Notations/Abréviations/Vocabulaire/Définition

@ : un titre ou un paragraphe précédé du symbole @ ne peut pas faire l'objet d'une évaluation du cours.
$\mathscr{P}(A)$: l'ensemble des parties de A où A est un ensemble.
$|A|$: le cardinal de A où A est un ensemble fini.
$|a|$: la valeur absolue de a où a est réel ou un élément d'un corps ordonné.
$[n]$: l'ensemble $\{1, 2, 3, 4, \ldots, n\}$ où n est un entier strictement positif .
$\mathbb{N}$: l'ensemble des nombres entiers positifs.
$\mathbb{Z}$: l'ensemble des nombres entiers (positifs ou négatifs).
$\mathbb{Q}$: l'ensemble des nombres rationnels (que l'on peut écrire sous la forme d'une fraction de deux nombres entiers, ou dont la fin du développement décimale est une répétition).
$A \setminus B$: l'ensemble A privé des éléments de l'ensemble B (différence ensembliste).
$\mathbb{R}$: l'ensemble des nombres réels.
$\mathbb{R}_+$: l'ensemble des nombres réels positif.
$\mathbb{R}_+^*$: l'ensemble des nombres réels strictement positifs.
$\sqrt{x}$: racine carrée d'un nombre x.
$\sqrt[n]{x}$: racine n-ième d'un nombre x.
$\wedge$: ET logique
$\vee$: OU logique
$\neg$: Négation logique
$\Rightarrow$: Implication logique
$\Leftrightarrow$: équivalence logique
ssi : abreviation de "si et seulement si" (équivalence)
$\forall$: $\forall$ est le symbole (standard) du quantificateur universel.
$\exists$: $\exists$ est le symbole (standard) du quantificateur existentiel.
$\forall x \in A, P$ est la contraction de $\forall x, (x \in A) \Rightarrow P$
$\exists x \in A, P$ est la contraction de $\exists x, (x \in A) \wedge P$
$\subset$: $A \subset B$ (ou $B \supset A$) signifie $\ll A$ est inclus dans $B \gg$ si A et B sont des ensembles.
$\lfloor a \rfloor$: La partie entière (ou partie entière inférieure) d'un nombre a (noté $\lfloor a \rfloor$) est le plus grand entier k vérifiant $k \leqslant a$. Autrement dit $\lfloor a \rfloor =: \max\{k : (k \leqslant a) \wedge (k \in \mathbb{Z})\}$ ou $k \leqslant a < k + 1$, avec $k \in \mathbb{Z}$
$\lceil a \rceil$: Si a est un nombre réel alors $\lceil a \rceil$ est un entier (relatif) k qui vérifie $k - 1 < a \leqslant k$, on l'appelle aussi partie entière supérieure.
$\{a\}$: La partie fractionnaire d'un nombre réel a, notée $\{a\}$, est $a - \lfloor a \rfloor$ (donc c'est un nombre réel, entre 0 (compris) et 1 (non compris).

Proposition

Proposition

On peut voir une proposition (logique) comme une phrase qui peut être "évaluée" vraie ou fausse.

Exemples :

Le nombre 2 est pair.
Napoléon est mort à Saint-Hélène.
Le nombre 3 est pair (c'est une proposition mais elle est fausse).

Remarques

En langue naturelle (ici en français) certaines phrases ne sont pas des propositions ou sont de "mauvaises" propositions pour différentes raisons. En voici quelques-unes :

- La phrase n'est n'est pas une déclaration (c'est une question, interjection, un ordre,...).
- La phrase est une déclaration mais contient des mots dont le sens varie selon le contexte (en utilisant des mots comme, "maintenant", "ici", "tu").
- La phrase est une déclaration mais contient des mots dont le sens premier est approximatif, "tas" par exemple, voir le "paradoxe" du tas.
- La phrase est grammaticalement une déclaration correcte mais avec aucune (ou trop d') interprétation possible on est obligé d'essayer d'étendre le sens des mots donc le sens devient vague. Exemple : "Le différentiel cascade la véracité du nouveau siècle ponctuel." ou "Le respect agile n'a plus d'eau.", "L'absurdité est verte mais n'a pas d'oiseau.", "Vous respirez le ciel persuasif avec amitié."

On se limitera dans la suite aux propositions dont la véracité ne dépend que d'"éléments"facilement vérifiables et issues de définitions (formelles) que nous auront établies ou reprises des disciplines formelles comme les maths, la logique, l'informatique.

Par exemple "Jules César est né durant l'année 1003 du calendrier Julien" fait appel à un fait issue d'une observation "réel" donc difficile à vérifier alors que "3 est pair" est facilement vérifiable.

Cela ne veut pas dire que les propositions que nous formeront seront facilement vérifiable.

Combinaison de propositions

On peut combiner ensemble des propositions avec un opérateur pour produire une nouvelle proposition. Ce genre d'opérateur est appelé *opérateur logique*. La valeur de vérité de la proposition produite dépend : de l'opérateur et des valeurs de vérité des propositions précédentes.

Plusieurs opérateurs sont présentés dans la suite.

Conjonction (définition)

La conjonction, appelée/notée ET (ET logique, $\wedge$, `&&` (en C et C++), *and*), combine 2 propositions pour en produire une nouvelle. La nouvelle proposition est vraie si et seulement si les deux propositions de départ sont vraies.

Voici la table de vérité de la conjonction (F : faux, V : vrai)

P	Q	$P \wedge Q$
F	F	F
F	V	F
V	F	F
V	V	V

Disjonction (définition)

La disjonction, appelée/notée OU (OU logique, $\vee$, `||` (en C et C++), *or*), combine 2 propositions pour en produire une nouvelle. La nouvelle proposition est vraie si et seulement si au moins une des deux propositions de départ est vraie.

Voici la table de vérité de la disjonction (F : faux, V : vrai)

P	Q	$P \vee Q$
F	F	F
F	V	V
V	F	V
V	V	V

Négation (définition)

La négation, appelée/notée NON (NON logique, $\neg$, `!` (en C et C++), *not*), s'applique à une seule proposition pour en produire une nouvelle. La nouvelle proposition est vraie si et seulement si la proposition de départ est fausse.

Q	$\neg Q$
F	V
V	F

Implication (définition)

L'implication notée $\Rightarrow$ (ou $\Leftarrow$) s'applique à deux propositions pour en produire une nouvelle. Elle est inspirée des phrases utilisant le conditionnel "si A alors B" (s'écrit $A \Rightarrow B$, peut se prononcer : A implique B). Le seul cas ou elle est fausse est le cas $V \Rightarrow F$ ("vrai implique faux" est faux), les autres cas donnent la valeur vrai (notamment "faux implique vrai").

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

Remarque

Le fait qu'elle soit inspirée des phrases "si A alors B" perturbe souvent les étudiants. Il faut vraiment la voir (pour l'instant) comme un opérateur bête et dont la table de vérité est fixée sans forcément donner du sens à ce qu'elle implique. On verra à travers des exemples dans quels cas elle est pertinente.

Exemple : <si "3 est pair" alors "$\pi = 4$"> est une proposition vraie car "3 est pair" est faux.

Une autre façon d'expliquer l'implication est de voir $A \Rightarrow B$ comme un raccourci d'écriture de $(\neg A) \vee B$.

Équivalence (définition)

L'équivalence notée $\Leftrightarrow$ s'applique à deux propositions pour en produire une nouvelle.

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

Remarque (si et seulement si)

Lorsque l'équivalence entre deux propositions A et B (ou expression propositionnelle) est vraie, on l'exprime souvent par la locution "A *si et seulement si* B". Par exemple : "un nombre a divise un nombre b si et seulement si le reste de la division de a par b est nul".

En abrégé on peut aussi écrire A *ssi* B.

Ensemble en compréhension

Ensemble en compréhension

Si P est une expression qui est "presque" une proposition, on peut décrire un ensemble d'éléments par une expression de la forme :

$$\{x : P\}$$

Un élément s appartient à A si lorsqu'on remplace les symboles libres x de P par s dans A alors la proposition est vraie (les exemples ci-dessous sont peut-être plus clairs).

Exemples

On a $3 \in \{x : (x \in \mathbb{N}) \wedge (x < 5)\}$ car $\quad (3 \in \mathbb{N}) \wedge (3 < 5) \quad$ est vrai.
On a $7 \notin \{x : (x \in \mathbb{N}) \wedge (x < 5)\}$ car $\quad (7 \in \mathbb{N}) \wedge (7 < 5) \quad$ est faux.
$\{x : (x \in \mathbb{N}) \wedge (x < 5) \wedge (x > 0)\} = \{1, 2, 3, 4\}$

Remarques/notation

On peut voir un ensemble en compréhension comme une proposition incomplète avec des trous. Si on remplace chaque trou par le même symbole et que la proposition est vraie alors le symbole appartient à l'ensemble, si la proposition est fausse alors le symbole n'appartient pas à l'ensemble.

Attention on parle bien de remplacer, dans P, uniquement les symboles x libres, pas ceux qui sont liés (voir suite pour la différence entre symbole libre et symbole lié).

Souvent en notation "raccourcie" on contracte le nom de la variable avec une des composantes de la conjonction P (s'il y en a une). Par exemple, l'expression $\{x : (x \in \mathbb{N}) \wedge (x < 5)\}$ peut être contractée en $\{x \in \mathbb{N} : x < 5\}$.

On peut aussi rencontrer la notation $\{x/P\}$ à la place de $\{x : P\}$.

Symbole libre, symbole lié

Dans une expression, certaines apparitions de symboles sont dites *libres* et d'autres dites *liées* (et d'autres comme souvent les parenthèses ou bien les accolades ne sont ni l'un ni l'autre mais servent à structurer l'expression).

Une apparition de symbole est dit liée si on peut le remplacer par un symbole différent (en remplaçant éventuellement à d'autres endroits) sans changer le sens de l'expression. Un symbole est dit libre si il n'est pas remplaçable.

Exemple

Dans l'expression $\{x : (x < y) \wedge (x \in \mathbb{N})\}$ (à priori on ne connaît pas la valeur de y) les trois apparitions de x sont liées ensemble mais l'apparition de y est libre.

Pour illustrer cette affirmation on peut remplacer toute apparition de x par z sans changer le sens de l'expression :

$$\{x : (x < y) \wedge (x \in \mathbb{N})\} \text{ est la même chose que } \{z : (z < y) \wedge (z \in \mathbb{N})\}$$

L'importance de la position

Ce n'est pas parce que une apparition du symbole x est liée que toutes les autres apparitions de x sont aussi liées.

Dans l'expression suivante

$\{ \quad y : (y \in \mathbb{Z}) \quad \wedge \quad (y < x) \quad \wedge \quad y \in \{x : (x^2 = 5x + 4)\} \quad \}$, la première apparition de x est libre mais les secondes et troisièmes apparitions sont liées. Ces symboles liés ensembles forment une "entité" appelée *variable*.

Les symboles "constant"

Dans une expression on peut parler d'une "troisième" catégorie de symbole (en plus des symboles libres et liés et sans compter les symboles comme les parenthèses) qui sont les symboles ayant un sens implicite défini par ailleurs. On peut les appeler symbole "constant". Par exemple, dans l'expression $x < y$, $<$ pourrait très bien être un symbole "constant" signifiant "strictement inférieur".

Voici d'autres symboles, chacun (souvent) associé implicitement toujours au même sens : 1 (le second nombre entier), $\wedge$ (le ET logique), $\mathbb{N}$ (l'ensemble des entiers).

Remarque :

Si une expression contient un symbole libre alors ce n'est pas une proposition car il nous manque des informations sur le symbole en question pour donner un sens à l'expression (ce qui ne signifie pas qu'une expression sans symbole libre est une proposition, par exemple : un ensemble défini en compréhension ne contient pas de symbole libre).

Opérations sur les ensembles (exemples)

Voici quelques opérations sur les ensembles, définies par compréhension.

Si A et B sont deux ensembles (quelconques), on peut noter $A \cap B$, $A \cup B$, $A \backslash B$, $\mathcal{P}(A)$ les ensembles suivants :

— $A \cap B := \{x : (x \in A) \wedge (x \in B)\}$
— $A \cup B := \{x : (x \in A) \vee (x \in B)\}$
— $A \backslash B := \{x : (x \in A) \vee \neg(x \in B)\}$
— $\mathcal{P}(A) := \{x : (x \subset A)\}$ (où $x \subset A$ signifie que x est un-sous ensemble de A).

Remarque :

Nous donnerons une définition formelle de l'inclusion ($\subset$) après avoir parlé des quantificateurs.

Dans cas $\mathcal{P}(A)$, on constate qu'un élément d'un ensemble peut lui aussi être considéré comme un ensemble.

Souvent, dans un contexte où les éléments et les ensembles sont distincts, on a tendance à nommer les ensembles par des lettres capitales (ex : A) et les éléments par des lettres minuscules (ex a).

Si on doit parler d'ensemble d'ensembles (comme $\mathcal{P}(A)$) ces derniers sont souvent nommés par une lettre capitale ronde (ex : $\mathcal{A}$).

@Binaire

Pas de note complète pour ce chapitre

Conversion nombre binaire

On part du nombre initial en bas. À chaque étape on écrit le quotient entier de la division par 2 au dessus. On lit ensuite de haut en bas en remplaçant

— pair $\rightarrow 0$
— impair$\rightarrow 1$.

Exemple :

0	0
1	1
1	3
1	7
0	14
0	28
1	57

Donc $57_{\text{dix}} = 0111001_{\text{deux}} = 111001_{\text{deux}}$.

Pour la partie fractionnaire

On part du haut, à chaque étape, on multiplie par deux la partie fractionnaire (partie fractionnaire : ce qu'il y a à droite de la virgule), et on écrit le résultat au dessous.

$\ldots$, $\ldots$
0 , 16
0 , 32
0 , 64
1 , 28
0 , 56 (car $0,28 \times 2 = 0,56$)
1 , 12
. , ..
. , ..

On en déduit $0,16_{\text{dix}} = 0,00101\ldots_{\text{deux}}$.

Puisque $57_{\text{dix}} = 111001_{\text{deux}}$ et que $0,44_{\text{dix}} = 0,01110\ldots_{\text{deux}}$ alors on a $57,44_{\text{dix}} = 111001,011100...$

Remarque

Attention : on a bien $16_{\text{dix}} = 10000_{\text{deux}}$ mais $0,16_{\text{dix}} \neq 0,10000_{\text{deux}}$. En fait $0,10000\ldots_{\text{deux}} = 0,10\ldots_{\text{deux}} = 0,5_{\text{dix}}$)

Couples

Vocabulaire (couple)

Si a et b sont des éléments on peut parler du couple (a,b) et aussi parler d'ensemble de couples.

Exemple

$E = \{(1,2),(3,5)\}$
$A = \{(x,y) : (x \in N) \wedge (y \in N) \wedge (x < 10) \wedge (x = 1+y)\}$
$(3,4) \in A$
$(4,3) \notin A$

Remarques

$(1,2) \neq (2,1)$ alors que $\{1,2\} = \{1,2\}$
On peut parler de triplet (x,y,z) de quadruplet (x,y,z,t) ou de n-uplet $(x_1,...,x_n)$.

Produit cartésien (définition)

Soient A et B deux ensembles. Le produit cartésien de A par B est l'ensemble des couples (a,b) où $a \in A$ et $b \in B$. Il est noté $A \times B$.

$$A \times B = \{(a,b) : (a \in A) \wedge (b \in B)\}$$

Remarque

En notant $|A|$ le cardinal d'un ensemble fini A, si B, C sont deux ensembles finis alors on a $|B \times C| = |B| \times |C|$.
On peut noter $A \times A$ par A^2, de même $A^3 := A \times A \times A$.

Quantificateur

Quantificateur universel

L'ensemble universel est l'ensemble qui contient tout le monde. Si $A := \{x : P\}$, une façon d'exprimer "A est l'ensemble universel" est d'écrire :

$$\forall x, P$$

Le symbole $\forall$ (un A à l'envers) peut se lire "pour tout x", la formule ci-dessus peut donc se lire "pour tout x on a P" (c'est une proposition).

Exemple :

On dit que $\ll A$ est inclus dans $B \gg$ (ou $A \subset B$) si $\quad \forall x, ((x \in A) \Rightarrow (x \in B))$.

La proposition $\quad \forall x, \Big(\boxed{x \text{ est un entier pair}} \Rightarrow \boxed{x+1 \text{ est un entier impair}}\Big) \quad$ est vraie car l'ensemble $\{x : (x \text{ est un entier pair}) \Rightarrow \ (x+1 \text{ est un entier impair})\}$ contient tout le monde (est l'ensemble universel, $x+1$ représentant la somme d'un nombre x et de 1).

On rappelle par exemple que $\boxed{\text{"1 est un entier pair"} \Rightarrow \text{"2 est un entier impair"}}$ est vrai car "1 est un entier pair" est faux.

Quantificateur existentiel

L'ensemble vide est l'ensemble qui ne contient personne. Si $A := \{x : P\}$, une façon d'exprimer "A *n'est pas* l'ensemble vide" est d'écrire :

$$\exists x, P$$

Le symbole $\exists$ (le miroir de la lettre E) peut se lire "il existe", la formule se lit donc "il existe x tel que P" (c'est une proposition).

Exemples :

L'énoncé $\ll$ Toute partie de $\mathbb{N}$ non vide admet un plus petit élément $\gg$ (qui est une proposition vraie) peut s'écrire

$$\forall x, \Big(\big(x \in \mathscr{P}(\mathbb{N}) \backslash \{\emptyset\}\big) \Rightarrow \Big(\exists y, \big((y \in x) \wedge \big(\forall z, ((z \in x) \Rightarrow (y \leqslant z))\big)\big)\Big)\Big)$$

Négation d'une proposition avec quantificateur (remarque)

On a $\neg(\forall x, P)$ si et seulement si $\exists x, \neg P$.

On a $\neg(\exists x, P)$ si et seulement si $\forall x, \neg P$, (si on admet que le principe du tiers exclu est vrai).

Ordre des quantificateurs (remarque)

L'ordre des quantificateurs est important et changer cet ordre peut changer le sens de la proposition. Voici deux propositions. La seconde a été obtenue en changeant l'ordre des quantificateurs de la première.

$$(1) \qquad \forall x \in \mathbb{N}, \exists y \in \mathbb{N}, x < y$$

$$(2) \qquad \exists x \in \mathbb{N}, \forall y \in \mathbb{N}, x < y$$

La proposition (1) est vraie alors que la seconde (2) est fausse.

La proposition suivante est également fausse.

$$\exists y \in \mathbb{N}, \forall x \in \mathbb{N}, x < y$$

En revanche, échanger l'ordre de deux quantificateurs de même type ne change pas la valeur de vérité de la proposition. Exemple : $\forall x, (\forall y....)$ est équivalent à $\forall y, (\forall x, ...)$. Ou bien $\exists x, (\exists y....)$ est équivalent à $\exists y, (\exists x, ...)$.

Notations

Si E et P sont des expressions, alors l'expression $\boxed{\forall x A, P}$ est une contraction de $\boxed{\forall x, (xA) \Rightarrow P}$. Exemple : $\forall x > 0 \wedge x < 10, \exists y, x < y$ signifie $\forall x, (x > 0 \wedge x < 10) \Rightarrow (\exists y, x < y)$

Si A est un ensemble et P une proposition, alors l'expression $\boxed{\exists x \in A, P}$ est une contraction de $\boxed{\exists x, (x \in A) \wedge P}$.

Si Q et T sont des symboles de quantification (donc choisis dans $\{\exists, \forall\}$), alors l'expression $\boxed{Qx, Ty, P}$ est une contraction de $\boxed{Qx, (Ty, P)}$.

Si Q est un quantificateur, et P une expression alors l'expression $\boxed{Qx, y, P}$ est une contraction de $\boxed{Qx, (Qy, P)}$.

De manière générale on rencontre souvent quelques raccourcis d'écriture de formules quantifiées par exemple la formule

$$\forall \varepsilon > 0, \exists \eta > 0, \forall x \in D \text{ tq } |x - a| < \eta, |f(x) - l| < \varepsilon$$

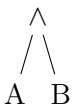
s'écrit de manière plus rigoureuse ainsi

$$\forall \varepsilon, ((\varepsilon \in \mathbb{R} \wedge \varepsilon > 0) \Rightarrow (\exists \eta, (\eta > 0 \wedge \eta \in \mathbb{R} \wedge (\forall x, (x \in D \wedge |x - a| < \eta) \Rightarrow (|f(x) - l| < \varepsilon)))))$$

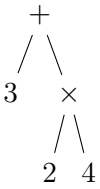
Expressions et parenthèses

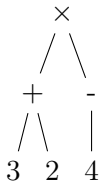
Les expressions écrites jusqu'à présent utilisent des parenthèses pour indiquer leur structure. On peut aussi les voir comme des arbres.

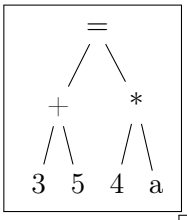
Exemple :

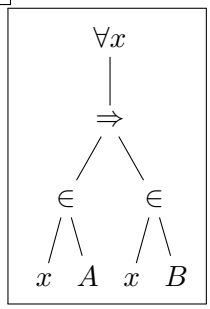
L'expression $\boxed{A \wedge B}$ peut être représentée par l'arbre 

et $\boxed{(A \vee B) \Rightarrow (\neg C)}$ représentée par 

L'expression $\boxed{3 + 2 \times 4}$ peut être représentée par l'arbre 

et $\boxed{(3 + 2) \times (-4)}$ par 

L'expression $3 + 5 = 4 * a$ peut être représentée par l'arbre 

L'expression $\boxed{\forall x, x \in A \Rightarrow x \in B}$ peut être représenté par l'arbre suivant 

Relation binaire et relation interne

Relation binaire (définition)

Soient A et B deux ensembles et R une partie de $A \times B$, on dit que R est une *relation binaire* (ou relation) entre A et B (on peut dire de A vers B). On peut dire aussi que (A, B, R) est une relation.

Notation

Soit $(A, B, R) = G$ une relation, l'expression $(x, y) \in R$ est souvent notée xRy, on peut voir aussi xGy Quelquefois on identifie R à G et on parle de la relation R.

Relation miroir (définition)

Soit (A, B, R) une relation, on pose $Я := \{(x, y) : yRx\}$. Le triplet $(B, A, Я)$ est une relation appelée *la relation miroir* de (A, B, R).

Image par une relation (définition)

Soit $(A, B, R) = \mathcal{G}$ une relation entre les ensembles A et B. Soit E tel que $E \subset A$. On appelle l'image de E par la relation $\mathcal{G}$ l'ensemble $\{x : \exists y, (y \in E) \wedge (yRx)\}$.

Image réciproque par une relation (définition)

Soit $(A, B, R) = \mathcal{G}$ une relation entre les ensembles A et B. Soit F tel que $F \subset B$. On appelle l'image réciproque de F par la relation $\mathcal{G}$ l'ensemble $\{x : \exists y, (y \in F) \wedge (xRy)\}$.

Relation interne (définition)

Soit (A, B, R) une relation, si $A = B$ on dit que c'est une relation *interne* sur A. Dans ce cas on peut dire que (A, R) est une relation interne.

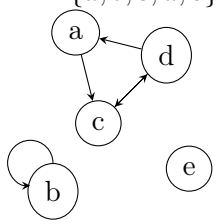
Graphe d'une relation

Si (E, R) est une relation interne avec E fini c'est un cas particulier dit de graphe orienté.

On représente ce graphe par un schéma où chaque élément de E est représenté par un point ou un cercle appelé *sommet* (ou noeud) et chaque élément $(e, b) \in R$ est représenté par une flèche appelée *arc* allant du sommet e au sommet b.

Exemple

$E = \{a, b, c, d, e\}$, $R = \{(a, c), (c, d), (b, b), (d, c), (d, a)\}$.



Propriétés d'une relation interne

Soit R une relation interne d'un ensemble E. On dit que R est ...
- ...*transitive* si $\forall x, y, z \in E, (xRy) \wedge (yRz) \Rightarrow (xRz)$
- ...*réflexive* si $\forall x \in E, (xRx)$
- ...*irréflexive* si $\forall x \in E, \neg(xRx)$
- ...*symétrique* si $\forall x, y \in E, (xRy) \Rightarrow (yRx)$
- ...*antisymétrique* si $\forall x, y \in E, (xRy) \wedge (yRx) \Rightarrow (x = y)$

Relation d'équivalence (définition)

Une relation interne est dite *relation d'équivalence* si elle est transitive, symétrique et réflexive.

Notation

Une relation d'équivalence est souvent notée $\equiv$.

Équivalence et partition (théorème)

Pour un ensemble E il y a une correspondance entre les partitions et les relations d'équivalences.

Exemple

Voici A,E,R. A est une partition de E et (E, R) la relation d'équivalence associée à A.
$E = \{1, 2, 3, 4, 5, 6\}$, $A = \{\{1, 4\}, \{2, 5, 3\}, \{6\}\}$,
$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (1, 4), (4, 1), (2, 5), (5, 3), (3, 2), (5, 2), (3, 5), (2, 3)\}$

Circuit et chemin dans un graphe

Chemin dans un graphe (définition)

Soit (E, R) une relation interne sur E (ou un graphe). Un chemin dans un graphe est une suite finie non vide $x_0x_1x_2 \dots x_k$ de sommets de E telle que $\forall i \in \mathbb{N}, 1 \leqslant i < k \Rightarrow x_iRx_{i+1}$.

Remarques :

En identifiant un graphe par son schéma avec noeud et flèche, un chemin est un déplacement de noeud en noeud en empruntant des flèches dans le bon sens.

Dans des graphes d'une autre nature, ceux où pour chaque couple de sommet il peux exister plusieurs arcs allant du premier au second, la définition d'un circuit doit également inclure le choix de l'arc emprunté entre chaque sommet.

Une liste de 1 seul sommet est aussi un chemin (qui n'emprunte aucun arc).

Longueur d'un chemin (définition)

La longueur d'un chemin dans un graphe est le nombre de sommets du chemin retranché de 1.

Remarques :

La longueur d'un chemin est en fait le nombre d'arcs traversés.

Dans d'autre cas de graphe, par exemple lorsque les arcs sont étiqueté par des nombre, on peut donner d'autre définition de la longueur d'un chemin.

Circuit d'un graphe (définition)

Un circuit d'un graphe est un chemin dont le premier et le dernier sommet de la liste sont égaux.

Graphe sans circuit (définition)

Un graphe est dit *sans circuit* s'il n'existe aucun circuit du graphe de longueur non nulle.

Propriété des graphes sans circuit

Soit un graphe $G = (E, R)$ fini (autrement dit (E, R) relation interne sur E) (fini : $|E| < \infty$). Les propriétés suivantes sont équivalentes :

- G est sans circuit.
- Il n'existe pas de chemin de G passant deux fois par le même sommet.
- Les longueurs des chemins de G sont bornées par $|E|$.
- Les longueurs des chemins de G sont bornées.
- Le nombre de chemins est borné par $|R|^{|E|}$).
- Le nombre de chemins est fini.

Relation d'ordre

Relation d'ordre strict (définition)

Soit (E, R) une relation interne. On dit c'est une relation d'*ordre strict* si elle est irréflexive et transitive. On peut aussi dire que (E, R) est un ensemble *strictement ordonné*.

Notation :

Souvent, une relation d'ordre stricte est notée $<$.

Relation d'ordre large (définition)

Soit (E, R) une relation interne. On dit c'est une une relation d'*ordre large* si elle est réflexive, antisymétrique et transitive. On peut aussi dire que (E, R) est un *ensemble ordonné*(*).

Notation, vocabulaire :

Souvent, une relation d'ordre large est notée $\leqslant$.

Attention, on rencontre quelquefois le terme ensemble ordonné pour parler d'un ensemble strictement ordonné à cause de la correspondance entre deux relations (voir théorème).

Exemple

La relation d'inclusion sur les parties d'un ensemble, est une relation d'ordre (large).

Vocabulaire

Si R est une relation d'ordre strict et que aRb on peut dire que *a est strictement plus petit que b*, ou que *a est strictement inférieur à b* .

Si R est une relation d'ordre large et que aRb on peut dire que *a est plus petit ou égale à b*, ou que *a est inférieur ou égale à b*.

Correspondance ordre strict et large (théorème)

Il y a une correspondance entre les ordres stricts et larges.

Soit $(E, <)$ une relation d'ordre strict. Alors la relation T, $xTy := x, y \in E \wedge ((x < y) \vee (x = y))$ est une relation d'ordre large. Étant associée à $<$, T est plutôt notée $\leqslant$.

Soit $(E, \leqslant)$ une relation d'ordre large Alors la relation S, $xSy := x, y \in E \wedge ((x \leqslant y) \wedge (x \neq y))$ est une relation d'ordre strict. Étant associée à $\leqslant$, S est plutôt notée $<$.

Ordre total (définition)

Soit $(E, <)$ un ensemble ordonné (par un ordre strict ou large). On dit que l'ordre est *total* si

$$\forall x, y \in E, (x < y) \vee (y < x) \vee (x = y)$$

Remarques :

Si un ordre $\leqslant$ n'est pas total alors "$\neg(a \leqslant b)$" n'implique pas forcément "$b < a$".

La relation d'inclusion d'ensemble (sur les sous-ensemble d'un ensemble de cardinal au moins 2) est une relation d'ordre qui n'est pas totale.

Majorant (définition)

Soit $(E, \leqslant)$ un ensemble ordonné (par un ordre large ou strict). Soient $P \subset E$ et $m \in E$. On dit que m est un majorant de P si

$$\forall x \in P, (x \leqslant m) \vee (x = m)$$

Maximum (définition)

Soit $(E, \leqslant)$ un ensemble ordonné (par un ordre large ou strict). Soit $m \in E$ majorant de E. On dit que m est un (le) *maximum* de $(E, \leqslant)$.

Maximal (définition)

Soit $(E, <)$ ensemble ordonné (par un ordre large ou strict). Soit $M \in E$. On dit que M est un élément *maximal* de $(E, <)$ si

$$\forall x \in E, \neg(M < x) \vee (x = M)$$

Remarque

Si un maximum existe alors il est unique et c'est un maximal.

Si l'ordre est total alors tout élément maximal est maximum.

Ordre (ordre miroir)

Soit $(E, <)$ une relation d'ordre stricte alors la relation R, $xRy := (x, y \in E) \wedge (y < x)$ est un ordre strict appelée miroir de $<$. Souvent on le note en renversant le symbole d'origine (ici $>$ donc).

Définition (minorant, minimum, minimal)

Soit $(E, <)$ une relation d'ordre strict. Soit $m \in E$. On dit que ...

— ...m est un minimum si m est un maximum de $(E, >)$.

— ...m est minimal si m est un maximal de $(E, >)$.

— ...m est un minorant de P ($P \subset E$), si m est un majorant de P dans $(E, >)$.

Fonctions (ou applications)

Vocabulaire relation (définitions)

Soit (A, B, R) une relation (R une relation entre les deux ensembles A et B).

— A est appelé l'ensemble de départ.

— B est appelé l'ensemble d'arrivé.
— l'ensemble $\{x : \exists y, xRy\}$ est appelé *l'ensemble de définition* (ou *domaine*) de la relation.
— l'ensemble $\{x : \exists y, yRx\}$ est appelé *l'image* de la relation.
— Si xRy, x est appelé un *antécédent* de y et y est appelé une *image* de x.

Exemple

On considère la relation (X, T, U) avec $X = \{a, b, c\}, T = \{1, 2, 3, 4\}, U = \{(a, 3), (c, 3), (a, 4), (c, 2)\}$
Son ensemble de départ est X (donc $\{a, b, c\}$),
son domaine est $\{a, c\}$,
son ensemble d'arrivé est T (donc $\{1, 2, 3, 4\}$),
son image est $\{2, 3, 4\}$.

Fonction partielle (définition)

Soit (A, B, R) une relation. On dit que c'est une *fonction partielle* (à gauche) si tout élément de A est en relation avec au plus 1 élément de l'ensemble B.

Formulation symbolique

Grâce aux symboles on peut reformuler cette définition : La relation $R = (A, B, T)$ est une fonction partielle si et seulement si $\forall x, y, z, (xTy \wedge xTz) \Rightarrow y = z$

Remarque

On dit que R est une fonction partielle à droite si tout élément de B est en relation avec au plus 1 élément de l'ensemble A.

Si on omet d'indiquer ≪à gauche≫ ou ≪à droite≫, la convention est ≪à gauche≫.

Quelquefois on trouve l'utilisation du terme *fonction* comme synonyme du terme fonction partielle.

Application (définition)

Soit (A, B, R) une relation. On dit que c'est une *application à gauche* (ou application) si c'est une fonction partielle et que son domaine de définition est A.

Notation :

Si une relation est une application, on a tendance la nommer par des lettres minuscules grandes (comme f, t, d, l et pas comme a, i, o, u, U, R).

Si f est l'application alors xfy se note $f : x \mapsto y$. On dit que y est l'image de x par f et que x est un antécédent que y par f.

≪ La relation (A, B, f) est une application ≫ se note $f : A \longrightarrow B$.

Si $f : A \longrightarrow B$ et que $x \in A$ alors l'unique élément y tel que $f : x \mapsto y$. est noté $f(x)$.

Remarque :

On peut voir des opérations binaires (comme l'addition ou la multiplication) comme des applications partant d'un produit cartésien. Exemple : l'addition sur les nombres entiers est une application de $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, la division est une application de $/ : \mathbb{R} \times (\mathbb{R} \setminus \{0\}) \longrightarrow \mathbb{R}$.

Exemple :

Si on pose $g : \mathbb{N} \longrightarrow \mathbb{N}$ avec $g : x \mapsto x + 1$ alors on a $g : 0 \mapsto 1$, $g : 12 \mapsto 13$, $g(39) = 40$.

Suite (définition)

Soit A un ensemble. Soit f une application de $\mathbb{N}$ dans A est f est appelée une *suite* de A.

Remarque :

Lorsque l'ensemble d'arrivé (ici A) de la suite est $\mathbb{R}$ on parle d'une suite de nombres ou de *suite numérique*.

On peut également utiliser le terme *suite* lorsque l'ensemble de départ est de la forme $\{i, i + 1, i + 2, i + 3, ...\}$ où i est un nombre entier autre que 0 (positif ou négatif).

Notation :

On utilise souvent des lettres U, V, W, Y, X pour nommer les suites.

Pour une suite $U : \mathbb{N} \longrightarrow \mathbb{R}$ et un nombre entier k on voit souvent écrit U_k au lieu de $U(k)$.

On introduit quelquefois une suite avec la notation suivante : $(U_n)_{n \in \mathbb{N}}$

On peut voir une suite numérique comme une liste infinie de nombre.

Exemple

$U : n \mapsto 3 \times n$ est une suite. $U(0) = U_0 = 3 \times 0 = 0, \quad U_1 = 3 \times 1 = 3, \quad U_2 = 3 \times 2 = 6, U_3 = 3 \times 3 = 9, \ldots$.

Ensemble image (définition)

Soit E un ensemble. Soit $f : E \longrightarrow F$, et A tel que $A \subset E$. On pose G ainsi

$$G := \{y : \exists x, (x \in A) \wedge (y = f(x))$$

G est appelé l'*image de A par f*.

Notation

L'image d'un ensemble A par une application f est notée $f(A)$.

Remarque

Une application $f : E \longrightarrow F$ induit une application de l'ensemble des parties de E vers l'ensemble des parties de F.

Image réciproque (définition)

Soient E, F des ensembles, soit B tel que $B \subset F$. Soit $f : E \longrightarrow F$. On pose H ainsi

$$H := \{x : f(x) \in B)$$

H est appelé l'*image réciproque* de A par f.

Notation (abusive)

L'image réciproque d'un ensemble B par une application f est (abusivement) notée $f^{-1}(A)$.

Remarque

Une application $f : E \longrightarrow F$ induit une application de l'ensemble des parties de F vers l'ensemble des parties de E.

Composition de relation (définition, théorème)

Soient $(A, B, R) = U$ et $(B, C, T) = V$ deux relations. On pose $H := \{(x, y) : \exists b, (xRb) \wedge (bTy)\}$. (A, C, H) est une relation appellée la *composition* de U puis V.

Composition d'applications (théorème)

Soient $f : A \longrightarrow B$ et $g : B \longrightarrow C$ deux applications.
Alors la composition de f puis g est aussi une application notée $g \circ f$.

Remarque

Le théorème reste valable en remplaçant le terme "application" par le terme "fonction partielle".

La notation $g \circ f$ (f à droite) est bien la composition de f puis g. Cette inversion est due à l'écriture traditionnelle préfixe des fonctions : $g(f(x))$ est la notation de l'image x auquel on a applique f puis g.

Injective (définition)

Soit $f : A \longrightarrow B$ une application. On dit que f est *injective* si c'est une fonction partielle à droite.

Remarque

On peut dire aussi que f est une *injection*.

Surjective (définition)

Soit $g : A \longrightarrow B$ une application. On dit qu'elle est *surjective* si son image est B.

Remarque

On peut dire que g est une *sujection*.

S'il existe une injection d'un ensemble A vers B alors il existe une surjection de B vers A.

Bijective (définition)

Soit $h : A \longrightarrow B$ une application. On dit qu'elle est *bijective* si elle est injective et surjective.

Exemple/Remarques

On dit aussi que h est une *bijection*.

La fonction $x \mapsto x + 1$ sur $\mathbb{N} \longrightarrow \mathbb{N}$ est injective mais non bijective car non surjective (son image ne contient pas 0).

En revanche, la fonction $x \mapsto x + 1$ sur $\mathbb{Z} \longrightarrow \mathbb{Z}$ est bijective.

Application réciproque (définition, théorème)

Soit $f : E \longrightarrow F$ une application bijective alors le miroir de f (vue en tant que relation) est aussi une application appelée *application réciproque* de f.

Notation

Si f est une application bijective, on note f^{-1} son application réciproque.

Si f est bijective alors l'image réciproque d'un ensemble B par f est également l'image directe de B par f^{-1} où f^{-1} est la réciproque de f (d'où peut-être la notation abusive).

Ensemble en bijection (définition)

Soit $h : A \longrightarrow B$ une application bijective. On dit que A *est en bijection avec* B.

Remarque :

La relation "est en bijection avec" est une relation d'équivalence sur les ensembles.

Si A est en bijection avec B dit qu'ils *équipotents* ou qu'ils ont le même cardinal.

Barbier (théorème)

Il n'existe pas de bijection d'un ensemble E vers l'ensemble de ses parties (ensemble des parties de E : $\mathscr{P}(E)$).

Idée de preuve

Par l'absurde. On suppose qu'il existe f une telle bijection (i). On pose $A := \{x : x \notin f(x)\}$. On choisit r tel que $f(r) = A$. Si $r \in A$ alors par définition de A on a $r \notin f(r)$, c'est à dire $r \notin A$, contradiction. Si $r \notin A$, c'est à dire $r \notin f(r)$ donc $r \in A$ par définition de A donc contradiction.

En définitive, on ne peut avoir ni $r \in A$ ni $r \notin A$ ce qui est absurde, la supposition (i) ne tient pas.

Remarque

Le théorème est valable si on remplace bijection par surjection.

Double injection (théorème)

S'il existe une injection d'un ensemble A dans un ensemble B et s'il existe une injection de B dans A alors

A est en bijection avec B.

Remarques :

Il existe une injection d'un ensemble A vers un ensemble B si et seulement si il existe une surjection de B vers A (pour information la réciproque nécessite l'axiome du choix).

Dénombrable (définition)

Un ensemble en bijection avec $\mathbb{N}$ est dit *dénombrable*.

Exemple

$\mathbb{N}$ est dénombrable.

$\mathbb{Z}$ est dénombrable.

$\mathbb{Q}$ est dénombrable.

$\mathbb{N} \times \mathbb{N}$ est dénombrable (on peut écrire $\mathbb{N}^2$ est dénombrable).

Remarque

Quelques auteurs rangent les ensembles finis parmi les ensembles dénombrables (c'est une question de convention). On pourrait aussi parler d'un ensemble "au plus dénombrable".

Un ensemble est dénombrable si on peut énumérer un à un tous ses éléments.

L'ensemble $\mathbb{R}$ est en bijection avec $\mathscr{P}(\mathbb{N})$ et n'est donc pas dénombrable.

Fonctions de $\mathbb{R}$ dans $\mathbb{R}$ usuelles

Fonction numérique (définition)

On appellera *fonction numérique* une fonction partielle ayant $\mathbb{R}$ pour ensemble de départ et d'arrivé.

Remarque :

Ici on fait bien une différence entre l'ensemble de départ et le domaine de définition d'une fonction. Le domaine de définition est inclus dans l'ensemble de départ.

Les fonctions numériques forment un ensemble contenant les applications de $\mathbb{R}$ dans $\mathbb{R}$.

Le domaine de définition d'une fonction numérique est en pratique très souvent un intervalle de $\mathbb{R}$ ou l'union de plusieurs intervalles.

Les nombres réels (vocabulaire)

L'ensemble des nombres réels, noté $\mathbb{R}$ n'est pas aussi simple à "cerner" que les ensembles $\mathbb{Q}$ (rationnels) ou $\mathbb{N}$ (naturels).

Une façon courante (et correcte) de décrire cet ensemble est de dire que chacun de ses éléments (les nombres réels) peut être représenté par une liste infinie de chiffres (chiffre : élément de {0,...,9} ; ou de {0,1} en binaire) avec une virgule quelque part (exemple 008511,597230732053.....) et éventuellement un signe devant. Cette représentation est appelée le *développement décimal d'un nombre.*

Cette représentation pose plusieurs problèmes dont le problème majeur suivant : comment décrire cette liste infinie de chiffre ? La réponse est simple lorsque cette liste infinie se termine en réalité par une série finie de chiffres infiniment répétée (par exemple $1,0000...$ ou $\frac{1}{7} = 0,14285714285714....$), mais comment donner le développement décimal de n'importe quel nombre réel ?

La réponse est plutôt démoralisante : pour la "majorité" des nombres réels on ne peut pas (voir remarque), cependant pour certains nombres réels remarquables (comme π ou $\sqrt{2}$) c'est possible. Pour représenter une liste infinie, on pourrait utiliser une suite de chiffre (c'est a dire une application de $\mathbb{N}$ dans $\{0,1,...,9\}$) qui nous donnerait directement la liste. Cette méthode est difficile à manipuler (par exemple comment faire la somme de deux nombres où commence-t-on l'opération ?). Les mathématiciens (dont Cauchy) utilisent une manière plus "souple" : ≪Chaque nombre réel peut être représenté par une suite de nombres rationnels vérifiant la propriété de Cauchy≫ (dite "suite de cauchy rationnelle").

Pour se faire une idée plus concrète de ce que ça représente on peut prendre l'idée intermédiaire suivante : chaque nombre réel est une suite de nombre décimal (décimal : qui peut s'écrire comme une liste finie de chiffre avec une virgule) et la propriété de Cauchy d'une telle suite signifie en gros que chaque position décimal (exemple de position décimale : chiffre des dizaine, chiffre des millième) finit par se fixer. Par exemple π (3,1415926535..) peut être représentée par la suite de nombre qui commence ainsi :
6,4 5,1 4,452 3,21 3,145 3,1415 3,145446 3,141592544
Le chiffre des dizainez se fixe à 0, le chiffre des unités finit par se fixer à 3, pareil pour celui des dixièmes qui se fixe à 1, pareil pour les centièmes, ...

En réalité les mathématiciens ne se restreignent pas suite de nombres décimaux mais acceptent toute suite de nombres rationnels, ce qui rend leur manipulations encore plus facile (mais restant cependant "consistant" avec l'idée d'une liste infinie). Par exemple voici une suite de rationnels u qui pourrait servir à représenter $\sqrt{2}$, $u_0 = 1$ $u_{n+1} = \frac{u_n + \frac{2}{u_n}}{2}$. $u_1 = 3/2$ $u_2 = 17/12$ En calculant $u_2 \times u_2$ on trouve déjà un nombre proche de 2,0069.

Les opérations sur $\mathbb{R}$ se font naturellement, pour deux nombres réels a et b, donc ayant deux suites de rationnels associées A et B la somme de a et b sera donnée par la suite $n \mapsto A_n + B_n$, les autres opérations, valables sur les nombres rationnels s'étendent ainsi aux nombres réels.

C'est pour la comparaisons de réels que cette représentation sous la forme de suite de rationnels nous pose plus de problème par rapport au developpement décimal : deux suites différentes sur les premiers termes peuvent finalement "se rapprocher infiniment" sur les derniers

termes (exemple $n \mapsto 1/n$ et $n \mapsto -1/n$), il est quelquefois difficile de s'en rendre compte, donc comment savoir si ces deux suites ne sont pas en fait le même nombre réel. En fait le problème survient aussi sous forme de developpemnet décimal, par exemple le nombre 0,99999999... est égale au nombre 1.

Les paragraphes qui suivent, entre autres, formalisent les idées présentées ici.

Remarque :

Vu comme une liste infinie de chiffre (binaire ou décimaux) un réel peut être vu comme un point sur une droite.

On ne peut trouver un moyen concret de représenter chacun des nombres réels comme on le fait par exemple avec les fractions pour les nombres rationnels. La raison est que les nombres réels sont "beaucoup plus nombreux" que les "phrases/formules/expression/liste de mots énonçables". Les listes finies de mots forment un ensemble dénombrables et les réels sont en bijections avec les parties d'un ensemble dénombrable or le théorème intitulé (barbier) permet de conclure.

Nature corpusculaire* de $\mathbb{R}$

L'ensemble des nombres réels n'est pas vide il contient au moins l'élément 0 et l'élément 1.

L'ensemble est ordonné par une relation $<$. Il y a deux opérations importantes sur les réels très universellement notées $+$ et $\times$. On peut voir chacune d'elles comme une application de $\mathbb{R} \times \mathbb{R}$ (l'ensemble des couples d'éléments de $\mathbb{R}$) vers $\mathbb{R}$.

— $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$

— $\times : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ (quelquefois on note $ab = a \times b$).

De plus pour tout nombre réel x, y, z on a :

(a) $(x + y) + z = x + (y + z)$ ($+$ associative)

(b) $0 + x = x + 0 = x$ (0 élément neutre de $+$).

(c) $\exists x', x + x' = 0$ (inverse pour $+$) (x' est noté $-x$)

(d) $x + y = y + x$ ($+$ commutative)

(e) si $y < z$ alors $x + y < x + z$ (relation compatible avec $+$).

(f) $0 < 0$ est faux (irreflexivité de $<$**)

(g) si $0 < y$ et $0 < x$ alors $0 < x + y$ (transitivité de $<$**)

(h) on a soit $x = 0$, soit $0 < x$, soit $x < 0$ (ordre total*)

(i) $x \times (y \times z) = (x \times y) \times z$ ($\times$ associative)

(j) $x \times (y + z) = (x \times y) + (x \times z)$ ($\times$ distributive à gauche sur $+$)

(k) $1 \times x = x \times 1 = x$ (1 élément neutre de $\times$)

(l) si $0 < x$ et $0 < y$ alors $0 < x \times y$ (anneau ordonné).

(m) si $y \neq 0$ alors $\exists y', y \times y' = 1$ (inverse pour $\times$) (y' noté $\frac{1}{y}$ ou $1/y$)

(n) $x \times y = y \times x$ ($\times$ commutative)

Remarque :

**Vu que la relation $<$ est compatible avec $+$, c'est ainsi que l'on peut simplifier les propriétés de transitivité, d'irreflexivité et d'exhaustivité de $<$ (car dire que $a < b$ est équivalent à dire que $0 < b + (-a)$).

*Un meilleur titre serait : propriétés de l'ensemble des réels dues à sa qualité de corps.

Les propriétés (a) et (b) font de $\mathbb{R}$ munit de l'opération $+$ un monoïde. Les propriétés (a), (b) et (c) font de $\mathbb{R}$ munit de l'opération $+$ un groupe. $\mathbb{R}$.

Toutes ces propriétés, qui sont vérifiés par $\mathbb{R}$, font de $(\mathbb{R}, +, \times, <)$ (ou $\mathbb{R}$) un corps ordonnés. Il existe plusieurs corps ordonnés par exemple $(\mathbb{Q}, +, \times, <)$. Certains auteurs considère aussi le corps contenant un seul élément (qui vérifie aussi les propriété précédentes). Nous verrons dans la suite, que $\mathbb{R}$ vérifie en plus la propriété de la borne supérieure ce qui le distingue de tout autre corps.

On a, soit un corps ordonné est le corps à un élément, soit le corps ordonné "contient" $(\mathbb{Q}, +, \times, <)$ et vérifie $1 \neq 0$.

Notation :

Pour $a \in \mathbb{R}$ on note $|a|$ la *valeur absolue* de a. $|a|$ vaut $-a$ si $a \leqslant 0$ et a si $a > 0$.

$a \times \frac{1}{b}$ est noté $\frac{a}{b}$.

$a + (-b)$ est noté $a - b$.

Si $k \in \mathbb{Z}$, et a réel. Si $k > 0$ on note $a^k = a \times a \times .... \times a$ k fois. Si $k < 0$ et $a \neq 0$ on note $a^k = \left(\frac{1}{a}\right)^{-k}$. Si $k = 0$ et $a \neq 0$ on note $a^0 = 1$. Il n'y a pas de convention universelle pour la valeur de 0^0.

Les deux opérations ne sont pas symétriques l'une est distributive sur l'autre. On note $\times$ implicitement, sans parenthèse elle l'emporte sur $+$. Par exemple $(a \times b) + c = ab + c$.

Propriétés dérivées

Les propriétés suivantes sont valables sur $\mathbb{R}$ (ou sur tout corps ordonné contenant plus d'un seul élément). On peut les déduire des propriétés (a) à (n) précédentes. Soient x, y, z, t des éléments quelconques de $\mathbb{R}$ (ou du corps) alors

— $0 < 1$
— La valeur absolue de $\left|\frac{x}{y}\right|$ vaut $\frac{|x|}{|y|}$.
— $(x + y)(z + t) = xz + xt + yz + yt$
— l'inverse de 1 est 1.
— $(-x)y = x(-y) = -xy$
— si $x \neq 0$ l'inverse de $\frac{x}{y}$ existe et vaut $\frac{y}{x}$.
— $<$ est un ordre strict.
— $x < y$ ou $y < x$ ou $x = y$ (ordre total).
— $x \times y = 0$ si et seulement si $a = 0$ ou $b = 0$.
— si $z \neq 0$ et $t \neq 0$ alors $\frac{x}{t}\frac{y}{z} = \frac{xy}{zt}$ et $\frac{x}{t} + \frac{y}{z} = \frac{xz+yt}{zt}$.
— si $x < y$ et $t < z$ alors $x + t < y + z$ et si de plus $0 < x$ et $0 < t$ alors $x \times t < y \times z$.
— si $x < y$ et $t < 0$ alors $y \times t < x \times t$.
— si $a \neq 0$ $\frac{a}{a} = 1$.

@Suite de $\mathbb{Q}$-Cauchy (définition)

Soit U une suite à valeurs dans $\mathbb{Q}$ ($U : \mathbb{N} \to \mathbb{Q}$), on dit que U est une suite de $\mathbb{Q}$-Cauchy si

$$\forall K \in \mathbb{N} \setminus \{0\}, \exists N \in \mathbb{N}, \forall n \in \mathbb{N} \wedge n > N, \forall k \in \mathbb{N} \wedge k > N, |U_n - U_k| < \frac{1}{K}$$

@Corps des réels (définition/construction)

L'ensemble des réels est l'ensemble des classes d'équivalences des suites de $\mathbb{Q}$-Cauchy sur $\mathbb{Q}$ dont la différence $\mathbb{Q}$-tend vers 0. Ces classes étant compatibles avec l'addition et la multiplication sur $\mathbb{Q}$, on peut définir ces opérations sur l'ensemble des classes ce qui en fait un corps.

Pour l'ordre, on peut considérer les suites de Cauchy qui ne convergent pas vers 0 et qui sont strictement positives après un certain rang et constater que cet ensemble est compatible avec les classes d'équivalence formant ainsi les réels positifs. Finalement on constate que cet ensemble engendre une relation d'ordre total qui fait de $\mathbb{R}$ un corps totalement ordonné qui de plus vérifie l'axiome de la borne supérieure.

@Limite de suite (définition)

Soit U une suite numérique, et ℓ un nombre réel. On dit que U admet ℓ comme limite (ou que U converge vers ℓ) si $\forall \epsilon$ tq $(\epsilon > 0) \wedge (\epsilon \in \mathbb{R}), \exists N \in \mathbb{N}, \forall n > N, |U_n - \ell| < \epsilon$

Remarques/notations :

Si une suite admet une limite on dit que la suite converge. On dit aussi que U converge vers ℓ.

Tout suite qui admet une limite est une suite de cauchy.

Dans $\mathbb{R}$ toute suite de cauchy admet une limite c'est d'ailleurs une des raisons pour laquelle on travail avec $\mathbb{R}$.

On peut noter $\lim_{n\to\infty} U_n = \ell$ pour dire que la suite U converge vers ℓ.

Une autre manière de dire que U converge vers ℓ est de dire que
Pour tout nombre ϵ strictement positif, les éléments de la suite U qui sont à une distance de ϵ ou plus de ℓ sont en nombre fini.

@Les suites bornées croissantes de $\mathbb{R}$ convergent (théorème)

Soit U une suite numérique. Si

i $\forall k, \ell, (k \leqslant \ell) \Rightarrow (U_k \leqslant U_\ell)$ (i.e : U est croissante).
ii $\exists M \in \mathbb{R}, \forall n, U_n < M$ (i.e : U est majorée).
alors la suite U converge dans $\mathbb{R}$.

Remarque :

Une autre manière d'énoncer le théorème est de dire que toute suite numérique croissante et bornée admet une limite dans $\mathbb{R}$.

Si un corps ordonné verifie une sorte d'équivalent du théorème (en remplaçant $\mathbb{R}$ par le corps et en remplaçant la notion de convergence car cette dernière utilise la notion de valeur absolue) alors ce corps est *isomorphe* à $\mathbb{R}$ (isomorphe un peu comme "pareil à").

@Caractérisation des réels (théorème)

Soit $K = (E, +, \times, <)$ un corps ordonné ayant au moins deux éléments. Les quatres propriétés suivantes sont équivalentes.

- K est isomorphe à $\mathbb{R}$ (isomorphe : il existe une bijection de K et $\mathbb{R}$ qui respecte(ou conserve) les opérations et relations $+, \times, <$ de $\mathbb{R}$).
- K vérifie la propriété de la borne supérieure. (c-a-d : pour toute partie P de E l'ensemble de ses majorants... soit est E si $P = \emptyset$, soit est vide si P non majoré, soit admet un minimum).
- Toute suite croissante et majorée de K, K-converge.
- K est archimédien(*) et K-complet.

Remarque :

Pour un corps ordonné K selon une relation $<$

1. La notion de K-convergence est de converger mais selon une notion particulière de distance entre deux éléments a et b qui est la plus grande valeur (selon $<$) entre $a - b$ et $b - a$.
2. la notion d'une suite de K-Cauchy est celle d'être une suite de Cauchy en ayant remplacé la notion de distance entre deux éléments a et b par la plus grande valeur (selon $<$) entre $a - b$ et $b - a$.
3. La notion K-Complet est d'être complet relativement aux suites de K-Cauchy.
4. On dit qu'un corps ordonné est archimédien si tout élément du corps est plus petit qu'une somme de la forme $1 + 1 + 1..... + 1$.

@Point d'accumulation d'un ensemble (définition)

Soit D une partie de $\mathbb{R}$ et soit $a \in \mathbb{R}$.
Si on peut trouver une suite dont les termes sont dans $D \backslash \{a\}$ et qui converge vers a
alors on dit que a est un point d'accumulation de D.

Remarque/exemple :

Autrement dit D contient une infinité de points infiniment proches de a.

Un point d'accumulation de D n'appartient pas forcément à D.

Exemple : 0 est un point d'accumulation de $]0, 1]$.

Un point de $\mathbb{R}$ qui n'est pas un point d'accumulation de D peut être appelé *point isolé* de D (souvent on sous-entend qu'un point isolé appartient à l'ensemble).

La notion de point d'accumulation nous sera utile pour la définition du nombre dérivé et limite d'une fonction.

@Limite d'une fonction (définition)

Soit f une fonction numérique ayant pour domaine D ($D \subset \mathbb{R}$), soit a un point d'accumulation de D ou appartenant à D et soit ℓ un nombre réel.

On dit que la limite de f en a est ℓ si $\forall \epsilon > 0, \exists \eta > 0, \forall x \in D$ tq $|x - a| < \eta, |f(x) - \ell| < \epsilon$.

Remarque

Si la limite existe elle est unique.

Il faut que $a \in D$ ou que a soit un point d'accumulation de D autrement la limite n'est pas unique (tout réel pourrait convenir).

Lorsque $a \in D$ alors forcément $l = f(a)$ et on dit que f est continue en a.

Si $a \in D$ et a n'est pas un point d'accumulation de D alors la limite existe et vaut $f(a)$. C'est un cas peu interessant.

Si E est une expression, et que on peut considérer que soit a est soit un élément soit un point d'accumulation du domaine de définition de la fonction $x \mapsto E$ alors l'expression $\lim_{x \to a} E = \ell$ signifie que la fonction $x \mapsto E$ admet une limite en a.

ℓ est la limite de f est équivalent à dire que pour toute suite U de D qui converge vers a alors la suite $n \mapsto f(U_n)$ converge vers ℓ.

@Nombre dérivé d'une fonction (définition)

Soit f une fonction (partielle) de $\mathbb{R}$ dans $\mathbb{R}$ ayant D comme domaine de définition. Soit a un réel qui est un point d'accumulation de D tel que f ait pour limite l en a. Soit d un nombre réel.

On dit que d est le *nombre dérivé* de f en a si

$$\lim_{x \to a} \frac{f(x) - l}{x - a} = d.$$

Remarques/exemples/vocabulaire :

Dans la notation ci-dessus, il est sous-entendu que le symbole muet x vérifie $x \in D$ (car $f(x)$ est présent) et que $x \neq a$ (car on divise par $x - a$).

Une fonction en un point d'accumulation de son domaine de définition (ici D) n'admet pas forcément de nombre dérivé. Par exemple, la fonction valeur absolue $|x|$ n'admet pas de dérivée en 0.

Dans le cas où f admet un nombre dérivé d en un point d'accumulation a on dit aussi que f est *dérivable* en a de dérivée d. On peut également dire que la dérivée de f en a est d, que f admet d comme dérivée en a.

Si un nombre dérivé d'une fonction en un point d'accumulation existe alors il est unique.

Il ne suffit pas (et il n'est même pas nécessaire) que a soit un point de D (D domaine de définition de f) il faut (et il suffit) que a soit un point d'accumulation de D autrement il pourrait exister plusieurs nombres d satisfaisants la formule ci-dessus.

Notre définition de la dérivée n'est pas traditionnelle elle est légèrement plus générale. La définition commune énonce plus de contraintes sur a, lorsqu'elle s'applique notre définition s'applique également et est équivalente à la définition commune.

Lorsqu'il existe, le nombre dérivé de f en a est le coefficient principal de la fonction affine (simple) qui est la plus *proche* de f au point a.

Dans le cas où l'on peut tracer la courbe de f dans un voisinage de a alors cette courbe passe par le point (a,l) et le nombre dérivé s'il existe est la pente d'une droite qui serait tangente à la courbe de f au point (x,l). L'équation de cette droite est $x \mapsto d \cdot (x - a) + l$.

Le nombre d est aussi la tangente de l'angle ("la tangente d'un angle" $\neq$ "la tangente à une courbe en un point") formée par cette droite avec l'axe des abscisses d'un repère orthonormé. En pratique on rencontre souvent cette valeur sous forme de pourcentage : un pourcentage de 100 représente une pente qui forme un angle de 45 degrés avec l'axe des abscisses (horizontale) (exemple : indication de la pente sur un autoroute).

Fonction dérivée (définition)

Soit f une fonction numérique on note f' la fonction qui en chaque point où f est dérivable associe son nombre dérivé en ce point on l'appelle la *dérivée* de f.

Notations et fonctions usuelles

notation exposant entier positif Si n est un entier non nul et a un réel, le produit $a \times a \times a \times \cdots a$ est noté a^n (a apparaît n fois dans le produit). Exemple $a^3 = a \times a \times a$. Particularité : $a^1 = a$ et si a est non nul on a $a^0 = 1$. Par contre la valeur de 0^0 ne fait pas consensus.

notation exposant entier négatif si n est un entier strictement négatif et a un réel non nul $a^n = \frac{1}{a} \dots \frac{1}{a}$ où $\frac{1}{a}$ est l'inverse de a et apparait $-n$ fois dans le produit.

exponentielle L'exponentielle, notée exp est une application bijective de $\mathbb{R}$ vers l'ensemble des réels strictement positifs (ce dernier est noté $\mathbb{R}^{*+}$).
On peut définir la fonction ainsi pour tout réel x $\exp(x) = \lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n$.
Pour un nombre réel x on note souvent $e^x := \exp(x)$ l'image de x par l'exponentielle. Cette notation, qui ressemble à la notation de la puissance, est choisie car l'exponentielle vérifie $\forall x, y, \exp(x+y) = \exp(x) \times \exp(y)$ (d'où $e^{x+y} = e^x \times e^y$). De plus, parmi les applications de $\mathbb{R}$ vérifiant cette propriété, elle est la seule qui admet le nombre dérivé 1 en 0.
La fonction exponentielle est la seule application numérique définie sur $\mathbb{R}$ qui soit égale à sa dérivée et prenant la valeur 1 en 0.

logarithme népérien La fonction exponentielle étant une bijection de $\mathbb{R}$ vers $\mathbb{R}^{+*}$ son miroir est aussi une application (de $\mathbb{R}_+^*$ vers $\mathbb{R}$) appelée *logarithme népérien*. Si x est un nombre strictement positif, l'image de x par la fonction logarithme népérien est notée $\ln(x)$. Étant la réciproque de l'exponentielle on a la propriété suivante $\forall x, y \in \mathbb{R}_+^*, \ln(x \times y) = \ln(x) + \ln(y)$.

notation puissance Pour a un réel strictement positif et x un réel quelconque, on note a^x le nombre $\exp(\ln(a) \times x)$. Si $x > 0$ on note $0^x = 0$. Cette notation recouvre la notation exposant lorsque x est entier, ça tombe bien, les réels designés sont égaux.
Pour finir la notation a^x n'a **pas** de sens (ou alors a un sens non traditionnel) dans les deux cas suivants
— $a = 0$ et $x \leqslant 0$.
— si $a < 0$ et x non entier.

racine carré On pose $\mathbb{R}_+^*$ l'ensemble des nombres positifs ou nuls. L'application $x \mapsto x^2 : \mathbb{R}_+^* \to \mathbb{R}_+^*$ est bijective. Pour $x \in \mathbb{R}_+$ on note $\sqrt{x}$ son antécédent par cette fonction. On a $\forall x \in \mathbb{R}_+, \sqrt{x} = x^{\frac{1}{2}}$.

racine n-ième Soit n un nombre entier positif. On pose $\mathbb{R}_+$ l'ensemble des nombres positifs ou nuls. L'application $x \mapsto x^n : \mathbb{R}_+^* \to \mathbb{R}_+^*$ est bijective. Pour $x \in \mathbb{R}_+$ on note $\sqrt[n]{x}$ son antécédent par cette fonction. On a $\forall x \in \mathbb{R}_+$, $\sqrt[n]{x} = x^{\frac{1}{n}}$

cosinus et sinus En identifiant un angle à un point sur le cercle de rayon 1 et ayant comme origine le centre d'un repère orthonormé, le cosinus d'un angle est son abscisse et le sinus d'un angle est son ordonné.
Pour faire correspondre un point du cercle et un angle : L'angle 0 est le point $(1, 0)$, on se déplace sur le cercle dans le sens inverse des aiguilles d'une montre. Pour un angle en degrés le tour complet donne 360. Pour un angle en radians le tour complet donne $2 \times \pi$ (avec $\pi \simeq 3,1415\ldots$), c'est la "vraie" longueur parcourue sur le cerle).
La fonction cosinus est souvent notée cos et la fonction sinus souvent notée sin ($\cos(0) = 1$ alors que $\sin(0) = 0$).

partie entière supérieure Pour un nombre réel x il existe un unique nombre entier k vérifiant $k - 1 < x \leqslant k$. k est appelé la partie entière supérieure de x. Un tel nombre k est noté $\lceil x \rceil$.

partie entière (inférieure) Pour un nombre réel x il existe un unique nombre entier k vérifiant $k \leqslant x < k + 1$. Le nombre k est appelé la partie entière inférieure (ou simplement partie entière) de x. Un tel nombre k est noté $\lfloor x \rfloor$.

partie fractionnaire La partie fractionnaire d'un nombre réel x, souvent notée $\{x\}$, vérifie $\{x\} = x - \lfloor x \rfloor$. On a toujours $0 \leq \{x\} < 1$.

valeur absolue La fonction valeur absolue appliquée à un nombre réel x est notée $|x|$. Elle vaut x si x est positif et $-x$ si x est négatif.

division euclidienne réelle. Pour deux nombres réels x et y avec $y \neq 0$ il existe un nombre entier k et un nombre réel r vérifiant $x = ky + r$ et $0 \leqslant r < |y|$. De plus le couple (k, r) est unique. Le nombre k est appelé le quotient entier de la division de x par y et r le reste de la division de x par y.

Calcul de dérivée

Voici différents théorèmes et formules permettant de calculer le nombre dérivé d'une fonction exprimée comme une composition de plusieurs autres fonctions.

(f0) La dérivée est une notion locale (théorème)

Soient $f : F \to \mathbb{R}$ et $g : G \to \mathbb{R}$ deux applications numériques avec $F \subset G$ et vérifiant $\forall x \in F, g(x) = f(x)$. Soit a point d'accumulation de F (donc aussi de G).

Si g admet le nombre dérivé d en a alors f aussi.

Il existe des contres exemples à la réciproque, cependant si il existe I un intervalle ouvert de $\mathbb{R}$ contenant a tel que $I \cap G \subset F$ et si f admet le nombre dérivé d en a alors g aussi.

(f1) La dérivée de l'identité ou d'une fonction constante (théorème)

Si f est une fonction numérique constante (constante : ayant pour image un ensemble à un seul élément) elle admet la dérivée 0 en n'importe lequel des points d'accumulations de son domaine de définition. La fonction $x \mapsto x : \mathbb{R} \to \mathbb{R}$ (l'identité) admet pour dérivé 1 en tout point de $\mathbb{R}$.

(f2) Dérivée de composition de fonction (théorème)

Soit a un nombre réel et soient f et g des fonctions numériques telles que l'image de g soit incluse dans le domaine de définition de f. On suppose que :

- g admet un nombre dérivé en a (que l'on notera $g'(a)$). (Cela a entre autre pour conséquence que $g(a)$ est un point d'accumulation de l'image de g donc du domaine de f).
- f admet un nombre dérivé en $g(a)$ (que l'on notera $f'(g(a))$).

Alors la fonction $x \mapsto f(g(x))$ admet $g'(a) \times f'(g(a))$ comme nombre dérivé en a.

(f3) Produit, somme de dérivées (théorème)

Soient K, C deux nombres réels. Soient f et g des fonctions numériques ayant le même domaine de définition D. Soit a un point d'accumulation de D tel que f et g dérivables en a. On note eventuellement $f(a)$, $g(a)$ leurs limites en a et $f'(a)$, $g'(a)$ leurs nombres dérivés en a. On a les conséquences suivantes :

- (f4) La fonction $x \mapsto K \times f(x) + C \times g(x)$ est dérivable en a de dérivée $K \times f'(a) + C \times g'(a)$.
- (f5) La fonction $x \mapsto f(x) \times g(x)$ est dérivable en a de dérivée $f'(a) \times g(a) + g'(a) \times f(a)$.
- (f6) Si $g(a) \neq 0$ alors la fonction $x \mapsto \frac{f(x)}{g(x)}$ (définie pour $g(x) \neq 0$) est dérivable en a de dérivée $\frac{f'(x) \times g(a) - f(a) \times g'(a)}{g(a)^2}$
- (f7) Si $0 < g(a)$ ou si $K > 1$ la fonction $x \mapsto C \times (g(x))^K$ est dérivable en a de dérivé $C \times K \times g'(a) \times (g(a))^{K-1}$.

(f8) Dérivée de réciproque (théorème)

Soit D une partie de $\mathbb{R}$ et a un point d'accumulation de D. Soit $g : D \to G$ bijective et $f : G \to D$ sa fonction réciproque. g admet un nombre dérivé non nul (appellons-le $g'(a)$) en a si et seulement si f admet le nombre dérivé $\frac{1}{g'(a)}$ en $g(a)$ (ça implique notamment que $g(a)$ est un point d'accumulation de G).

Remarques :

Chacune de ces formules est évidemment démontrable (sauf erreur dans la formule) à partir de la définition donnée plus haut, démonstration que nous ne donnerons pas ici.

(f8) Il existe des bijections de $\mathbb{R}$ dans $\mathbb{R}$ dont les dérivées s'annulent en certains points, en conséquence leurs réciproques ne sont pas dérivables (ou de dérivée infinie). Par exemple la dérivée de $x \mapsto x^3$ s'annule en 0 ainsi sa réciproque, $x \mapsto \sqrt[3]{x}$, est en 0 de dérivée infinie (formellement la fonction n'est donc pas dérivable en 0).

Dérivée de fonction (théorèmes)

Soit x un nombre réel quelconque

- La fonction cos est dérivable en x, $\cos'(x) = -\sin(x)$
- La fonction sin est dérivable en x, $\sin'(x) = \cos(x)$
- La fonction exp est dérivable en x, $\exp'(x) = \exp(x)$
- Si $x > 0$ la fonction ln est dérivable en x, $\ln'(x) = \frac{1}{x}$.

Résumé

- exposant Pour $a, b \in \mathbb{R}$, a^b a un sens sauf lorsque $a < 0$ et b non entier ou si $a = 0$ et $b \leqslant 0$. Lorsque cela à un sens on a : $\left(\frac{a}{b}\right)^c = \frac{a^c}{b^c}$ $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$ $(ab)^c = a^c b^c$ $a^{bc} = \left(a^b\right)^c$ $a^{b+c} = a^b a^c$

Induction

Suite par récurrence (vocabulaire)

Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ une application de $\mathbb{R}$ dans $\mathbb{R}$ et soit $a \in \mathbb{R}$. On peut définir une suite numérique U en posant

$U_0 = a$

$U_{n+1} = f(U_n)$ si $n > 0$.

Remarque

On a donc $U_0 = a$, $U_1 = U_{0+1} = f(U_0) = f(a)$, $U_2 = U_{1+1} = f(U_1) = f(f(a))$, $U_3 = U_{2+1} = f(U_2) = f(f(f(a)))$, ...

On dit que la suite U est définie par *récurrence*. On peut definir U_{n+1} en fonction de plusieurs termes précédents.

Exemple

On pose $V_0 = 3$ et $V_{n+1} = 2 \times V_n + 1$. On a $V_0 = 3$, $V_1 = 7$, $V_2 = 15$, $V_3 = 31$, $V_4 = 63$,...

La suite de Fibonacci (appellons-la F), est définie par $F_0 = 0$ $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$.

Si F est la suite de Fibonacci on a $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$,...

Par récurrence (théorème)

Soit A une partie de $\mathbb{N}$. Si $0 \in A$ et si $\forall n, (n \in A) \Longrightarrow (n + 1 \in A)$ alors

$\mathbb{N} = A$.

Remarque

Une preuve qui utilise ce théorème est appelé un raisonnement *par récurrence*.

Ce théorème donne une propriété sur les entiers.

Exemple

On peut montrer par récurrence que la suite V précédemment définie ainsi $V_0 = 3$ et $V_{n+1} = 2V_n + 1$ (donc par récurrence), vérifie $V_n = 2^{2+n} - 1$.

Ensemble défini par induction

On peut définir un ensemble par une sorte de récurrence. On appelle ça définir par induction (ou une définition inductive).

Exemple :

L'ensemble des nombres entiers $\mathbb{N}$ peut être ainsi défini

$n \in \mathbb{N} := (n = 0) \vee (\exists r, (n = (T, r)) \wedge (r \in \mathbb{N}))$ (où T est un symbole qu'on introduit pour la définition)

Arbre binaire

On appelle arbre binaire les éléments de l'ensemble A.

$$a \in A : (a = \bot) \vee (\exists r, \exists l, (l \in A) \wedge (r \in A) \wedge ((r, l) = a))$$

Langage

Mot sur un ensemble (définition)

Soit A un ensemble. On définit l'ensemble des mots sur A comme l'ensemble de toutes les suites finies d'éléments de A.

Exemple/notation/remarque

Si A est un ensemble, on note A^* : les mots sur A.

Dans ce contexte, A est nommée l'*alphabet* de A^* et les éléments de A sont nommés les *lettres*.

Le mot vide est un mot, on le note souvent ϵ, il ne contient aucune lettre.

On a $\{a, b\}^* = \{\epsilon, a, b, aa, bb, ab, ba, aaa, aab, aba, baa, bba, bab, abb, bbb, aaaa, \dots\}$

Souvent, on identifie abusivement une lettre à un mot de longueur 1 (i.e $A \subset A^*$)

Si w est un mot on peut écrire w_1 comme la première lettre de ce mot, w_2 comme la seconde, w_k étant la k ième lettre du mot si w est de longueur k. Par exemple : si w est le mot $abcda$ alors $w_1 = a$, $w_4 = d$, $w_5 = a$.

Longueur d'un mot (définition)

La longueur d'un mot est le nombre de lettre (avec répétitions) qu'il contient.

Exemple/remarque/notation

On peut identifier un mot de longueur n avec un n-uplet, ainsi $A^* = A^0 \cup A^1 \cup A^2 \cup A^3 \cup \dots$

On pourrait définir l'ensemble des mots par induction : $w \in A^* := (w = \epsilon) \vee (w = (x, m) \wedge x \in A \wedge m \in A^*)$.

Si $\{x, y\}$ est l'alphabet, la longueur de xyx est 3, la longueur de ϵ est 0, la longueur de $aaaa$ est 4.

Pour un mot w on note $|w|$ sa longueur, $|bbbb| = 4$, $|\epsilon| = 0$.

On a $|\{w : w \in \{i, j, k\}^* \wedge |w| = 5\}| = 3^5$.

Concaténation de mots (définition)

Soient w et m deux mots sur un alphabet fini A. On appelle la *concaténation* de w avec m le nouveau mot formé en écrivant w puis m l'un à la suite de l'autre.

Exemple/notation

L'opération de concaténation est quelquefois notée $\circ$.

Pour deux mots m et w, on note aussi mw la concaténation de m et w.

Si $m = xyx$ et $w = yxx$ alors $mw = xyxyxx$ et $wm = yxxxyx$ La concaténation du mot abb avec le mot ba donne le mot $abbba$.

$bab \circ aa = babaa$.

Mot miroir (définition)

Soit A un ensemble fini, soit n un entier positif ou nul et soit w un mot de longueur n. Le miroir du mot w, souvent noté w', est le mot $w_n w_{n-1} \dots w_2 w_1$. Le mir

Exemples :

Le miroir du mot $abcde$ est $edcba$. Le miroir du mot vide ϵ est lui-même. Le miroir d'un mot à une lettre est lui-même. Le miroir de abc est lui-même.

Lorsque le miroir d'un mot est lui-même on dit que c'est un *palindrome*.

Ordre lexicographique (définition,théorème)

Soit A un alphabet fini totalement ordonné, par un ordre $<_A$.

On va définir $<_{\text{lex}}$ une relation d'ordre totale sur A^* à partir de $<_A$.

— On pose $\forall m \in A^* \backslash \{\epsilon\}$, $\epsilon <_{\text{lex}} m$.

— $\forall x, y \in A$, si $x <_A y$ alors $\forall m, w \in A^* \, xw <_{\text{lex}} ym$

— $\forall w, m, v \in A^*$, si $w <_{\text{lex}} v$ alors $mw <_{\text{lex}} mv$.

Remarque

Si A est notre alphabet usuelle avec l'ordre alphabetique $a < b < c < d \cdots < z$ l'ordre lexicographique sur A est tout simplement notre classement alphabétique.

Ordre militaire (définition)

On définit un ordre (noté $<_{\text{mil}}$ ainsi : pour deux mots w, m sur un alphabet A on dira que $w <_{\text{mil}} m$ soit si $|w| < |m|$, soit si $|w| = |m|$ et $w <_{\text{lex}} m$.

Remarque

Dit autrement, avec l'ordre militaire, on compare deux mots en comparant leurs longueurs et si les mots sont de même longueur on les compare avec l'ordre lexicographique.

Langage (définition)

Soit A un alphabet. On appelle langage sur A (ou langage) un sous ensemble de A^*.

Remarque

Un langage n'est qu'un simple ensemble de mots.

Produit de langage (définition)

Soient L et M deux langages. Le produit de L par M est l'ensemble des mots :

$$\{u/u = w \circ v \wedge (w \in L) \wedge (v \in M)\}$$

Remarque/notation/exemple

On parle aussi de concaténation de langages à la place de produit de langage.
Attention l'ordre du produit est important (le produit n'est pas commutatif).
Le produit de deux langages est un langage.
On note LM le produit de L par M, on peut aussi le noter $L \circ M$.
Si M est un langage. MM peut être noté M^2, $MMM = M^3$,...
Par convention on note $M^0 = \{\epsilon\}$ où ϵ représente le mot vide.
Si $M = \{ab, c, d\}$ et $L = \{b, a\}$ alors $ML = \{abb, aba, cb, ca, db, da\}$.
Si $H = \{aa, a\}$ et $N = \{b, ab\}$ alors $HN = \{ab, aaab, aab\}$.

Étoile de Kleen (définition)

Pour un langage L, l'ensemble $\{\epsilon\} \cup L \cup L^2 \cup L^3$.... est appelé *fermeture itérative* de L et est noté L^*.

Remarque

Pour un langage L on note L^* la fermeture itérative de L.

Si on identifie un alphabet A avec l'ensemble des mot à une lettre sur A on a justement A^* comme l'ensemble de tous les mot sur A.

La fermeture itérative est également appelée Étoile de Kleen ou cloture itérative.

Si $L = \{c, ab\}$ alors
$L^* = \{\epsilon, \quad c, ab, \quad cc, cab, abc, abab, \quad ccc, cabab, ababab, abcc, cabc, ccab, abcab, ababc \quad , \dots\}$

Expression régulière (définition)

Une *expression régulière* (ou *expression rationnelle*) est une expression qui représente un langage. Elle utilise des lettres, le symbole | qui représente l'union ensembliste en notation infixe, le symbole * qui représente l'opération "étoile de Kleen" d'un langage en notation suffixe, le symbole 1 qui représente $\{\epsilon\}$ (un singleton contenant le mot vide) et le symbole 0 qui représente $\emptyset$ (l'ensemble vide). Chaque lettre a représente l'ensemble $\{a\}$ (ensemble avec un le mot a à une lettre). L'opération "produit de langage" est notée implicitement.

Remarques :

Aux symboles des expressions régulière ci-dessus s'ajoute les parenthèses.

L'expression rationnelle $\boxed{\text{(a|b)c}}$ représente l'ensemble $\{\text{ac}, \text{bc}\}$.

Dans une expression régulière le symbole | est quelquefois remplacé par +.

0 n'est vraiment utile que pour représenter l'ensemble vide. Toute expression régulière représentant un langage non vide peut facilement et avantageusement se passer de 0.

Plusieurs expressions régulières différentes peuvent représenter un même langage.

Langage rationnel (définition)

Un langage que l'on peut décrire par une expression régulière est appelé un langage *rationnel*.

Remarques

Un langage rationnel est aussi appelé un langage *régulier*, de façon générale pour qualifier un langage ou une expression les mots rationnel/rationnelle régulier/régulière sont synonymes.

Il existe des langages qui ne sont pas rationnels, par exemple ≪les mots sur $\{a, b\}$ ayant autant de fois la lettre a que la lettre b≫ n'est pas un langage rationnel.

Stabilité des langages rationnels (théorème)

Soient K et L deux langages rationnels. Alors
— KL (le produit de K et L) est un langage rationnel.
— $K \cup L$ (l'union de K et L) est un langage rationnel.

— $K \cap L$ (l'intersection de K et L) est un langage rationnel.
— $K \backslash L$ (la différence ensembliste de K privé de L) est un langage rationnel.
— K^* (la cloture itérative de K) est un langage rationnel.

Remarque :

On peut résumer le théorème précédent en disant que l'ensemble des langages rationnels est stable par : union, intersection, différence, produit, cloture itérative.

Une idée de la preuve de ce thèorème figure plus tard, dans la partie automate.

Automate

Automate (définition)

Soit A un aphabet fini. On dit qu'un quintuplet (E, T, f, I, F) est un automate sur A si les conditions suivantes sont toutes vérifiées :

1. E est un ensemble fini, appelé ensemble des *états* de l'automate.
2. T est un ensemble fini, appelé ensemble des *transitions* de l'automate.
3. f est une applications de T dans $E \times A^* \times E$.
4. I et F sont des sous ensembles de E, appelé respectivement les états *initiaux* et les états *terminaux* de l'automate.

Remarques/vocabulaire

On peut représenter un automate sur un alphabet A sous la forme d'un graphe orienté dont les noeuds (E) sont les sommets et les transitions (T) sont les arcs étiquetés par des mots sur A.

On peut décomposer f en trois fonctions $f_i : T \to E$ $f_t : T \to A^*$ et $f_f :\to E$. Pour $\ell \in T$ on a $f(\ell) = (f_i(\ell), f_t(\ell), f_f(\ell))$ que l'on appelera respectivement état de *départ*, *étiquette*, et état d'*arrivée* de la transition ℓ.

Chemin dans un automate (définition)

Un chemin (fini) dans un automate (E, T, f, I, F) est une liste finie de transitions $t_1, t_2, \ldots, t_{k-1}, t_k$, telle que l'état de départ de t_1 soit un état initial (état de I), que l'état d'arrivé de t_k soit un état terminal (état de F). et que pour deux transitions du chemin qui se suivent, l'état d'arrivé de la première soit l'état de départ de la seconde. La liste des transitions peut eventuellement être vide mais dans ce cas il faut la "remplacer" par un état qui soit un état initial et terminal en même temps.

Remarque

k est appellée la longueur du chemin.

Mot associé à un chemin (définition)

A tout chemin de l'automate (de la forme $t_1, t_2, \ldots, t_k$ où les t_i sont des transitions de l'automate) on associe un mot qui est la concaténation, dans l'ordre, des étiquettes des transitions.

Mot reconnu (définition)

Soit B un automate sur l'alphabet A. On dit qu'un mot w sur A est *reconnu* par l'automate B s'il existe dans B un chemin associé au mot w allant d'un état initial à un état terminal de B.

Langage reconnu par un automate (définition)

Soit B un automate. L'ensemble des mots reconnus par B est appelé le *langage reconnu* par B.

Langages rationnels=langages reconnus (théorème)

Les langages rationnels sont **les** langages reconnaissables par un automate.

@idée de preuve

On transforme facilement une expression régulière en automate équivalent. Pour transformer un automate en expression régulière équivalente on peut procéder ainsi : Commencer par

décrire l'automate par trois matrices dont les coefficients sont des expressions régulière : une matrice carrée T (d'adjacence) pour les transitions, une matrice colonne F indiquant par un 1 les états terminaux (0 sinon) et une matrice ligne I indiquant états initiaux de la même manière. Calculer le produit matriciel $I(T^0 + T + T^2..)F = IT^*F$, où la somme usuelle est remplacée par l'union, le produit remplacé par le produit de langage et voir que le résultat est une matrice 1×1 dont le (seul) coefficient est l'expression rationnelle du langage reconnu par l'automate. En exemple, si l'automate possède deux états et si on pose $T = [a \quad b; c \quad d]$ alors on peut écrire $T^* = [k \quad kbd^*; d^*ck \quad d^*ckbd^*]$ avec $k = (a|bd^*c)^*$ (il n'y a pas qu'une seule expression pour T^*). Pour calculer T^* pour plus de deux états on peut décomposer T en sous-matrices.

Problème :

La suite essaye de répondre à la question ≪Comment savoir si un mot donné est reconnu par un automate ?≫.

Automate déterministe complet (définition)

On dit qu'un automate sur un alphabet A est *déterministe complet* s'il vérifie les deux propositions suivantes :

— il possède exactement un seul état initial,
— pour chacun de ses état e et pour chaque lettre a de A, il existe une seule transition sortant de l'état e étiqueté par le mot a (mot à une seule lettre),
— de plus ces transitions sont les seules qui sortent de e.

Remarque

La définition d'un automate déterministe complet implique que chaque transition d'un automate déterministe complet est étiquetée par un mot à une lettre, et que chaque état possède exactement $|A|$ transitions sortantes.

Savoir si un mot est reconnu par un automate déterministe complet est relativement simple (contrairement au même problème dans un automate quelconque).

Équivalence d'automate (définition)

Soient deux automates B et C. On dit qu'ils sont équivalents si le langage reconnu par B est égale au langage reconnu par C.

Déterminisation d'un automate (théorème, algorithme)

Pour un automate B (sur un alphabet A) quelconque il existe un automate complet déterministe C (et un algorithme pour le contruire) tel que C et B reconnaissent le même langage.

Idée de preuve, de construction d'un automate déterministe

Etape 1 : chaque transition étiqueté par un mot à plusieurs lettres est transformé par une suite de transitions étiquetées par un mot à une lettre. Après il ne reste donc que des transitions étiquetés par le mot vide ou un mot à une lettre.

Étape 2 : Les états du nouvel automate seront des ensembles d'états de l'ancien. L'idée est de lire en parallèle chaque lettre de l'alphabet de l'automate A pour savoir quel est l'ensemble des états atteints. L'état initial du nouvel automate est l'ensemble des état initiaux de l'ancien. Il faut penser aussi que si il existe une transition étiqueté par le mot vide allant d'un état e à un état i alors si e est dans un ensemble d'état du nouvel automate, i doit l'être aussi (le contraire n'est pas toujours vrai).

En pratique on ne s'interesse qu'aux ensembles d'états accessibles en partant de I.

@idée de preuve du théorème "stabilité des langages rationnels"

Il suffit de montrer que chaque opération sur un ou plusieurs langages se transforme en opération sur un automate qui reconnaît le langage. Complémentaire : échanger état terminaux et non terminaux sur l'automate déterministe équivalent au langage. Intersection : faire un nouvel automate, avec entre autre un produit cartésien des états des deux automates. Pour l'union, le produit, et la clôture (*) il suffit de rajouter des états et transitions bien choisis aux automates de départ.

@Problème :

Une solution à la question ≪Comment savoir si deux expressions rationnelles (ou deux automates) représentent (ou reconnaissent) le même langage ?≫ utilise la notion d'automate minimal (sous-entendu : automate déterministe complet ayant le plus petit nombre d'états).

@Automate déterministe complet minimal (définition)

Un automate déterministe complet M est dit minimal s'il n'existe pas d'automate déterministe complet ayant strictement moins d'états que M.

@Remarque :

Il existe peut-être un automate ayant moins d'états qu'un automate déterministe complet minimal mais dans ce cas cet automate n'est pas déterministe.

@Isomorphe (définition)

Soient deux automates (E, T, f, I, F) et (E', T', f', I', F'). On dit que ces deux automates sont isomorphes si il existe deux bijections $\ell : E \to E'$ et $t : T \to T$ telles que $\ell(I) = I'$, $\ell(F) = F'$ et pour tout $\tau \in T$ $f'(t(\tau)) = (\ell(f_i(\tau)), f_t(\tau), \ell(f_f(\tau)))$.

@Remarque :

Deux automates sont dit isomorphes lorsqu'ils sont "égaux" mais pas formellement.

Lorsque deux automates sont isomorphes alors il reconnaissent le même langage, la réciproque n'est pas toujours vraie même si les deux automates sont déterministes.

Savoir si deux automates donnés sont isomorphes est un problème difficile dans le cas général. Si les deux automates sont déterministes complets alors le problème est simple, il suffit de partir de l'état initial de chacun.

@Unicité de l'automate déterministe complet minimal (théorème)

Soient deux automates déterministes complet minimaux, alors on a ils reconnaissent le même langage ssi ils sont isomorphes.

États équivalents

Soit un automate B, on dit que deux états p et q de B sont *équivalents* si l'ensemble des mots associés aux chemins partant de p et aboutissant sur un état final sont les mêmes que pour les chemins partant de q (et aboutissant sur un état final).

Remarques :

Si deux états d'un automate sont équivalents alors on peut en supprimer un des deux tout en "déplaçant" toutes les transitions y aboutissant vers l'état restant sans changer le langage reconnu par l'automate.

@Critère pour être complet et minimal (théorème)

Soit un automate déterministe complet alors cet automate est déterministe complet minimal si et seulement si tout état est "accessible" à partir de l'état initial, et s'il ne possède pas deux états équivalents.

Remarque :

De ces théorèmes on peut en déduire un algorithme pour savoir si deux automates (ou deux expressions régulières) quelconques sont équivalents (ie : représente le même langage).

Machine de Turing

Machine de turing (définition)

Soit A un alphabet fini. On dit qu'un quintuplet (E, f, i, a, r) est une machine de turing sur A si les conditions suivantes sont toutes vérifiées :

1. E est un ensemble fini, appelé ensemble des *états* de la machine.
2. i, a et r sont des états de E, a est appelé l'état acceptant, r est appelé l'état réfutant et i est appelé l'état initial.
3. f est une application de $(E\backslash\{a, r\}) \times (A \cup \{\perp\})$ dans $E \times (A \cup \{\perp\} \cup \{\rightarrow, *, \leftarrow\})$ où $\perp$, $*$, $\rightarrow$ et$\leftarrow$ ne sont pas des éléments de A.
   f peut être appelé le programme de la machine.

Mot pointé (ou ruban) (définition)

Soit A un alphabet fini et $M = (E, f, i, a, r)$ une machine de Turing sur A. On appelera mot pointé (ou ruban) de la machine M un triplet (w, e, u) où w et u sont des mots sur l'alphabet $A \cup \{\perp\}$ et e un état de M différent de a et r.

Remarque :

On a l'habitude de représenter un mot pointé par un ruban sans extremité, découpé en une inifinité de cases et ayant une tête de lecture, étiquetée par l'état e de la machine, qui pointe vers une des cases. Chaque case contient un élément de $A \cup \{\perp\}$, les valeurs des cases sont determinées par w et u, la tête pointant sur la case représenté par la première lettre de u. Les cases non décrites par w et u contiennent la valeur $\perp$.

Action élémentaire d'une machine sur un mot pointé (ou ruban) (définition)

Une machine de Turing définit une application de l'ensemble des mots pointés vers l'ensemble des mots pointés de la façon décrit ci-après. Nous appelerons cette application *action élémentaire* de la machine sur un mot pointé (ou ruban).

Soit $M = (E, f, i, a, r)$ une machine de Turing sur l'alphabet A. Soit $W = (w, e, u)$ un mot pointé de M.

1. Si $u = \epsilon$ (ϵ=le mot vide) alors on pose $s = \perp$ et $v = \epsilon$. Si u n'est pas vide alors on pose s la première lettre de u et v le reste du mot (donc $u = sv$, avec eventuellement $v = \epsilon$). Si $w = \epsilon$ alors on pose $t = \perp$ et $m = \epsilon$. Sinon w n'est pas vide et on pose t la dernière lettre de w et m le reste du mot (donc $w = mt$, avec eventuellement $m = \epsilon$).
2. Finalement on peut écrire $W \simeq (mt, e, sv)$. On pose $(e', k) = f(e, s)$ (possible car $e \neq a$ et $e \neq r$) e' étant un état. On a soit $k \in A$, soit $k = \perp$, soit $k = \rightarrow$, soit $k = \leftarrow$, soit $k = *$.
3. — si $k = *$ alors le nouveau mot pointé est (mt, e', sv).
   — si $k = \rightarrow$ alors le nouveau mot pointé est (wts, e', v).
   — si $k = \leftarrow$ alors le nouveau mot pointé est (w, e', tsv).
   — si $k \in A$ ou $k = \perp$ alors le nouveau mot pointé est (mt, e', kv).

Remarque :

Si on assimile un mot pointé par une tête de lecture pointant un état de la machine et une case d'un ruban infini alors on peut résumer l'opération ainsi :

1. f nous donne un couple (e', k) en fonction du symbole et de l'état pointé par la tête de lecture.
2. Après coup la tête est étiqueté par l'état e', et modifie le ruban en fonction de k.
   — si $k = \rightarrow$ la tête se déplace vers la droite (vers la gauche si $k = \leftarrow$, reste sur place si $k = *$),
   — si $k \in A$ ou $k = \perp$ alors le symbole de la case pointé est remplacé par k.

Fonction sur les mots, associée à une machine de Turing

Une machine Turing définit une fonction partielle de A^* vers $A^* \times \{a, r\}$ de la manière suivante :

Soit w un mot de A^*, en partant mot pointé (ϵ, i, w), on applique plusieurs fois l'action élémentaire de la machine, à chaque fois sur le dernier mot pointé obtenu, jusqu'à possiblement atteindre l'état a ou r et ainsi terminer le processus (attention rien ne garanti qu'un de ces états sera atteint). Le mot pointé final sera donc de la forme (m, a, u) ou (m, r, u). On retire tous les symboles $\perp$ de u et m pour obtenir u' et m', des mots de A^*. Le résultat final est soit le couple $(m'u', a)$, dans ce cas on dit que que le mot w est accepté soit le couple $(m'u', r)$ et dans ce cas on dit que le mot w est refusé dans tous les cas l'image de w par la machine est de la forme $(m'u', x)$ (où $x \in \{a, r\}$).

La fonction n'est pas forcément définie sur tout mot car il est possible de ne jamais atteindre l'état a ou l'état r.

Remarques :

Pour certaines machines il est difficile de savoir si un mot w possède une image. Encore plus pour tous les mots de A^*.

La machine de Turing est un des premiers modèles historiques d'ordinateur.

Une machine de Turing possède un aspect supérieur à un ordinateur réel car elle possède un nombre infini d'états (ruban infini) cependant elle n'est (actuellement) pas materiellement constructible pour cette raison.

La machine de Turing, modèle universel

Une machine de Turing a l'avantage d'avoir un modèle de fonctionnement relativement simple. En contrepartie, pour un problème donné, même simple, construire la fonction f qui résout ce problème (on pourrait voir ça comme "programmer" la machine) peut s'avérer fastidieux.

Du à la simplicité de fonctionnement, tenter de simuler une machine de Turing à partir d'un autre modèle de calcul est d'ordinaire un problème simple à résoudre.

On peut construire une machine de Turing capable de simuler n'importe quelle autre machine de Turing. On appelle une telle machine une machine de Turing universelle. Plus précisément, on dit qu'une MdT(A) (Machine de Turing sur l'alpabet A) M est universelle si

$$\forall N \in \text{MdT}(B), \forall m \in B^*, \exists u \in A^*, M \text{ appliqué à } u \text{ simule le calcule de } N \text{ appliqué à } m$$

Actuellement, tout modèle de calcul materiellement constructible connu peut être simulé par une machine de Turing bien choisie. Autrement dit, il n'existe pas de modèle de calcul pouvant faire plus que ce que peut faire une machine de Turing universelle.

En conséquence du fait précédent, lorsqu'un modèle de calcul peut simuler n'importe quelle machine de Turing il peut simuler n'importe quel autre modèle. On dit que ce modèle est *Turing complet*. Souvent on abuse du terme (un ordinateur réel n'est pas Turing complet par exemple, mais en supposant que sa mémoire RAM est infinie alors il l'est).