{N+1}, \ldots), e - N)$, ce sont bien des flottants puisque a_{N+M} est non nul par définition de M tandis que $b_N - a_N$ est bien un chiffre non nul, puisque b_N est un chiffre et a_N un chiffre strictement plus petit. On affirme que ces deux flottants représentent le même réel. C'est évident si on a compris ce qu'était concrètement l'opération faite en introduisant ces deux flottants : c'est tronquer dans les deux représentations du réel x les $N - 1$ premiers chiffres. Si on ne comprend pas, on peut toujours faire une vérification formelle ; soit (u'_n) et (v'_n) les suites de valeurs approchées associées à ces deux nouveaux flottants, on vérifie en se concentrant bien que pour tout $n \geq 0$:

$$u'_n = u_{n+M} - u_n \text{ et } v'_n = v_{n+M} - v_n + 10^e \frac{b_N - a_N}{10^{N+1}} = v_{n+N} - u_N.$$

et donc que ces deux suites convergent toutes deux vers le réel $x - u_N$. Mais cette fois, comme $1 \leq M$, elles ont des exposants différents donc ce stratagème nous a ramené au premier cas. On en déduit que $x - u_N$ est une puissance de 10, donc - étant bien clair que u_N est un nombre décimal - que x est un nombre décimal.

On a donc à ce stade bien prouvé que les réels non décimaux ne sont représentables que d'une et une seule façon.

2°) En précisant quelques détails, on saurais prouver que les décimaux n'ont que les deux écritures auxquelles on pense :

$$a_0, a_1 a_2 \ldots a_n 0000 \ldots = a_0, a_1 a_2 \ldots a_n 9999...$$

Montrons d'abord l'équivalence de

i) d est un nombre décimal.

ii) La représentation décimale propre de d est finie.

iii) Le nombre d admet une représentation décimale impropre.

Montrons i) $\Rightarrow$ ii). Un nombre décimal d peut s'écrit sous forme

$$d = \tfrac{b}{10^m} \text{ avec pgcd } (10, b) = 1.$$

Ecrivons b en base 10

$$b = a_0 10^m + a_1 10^{m-1} + ... + a_m \Rightarrow d = a_0 + \frac{a_1}{10} + ... + \frac{a_m}{10^m}.$$

Ainsi, d est déterminé par la suite d'entiers (a_i) finie où $0 \leq a_i \leq 9$ si $1 \leq i \leq m$.

Montrons ii) $\Rightarrow$ iii). Soit $m \geq 1$ le plus petit entier tel que

$$n \geq m \Rightarrow a_n = 0.$$

On définit une suite décimale impropre (a^*_n) par

$$\begin{array}{l} a^*_k = a_k \text{ si } 0 \leq k \leq m-2 \\ a^*_{m-1} = a_{m-1} - 1 \\ a^*_k = 9 \text{ si } k \geq m. \end{array}$$

En posant

$$u_n = \sum_{k=0}^{n} \frac{a^*_k}{10^k} = u_{m-1} + 9 \sum_{k=m}^{n} \frac{1}{10^k},$$

il est clair que $\lim_{n\to+\infty} u_n = d$.

Montrons iii) $\Rightarrow$ i). Soit (a_n) une représentation décimale impropre de d. Il existe un n_0 tel que

$$n \geq n_0 \Rightarrow a_n = 9.$$

Il vient

$$u_n = u_0 + 9\sum_{k=n_0+1}^{n} \frac{1}{10^k} = u_0 + \frac{1}{10^{n_0}} - \frac{1}{10^n}.$$

$\Rightarrow d$ est un nombre décimal.

Il reste à montrer que d possède une seule représentation décimale impropre. Pour cela, on voit que dans l'implication ii) $\Rightarrow$ iii), on a fait correspondre à la suite décimale propre (a_n) représentant le nombre décimal non nul d une suite décimale impropre (a_n^*). Soit φ cette correspondance. Il est clair que φ est injective.

Soit (d_n) une autre suite impropre de d et $n_0 \geq 1$ le plus petit entier tel que $n \geq n_0$ implique $a_n = 9$. On définit une suite décimale finie (a_n) par

$b_n = a_n$ si $n < n_0 - 1$

$b_{n_0-1} = a_{n_0-1} + 1$

$b_n = 0$ si $n \geq n_0$.

L'entier $n_0 - 1$ est le plus petit entier tel que $(n > n_0 - 1)$ implique $b_n = 0$, d'où

$$\varphi((b_n)) = (a_n).$$

Ainsi, φ est surjective, donc bijective entre l'ensemble des suites décimales finies et l'ensemble des suites décimales impropres. De plus, (a_n) et $\varphi((a_n))$ représente le même nombre décimal, ce qui entraîne en particulier qu'un nombre décimal possède une seule représentation décimale impropre.

Exemple

☐ Il existe toujours un décimal tel que $a < d < b$ pour a et b des réels. Si

$$a = a_0, a_1a_2.....a_n.... \text{ et } b = b_0, b_1b_2.....b_n....,$$

soit n tel que $a_n < b_n$ et $m > n$ tel que

$$a_m < 9.$$

Considérez le décimal $d = a_0, a_1a_2.....a_n....a_{m-1}$ obtenu à partir de a en ajoutant 1 au chiffre a_m et en remplaçant les chiffres suivants par 0.

☐ On peut utiliser le développement décimal illimité pour prouver que $\mathbb{R}$ n'est pas dénombrable, mais équipotent à $\mathcal{P}(\mathbb{N})$.

☐ On rappel que

$$q^n + \ldots + q^p = \tfrac{q^n - q^{p+1}}{1-q}$$

$$9(\frac{1}{10^{n+1}} + \ldots + \frac{1}{10^p}) = \frac{1}{10^n} - \frac{1}{10^p}$$

$$\frac{1}{10^{n+1}} + \ldots + \frac{1}{10^p} < \frac{1}{10^n}$$

Dénombrement

On pourrait penser qu'il n'y a que deux types d'ensembles, les ensembles finis et les ensembles infinis, ces derniers étant tous de même nature. Cette vision a été mise en défaut par Georg Cantor (1845 -1918). Ses travaux ont permis de définir plusieurs types d'infinis. Galilée a bien remarqué que les termes "autant d'éléments", "moins d'éléments" ou "plus d'éléments" ne peuvent s'appliquer sans paradoxe aux ensembles infinis.

Un ensemble infini est en bijection avec l'une de ses parties strictes. Par exemple, $\mathbb{N}$ est en bijection avec $\mathbb{N}^*$, au moyen de la bijection suivante :

$$\begin{aligned} \mathbb{N} &\to \mathbb{N}^* \\ n &\mapsto n+1 \end{aligned}$$

Soit plusieurs ensembles infinis, par exemple $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$. Sont-ils en bijection les uns avec les autres ? On prouvera que $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$ sont effectivement en bijection, mais ce n'est pas le cas de $\mathbb{R}$. Les premiers sont dits dénombrables.

I) Ensembles finis, infinies et dénombrables

A) Quelques rappels

Rappel

1°) $\mathbb{N}$ a un plus petit élément 0 et n'a pas de plus grand élément.

2°) Toute partie non vide de $\mathbb{N}$ a un plus petit élément.

3°) Toute partie non vide majorée de $\mathbb{N}$ admet un plus grand élément.

4°) Soit $(a_i)_{i\in I}$ une suite de réels ou de complexes ou d'un ensemble E muni d'une addition commutative. On définie $F(n) = \sum_{i=0}^{n} a_i$ par

$$F(0) = a_0 \text{ et } F(n+1) = F(n) + a_{n+1}.$$

Remarque

– En fait, on peut écrire

$$\mathbb{N} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \ldots\}.$$

En posant $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$ etc., on a

$$\mathbb{N} = \{0, 1, 2, \ldots\}.$$

– Pour un entier n, son élément suivant est

$$(n+1) = \min\{m \in \mathbb{N} \mid m > n\}.$$

Théorème (récurrence)

Soit A un ensemble inclus dans $\mathbb{N}$ tel que

i- $0 \in A$

ii- $\forall n \in \mathbb{N}, n \in A \Rightarrow n+1 \in A$,

| alors $A = \mathbb{N}$.

Preuve

Raisonnons par l'absurde en supposant que $A \neq \mathbb{N}$, alors $\complement_{\mathbb{N}} A$ n'est pas vide car $A \subset \mathbb{N}$. Il admet donc un plus petit élément noté $n_0 = \min A$. Comme $n_0 \in \complement_{\mathbb{N}} A$, il n'appartient pas à A. Donc il est différent de 0 car $0 \in A$. Comme

$$n_0 - 1 < n_0 = \min \complement_{\mathbb{N}} A,$$

$(n_0 - 1)$ n'est pas un élément de $\complement_{\mathbb{N}} A$, c'est-à-dire que $(n_0 - 1)$ appartient à A.

D'après la propriété ii, on a

$$(n_0 - 1) \in A \Rightarrow (n_0 - 1) + 1 = n_0 \in A.$$

C'est contradictoire avec le fait que n_0 n'appartient pas à A. Donc $A = \mathbb{N}$.

Théorème (récurrence)

| 1°) Soit $P(n)$ une propriété dépendant de la variable n. On suppose
| i- $P(0)$
| ii- $\forall k \in \mathbb{N}$, $P(k) \Rightarrow P(k+1)$,
| alors $\forall n \in \mathbb{N}$, $P(n)$.
| 2°) Soit $P(n)$ une propriété dépendant de la variable n. On suppose
| i- $P(n_0)$
| ii- $\forall k \in \mathbb{N}$, $(\forall k \geq n_0$ et $P(k)) \Rightarrow P(k+1)$,
| alors $\forall n \in \mathbb{N}$, $n \geq n_0 \Rightarrow P(n)$.

Preuve

1°) Posons

$$A = \{n \in \mathbb{N} \mid P(n)\}.$$

i- Il est clair que $0 \in A$.

ii- Si $k \in A$, alors $P(k)$ qui implique $P(k+1)$. Donc $(k+1)$ appartient A.

D'après le théorème précédent, on a $A = \mathbb{N}$, c'est-à-dire

$$\forall n \in \mathbb{N},\ P(n).$$

2°) Considérons la propriété Q définie par

$$Q(n) \Leftrightarrow (n < n_0 \text{ ou } P(n)).$$

On a

i- $Q(0)$ car $0 < n_0$

ii- Supposons $Q(k)$. On a plusieurs cas à voir :

Si $k < n_0 - 1$, alors $k + 1 < n_0$, donc $Q(k+1)$.

Si $k = n_0 - 1$, alors $k + 1 = n_0$, donc $Q(k+1)$ car $P(n_0)$.

Si $k \geq n_0$, alors $P(k)$ implique $P(k+1)$, donc $Q(k+1)$.

En conclusion, on a

$$\forall n \in \mathbb{N},\ n \leq n_0 \text{ ou } P(n).$$

Par contraposition, on a

$$\forall n \in \mathbb{N},\ n > n_0 \Rightarrow P(n).$$

Théorème (récurrence double)

| Soit $P(n)$ une propriété dépendant de la variable n. On suppose

i- $P(0)$ et $P(1)$
ii- $\forall k \in \mathbb{N}$, $(P(k)$ et $P(k+1)) \Rightarrow P(k+2)$,
alors $\forall n \in \mathbb{N}$, $P(n)$.

Preuve

Considérons la propriété Q définie par

$$Q(n) \Leftrightarrow (P(n) \text{ et } P(n+1)).$$

On a

i- $Q(0)$ car $P(0)$ et $P(1)$.

ii- Supposons $Q(k)$, alors on a $P(k)$ et $P(k+1)$. Mais

$$(P(k) \text{ et } P(k+1)) \Rightarrow P(k+2).$$

D'après l'hypothèse, on a

$$(P(k+1) \text{ et } P(k+2)) \Leftrightarrow Q(k+1).$$

Donc pour tout $n \in \mathbb{N}$, $Q(n)$, c'est-à-dire : $\forall n \in \mathbb{N}$, $P(n)$.

Preuve

1°) Soit (a_{ij}) les éléments d'un tableau $[\![1,p]\!] \times [\![1,q]\!] = I \times J$, on a

$$\sum_{(i,j)\in I\times J} a_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{p} a_{ij} = \sum_{j=1}^{p}\sum_{i=1}^{n} a_{ij}.$$

2°) $\sum_{i\in A} a_i = \sum_{j\in A} a_j$(variable muette).

3°) Soit $f : A \to B$ une bijection. On a

$$\sum_{j\in B} a_j = \sum_{i\in A} a_{f(i)}.$$

4°) $\sum_{i\in A} (\lambda a_i + \mu b_i) = \lambda \sum_{i\in A} a_i + \mu \sum_{i\in A} b_i$.

Exemple

□ Calculons $S = \sum_{i=1}^{n} i$. Posons $i = n+1-j$, alors l'application $f : j \mapsto n+1-j$ de $[\![1,n]\!]$ dans lui-même est une bijection. On a donc

$$\begin{aligned} S &= \sum_{j\in\{1,2,\ldots,n\}} (n+1-j) \\ &= \sum_{j=1}^{n} (n+1-j) \\ &= \sum_{i=1}^{n} (n+1-i) \\ &= \sum_{i=1}^{n} (n+1) - \sum_{i=1}^{n} i \\ &= \sum_{i=1}^{n} (n+1) - S, \end{aligned}$$

d'où

$$2S = n(n+1) \Rightarrow S = \frac{n\,(n+1)}{2}.$$

□ Calculons $S = \sum_{i=1}^{n} x^i$ et montrons que

$$b^n - a^n = (b-a)\sum_{i=0}^{n-1} a^i b^{n-1-i}.$$

Calculons

$$xS = \sum_{i=0}^{n} x^{i+1}.$$

Posons $j = i+1$ et l'application $j \mapsto j-1$ de $[\![1,n]\!]$ dans $[\![0,n-1]\!]$ est une bijection. On a donc

$$xS = \sum_{j=1}^{n} x^j = \sum_{i=1}^{n} x^i.$$

Calculons

$$(1-x)S = S - xS = \sum_{i=0}^{n-1} x^i - \sum_{i=1}^{n} x^i = 1 - x^n.$$

Donc

$$S = \frac{1-x^n}{1-x}.$$

Posons $x = \dfrac{a}{b}$ dans cette formule, alors

$$\begin{aligned} (1-\frac{a}{b})\sum_{i=0}^{n-1}(\frac{a}{b})^i &= 1-\left(\frac{a}{b}\right)^n \\ \Rightarrow \quad \frac{b-a}{b}\sum_{i=0}^{n-1} a^i b^{-i} &= \frac{b^n-a^n}{b^n} \\ \Rightarrow \quad b^{n-1}(b-a)\sum_{i=0}^{n-1} a^i b^{-i} &= b^n - a^n. \end{aligned}$$

D'où

$$b^n - a^n = (b-a)\sum_{i=0}^{n-1} a^i b^{n-1-i}.$$

Il peut paraît téméraire de comparer entre eux les ensembles infinis, c'est néanmoins ce que l'on peut faire grâce à la notion de bijection. Nous allons tout d'abord examiner les propriétés des intervalles de $\mathbb{N}$ puisque ce sont eux qui servent de référence.

B) Propriétés liées aux intervalles de $\mathbb{N}$

Propriété

1) Soit p et q de $\mathbb{N}^*$. Pour qu'il existe une application injective de $[\![1,p]\!]$ dans $[\![1,q]\!]$, il faut et il suffit que $p \leq q$.

2) Soit p et q de $\mathbb{N}^*$. Pour qu'il existe une application surjective $[\![1,p]\!]$ sur $[\![1,q]\!]$, il faut et il suffit que

$$p \geq q.$$

3) Soit p et q de $\mathbb{N}^*$. Pour qu'il existe une bijection de $[\![1,p]\!]$ sur $[\![1,q]\!]$ il faut et il suffit que $p = q$.

En particulier, si un ensemble E est équipotent à $[\![1,m]\!]$ et à $[\![1,n]\!]$, alors $m = n$.

Preuve

1) Si $p \leq q$, alors $[\![1,p]\!] \subset [\![1,q]\!]$,. Il est alors clair que l'injection canonique $x \mapsto x$ de $[\![1,p]\!]$ dans $[\![1,q]\!]$ est injective.

Inversement, nous allons prouver par récurrence la propriété $P(p)$:

pour p, s'il existe une application injective de $[\![1,p]\!]$ dans $[\![1,q]\!]$, alors $p \leq q$.

Le cas où $p = 0$ est évident. Pour $p = 1$, il n'y a rien à prouver, car alors $[[1,p]\!]$ est un singleton. Supposons $p \geq 1$ et $P(p)$ vraie. Soit $q \in \mathbb{N}^*$ et $f : [\![1,p+1]\!] \to [\![1,q]\!]$ une application injective. Notons que $p+1 \neq 1$, $[\![1,q]\!]$ n'est donc pas un singleton, puisque f est injective, donc $q \geq 2$. Distinguons deux cas :

$\underline{1^{er}}$ cas : $f(p+1) = q$.

Alors par injectivité de f, $f([\![1,p]\!]) \subset [\![1,q-1]\!]$. $f\big|_{[\![1,p]\!]}$ est une injection de $[\![1,p]\!]$ dans $[\![1,q-1]\!]$, donc $q-1 \geq p$ à cause de l'hypothèse de récurrence, d'où $q \geq p+1$.

$\underline{2^{eme}}$ cas : $f(p+1) < q$.

Soit alors $g : [\![1,q]\!] \to [\![1,q]\!]$ la bijection telle que

$$g(q) = f(p+1),\ g[f(p+1)] = q \text{ et } g(i) = i \text{ pour } i \neq q,\ i \neq f(p+1).$$

Alors

$$g \circ f : [\![1,p+1]\!] \to [\![1,q]\!]$$

est une injection, et

$$(g \circ f)(p+1) = q$$

d'où $q \geq p+1$ par le 1^{er} cas.

2) Supposons qu'il existe une surjection f de $[\![1,p]\!]$ sur $[\![1,q]\!]$. Pour chaque $j \in [\![1,q]\!]$, l'ensemble $E_j = f^{-1}(\{j\})$ est non vide, donc admet un plus petit élément, que nous notons $g(j)$. On a ainsi construit

$$g : [\![1,q]\!] \to [\![1,p]\!].$$

L'application g associe à tout élément j de $[\![1,q]\!]$ l'un quelconque des éléments k de $[\![1,p]\!]$. Par construction, l'application $f \circ g$ est l'identité de $[\![1,q]\!]$. Puisque $f \circ g$ est injective, il en est de même de g. L'existence d'une injection de $[\![1,q]\!]$ dans $[\![1,p]\!]$ implique $q \leq p$ d'après 1).

Réciproquement si $p \geq q$, l'application $f : [\![1,p]\!] \to [\![1,q]\!]$ définie par

$$f : k \mapsto \min\{k,q\}$$

est surjective.

3) Si $p = q$, alors $[\![1,p]\!] = [\![1,q]\!]$. Il est clair que l'injection $x \mapsto x$ canonique de $[\![1,p]\!]$ dans $[\![1,q]\!]$ est une bijection.
La réciproquement est une conséquence de 1) et 2).

Remarque

La propriété 1) s'appelle le principe des tiroirs de Dirichlet car c'est lui qui fut le premier mathématicien à remarquer qu'on pouvait s'en servir pour démontrer des résultats difficiles. De façon intuitive, on peut l'énoncer comme suit : si $(n+1)$ chaussettes sont rangées dans n tiroirs, alors au moins un tiroir contiendra deux chaussettes ou plus. On le démontre par l'absurde. Si c_i était le nombre de chaussettes tel que $c_i \leq 1$, alors en sommant on obtiendrait $n+1 \leq n$, ce qui est absurde.

Propriété

Si $p \in \mathbb{N}^*$, toute injection de $[\![1,p]\!]$ dans lui-même est une bijection.
Toute surjection de $[\![1,p]\!]$ dans lui-même est aussi une bijection.

Preuve

Nous allons prouver cette propriété en deux étape :

1) Soit $f : [\![1,p]\!] \to [\![1,p]\!]$ une injection. Montrons par l'absurde que f est surjective. Si ce n'était pas le cas, il existerait $a \in [\![1,p]\!]$ qui ne soit pas antécédent par f et on pourrait choisir $a \in [\![1,p]\!] \setminus \mathrm{Im}(f)$. Ce la implique $p > 1$. On définirait alors $g : [\![1,p]\!] \to [\![1,p-1]\!]$, ainsi

$$g(n) = f(n) \text{ si } f(n) < a,$$
$$g(n) = f(n) - 1 \text{ si } f(n) > a,$$

et g serait une injection de $[\![1,p]\!]$ dans $[\![1,p-1]\!]$ ce qui contredirait le théorème précédent.

2) Soit $f : [\![1,p]\!] \to [\![1,p]\!]$ une surjection. Pour tout $k \in [\![1,p]\!]$, il existe $x \in [\![1,p]\!]$ tel que $f(x) = k$. On peut alors définir $g : [\![1,p]\!] \to [\![1,p]\!]$ par

$$g(k) = \min\{x \in [\![1,p]\!], f(x) = k\},$$

et g est injective, donc bijective d'après la première étape de la démonstration . Le fait que g est bijective et que $g \circ f = Id_{[\![1,p]\!]}$ montre que f est bijective.

Attaquons maintenant la notion d'ensemble fini. Alfred Tarski (1902 - 1983) a proposé une autre définition de la finitude : un ensemble E est fini si toute partie non-vide X de $\mathcal{P}(E)$, a un élément A, qui est minimal pour l'inclusion (il n'existe pas $Y \in X$, donc $Y \subset E$, tel que $Y \subset A$ et $Y \neq A$).

C) Les ensembles finis

Définition

☐ Deux ensembles E et F sont dits équipotents si et seulement s'il existe une bijection f de l'un sur l'autre. Dans ce cas, on écrit $E \sim F$. La relation d'équipollence est une relation d'équivalence entre ensembles. Une classe d'équivalence, c'est-à-dire la classe de tous les ensembles équipotents à un ensemble donné, est ce que l'on appelle une puissance ou un nombre cardinal.

☐ Si E et F sont équipotents, on notera Card E = Card F.

☐ On dit qu'un ensemble E est fini et possède n éléments si et seulement si il peut être mis en bijection avec le sous-ensemble $S_n = \{1, 2, \ldots, n\}$ des n premiers entiers naturels. On notera dans ce cas Card $E = n$.

L'ensemble E est dit infini s'il n'est pas fini.

☐ On dit que le cardinal de E est inférieur au cardinal de F (on dit aussi que E est moins puissant que F) et on écrit Card $E \leq$ Card F si et seulement s'il existe une surjection de E dans F. On dit que le cardinal de E est strictement inférieur au cardinal de F et on écrit Card $E <$ Card F si et seulement si

$$\text{Card } E \leq \text{Card } F \text{ et Card } E \neq \text{Card } F.$$

Propriété

i) La relation d'équipollence est une relation d'équivalence.

ii) Si E est un ensemble fini non vide, il existe un unique $p \in \mathbb{N}^*$ pour lequel on puisse trouver une bijection de E sur $[\![1,p]\!]$.

Preuve

i) E est équipotent à F si et seulement si il existe une bijection f de E dans F.

Réflexivité : Pour chaque ensemble E, l'identité $Id_E : E \to E$ est une bijection de E sur E.

Symétrique : Soit E un ensemble équipotent à F. Il existe alors une bijection f de E dans F. Comme l'application réciproque d'une bijection est une bijection, F est équipotent à E. Donc la

relation d'équipollence est symétrique.

Transitivité : Soit E équipotent à F et F équipotent à G. Il existe deux bijections $f : E \to F$ et $g : F \to G$. Comme la composé de deux bijections est une bijection, il existe une bijection de E dans G. On en déduit que la relation d'équipollence est transitive.

ii) Soit p et q deux tels entiers, et $f : E \to [\![1, p]\!]$, $g : E \to [\![1, p]\!]$ des bijections. Alors $g \circ f^{-1}$ est une bijection de $[\![1, p]\!]$ sur $[\![1, q]\!]$, d'où $p = q$.

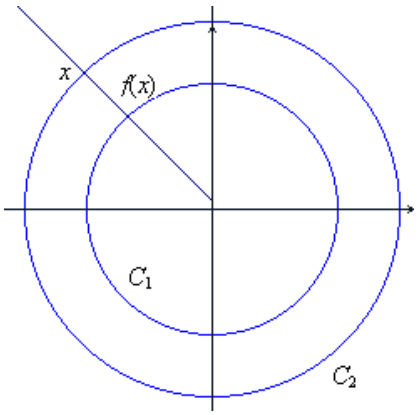
Exemple

☐ Soit $f : \mathbb{N} \to 2\mathbb{N}$ définie par $f : x \mapsto 2x$. C'est une bijection, donc $\mathbb{N}$ est équipotent à $2\mathbb{N}$.

☐ Considérons les cercles concentriques

$$C_1 = \{(x, y) \ / \ x^2 + y^2 = a^2\}, \ C_2 = \{(x, y) \ / \ x^2 + y^2 = b^2\}.$$

où $0 < a < b$. Soit $x \in C_2$ et $f : C_2 \to C_1$ une application définie comme suit :



$f(x)$ est la point d'intersection de C_1 et du rayon allant du centre de C_2 et de C_1 au point x.

L'application f est à la fois injective et surjective.

☐ **Théorème de Schroeder-Berstein** : Soient $X_1 \subset Y \subset X$. Montrons que si X est équipotent à X_1, alors X est équipotent à Y.

Puisque X est équipotent à X_1, il existe une application $f : X \to X_1$ qui est bijective. Or $Y \subset X$, donc la restriction de f à Y est aussi injective. Ainsi Y est équipotent à une partie de X_1, c'est-à-dire Y équipotent à Y_1 où

$$Y_1 \subset X_1 \subset Y \subset X$$

et il existe une application $f : X_1 \to X_2$ qui est une bijection. Par conséquent, il existe une suite d'ensembles X_1, X_2, X_3, ... tous équipotents et une autre suite d'ensembles Y_1, Y_2, Y_3, ... tous équipotents, ces deux suites étant telles que

$$\ldots \subset Y_2 \subset X_2 \subset Y_1 \subset X_1 \subset Y \subset X.$$

Soit

$$B = X \cap Y \cap X_1 \cap Y_1 \cap X_2 \cap Y_2 \cap \ldots$$

Alors

$$X = (X \backslash Y) \cup (X_1 \backslash Y_1) \cup (Y_1 \backslash X_2) \cup \ldots \cup B.$$

Notons en outre que $(X \backslash Y)$ équipotent à $(X_1 \backslash Y_1) \sim (X_2 \backslash Y_2) \sim \ldots$

De façon explicite l'application $f : (X_n \backslash Y_n) \to (X_{n+1} \backslash Y_{n+1})$ est une bijection. Considérons alors l'application $g : X \to Y$ qui est définie par

$$g(x) = \begin{cases} f(x) & \text{si } x \in X_i - Y_i \text{ ou } x \in X - Y \\ x & \text{si } x \in Y_i - X_i \text{ ou } x \in B. \end{cases}$$

g est une bijection.

Un ensemble fini étant défini, voyons ses différentes propriétés.

Lemme

Soient A et B des parties de $\mathbb{N}$.

1°) Une partie A de $\mathbb{N}$ est fini si et seulement si elle est majorée.

2°) Supposons $B \subset A$. Si A est fini, B l'est aussi. En particulier, toute intersection de parties finies de $\mathbb{N}$ est finie.

3°) Si A et B sont finies, $A \cup B$ l'est aussi.

4°) Si A est finie, $\mathbb{N}\backslash A$ est infini. En particulier, $\mathbb{N}$ est infini.

Preuve

1°) Si A est fini et non vide, il existe par définition un entier $p \in \mathbb{N}^*$ et une application bijective f de $[\![1, p]\!]$ dans A. Raisonnons par récurrence, si $p = 1$, alors $A = \{f(1)\}$ est majorée. Supposons le résultat établi pour p, et soit g une bijection de $[\![1, q]\!]$ dans A. Cette application induit une bijection de $[\![1, p]]$ sur $B = A\backslash g(q)$. D'après l'hypothèse de récurrence il existe $m \in \mathbb{N}$ tel que $x \leq m$ pour tout $x \in B$. On en déduit

$$y \leq \min\{m, g(q)\} \text{ pour tout } y \in A.$$

Réciproquement, si A est majorée, elle a un plus grand élément p. Si $p = 0$, on a $A = \{0\}$ qui est en bijection avec $\{1\}$, donc finie. Raisonnons par récurrence, et soit A une partie finie de $\mathbb{N}$ de plus grand élément q. Posons $B = A\backslash\{q\}$. Si $B = \emptyset$, on a le résultat. Supposons $B \neq \emptyset$. Alors $\max(B) \leq p$. D'après l'hypothèse de récurrence, il existe $r \in \mathbb{N}$, et une bijection $f : B \to [\![1, r]\!]$. On en déduit une bijection de A sur $[\![1, s]\!]$, en posant $g(q) = s$, et $g_{|B} = f$.

2°) Si A est majorée, et si $B \subset A$, alors B est majorée.

3°) Si A et B sont majorées par m et n, $A \cup B$ l'est par $\max\{m, n\}$.

4°) Si A et $C = N\backslash A$ sont finis, $A \cup C = \mathbb{N}$ l'est aussi, donc majoré, ce qui est contradictoire.

$\mathbb{N}$ n'étant pas majoré est infini.

Théorème fondamental

Soient E un ensemble fini, et $A \subset E$. Alors A est fini, et Card $A \leq$ Card E.

De plus, Card $A =$ Card E si et seulement si $A = E$.

Preuve

Pour $E = \emptyset$, alors $A = \emptyset$, donc A est fini.

Supposons ce cas exclu. Comme E est fini, par définition il existe une bijection f de E sur $[\![1, n]\!]$. Supposons g la bijection de A sur $f(A)$ qui coïncide avec f sur A. On sait par hypothèse que $f(E) = [\![1, n]\!]$. Comme $A \subset E$, alors $f(A) \subset f(E)$, donc $f(A) \subset [\![1, n]\!]$. Comme $[\![1, n]\!]$ est majoré, $f(A)$ est majoré, donc $f(A) = g(A)$ est fini. Comme g est une bijection de A dans $f(A)$, A est fini. Comme A est fini, il existe une bijection $h : A \to [\![1, m]\!]$ de A dans $[\![1, m]\!]$, considérons $j : A \to E$ l'injection canonique. L'application $f \circ j \circ h^{-1} : [\![1, m]\!] \to [\![1, n]\!]$ est injective comme composée d'injections. Ainsi A est fini et Card $A \leq$ Card E.

Si Card $A =$ Card E, alors $m = n$. Dans ce cas, l'application $f \circ j \circ h^{-1}$ est bijective. Il en résulte que j est bijective, d'où $A = E$.

Corollaire

1°) Si E et F sont des ensembles finis, alors $E \cap F$ l'est aussi.

2°) Si E et F sont des ensembles finis, $E \cup F$ l'est aussi.

Preuve

1°) On a $E \cap F \subset E$, l'application du théorème fondamental permet de conclure.

Par récurrence, on peut même montrer que l'intersection d'une famille d'ensembles finis est fini.

2°) Comme $E \cup F = E \cup (F \backslash E)$, on peut supposer que $E \cap F = \emptyset$.

Si $E = \emptyset$, on a $E \cup F = F$, et le résultat est clair. Supposons le établi pour $E \cup F$ avec Card $E \leq n$, et envisageons le cas où

$$\text{Card } E = n + 1 \text{ et } E \cap F = \emptyset.$$

Soient $a \in E$ et $G = E \backslash \{a\}$. D'après l'hypothèse de récurrence, il existe $n \in \mathbb{N}$, et f une bijection de $G \cup F$ sur $[\![1, n]\!]$. On définit alors une bijection de sur $[\![1, n+1]\!]$, en posant

$$\begin{cases} g(a) = n + 1 \\ g(x) = f \text{ avec } x \in G \cup F \end{cases}$$

Théorème

Soient E et F des ensembles.

1°) Si E est fini, $f(E)$ l'est aussi , et Card $f(E) \leq$ Card E.

En outre, on a Card $f(E) =$ Card E si et seulement si, f est injective.

2°) Si E est fini, et si f est surjective, alors F est fini, et Card $F \leq$ Card E.

En outre, on a Card $F =$ Card E si et seulement si, f est bijective.

3°) Si f est injective, alors E est fini si et seulement si, $f(E)$ l'est.

4°) Si F et $f^{-1}(\{y\})$ sont finis pour tout $y \in F$, alors E est fini.

5°) Si E et F sont finis, il en est de même de $E \times F$.

Démonstration

1°) Supposons E fini. Pour $y \in f(E)$, fixons $x_y \in E$ antécédent de y par f. Posons

$$A = \{x_y; y \in f(E), f(x_y) = y\}.$$

Puisque A est inclus dans E, A est fini comme partie d'un ensemble fini, et on a :

$$\text{Card } A \leq \text{Card } E.$$

Considérons maintenant l'application g de A dans $f(E)$ coïncidant avec f sur A. Par construction, g est bijective, il vient que $f(E)$ est fini et

$$\text{Card } f(E) = \text{Card } A \leq \text{Card E}.$$

D'autre part d'après le théorème fondamental, on a :

$$\text{Card } f(E) = \text{Card } E \Leftrightarrow \text{Card } A = \text{Card } E \Leftrightarrow A = E,$$

c'est-à-dire si et seulement si, f est injective.

2°) C'est un cas particulier de 1°). Comme f est surjective, il vient $F = f(E)$. E étant fini, $f(E)$ l'est aussi d'après 1°). Par conséquent, F est également fini et on a :

$$\text{Card } F = \text{Card } f(E) \leq \text{Card } E.$$

Par ailleurs toujours d'après 1°), on a :

$$\text{Card } F = \text{Card } f(E) = \text{Card } E \Leftrightarrow f \text{ est injective},$$

c'est-à-dire f est bijective.

3°) Supposons f injective. D'après 1°), on a :

$$E \text{ fini} \Rightarrow f(E) \text{ fini}.$$

Inversement, supposons $f(E)$ fini. Comme f est injective, on a :

$$\text{Card } f(E) = \text{Card } E.$$

Pour $y \in f(E)$, on peut choisir $x_y \in E$ tel que $f(x_y) = y$. Posons

$$A = \{x_y \in E \ / \ f(x_y) = y\}.$$

A est une partie de E. L'application $g : A \to f(E)$ coïncidant avec f est une bijection. Il vient

$$\text{Card } f(E) = \text{Card } A = \text{Card } E \Leftrightarrow A = E$$

et f est une bijection.

4°) Définissons une relation d'équivalence $\Re$ sur E dite associé à f, en convenant :

$$x \Re y \Leftrightarrow f(x) = f(y).$$

L'application f est alors compatible avec $\Re$. Soit $\varphi : E \to E\backslash\Re$ la surjection canonique et $g : E\backslash\Re \to F$ l'unique application telle que $f = g \circ \varphi$.

Montrons que g est injective. Si $g(\overline{x}) = g(\overline{y})$, on a

$$f(x) = g(\overline{x}) = g(\overline{y}) = f(y).$$

Par suite, $x \Re y$ et $\overline{x} = \overline{y}$. Donc l'application g est injective.

Soit $j : f(E) \to F$ l'injection canonique, et $\overline{f}$ la bijection de $E\backslash\Re$ dans $f(E)$ coïncidant avec g sur $E\backslash\Re$. Il vient

$$f = j \circ \overline{f} \circ \varphi.$$

Comme $f(E)$ est inclus dans F, $f(E)$ est fini comme partie d'un ensemble fini. Comme $\overline{f}$ est bijective de $f(E)$ sur $E\backslash\Re$, on en déduit que $E\backslash\Re$ est aussi fini. Dans ce cas, E est réunion d'un nombre fini de classes $f^{-1}(\{y\})$ pour $y \in F$, donc est fini.

5°) Soit $p : E \times F \to E$ la projection canonique. Pour $a \in E$ fixé, l'application

$$f : F \to \{a\} \times F,\ y \mapsto (a, y)$$

est bijective. En effet, l'application f admet une application réciproque, donc f est bijective. Par suite

$$\text{Card } p^{-1}(\{a\}) = \text{Card } F.$$

Comme $p^{-1}(\{a\})$ et E sont finis, $E \times F$ est fini par application de 4°).

Théorème

Soient E, F deux ensembles finis équipotents et une application de E dans F. Les conditions suivantes sont équivalentes :

i) f est injective

ii) f est bijective

iii) f est surjective.

Démonstration

Montrons (i) ⇒ (ii). Si f est injective, alors d'après le théorème précédent

$$\text{Card } f(E) = \text{Card } E.$$

Comme E et F sont équipotents, il vient

$$\text{Card } E = \text{Card } F.$$

$f(E)$ étant une partie de F, on a

$$\text{Card } f(E) = \text{Card } F \Leftrightarrow f(E) = F.$$

f est donc surjective, c'est-à-dire bijective.

L'implication (ii) ⇒ (iii) est évidente.

Montrons (iii) ⇒ (i). Le résultat est clair si $E = F = \emptyset$. Supposons E et F non vides.

Comme f est surjective, il existe un élément $s(y)$ de $f^{-1}(\{y\})$. Ceci définit une application $s : F \to E$ telle que

$$f \circ s = Id_F.$$

L'application s ainsi définie est injective et l'implication (i) $\Rightarrow$ (ii) montre que s est bijective. Par suite

$$f = f \circ s \circ s^{-1} = Id_F \circ s^{-1} = s^{-1}$$

et f est injective.

D) Ensembles dénombrables

Définition

☐ On appelle puissance du dénombrable et on notera $\aleph_0$ (lire Aleph 0, c'est la première lettre de l'alphabet hébraïque) la puissance de l'ensemble $\mathbb{N}$.

☐ Un ensemble est dit dénombrable s'il est équipotent à $\mathbb{N}$, c'est-à-dire si son cardinal est $\aleph_0$.

☐ Un ensemble est dit au plus dénombrable s'il est fini ou dénombrable.

Propriété

i) Toute partie de $\mathbb{N}$ est dénombrable.

ii) Soient E un ensemble dénombrable et A une partie de E. Alors A est au plus dénombrable.

iii) Si $f : E \to F$ est une injection et F dénombrable, alors E est dénombrable.

iv) Si $f : E \to F$ est une surjection et E dénombrable, alors F est dénombrable.

v) Un ensemble E est dénombrable si et seulement si il existe une surjection de $\mathbb{N}$ sur E.

Preuve

i) Soit A une partie de $\mathbb{N}$. Si A est finie, il n'y a rien à prouver. Supposons A infinie et définissons

$$f : \mathbb{N} \to A,\ n \mapsto a_n,$$

par récurrence en posant $a_0 = \min A$ et, pour $n \geq 1$, $a_n = \min\{A \backslash \{a_0, ..., a_{n-1}\}\}$ (qui existe car, A étant infinie, on a $A \neq \{a_0, ..., a_{n-1}\}$). Par construction, la suite (a_n) est strictement croissante. Il est alors clair que f est injective, car f est strictement monotone. Montrons maintenant par l'absurde que f est aussi surjective, c'est-à-dire f bijective.

Soit F l'image de A par f. Si f n'est pas surjective, il existerait $a \in A$ tel que $f(n) \neq a$ pour tout n. Mais si

$$a \in A \backslash \{a_0, ..., a_{n-1}\},$$

alors $a > f(n) \geq n$ pour tout n, c'est une contradiction avec le fait que $\mathbb{N}$ est archimédien.

On peut aussi raisonner de la façon suivante :

$$a \in A \backslash F \Rightarrow a_n \leq a,\ \forall n \in \mathbb{N} \Rightarrow F \subset [\![0, a]\!].$$

Comme f est injective, on voit alors que $\mathbb{N}$ est fini. Il y a contradiction. Par suite, f est bijective.

ii) Si E est fini, toute partie de E est finie. Supposons que E est infini. Alors, il existe une bijection f de $\mathbb{N}$ sur E. Pour toute partie A de E, on a $f^{-1}(A) \subset \mathbb{N}$. D'après i), $f^{-1}(A)$ est dénombrable.

Si $f^{-1}(A)$ est fini, alors $A = f(f^{-1}(A))$ est également finie.

Si $f^{-1}(A)$ est infini, il existe une bijection g de $\mathbb{N}$ sur $f^{-1}(A)$ et on obtient une bijection $f \circ g$ de $\mathbb{N}$ sur A.

iii) Comme f est injective, f est une bijection de E sur $f(E)$. Mais $f(E) \subset F$ avec F dénombrable, $f(E)$ est dénombrable comme partie d'un ensemble dénombrable. Ainsi, E est dénombrable.

iv) L'application f étant une surjection, on peut définir $g : F \to E$ pour tout $b \in F$ par

$$g(b) = \min\{f^{-1}(\{b\})\}.$$

Il vient $f \circ g = Id_F$. Par suite, g est injective. D'après iii), F est dénombrable.

v) Si E est dénombrable, il existe une bijection de $\mathbb{N}$ sur E, c'est-à-dire une surjection de $\mathbb{N}$ sur E.

La réciproque est une conséquence de iii).

Lemme

1°) On a :

Card $]0,1[$= Card $[0,1[$= Card $]0,1]$ = Card $[0,1]$ = Card $]a,b[$= Card $[a,b[$= Card $]a,b]$ = Card $[a,b]$.

2°) Card $]0,1[$= Card $\mathbb{R}$.

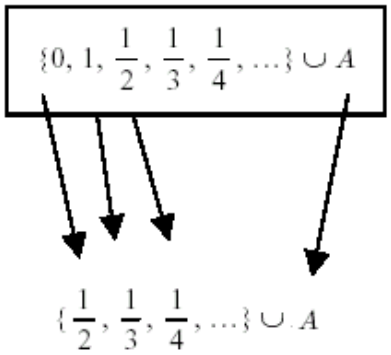
Preuve

1°) Remarquons que

$$[0,1] = \{0, 1, \frac{1}{2}, \frac{1}{3}, \ldots\} \cup A$$
$$]0,1[= \{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\} \cup A$$

où $A = [0,1]\backslash\{0, 1, \frac{1}{2}, \frac{1}{3}, \ldots\} =]0,1[\backslash\{\frac{1}{2}, \frac{1}{3}, \ldots\}$.

Considérons l'application $f : [0,1] \to]0,1[$ définie par



Autrement dit

$$f : x \mapsto \begin{cases} \frac{1}{2} & \text{si } x = 0 \\ \frac{1}{n+2} & \text{si } x = \frac{1}{n} \\ x & \text{si } x \neq 0, \frac{1}{n}. \end{cases} , n \in \mathbb{N}.$$

Il est clair que f est une bijection.

L'application $f : [0,1] \to [0,1[$ définie par

$$f : x \mapsto \begin{cases} \frac{1}{n+1} & \text{si } x = \frac{1}{n} \\ x & \text{si } x \neq \frac{1}{n} \end{cases}$$

est une bijection.

L'application $f : [0,1[\to]0,1]$ définie par $f : x \mapsto 1 - x$ est une bijection.

Soit l'application $f : x \mapsto a + (b-a)x$

$$[0,1] \to [a,b],\ [0,1[\to [a,b[$$
$$]0,1[\to]a,b[,\ ]0,1] \to]a,b]$$

est une bijection.

2°) L'application de $]0,1[$ dans $\mathbb{R}$ définie par $f : x \mapsto \dfrac{1-2x}{x\,(x-1)}$ est une bijection. En effet, on a :

$$f' : x \mapsto \frac{2x^2-2x+1}{x^2\,(1-x)^{\,2}}.$$

On voit bien que $f'(x) > 0$, $\forall x \in]0,1[$, car le numérateur a un discriminant négatif. f continue et strictement croissante de $]0,1[$ dans $]-\infty,+\infty[$ est bijective.

Théorème

i) Tout ensemble infini X contient un sous-ensemble D qui est dénombrable.

ii) Un produit fini d'ensembles dénombrables l'est aussi.

Preuve

i) L'axiome du choix permet d'affirmer l'existence d'une fonction $f : P(X) \to X$ tel que pour toute partie non vide A, $f(A) \in A$. Considérons la suite

$$\begin{aligned} a_1 &= f(X) \\ a_2 &= f(X\backslash\{a_1\}) \\ a_3 &= f(X\backslash\{a_1,a_2\}) \\ &... \\ a_n &= f(X\backslash\{a_1,\ldots,a_{n-1}\}. \end{aligned}$$

L'ensemble X étant infini, pour tout $n \in \mathbb{N}$ l'ensemble $X\backslash\{a_1,\ldots,a_{n-1}\}$ est non vide. La fonction f est une fonction de choix, donc pour tout $n > 0$ et tout $i < n$, on a $a_n \neq a_i$. Les éléments $a_n \in X$ sont donc tous distincts et $D = \{a_1, a_2, \ldots\}$ est une partie dénombrable de X.

ii) Par récurrence, on se ramène au produit de deux ensembles dénombrables, et il suffit de prouver que $E = \mathbb{N}^2$ est dénombrable. Pour $n \in \mathbb{N}$, posons $u_n = 0 + 1 + ... + n$.

L'application $n \mapsto u_n$ est strictement croissante. On en déduit facilement que, pour $b \in \mathbb{N}$, il existe un unique entier p tel que $u_p \leq b \leq u_{p+1}$. Soit $f : E \to \mathbb{N}$, $(x,y) \mapsto y + u_{x+y}$. Prouvons que f est bijective.

– Soit $a \in \mathbb{N}$. Il existe un unique entier m tel que $u_m \leq a \leq u_{m+1}$. Posons $v = a - u_m$.On a

$$0 < v < u_{m+1} - u_m = m + 1.$$

On peut donc définir $u = m - v$, et il vient $f(u,v) = a$; l'application f est surjective.

– Soient x, $y \in \mathbb{N}$, $a = f(x,y)$, et m l'unique entier tel que $u_m \leq a < u_{m+1}$. On a

$$u_{x+y} \leq a < a + x + 1 = u_{x+y+1}.$$

Par suite, $m = x + y$. Alors $y = a - u_m$ et $x = m - y$, f est injective.

Théorème

1°) Une suite infinie composée d'éléments distincts est dénombrable.

2°) Card $\mathbb{N}$ = Card $\mathbb{N} \times \mathbb{N}$.

3°) Soit $\{A_1, A_2, \ldots\}$ une suite dénombrable d'ensembles dénombrables deux à deux disjoints.

Alors $\bigcup_{i=1}^{+\infty} A_i$ est aussi un ensemble dénombrable.

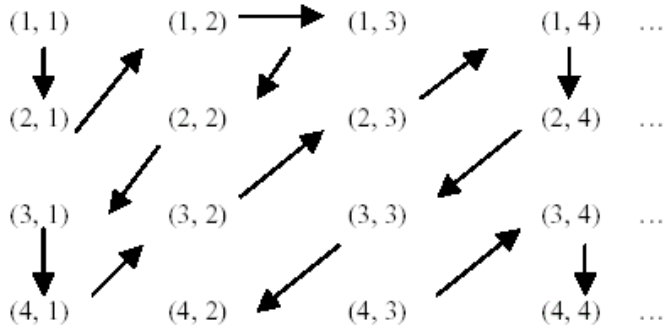
4°) Card $\mathbb{N}$ = Card $\mathbb{Z}$ = Card $\mathbb{Z} \times \mathbb{Z}$ = Card $\mathbb{Q} \neq$ Card $\mathbb{R}$.

Démonstration

1°) Une suite est essentiellement une fonction $f : n \mapsto u_n$ ayant pour domaine de définition $\mathbb{N}$. Donc si les u_n sont distincts, la fonction f est une bijection.

2°) **$1^{ère}$ preuve**

Montrons que Card $\mathbb{N}$ = Card $\mathbb{N}\times\mathbb{N}$. Pour cela, représentons le produit $\mathbb{N}\times\mathbb{N}$ de la façon suivante :



L'ensemble produit $\mathbb{N} \times \mathbb{N}$ est donc décrit par la suite infinie

$$u_0 = (0,0),\ u_1 = (1,1),\ u_2 = (2,1),\ u_3 = (1,3),\ \ldots$$

Ainsi Card $\mathbb{N}$ = Card $\mathbb{N} \times \mathbb{N}$.

2ème preuve

De façon plus formelle, on peut également trouver une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$. Ainsi, l'application f de $\mathbb{N}^2$ dans $\mathbb{N}$ est-elle une bijection :

$$f : (s,t) \mapsto \frac{(s+t)\,(s+t+1)}{2} + t.$$

Comme Card $\mathbb{N} \leq$ Card $\mathbb{N}^2$, pour montrer que f est une bijection, il suffit de vérifier que f est injective. Supposons que

$$f(s,t) = f(s',t').$$

On a plusieurs cas :

− si $s + t = s' + t'$, alors

$$\frac{(s+t)\,(s+t+1)}{2} + t = \frac{(s'+t')\,(s'+t'+1)}{2} + t' \Rightarrow t = t' \text{ et donc } s = s'.$$

− si $s + t < s' + t'$, alors

$$\begin{aligned} 2[f(s',t') - f(s,t)] &= (s'+t')(s'+t'+1) - (s+t)(s+t+1) + 2(t'-t) \\ &\geq (s+t+1)(s+t+2) - (s+t)(s+t+1) + 2(t\prime - t) \\ &\geq 2(s+t+1) + 2(t\prime - t) \\ &\geq 2(s+1) + 2t\prime. \end{aligned}$$

Cette quantité ne peut être nulle, donc contradiction avec le fait que $f(s,t) = f(s',t')$. De là, on en déduit que f est bijective.

2°) Puisque les ensembles A_i sont dénombrables, on peut écrire

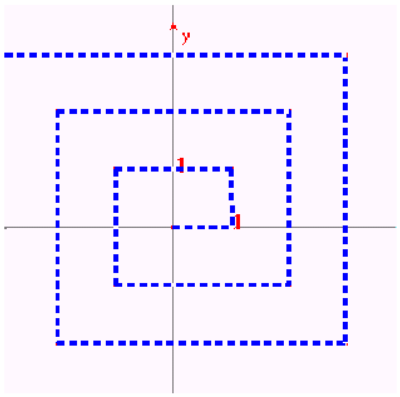
$$\begin{aligned} A_1 &= \{a_{11}, a_{12}, a_{13}, \ldots\} \\ A_2 &= \{a_{21}, a_{22}, a_{23}, \ldots\} \\ &\ldots \\ A_n &= \{a_{n1}, a_{n2}, a_{n3}, \ldots\}. \end{aligned}$$

Alors $\bigcup_{i=1}^{+\infty} A_i = \{a_{ij} \ / \ (i,j) \in \mathbb{N} \times \mathbb{N}\}$. Il est clair que la fonction $f : \bigcup_{i=1}^{+\infty} A_i \to \mathbb{N} \times \mathbb{N}$ définie par $f(a_{ij}) = (i,j)$ est une bijection. Par conséquent $\bigcup_{i=1}^{+\infty} A_i$ est dénombrable puisque $\mathbb{N} \times \mathbb{N}$ est dénombrable.

4°) Montrons que Card $\mathbb{N}$ = Card $\mathbb{Z}$. Pour cela, considérons l'application

$$\begin{array}{lll} f:0 & \mapsto & 0 \\ 1 & \mapsto & -1 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & -2 \\ 4 & \mapsto & 2 \\ & \ldots & \\ n & \mapsto & \frac{(-1)^n}{2}[n+\frac{1-(-1)^n}{2}] \end{array}$$

C'est bien une bijection.



Montrons que Card $\mathbb{N}$ = Card $\mathbb{Z} \times \mathbb{Z}$. On peut visualiser de la manière suivante :
L'ensemble $\mathbb{Z} \times \mathbb{Z}$ est ainsi décrit par la suite infinie composée d'éléments distincts :

$$u_0 = (0,0),\ u_1 = (1,0),\ u_2 = (1,1),\ u_3 = (0,1)\ \ldots$$

Montrons que Card $\mathbb{N}$ = Card $\mathbb{Q}$.

1ère preuve

Fixons n, il est clair que Card $S_n = \{\frac{m}{n} \ / \ m \in \mathbb{Z}\}$ = Card $\mathbb{Z}$. Donc S_n est dénombrable. Ecrivons ensuite $\mathbb{Q} = \bigcup_{n\in\mathbb{N}} S_n$, ce qui implique que $\mathbb{Q}$ est dénombrable.

2ème preuve

On peut aussi raisonner de la façon suivante : il est clair que l'on peut écrire

$$\mathbb{Q} = \mathbb{Q}_- \cup \{0\} \cup \mathbb{Q}_+.$$

Considérons l'application

$$f : \mathbb{Q}^+ \to \mathbb{N} \times \mathbb{N}$$

définie par

$$f : \frac{p}{q} \mapsto (p,q),\ p \text{ et } q \text{ premiers entre eux}$$

où $\frac{p}{q}$ est un rationnel arbitraire. La fonction f est injective et donc

$$\text{Card } \mathbb{Q} \leq \text{Card } \mathbb{N} \times \mathbb{N} = \text{Card } \mathbb{N}.$$

D'autre part, l'application $n \mapsto n$ de $\mathbb{N}$ dans $\mathbb{Q}$ est injective et on a :

$$\text{Card } \mathbb{N} \leq \text{Card } \mathbb{Q}.$$

En conséquence, Card $\mathbb{N}$ = Card $\mathbb{Q}$.

Montrons maintenant que Card $\mathbb{N} \neq$ Card $\mathbb{R}$.

1ère preuve

On a vu que l'application

$$f :]0,1[\to \mathbb{R}$$
$$x \mapsto \frac{2x^2 - 2x + 1}{x^2 (1-x)^2}$$

est une bijection. Par conséquent, $\mathbb{R}$ n'est pas dénombrable si et seulement si $]0,1[$ n'est pas dénombrable. Pour montrer que $]0,1[$ n'est pas dénombrable, on peut raisonner par l'absurde et supposer que les nombres de $]0,1[$ peuvent être rangé en une suite u_1, u_2, u_3, ...

Posons

$$A =]0,1[= \{u_1, u_2, \ldots\}.$$

Construisons maintenant une suite d'intervalles de la façon suivante. Considérons les trois intervalles de A :

$$[0, \frac{1}{3}],\ [\frac{1}{3}, \frac{2}{3}],\ [\frac{2}{3}, 1] \ (1)$$

ayant chacun une longueur $\frac{1}{3}$. Le nombre x_1 ne peut appartenir à la fois aux trois intervalles. Soit

$$I_1 = [a_1, b_1]$$

l'un des intervalles (1) qui est tel que $x_1 \notin I_1$.

Considérons maintenant les trois intervalles suivants inclus dans $I_1 = [a_1, b_1]$

$$[a_1, a_1 + \frac{1}{3}],\ [a_1 + \tfrac{1}{9}, a_1 + \tfrac{2}{9}],\ [a_1 + \tfrac{2}{9}, b_1] \ (2)$$

ayant chacun une longueur $\frac{1}{9}$. Comme précédemment, soit I_2 l'un des intervalles (2) qui est tel que $x_2 \notin I_2$.

En poursuivant de la même façon ces opérations, nous obtenons une suite d'intervalles fermés

$$I_1 \supset I_2 \supset I_3 \supset \ldots \ (3)$$

Qui sont tels que $x_n \notin I_n$ pour tout $n \in \mathbb{N}$. A l'aide du théorème des intervalles fermés emboîtés sur $\mathbb{R}$, on voit qu'il existe un réel $y \in A = [0,1]$ tel que y appartient à tout intervalle de (3).

Mais

$$y \in A = \{x_1, x_2, \ldots\} \Rightarrow y = x_{m_0} \text{ où } m_0 \in \mathbb{N}.$$

Alors par construction, $y = x_{m_0} \notin I_{m_0}$ ce qui est en contradiction avec le fait que y appartient à chacun des intervalles (3). Cette démonstration est connue sous le nom de diagonalisation de Cantor.

$2^{ème}$ preuve

Donnons une deuxième démonstration du fait que $\mathbb{R}$ n'est pas dénombrable. S'il l'était, il en serait de même de $[0,1[$. Considérons alors une énumération $(x_n)_{n \in \mathbb{N}^*}$ de $[0,1[$, obtenue au moyen d'une bijection

$$f : \mathbb{N}^* \to [0,1[,\ n \mapsto x_n,$$

et considérons le développement décimal des x_n.

$$\begin{array}{rcl} x_1 & = & 0, a_{11}a_{12}a_{13}...a_{1p}... \\ x_2 & = & 0, a_{21}a_{22}a_{23}...a_{2p}... \\ & .. & \\ x_n & = & 0, a_{n1}a_{n2}a_{n3}...a_{np}... \\ & .. & \end{array}$$

a_{np} est le $p^{ème}$ chiffre de la décomposition décimale de x_n. C'est un élément de $\{0,1,...,9\}$. Considérons maintenant l'élément y de $]0,1[$ défini de la façon suivante :

$$y = 0, b_1 b_2 b_3 ... b_p ... \text{ où } b_p = 0 \text{ si } a_{pp} \neq 0 \text{ et } b_p = 1 \text{ si } a_{pp} = 0.$$

Il est clair que y appartient à $[0,1[$. Mais, son développement décimal est distinct de tous les x_n car :

$$\forall n,\ b_n \neq a_{nn}.$$

Ainsi, il existe un $y \in [0,1[$ tel que

$$y \notin f(\mathbb{N}^*),$$

c'est-à-dire que $f(\mathbb{N}^*)$ est strictement inclus dans $[0,1[$, ce qui implique que f n'est pas surjective. Cela est contradictoire avec le fait que f est bijective. Donc $\mathbb{R}$ n'est pas dénombrable.

Exemple

□ Soit P l'ensemble de tous les polynômes à coefficients entiers et A l'ensemble des nombres algébriques. On rappelle qu'une racine d'un polynôme de P est un nombre algébrique. Montrons que P et A sont dénombrable. Soit $(n,m) \in \mathbb{N} \times \mathbb{N}$. Notons P_{nm} l'ensemble des polynômes $P(X)$ de degré égal à m tel que :

$$|a_0| + |a_1| + \ldots + |a_m| = n.$$

Notons que l'ensemble P_{nm} est fini et que

$$P = \bigcup\{P_{nm} \ / \ (n,m) \in \mathbb{N} \times \mathbb{N}\}.$$

P est une réunion au plus dénombrable d'ensembles au plus dénombrables. Comme P est un ensemble infini, P est dénombrable. Ceci permet d'affirmer que l'ensemble E des équations algébriques à coefficients entiers est dénombrable

$$E = \{P_1(x) = 0, P_2(x) = 0, \ldots\}$$

Soit $A_i = \{x \ / \ x$ est solution de $P_i(x) = 0\}$. Comme un polynôme de degré n admet au plus n racine, chaque ensemble A_i est fini. Donc

$$A = \bigcup\{A_i, i \in \mathbb{N}\}$$

est un ensemble dénombrable.

Puisque l'ensemble des nombres algébriques est dénombrable et $\mathbb{R}$ non dénombrable, l'ensemble des nombres transcendants existe.

□ Donnons enfin une conséquence curieuse de ce qui précède en informatique. On peut montrer que l'ensemble de tous les algorithmes possibles est dénombrable, alors que l'ensemble des fonctions de $\mathbb{N}$ dans $\mathbb{N}$ est équipotent à $\mathbb{R}$. Il y a donc des fonctions de $\mathbb{N}$ dans $\mathbb{N}$ qui ne sont calculables par aucun ordinateur. Aucun algorithme ne permet de les calculer. De telles fonctions ont été explicitement définies.

□ Prouvons que $\mathbb{R}$ est équipotent à $\mathcal{P}(\mathbb{N})$. A toute partie X de $\mathbb{N}$, on peut faire correspondre un développement décimal $x_n = 0, a_1a_2a_3...a_p...$ d'un élément de $[0,1[$ suivante $a_p = 0$ si $n-1 \in X$, 0 sinon. Et bien, il est clair que l'application $X \mapsto x_n$ est une injection de $\mathcal{P}(\mathbb{N})$ dans $[0,1[$, c'est-à-dire

$$\text{Card } \mathcal{P}(\mathbb{N}) \leq \text{Card } [0,1[.$$

Considérons maintenant le développement $x_n = 0, a_1a_2a_3...a_p...$ en base 2 ($a_p = 0$ ou 1) d'un élément $[0,1[$. L'application qui à x_n fait correspondre la partie de $\mathbb{N}$ ayant pour fonction caractéristique $n \mapsto a_n$ est une bijection de $[0,1[$ sur l'ensemble des parties de $\mathbb{N}$ n'ayant pas un complémentaire fini.

On peut aussi prouver que les trois ensembles suivants sont équipotents : $\mathcal{P}(\mathbb{R})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ et $C_0(\mathbb{R})$ ensemble des fonctions continues sur $\mathbb{R}$.

□ Signalons également une question étonnante. Peut-on trouver un ensemble E compris entre $\mathbb{N}$ et $\mathbb{R}$, mais qui ne soit équipotent ni à $\mathbb{N}$, ni à $\mathbb{R}$? On aurait seulement des injections de $\mathbb{N}$ dans E et de E dans $\mathbb{R}$. Rappelons que $\mathbb{Q}$ ne répond pas à la question puisqu'il est en bijection avec $\mathbb{N}$. On a prouvé qu'il était impossible de répondre à cette question. Cela ne signifie pas qu'on

n'ait pas encore trouvé si cette propriété était vraie ou fausse, mais bel et bien qu'on ne peut ni prouver qu'elle est vraie, ni prouver qu'elle est fausse. Elle est dite indécidable. Elle ne découle pas des axiomes de la théorie des ensembles, pas plus que sa négation. Cela signifie également qu'on peut prendre comme axiome supplémentaire l'existence d'un tel ensemble E sans apporter de contradiction à l'édifice des Mathématiques, ou au contraire, de prendre comme axiome la non-existence de E. Dans ce dernier cas, on adopte ce qu'on appelle l'hypothèse du continu. L'un ou l'autre choix conduit donc à deux théories mathématiques différentes.

II) Dénombrement

A) Propriété des cardinaux

Définition

☐ Pour tout entier, l'entier

$$A = n(n-1)...2.1$$

se note $n!$ (lire n factorielle) et s'appelle factorielle de n.

☐ Cette fonction de $\mathbb{N}$ dans $\mathbb{N}$ peut être aussi définie de façon récursive :

$$0! = 1! = 1 \text{ et } n! = n.(n-1)!$$

Théorème

Deux ensembles finis ont même nombre d'éléments s'ils peuvent être mis en bijection.

Preuve

Soient E et F deux ensembles finis et f une application de E dans F. On aura alors

$$\text{Card } f(E) \leq \inf \{\text{Card } E, \text{Card } F\}.$$

En effet, soient y_1, y_2, ..., y_r des éléments de $f(E)$, on sait que

$$\text{Card } E = \sum_{i=1}^{r} \left[\text{Card } \left(f^{-1}\left(\{y_i\}\right)\right)\right] \text{ si } i \in [\![1, r]\!],$$

alors

$$\text{Card } \left[f^{-1}\left(\{y_i\}\right)\right] \geq 1 \Rightarrow \sum_{i=1}^{r} \text{Card } \left[f^{-1}\left(\{y_i\}\right)\right] \geq r.$$

Or Card $f(E) = r$, donc Card $f(E) \leq$ Card E. Puisque $f(E)$ est une partie de F,

$$\text{Card } f(E) \leq \text{Card } F,$$

donc

$$\text{Card } f(E) \leq \inf \{\text{Card } E, \text{Card } F\}.$$

Pour que f soit injective, il faut et il suffit que Card $f(E) =$ Card E. Pour que f soit surjective, il faut et il suffit que Card $f(E) =$ Card F. Donc on en déduit que pour que Card $E =$ Card F, il faut et il suffit que f soit bijective.

Propriété

Pour un intervalle d'entiers naturels, si $p \leq q$, on a

$$\text{Card } [\![p, q]\!] = q - p \text{ et Card } [\![p, q]\!] = q - p + 1.$$

Preuve

Si $p \leq q$, il existe un entier naturel r tel que $p + r = q$. L'application $x \mapsto p + x$ est une bijection de $[\![0, r]\!]$ sur $[\![p, q]\!]$, donc Card $[\![p, q]\!]$ = Card $[\![0, r]\!] = r = q - p$.

Montrons que Card $[\![p, q]\!] = q - p + 1$. On a $[\![p, q]\!] = [\![p, q]\!] \cup \{q\}$ et $[\![p, q]\!] \cap \{q\} = \emptyset$ donc

$$\text{Card } [\![p, q]\!] = \text{Card } [\![p, q]\!] \cup \{q\} = \text{Card } [\![p, q]\!] + \text{Card } \{q\} - \text{Card } [\![p, q]\!] \cap \{q\}.$$

Théorème

i) Si A et B sont des ensembles finis et disjoints, on a

$$\text{Card } A + \text{Card } B = \text{Card } (A \cup B).$$

ii) Si E et A sont deux ensembles tels que $A \subset E$, on a alors Card $\complement_E A$ = Card $E -$ Card A.

iii) Si E et F sont deux ensembles finis, on a alors

$$\text{Card } (E \cup F) = \text{Card } E + \text{Card } F - \text{Card } (E \cap F).$$

Preuve

i) Soit a = Card A et b = Card B. Par définition, $[\![1, a]\!]$ et A sont équipotents, donc il existe une bijection f de A sur $[\![1, a]\!]$. De même, il existe une bijection g de B sur $[\![a + 1, a + b]\!]$. On définit

$$h : A \cup B \to [\![1, a + b]\!]$$

comme suit :

– si $x \in A$, alors $h(x) = f(x)$.

– si $x \in B$, alors $h(x) = g(x)$.

L'application h est une bijection car les restrictions à A et à B sont respectivement f et g. On en déduit que

$$A \cup B$$

est un ensemble fini, de cardinal

$$a + b = \text{Card } A + \text{Card } B = \text{Card } (A \cup B).$$

ii) On a $E = A \cup \complement_E A$. Alors

$$\text{Card } E = \text{Card } (A \cup \complement_E A) = \text{Card } A + \text{Card } \complement_E A$$

car A et $\complement_E A$ sont disjoints. D'où

$$\text{Card } \complement_E A = \text{Card } E - \text{Card } A$$

iii) On peut écrire

$$E \cup F = \complement_E (E \cap F) \cup \complement_F (E \cap F) \cup (E \cap F)$$

Or

$$\complement_E (E \cap F), \complement_F (E \cap F) \text{ et } (E \cap F)$$

sont trois ensembles disjoints. On a alors

$$\text{Card } (E \cup F) = \text{Card } \complement_E (E \cap F) + \text{Card } \complement_F (E \cap F) + \text{Card } (E \cap F).$$

Donc,

$$\text{Card } (E \cup F) = \text{Card } E + \text{Card } F - \text{Card } (E \cap F).$$

Par récurrence, on montre très facilement que Card $\left(\bigcup_i E_i\right) \leq \sum_i$ Card (E_i).

Pour compter des moutons, on compte le nombre de pattes et on divise par 4, ce principe s'appelle le principe des bergers. D'une façon abstraite, il s'énonce :

Théorème (Principe des bergers)

Soient E, F des ensembles finis et f une application de E dans F.

i) Si, pour tout $y \in E$, $f^{-1}(\{y\})$ est fini, alors E est fini et Card $E \leq \sum_{y\in F} \text{Card}\big(f^{-1}(\{y\})\big)$.

ii) On suppose que f est surjective et qu'il existe un entier p tel que Card $f^{-1}(\{y\}) = p$ pour tout y de F. Alors, l'ensemble E est fini et on a Card $E = p$ Card $f^{-1}(\{y\})$.

Preuve

i) E est un ensemble fini et on a

$$E = \bigcup_{y\in F} f^{-1}(\{y\}).$$

Par conséquent,

$$\text{Card } (E) \leq \text{Card } \left(f^{-1}(\{y\})\right) + ... + \text{Card } \left(f^{-1}(\{y\})\right),$$

d'où

$$\text{Card } (E) \leq \sum_{y\in F} \text{Card } \left(f^{-1}(\{y\})\right).$$

ii) Si Card $\left(f^{-1}(\{y\})\right) = p$, alors d'après i), on a : Card $(E) \leq p\cdot$Card $\left(f^{-1}(y)\right)$. Or f est surjective, cela veut dire que Card $(E) \geq$Card(F). Comme

$$\text{Card } (F) = \sum_{y\in F} \text{Card } \left(f^{-1}(\{y\})\right) = p \cdot \text{Card } \left(f^{-1}(\{y\})\right)$$

et l'inégalité est antisymétrique, on a :

$$\text{Card } (E) = p \cdot \text{Card } \left(f^{-1}(\{y\})\right).$$

Remarque

On a une autre forme du principe des Bergers : soit $f : E \to F$ telle que

$$\forall y \in F, \text{ Card } f^{-1}(\{y\}) = p,$$

alors

$$\text{Card } E = p \text{ Card } F.$$

Si on enlève l'hypothèse de la surjectivité de f, le principe des Bergers est encore vrai parce que $(f^{-1}(\{y\})_{y\in F}$ forme une partition de E. En effet comme f est une application, la famille $(f^{-1}(\{y\})_{y\in F}$ est constituée d'ensembles deux à deux disjoints de E car pour $i \neq j$ les ensembles

$$f^{-1}(\{y_i\}) = \{x \in E \mid f(x) = y_i\} \text{ et } f^{-1}(\{y_j\}) = \{x \in E \mid f(x) = y_j\}$$

n'ont pas d'éléments x commun. Dans ce cas,

$$\text{Card } E = \sum_{y\in F} \text{Card } f^{-1}(y) = \sum_{y\in F} p = np.$$

Théorème (de Cantor)

Soit E un ensemble et $\mathcal{P}(E)$ l'ensemble des parties de E.

i) Il n'existe aucune surjection de E sur $\mathcal{P}(E)$.

ii) Card $\mathcal{P}(E) >$ Card E.

Preuve

i) Supposons qu'il existe une surjection $f : E \to \mathcal{P}(E)$. On considère A l'ensemble des éléments de E n'appartenant pas à l'ensemble qui est leur image, c'est-à-dire :

$$A = \{x \in E; x \notin f(x)\}.$$

L'ensemble A est une partie de E, donc $A \in \mathcal{P}(E)$. Puisque l'application f est surjective, il existe $a \in E$ tel que $f(a) = A$. La question qui se pose est alors : a appartient-il à A oui ou non ?

$-$ si $a \in A$, alors par définition de A : $a \notin f(a) = A$.

$-$ si $a \notin A$, alors par définition de A : $a \in f(a) = A$.

Dans tous les cas, on aboutit à une contradiction.

ii) Cela est évident si E est fini, à n éléments, puisqu'alors $\mathcal{P}(E)$ possède 2^n éléments, et pour tout n, $2^n > n$. Cela reste encore vrai lorsque E est infini. En effet, l'application $g : E \to \mathcal{P}(E)$ qui assigne à chaque élément $x \in E$ le singleton $\{x\}$ c'est-à-dire $g(x) = \{x\}$ est injective. Donc

$$\text{Card } E \leq \text{Card } \mathcal{P}(E).$$

Si nous prouvons que E n'a pas le même puissance que $\mathcal{P}(E)$, le théorème sera démontré. D'après i), il n'existe aucune surjection de E sur $\mathcal{P}(E)$, donc il n'existe aucune bijection de E sur $\mathcal{P}(E)$. Finalement, on a

$$\text{Card } \mathcal{P}(E) > \text{Card } E.$$

Propriété (Formule de Poincaré (appelé aussi formule du crible)

Soient E un ensemble fini et $A_1, \ldots, A_n$ des parties de E. Posons $I = \{1, 2, \ldots, n\}$, il vient

$$\text{Card } \Big(\bigcup_{i=1}^{n} A_i\Big) = \sum_{J \subset I} (-1)^{1+ \text{ Card } (J)} \text{ Card } \Big(\bigcap_{i=1}^{n} A_i\Big).$$

Preuve

On peut démontrer cela par récurrence. Il est clair que, pour $n = 1$, on a :

$$\text{Card } \bigcup_{i=1}^{1} A_i = \text{Card } A_1.$$

Par ailleurs, $I = \{1\}$ et Card $J = 1$. Ainsi

$$\sum_{J \subset I} (-1)^{1+\text{Card } (J)} \text{ Card } \Big(\bigcap_{i=1}^{n} A_i\Big) = \sum_{J \subset I} (-1)^2 \text{ Card } \Big(\bigcap_{i=1}^{1} A_i\Big) = \text{Card } A_1.$$

Lorsque $n = 2$, on vérifiera que ça marche encore.

Pour $n = 3$, regardons comment ça marche. Soit $B = A_2 \cup A_3$, alors :

$$\begin{aligned} \text{Card } (A_1 \cup A_2 \cup A_3) &= \text{Card } (A_1 \cup B) \\ &= \text{Card } A_1 + \text{Card } B - \text{Card } (A_1 \cap B). \end{aligned}$$

Or

$$\text{Card } B = \text{Card } A_2 + \text{Card } A_3 - \text{Card } (A_2 \cap A_3).$$

Il vient donc

$$\text{Card } (A_1 \cup A_2 \cup A_3) = \text{Card } A_1 + \text{Card } A_2 + \text{Card } A_3 - \text{Card } (A_2 \cap A_3) - \text{Card } (A_1 \cap B).$$

Mais

$$\begin{aligned} A_1 \cap B &= A_1 \cap (A_2 \cup A_3) \\ &= (A_1 \cap A_2) \cup (A_1 \cap A_3). \end{aligned}$$

Finalement, on a :

$$\begin{aligned} \text{Card } (A_1 \cap B) &= \text{Card } (A_1 \cap A_2) + \text{Card } (A_1 \cap A_3) - \text{Card } [(A_1 \cap A_2) \cap (A_1 \cap A_3)] \\ &= \text{Card } (A_1 \cap A_2) + \text{Card } (A_1 \cap A_3) - \text{Card } (A_1 \cap A_2 \cap A_3). \end{aligned}$$

On trouve

$$\begin{aligned}\text{Card}\,(A_1\cup A_2\cup A_3) &= \text{Card}\,A_1+\text{Card}\,A_2+\text{Card}\,A_3-\text{Card}\,(A_1\cap A_2)-\text{Card}\,(A_1\cap A_3)\\ &\quad-\text{Card}\,(A_2\cap A_3)+\text{Card}\,(A_1\cap A_2\cap A_3).\end{aligned}$$

Supposons le résultat établie de l'ordre 1 jusqu'à l'ordre n :

$$\text{Card}\left(\bigcup_{i=1}^{n}A_i\right)=\sum_{J\subset\{1,\ldots,n\}}(-1)^{1+\text{ Card }(J)}\,\text{Card}\left(\bigcap_{i\in J}A_i\right).$$

Calculons :

$$\begin{aligned}\text{Card}\left(\bigcup_{i=1}^{n+1}A_i\right) &= \text{Card}\left[\left(\bigcup_{i=1}^{n}A_i\right)\bigcup A_{n+1}\right]\\ &= \text{Card}\left(\bigcup_{i=1}^{n}A_i\right)+\text{Card}\,A_{n+1}-\text{Card}\left[\left(\bigcup_{i=1}^{n}A_i\right)\cap A_{n+1}\right]\\ &= \text{Card}\left(\bigcup_{i=1}^{n}A_i\right)+\text{Card}\,A_{n+1}\text{ - Card}\left[\bigcup_{i=1}^{n}(A_i\cap A_{n+1})\right]\\ &= \sum_{J\subset\{1,\ldots,n\}}(-1)^{1+\text{ Card }(J)}\,\text{Card}\left(\bigcap_{i\in J}A_i\right)+\text{Card}\,A_{n+1}\\ &\quad-\sum_{J\subset\{1,..,n\}}(-1)^{1+\text{ Card }(J)}\,\text{Card}\left(\bigcap_{i\in J}(A_i\cap A_{n+1})\right)\\ &= \sum_{J\subset\{1,\ldots,n+1\},(n+1)\notin J}(-1)^{1+\text{ Card }(J)}\,\text{Card}\left(\bigcap_{i\in J}A_i\right)\\ &\quad+\sum_{J\subset\{1,..,n+1\},n+1\in J}(-1)^{1+\text{ Card }(J)}\,\text{Card}\left(\bigcap_{i\in J}A_i\right)\\ &= \sum_{J\subset\{1,..,n+1\}}(-1)^{1+\text{ Card }(J)}\,\text{Card}\left(\bigcap_{i\in J}A_i\right).\end{aligned}$$

Propriété

Si E et F sont finis, alors $E\times F$ est fini et Card $(E\times F)=$ Card (E) Card (F).

Plus généralement, si E_1, E_2, . . ., E_n sont finis, alors Card $\left(\prod_{i=1}^{n}E_i\right)=\prod_{i=1}^{n}$ Card E_i.

En particulier, si E est fini, alors pour tout $n\geq 1$: Card $(E^n)=$ Card $(E)^n$.

Preuve

Si E ou F est vide, alors $E\times F$ est vide et on a

$$\text{Card}\,(E\times F)=\text{Card}\,(E)\,\text{Card}\,(F)=0.$$

Sinon, soit f l'application de $E\times F$ vers F définie par :

$$\forall(x,y)\in E\times F,\ f(x,y)=y.$$

L'application f est surjective. Pour tout y de F, $A_y=f^{-1}(y)=\{(x,y),x\in E\}$.

L'application $g_y : E\to A_y$ définie par $g_y(x)=(x,y)$ est visiblement une bijection. Il en découle que pour tout y de F, on a

$$\text{Card}\,A_y=q=\text{Card}\,E.$$

Le principe des bergers donne :

$$\text{Card}\,(E\times F)=q\,\text{Card}\,F=\text{Card}\,(E)\,\text{Card}\,(F).$$

La suite de la proposition se démontre par une récurrence évidente sur n.

B) Application d'un ensemble fini dans un autre

Définition

☐ Soit E un ensemble ayant n éléments. On appelle p-liste de E toute une suite $(x_1, x_2, \ldots, x_p)$ où chaque x_k est un élément de E.

☐ On appelle 0-liste de E la suite vide.

☐ On va donner un exemple. Soit $E = \{1, 2, 3, 4, 5, 6\}$, alors $(1, 1, 2, 3, 1)$ est une 5-liste de E.

Propriété

i) Soit E un ensemble à n éléments. Le nombre de p-liste est donné par n^p.

ii) Soient E et F deux ensembles ayant respectivement p et n éléments. L'ensemble $\mathcal{F}(E, F)$ des applications de E sur F est fini et on a $\text{Card}(\mathcal{F}(E, F)) = n^p$.

iii) Soit E un ensemble fini et n son cardinal. $\mathcal{P}(E)$ est l'ensemble des parties de E, on a alors

$$\text{Card } \mathcal{P}(E) = 2^n.$$

Preuve

i) On peut dénombre les p-listes de E en comptant qu'il y a n façons de choisir le premier élément d'une liste ; puis celui-ci étant choisi, il y a n façons de choisir le deuxième ; pour chaque choix des deux premiers éléments, il y a n façons de choisir le troisième, etc. ... En tout, il y a

$$n \times n \times \ldots \times n = n^p$$

possibilités.

ii) Notons $\mathcal{F}(E, F)$ l'ensemble des applications de E dans F. Pour montrer que Card $(\Im(E, F)) = n^p$, il suffit d'exhiber une bijection entre $\mathcal{F}(E, F)$ et l'ensemble produit F^p. Considérons l'application

$$\varphi : \mathcal{F}(E, F) \to F^p,\ f \mapsto (f(x_1), f(x_2), \ldots, f(x_p)).$$

L'application φ est injective car si $\varphi(f) = \varphi(f')$, alors

$$(f(x_1), f(x_2), \ldots, f(x_p)) = (f'(x_1), f'(x_2), \ldots, f'(x_p)) \Rightarrow f(x_1) = f'(x_1), f(x_2) = f'(x_2), \ldots, f(x_p) = f'(x_p),$$

ce qui implique que $f = f'$.

L'application φ est surjective. En effet, pour $(y_1, \ldots, y_p) \in F^p$, on peut construire une application

$$f \in \mathcal{F}(E, F)$$

telle que

$$(f(x_1), f(x_2), \ldots, f(x_p)) = (y_1, y_2, \ldots, y_p)$$

en posant

$$f(x_1) = y_1, \ldots, f(x_p) = y_p.$$

L'existence de cette fonction montre que l'application φ est surjective, donc bijective. Par conséquent, il y a autant d'éléments dans $\mathcal{F}(E, F)$ que dans F^p. Or

$$\text{Card } F^p = n^p,$$

donc

$$\text{Card } \Im(E, F) = n^p.$$

iii)

1ère preuve

Si $n = 0$, alors $E = \emptyset$ et $\mathcal{P}(E) = \{\emptyset\}$. Dans ce cas, on a bien Card $\mathcal{P}(E) = 1$.

Si $n \neq 0$, alors on peut écrire $E = \{x_1, x_2, \ldots, x_n\}$. Soit φ l'application de $\mathcal{P}(E)$ dans $\mathcal{F}(E, \{0, 1\})$ définie par :

$$\varphi : \mathcal{P}(E) \to \{0,1\},\ A \mapsto \mathbf{1}_A,$$

où $\mathbf{1}_A$ est la fonction indicatrice de A. L'application φ admet pour application réciproque l'application qui à tout élément f de $\mathcal{F}(E,\{0,1\})$ associe $f^{-1}(1) = A$. Par suite, l'application φ est bijective car elle admet une application réciproque. Comme Card $(\{0,1\}) = 2$, on a, par application du point ii,

$$\text{Card } \mathcal{F}(E,\{0,1\}) = \text{Card } \mathcal{P}(E) = 2^n.$$

$2^{ème}$ preuve

On va procéder encore à une démonstration par récurrence sur l'entier$n$.

Dans le cas particulier où n vaut 0, l'ensemble E est vide. Son ensemble des parties est alors $\{\emptyset\}$, qui possède bien $1 = 2^0$ élément.

Soit n un entier fixé ($n \neq 0$). Supposons la proposition vraie pour tous les ensembles à n éléments et prouvons la pour un ensemble E fixé possédant $(n+1)$ éléments.

Puisque $n+1$ vaut au moins 1, E n'est pas vide. Soit a un élément de E. Notons F l'ensemble $E\backslash\{a\}$ (en clair, l'ensemble formé des autres éléments de E). Ainsi F est un ensemble qui possède n éléments.

Les parties de E se subdivisent en deux catégories : celles dont a est un élément, et les autres. Commençons par examiner les autres, pour nous apercevoir que ce sont exactement les parties de F. Il y en a donc 2^n, par application de l'hypothèse de récurrence.

Comptons maintenant les parties de E dont a est un élément. Etant donnée une telle partie A, l'ensemble $A\backslash\{a\}$ est alors une partie de F ; et réciproquement chaque fois qu'on part d'une partie B de F, l'ensemble $B \cup \{a\}$ est une partie de E dont a est un élément. Il y a donc autant de parties de E dont a est un élément que de parties de F, donc encore 2^n.

Le nombre total de parties de F est donc $2^n + 2^n$, soit 2^{n+1}.

C) Injection d'un ensemble fini dans un autre

Définition

☐ Etant donné un ensemble E contenant n élément distincts, on appelle arrangement de p éléments de E toute suite de p éléments distincts de E. On parle aussi de p-arrangement.

☐ Prenons un exemple avec $E = \{1,2,3,4,5,6\}$. Alors

– $(3,1,6,5)$ est un arrangement de 4 éléments de E.

– $(4,1,6,2,5,3)$ est un arrangement de 6 élément de E.

– $(3,1,3,4,2,5,6)$ n'est pas un arrangement de E.

☐ On désigne par A_n^p le nombre d'arrangements de p éléments d'un ensemble ayant n éléments.

☐ Une permutation d'un ensemble E est une bijection de E dans lui-même.

Théorème

i) Le nombre A_n^p d'arrangements est donné par

$$\mathrm{A}_n^p = n\,(n-1)\cdots(n-p+1) = \frac{n!}{(n-p)\,!}.$$

ii) Soient E et F des ensembles finis de cardinaux respectivement p et n, avec $0 \leq p \leq n$. L'ensemble $\Im(E,F)$ des injections de E dans F est fini, et $\mathrm{A}_n^p = n(n-1)\cdots(n-p+1) = \dfrac{n!}{(n-p)!}$.

iii) Soit E un ensemble finis de cardinal p. Le nombre de permutations de E est $p!$.

Preuve

i) Si E est vide, le seul arrangement possible est l'arrangement de 0 élément de E qui est la suite vide. Si E contient n éléments et $p > n$, alors il n'existe pas d'arrangement de p éléments de E. Donc on peut dénombrer les arrangements de p éléments de E quand $p \leq n$, en comptant qu'il y a n façons de choisir le premier élément d'un arrangement, puis pour chacune d'elles, $(n-1)$ façons de choisir le deuxième élément qui doit être distinct du premier ; les deux premiers éléments étant choisis, il reste $(n-2)$ possibilités pour le troisième, etc. ... enfin il reste $(n-(p-1))$ façons de choisir le $p^{ième}$ élément qui doit être distinct des $(p-1)$ précédents. Ce qui fait en tout

$$\mathrm{A}_n^p = n\,(n-1)\cdots(n-p+1) = \frac{n!}{(n-p)\,!}.$$

ii) Remarquons tout d'abord que si $p > n$, il y a aucune injection de E dans F car Card $E >$ Card F.

Si $p = 0$, on a exactement une injection de E dans F.

Si $p = 1$, alors on peut écrire $E = \{x\}$ et $F = \{y_1, \ldots, y_n\}$. Une application injective de E dans F est déterminée par l'image de x. Il y a donc exactement n injections, donc la formule est vraie.

Supposons le résultat établi à $p = q - 1$.

Envisageons le cas où $p = q$. Fixons un élément $x_p \in E$ et notons $G = E\backslash\{x_p\}$, alors

$$\text{Card } G = q - 1.$$

Comme

$$\text{Card } \Im(E,F) > \text{Card } \Im(G,F),$$

on peut définir une surjection $\varphi : \Im(E,F) \to \Im(G,F)$, $f \mapsto f|_G$ qui associe à chaque injection de E dans F sa restriction à G. Soit g une injection de G dans F. Le nombre d'éléments de F qui ne sont pas dans $g(G)$ est

$$\text{Card } F - \text{ Card } G = n - (q-1).$$

Donc, il existe $n-(q-1)$ applications injectives de E dans F dont la restriction à G est g. Dans ce cas, on a

$$\text{Card } \varphi^{-1}(g) = n - (q-1)$$

car, si $f \in \varphi^{-1}(g)$, f est déterminé par g et par $f(x_p) \in F\backslash g(G)$. Comme φ est une surjection et qu'il existe

$$n - (q-1)$$

tel que

$$\text{Card } \varphi^{-1}(g) = n - (q-1),$$

on a

$$\text{Card } \Im(E,F) = (n-q+1)\ \text{Card } \Im(G,F)$$

d'après le principe des bergers. Or on a, par hypothèse de récurrence,

$$\text{Card}(\Im\,(G,F)) = \mathrm{A}_n^{q-1} = \frac{n!}{(n-q+1)!} \text{ et Card } (\Im\,(E,F)) = \mathrm{A}_n^q.$$

Donc,

$$\mathrm{A}_n^q = (n-q+1)\cdot \mathrm{A}_n^{q-1} = (n-q+1)\cdot\frac{n!}{(n-q+1)\,!} = \frac{n!}{(n-q)\,!}.$$

iii) Une permutation est en fait une bijection d'un ensemble E dans lui-même. Or on sait que toute injection d'un ensemble E de cardinal p dans un autre ensemble de même cardinal est une bijection, en particulier toute injection d'un ensemble E dans lui-même est une bijection, donc une permutation. Donc le nombre de permutations est égal au nombre d'injections $\mathrm{A}_p^p = p!$.

D) Combinaisons

Définition

☐ Etant donné un ensemble E de n éléments distincts, on note $\mathcal{P}_p(E)$ l'ensemble des parties de E à p éléments. Un élément de $\mathcal{P}_p(E)$ s'appelle combinaison de p éléments de E. Donc une combinaison de p éléments de E est une partie de E contenant p éléments.

On appelle combinaison avec répétition de p éléments toute partie non ordonnée de p éléments non nécessairement distincts de E.

☐ Par exemple si $E = \{1, 2, 3, 4, 5, 6\}$, alors

– $\{1, 3, 5, 6)$ est une combinaison de 4 éléments de E.

– $\{1, 2, 5\} = \{5, 1, 2\}$ est une combinaison de 3 éléments de E.

– $\{2, 1, 3, 1, 5\} = \{1, 2, 3, 5\}$ n'est pas une combinaison de 5 éléments, mais de 4 éléments de E.

– $[3, 1, 3, 5, 6]$ est une combinaison avec répétition de 5 éléments de E.

– $[3, 1, 3, 5, 6] = [1, 3, 3, 5, 6] \neq [1, 3, 5, 6]$.

☐ On désigne par C_n^p le nombre des combinaisons de p éléments d'un ensemble à n éléments.

Théorème

i) Si $p \leq n$, alors $\mathrm{C}_n^p = \dfrac{\mathrm{A}_n^p}{p!} = \dfrac{n!}{p!(n-p)!}$.

ii) Le nombre de suites strictement croissantes de p éléments de $[\![1, n]\!] \subset \mathbb{N}$ est égal au nombre C_n^p de combinaisons de p éléments d'un ensemble à n éléments :

$$\text{Card } \{(i_1, \ldots, i_p) \in \mathbb{N}^p \ / \ 1 \leq i_1 < ... < i_p \leq n\} = \mathrm{C}_n^p.$$

Preuve

i) Si $E = \emptyset$, la seule combinaison dans E est $\emptyset$, qui est la combinaison de 0 élément de E. Si E contient n et

$$p > n,$$

alors il n'existe pas de combinaison de p éléments de E. On suppose maintenant que $p \leq n$. On remarquera qu'il y a $p!$ façons d'ordonner dans une suite p éléments distincts de E. Par conséquent, à chaque combinaison de p éléments correspondent $p!$ arrangements de ces p éléments de E. Il y a donc $p!$ fois moins de combinaisons que d'arrangements de p éléments. Donc

$$\mathrm{C}_n^p = \frac{\mathrm{A}_n^p}{p!} = \frac{n!}{p!\,(n-p)\,!}.$$

ii) Il suffit de voir qu'on définit une bijection de l'ensemble des combinaisons de p éléments de $[\![1, n]\!]$ dans celui des suites strictement croissantes de p éléments de $[\![1, n]\!]$ en associant à toute combinaison $\{i_1, ..., i_p\}$ l'unique suite où $i_1, ..., i_p$ sont rangés dans l'ordre croissant.

Propriété

i) Pour tout entier naturel p inférieur à n, on a : $\mathrm{C}_n^p = \mathrm{C}_n^{n-p}$, $\mathrm{C}_n^0 = \mathrm{C}_n^n = 1$, $\mathrm{C}_n^1 = \mathrm{C}_n^{n-1} = n$.

ii) $p\mathrm{C}_n^p = n\mathrm{C}_{n-1}^{p-1}$.

iii) Pour tout couple (n,p) avec $p \leq n$ d'entiers naturels non nuls, on a $\mathrm{C}_n^p = \mathrm{C}_{n-1}^p + \mathrm{C}_{n-1}^{p-1}$.

iv) Formule du binôme de Newton :

$$(a+b)^n = \sum_{p=0}^{n} \mathrm{C}_n^p a^p b^{n-p}.$$

En particulier, $\sum_{p=0}^{n} \mathrm{C}_n^p = 2^n$.

Preuve

i) On la démontre en remplaçant p par $(n-p)$ dans la formule

$$\mathrm{C}_n^p = \frac{n!}{p!\,(n-p)!}.$$

On vérifie d'ailleurs que toute combinaison à p élément admet une combinaison complémentaire à $(n-p)$ éléments et réciproquement. Le nombre des premières est donc égal à celui du second.

Par ailleurs, on a

$$\mathrm{C}_m^0 = \mathrm{C}_m^m = 1$$

car l'une correspond au sous-ensemble vide $\emptyset$, l'autre à l'ensemble E lui-même.

Il est également aisé de vérifier $\mathrm{C}_n^1 = \mathrm{C}_n^{n-1} = n$. Il suffit en effet de poser $p = 1$ dans la formule $\mathrm{C}_n^p = \mathrm{C}_n^{n-p}$. Mais, on a $\mathrm{C}_n^1 = n$, d'où on obtient la formule.

ii) Par calcul, on arrive facilement.

iii) On a

$$\begin{aligned} \mathrm{C}_{n-1}^p + \mathrm{C}_{n-1}^{p-1} &= \frac{(n-1)!}{p!(n-p-1)!} + \frac{(n-1)!}{(p-1)!(n-p)!} \\ &= \frac{(n-1)!}{p!(n-p)!}[(n-p)+p] \\ &= \frac{n!}{p!(n-p)!} \end{aligned}$$

iv) On démontre la formule du binôme de Newton par récurrence. Le cas où $n = 1$, 2 est évident. Supposons que cette formule soit vraie à l'ordre n. Calculons

$$\begin{aligned} (a+b)^{n+1} &= (a+b)(a+b)^n \\ &= (a+b)\sum_{p=0}^{n} \mathrm{C}_n^p a^p b^{n-p} \\ &= a\sum_{p=0}^{n} \mathrm{C}_n^p a^p b^{n-p} + b\sum_{p=0}^{n} \mathrm{C}_n^p a^p b^{n-p} \\ &= \sum_{p=0}^{n} \mathrm{C}_n^p a^{p+1} b^{n-p} + \sum_{p=0}^{n} \mathrm{C}_n^p a^p b^{n-p+1} \\ &= \sum_{p=1}^{n+1} \mathrm{C}_n^{p-1} a^p b^{n-p+1} + \sum_{p=0}^{n} \mathrm{C}_n^p a^p b^{n-p+1} \\ &= a^{n+1} + \sum_{p=1}^{n} \mathrm{C}_n^{p-1} a^p b^{n-p+1} + \sum_{p=1}^{n} \mathrm{C}_n^p a^p b^{n-p+1} + b^{n+1} \\ &= a^{n+1} + \sum_{p=0}^{n} \left(\mathrm{C}_n^{p-1} + \mathrm{C}_n^p\right) a^p b^{n-p+1} + b^{n+1}. \end{aligned}$$

Théorème

Soit E un ensemble fini à n éléments, $n \geq 1$, et $p \in \mathbb{N}$.

i) Le nombre des applications $u : E \to [\![0,p]\!]$ telles que

$$\sum_{x\in E} u(x) \leq p$$

est

$$C_{n+p}^{p} = C_{n+p}^{n}.$$

En prenant $E = [\![1, p]\!]$, l'assertion (i) signifie que le nombre des n-uplets $(a_1, ..., a_n) \in \mathbb{N}^n$ tels que

$$a_1 + ... + a_n \leq p$$

est C_{n+p}^{n}.

ii) Le nombre des applications $u : E \to [\![0, p]\!]$ telles que $\sum_{x\in E} u(x) = p$ est

$$C_{n+p-1}^{n-1} = C_{n+p-1}^{p}.$$

Démonstration

L'assertion (ii) se déduit de (i) grâce à la relation de Pascal (à l'aise Blaise)

$$C_{n+p}^{n} - C_{n+p-1}^{n} = C_{n+p}^{n-1}.$$

Prouvons (i). Pour cela, on peut supposer que $E = [\![1, n]\!]$. Soit E l'ensemble des $\alpha \in \mathcal{F}([\![1, n]\!], [\![0, p]\!])$ telles que $\sum_{i=1}^{n} \alpha(i) \leq p$, et F l'ensemble des applications strictement croissantes de $[\![1, n]\!]$ dans $[\![1, n + p]\!]$. Une application $\beta \in F$ se définit de manière unique par son image, d'où

$$\text{Card } (F) = C_{n+p}^{n}.$$

A chaque $u \in E$, associons $v = \Phi(u) \in F$ définie par $v(x) = x + \sum_{i=1}^{x} u(i)$ $(x \in [[1, n]])$. A chaque $v \in F$, associons $u = \Psi(v) \in E$ définie par

$$u(1) = v(1) - 1,\ u(x) = v(x) - v(x - 1) - 1 \text{ pour } x \geq 2.$$

On vérifie que $\Phi(u)$ (resp. $\Psi(v)$) est bien un élément de F (resp. de E), et que

$$\Phi \circ \Psi = Id_E, \quad \Psi \circ \Phi = Id_F,$$

donc Φ et Ψ sont bijectives, et

$$\text{Card } E = \text{Card } F = C_{n+p}^{n}.$$

E) Problèmes divers

Propriété

Il existe une suite double $S_{i,p}$ $(i,\ p \in \mathbb{N})$ telle que $S_{1,1} = 1$ et $\forall i \in \mathbb{N}^*$, $\forall p \in \mathbb{N}^*$,

$$n^p = \sum_{i=1}^{p} S_{i,p} \mathrm{C}_n^i.$$

Preuve

Supposons les $S_{i,p}$ définis pour $p \in \mathbb{N}^*$ fixé,

$$\begin{aligned} n^{p+1} &= n^p(n+1-1) = \sum_{i=1}^{p} S_{i,p}\mathrm{C}_n^i(n+1-1) \\ &= \sum_{i=1}^{p} S_{i,p}[(n+1)\mathrm{C}_n^i - \mathrm{C}_n^i]. \end{aligned}$$

Rappelons que $\mathrm{C}_\alpha^k = \mathrm{C}_{\alpha-1}^k + \mathrm{C}_{\alpha-1}^{k-1}$ et $\mathrm{C}_\alpha^k = \dfrac{k+1}{\alpha+1}\ \mathrm{C}_{\alpha+1}^{k-1}$. Avec ces formules, on obtient alors

$$\begin{aligned} n^{p+1} &= \sum_{i=1}^{p} S_{i,p}\left[(i+1)\,\mathrm{C}_{n+1}^{i+1} - \mathrm{C}_n^i\right] \\ &= \sum_{i=1}^{p} S_{i,p}\left[(i+1)\,\mathrm{C}_n^{i+1} + i\mathrm{C}_n^i\right]. \end{aligned}$$

D'où $n^{p+1} = \sum_{i=1}^{p} S_{i,p+1}\ \mathrm{C}_n^i$ avec

$S_{1,p+1} = S_{1,p} = 1$, $S_{p+1,p+1} = (p+1)S_{p,p}$ et $S_{i,p+1} = i(S_{i,p} + S_{i-1,p})$ pour $2 \le i \le p-1$.

Ce qui définit bien les $S_{i,p+1}$ par récurrence.

Théorème

Notons $B(n,p)$ la somme $1^p + 2^p + \cdots + n^p = \sum_{k=1}^{p} k^p$ pour $p \in \mathbb{N}$ et $n \in \mathbb{N}^*$. Alors

$$B(n,p) = \sum_{i=1}^{p} S_{i,p}\mathrm{C}_{n+1}^{j+1}.$$

En particulier, $1+2+\cdots+n = \frac{n(n+1)}{2}$, $1^2+2^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$, $1^3+2^3+\cdots+n^3 = \frac{n^2(n+1)^2}{4}$.

Démonstration

Nous avons déjà établi que $k^p = \sum_{i=1}^{p} S_{i,p}\mathrm{C}_k^i$. Il ne reste plus qu'à sommer de $k = 1$ à n pour obtenir

$$B(n,p) = \sum_{i=1}^{p} S_{i,p}\Big(\sum_{k=1}^{n} \mathrm{C}_k^i\Big).$$

Or si on utilise $\mathrm{C}_\alpha^k = \mathrm{C}_{\alpha-1}^k + \mathrm{C}_{\alpha-1}^{k-1}$, on obtient

$$\sum_{k=1}^{n} \mathrm{C}_k^i = \sum_{k=1}^{n}[\ \mathrm{C}_{k+1}^{i+1} - \mathrm{C}_k^{i+1}] = \ \mathrm{C}_{n+1}^{i+1}.$$

Finalement, on a bien $B(n,p) = \sum_{i=1}^{p} S_{i,p}(\sum_{k=1}^{n}\ \mathrm{C}_k^i)$. L'idée est que la somme $\sum_{k=1}^{n}\ \mathrm{C}_k^i$ est beaucoup plus facile à calculer que la somme $\sum_{k=1}^{n} k^p$.

Formule d'inversion de Pascal

Soit $B_0 = \{1, x, x^2, ..., x^n\}$ la base canonique de $\mathbb{R}_n[X]$.

1. Montrer que est $B' = \{1, x+1, (x+1)^2, ..., (x+1)^n\}$ aussi une base de $\mathbb{R}_n[X]$, et expliciter la matrice de passage P de B_0 à B'. (On pourra développer $(x+1)^k$ à l'aide de la formule du binôme).
2. Chercher la matrice de passage de B' à B_0 et en déduire la matrice P^{-1}. (On remarquera que $x = (x+1) - 1$).
3. En déduire la Formule d'inversion de Pascal :

   Si $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont deux suites réelles vérifiant : $\forall n \in \mathbb{N}$, $u_n = \sum_{k=0}^{n} \mathrm{C}_n^k v_k$, alors

$$\forall n \in \mathbb{N},\ v_n = \sum_{k=0}^{n} (-1)^{n-k} \mathrm{C}_n^k u_k.$$

---

1. B' est formée de $n+1$ polynômes à degrés échelonnés dans $\mathbb{R}_n[X]$. Par conséquent, c'est une base de $\mathbb{R}_n[X]$.

   Par ailleurs, $\forall k \in [0; n]$, $(1+x)^k = \sum_{i=0}^{k} \mathrm{C}_k^i x^i$. Cette relation nous permet de former la matrice de passage de :

$$P = \begin{pmatrix} \mathrm{C}_0^0 & \mathrm{C}_1^0 & \cdots & \cdots & \mathrm{C}_n^0 \\ & \mathrm{C}_1^1 & & & \mathrm{C}_n^1 \\ & & \ddots & & \vdots \\ & 0 & & \mathrm{C}_{n-1}^{n-1} & \mathrm{C}_n^{n-1} \\ & & & & \mathrm{C}_n^n \end{pmatrix}$$

2. P^{-1} est la matrice des coordonnées de 1, x, ..., x^n dans la base B'. Or

$$\forall k \in [\![0; n]\!], x^k = ((1+x)-1)^k = \sum_{j=0}^{k} \mathrm{C}_k^j (-1)^{k-j} (1+x)^j.$$

   Donc

$$P^{-1} = \begin{pmatrix} \mathrm{C}_0^0 & -\mathrm{C}_1^0 & \cdots & \cdots & (-1)^n \mathrm{C}_n^0 \\ & \mathrm{C}_1^1 & & & (-)^{n-1} \mathrm{C}_n^1 \\ & & \ddots & & \vdots \\ & 0 & & \mathrm{C}_{n-1}^{n-1} & -\mathrm{C}_n^{n-1} \\ & & & & \mathrm{C}_n^n \end{pmatrix}$$

3. Si $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont deux suites réelles vérifiant : $\forall n \in \mathbb{N}$, $u_n = \sum_{k=0}^{n} \mathrm{C}_n^k v_k$, alors

$$\begin{pmatrix} u_0 \\ \\ \vdots \\ \\ u_n \end{pmatrix} = \begin{pmatrix} \mathrm{C}_0^0 & & & & \\ \mathrm{C}_1^0 & \mathrm{C}_1^1 & & 0 & \\ \vdots & & \ddots & & \\ \vdots & & & \ddots & \\ \mathrm{C}_n^0 & \cdots & \cdots & \mathrm{C}_n^{n-1} & \mathrm{C}_n^n \end{pmatrix} \begin{pmatrix} v_0 \\ \\ \vdots \\ \\ v_n \end{pmatrix}.$$

En notant $U = \begin{pmatrix} u_0 \\ \vdots \\ u_n \end{pmatrix}$ et $V = \begin{pmatrix} v_0 \\ \vdots \\ v_n \end{pmatrix}$, on reconnaît le système $U = {}^tPV$, qui équivaut à $V = {}^t(P^{-1})U$. On obtient alors :

$$\forall k \in [\![0, n]\!],\ v_k = \sum_{i=0}^{k} (-1)^{k-i} \mathrm{C}_k^i u_i.$$

Enfin, en faisant varier n et en prenant $k = n$, on trouve :

$$\forall n \in \mathbb{N},\ v_n = \sum_{k=0}^{n} (-1)^{n-k} \mathrm{C}_n^k u_k.$$

Calcul du nombre de surjections d'un ensemble fini dans un autre

On note S_p^n le nombre de surjections de $[\![1, p]\!]$ dans $[\![1, n]\!]$.

1. Calculer S_p^n pour $p < n$. Calculer S_p^p, S_p^1, S_p^2.
2. En établissant l'existence d'un élément ayant deux antécédents, montrer que $S_{p+1}^p = \dfrac{p}{2}(p+1)!$.
3. Soit $k \in [\![1, n]\!]$. Montrer qu'il y a exactement applications de $[\![1, p]\!]$ dans $[\![1, n]\!]$ dont l'image soit un sous-ensemble donné de cardinal k de $[\![1, n]\!]$. En déduire que $\displaystyle\sum_{k=1}^{n} \mathrm{C}_n^k S_p^k = n^p$.
4. On pose $S_p^0 = 0$. Montrer à l'aide de la formule d'inversion de Pascal que $S_p^n = \displaystyle\sum_{k=0}^{n} (-1)^{n-k} \mathrm{C}_n^k k^p$.
5. En déduire que : $\forall p \geq 2,\ \forall n \geq 2,\ S_p^n = n(S_{p-1}^n + S_{p-1}^{n-1})$.
6. Montrer par récurrence que $S_{p+2}^p = \dfrac{p(3p+1)}{24}(p+2)$.
7. On note π_p^n le nombre de partitions de $[\![1, p]\!]$ en n sous-ensembles non vides.
   Quelle relation y-a-t'il entre π_p^n et S_p^n ? En déduire que $\pi_p^n = \pi_{p-1}^{n-1} + n\pi_{p-1}^n$.

Quelques bons conseils

☐ Le nombre de termes dans une somme ou un produit est le rang du terme le plus élevé moins le rang du terme de le moins élevé, plus 1 si les rangs des termes se suivent de 1 en 1.

– il y a $(n-p+1)$ termes dans la somme $\sum_{k=p}^{n} a_k$.

– il y a p termes dans le produit $n(n-1)(n-2)\dots(n-p+1)$.

☐ Apprenez par **cœur** les identités remarquables et les formules de dénombrement usuelles :

– $a^2+b^2=(a+ib)(a-ib)$

– $(a+b)^n=\sum_{p=0}^{n} \mathrm{C}_n^p a^p b^{n-p}$

– $\mathrm{C}_n^p=\mathrm{C}_n^{n-p}$, $\mathrm{C}_n^0=\mathrm{C}_n^n=1$, $\mathrm{C}_n^1=\mathrm{C}_n^{n-1}=n$, $p\mathrm{C}_n^p=n\ \mathrm{C}_{n-1}^{p-1}$, $\mathrm{C}_n^p=\mathrm{C}_{n-1}^p+C_{n-1}^{p-1}$, $\sum_{p=0}^{n}\mathrm{C}_n^p=2^n$.

– Rappeler que $(1+x)^n=\sum_{k=1}^{n}\mathrm{C}_n^k x^k$, et par dérivation on obtient beaucoup de formules.

☐ Il est commode de connaître les formules suivantes :

– $\sum_{k=0}^{n} k=\dfrac{n(n+1)}{2}$

– $\sum_{k=0}^{n} k^2=\dfrac{n(n+1)(2n+1)}{6}$

– $\sum_{k=0}^{n} k^3=\Big(\dfrac{n(n+1)}{2}\Big)^2$.

☐ Entraînons-nous à manipuler des sommes formelles et les changements d'indices :

– $\sum_{\substack{1\le i\le n\\ 1\le j\le p}} \sum a_i b_j=\sum_{i=1}^{n}\Big(\sum_{j=1}^{p} a_i b_j\Big)=\Big(\sum_{i=1}^{n} a_i\Big)\Big(\sum_{j=1}^{p} b_j\Big)$

– Soit $\sum_{k=p}^{n} a_{k+\alpha}$. Posons $k'=k+\alpha$, on obtient $\sum_{k=p}^{n} a_{k+\alpha}=\sum_{k=p+\alpha}^{n+\alpha} a_k$. Pour obtenir les bornes, il suffit de poser $k=p$ et $k=n$ dans k'.