Les nombres, d'où viennent-ils ?

Ils ont une propriété humaine extraordinaire : ils sont un concept universel, une idée indépendante de la culture, de la civilisation et de l'époque de l'histoire de l'humanité.
Dire *les nombres grecs, romains, indiens, égyptiens, mésopotamiens, chinois ou amérindiens* n'a pas de sens.
Mais dire *les numérations grecque, romaine, indienne, égyptienne, mésopotamienne, chinoise ou amérindienne* nous dit une riche réalité.
Un ensemble écrit {a , a , a , a , a , a , a} ou avec des bâtons IIIII II suggèrent dans nos cerveaux *hephta* et grec, *sept* en français, *seven* en anglais ou *sbe* en arabe, ces expressione désignant le même nombre entier naturel.
Alors existerait-il une conceptualisation de ce nombre commune à tous les humains quelle qu'en soit son écriture ou sa prononciation ?
Oui !
Ce document propose une *théorie ensembliste des nombres* pouvant convenir – moyennnnant bien entendu la mobilisation d'interprètes d'une langue à l'autre – à tout habitant de notre terre.

Disons " à la louche" …

Au commencemant est le *rien* et l'idée d'un ensemble qui ne contient rien, le *sunyata* sanskrit qui nous dit que *Tout est par nature interdépendant et donc vide d'existence propre*, le *sifr* arabe signifiant *vide*, devenu notre *zéro*, et par anamorphose et glissement de sens *chiffre*, cet ensemble vide écrit $\varnothing$.
Mais si $\varnothing$ ne contient rien, $\varnothing$ est un objet et on conçoit un ensemble contenant cet objet et lui seul et qu'on écrit $\{\varnothing\}$, appelle "un" et écrit 1.
Puis la *comptine* se poursuit : on réunit les ensembles 1 et {1}, c'est-à-dire conçoit l'ensemble $1 \cup \{1\}$ donc l'ensemble $\{\varnothing , \{\varnothing\}\}$ composé de deux objets, qu'on appelle "deux" et écris 2.
Puis on conçoit l'un après l'autre $2 \cup \{2\} = 3$, $3 \cup \{3\} = 4$, $4 \cup \{4\} = 5$, $5 \cup \{5\} = 6$, $6 \cup \{6\} = 7$, et vous devinez la suite.
Que ce soit quelque part dans une comptine ou en regardant une collectivité de sept cailloux ou des sept caractères "a" de {a , a , a , a , a , a , a} ou des sept bâtons 𝍸 II notre cerveau *pense* le même nombre, que les Français appellent sept et écrivent 7 parce que notre mémoire est *associative* (elle mémorise la simultanéité de ce que nous percevons) en une fraction de seconde. C'est possible que parce que des neurones de notre cerveau sont organisées d'une certaine manière permettant l'*apprentissage non supervisé* qui consiste à exciter en même temps quatre lots de neurones, l'un par la vue de la collectivité d'objets un autre par la pensée du nombre, et deux autres par son nom et son écriture, une activité très intense et inconsciente de notre cerveau durant notre petite enfance.

Les collectivités d'objets en mathématiques

Peut-on définir un ensemble par une phrase ?
Une phrase a un sujet, c'est-à-dire un mot désignant la chose dont elle parle.
Si une phrase $\mathcal{P}$ porte sur le sujet x – écrivons ça $\mathcal{P}(x)$ – elle nous dit des faits, vrais pour certains sujets x et fausse pour d'autres.
On pense à la collectivité des sujets x pour lesquels $\mathcal{P}(x)$ est vraie. C'est simple, non ?
Non.
Nommons par exemple A l'ensemble des sujets x – si il existe – pour lesquels la phrase "x n'appartient pas à x " est vraie. Considérone le cas $x = A$. Alors si cette phrase est vraie x est dans A et à cause de ce que dit la phrase x est hors de A ! C'est le **paradoxe de Russel**.
Voilà qui fait désordre dans nos idées.
La collectivité des x pour laquelle la phrase "x n'appartient pas à x " ne peut pas être un ensemble.
En mathématiques une phrase comme " x n'appartient pas à x " définit ce qu'on appellera une *collection*.
En conséquence, si dans le langage commun *ensemble* et *collection* sont synonymes, ces mots ne le sont pas en mathématiques !

Ordinaux et nombres entiers naturels

La théorie des ordinaux éclaire vivement l'origine conceptuelle des nombres. Chaque nombre est un ordinal.
Mais on va voir qu'il existe bien plus d'ordinaux que de nombres.
La récurrence définira un premier lot d'ordinaux, leur commencement de leur collection.
On montrera que la réunion des nombres vus comme des ordinaux est un ordinal qui sera l'ensemble des entiers naturels.

Référence sur la Toile :
http://tsmaths.free.fr/Prepa/LesNombres/Lesnombresreels.pdf

Ch01 Théorie des ensembles

§01 Les propositions en mathématiques

1. Une **proposition** est une phrase. On les désignera par un caractère *MONOTYPE CORSIVA* suivi d'une paire de parenthèses dans laquelle on écrit évetuellement son objet.
   Exemple : $\mathcal{P}(x)$ = "le nombre x est pair".
2. Une **proposition décidable** par définition ne peut être que vraie ou fausse. Exemple si $\mathcal{P}(x)$ = "le nombre x est pair", alors $\mathcal{P}(10)$ est vraie et $\mathcal{P}(7)$ est fausse.

$\mathcal{P}$	v	f	1
non$\mathcal{P}$	f	v	2

Tableau 1 : négation

3. Un **argument logique** est le sujet d'une proposition. Dans l'exemple précédent x est l'argument de $\mathcal{P}(10)$. Une proposition peut avoir plusieurs arguments. Par exemple "la multiplication de x par y donne z".
4. Selon le choix de valeur d'un des arguments appelé **paramètre** la vérité d'une proposition peut changer.
5. Exemple : pour $\mathcal{P}(x\ ,\ b)$ = "le nombre $x + b$ est pair" on a $\mathcal{P}(5\ ;\ 3)$ vraie et $\mathcal{P}(8\ ;\ 3)$ fausse. Ici 3 est une valeur du paramètre b et 5 et 8 deux valeurs de la variable x.
   Généralisons : "pour b donné $\mathcal{P}(x\ ,\ b)$" est une proposition qui a x comme **variable** et b comme **paramètre**.
6. Une **table de vérité** donne les vérités possibles d'une combinaison de propositions.
7. La **négation** d'une proposition consiste à inverser sa vérité (tableau 1).
8. Une **proposition** sans variable est dite **close** ou **nullaire**. Exemple : $\mathcal{P}$ = "il existe un ensemble qui ne possède pas d'élément". Une proposition **unaire** a une variable, **binaire** deux variables, etc.
9. La **théorie des ensembles** sépare le sens des deux mots **ensemble** et **collection** qui sont synonymes dans la langue courante (page 1). Elle est motivée par le **paradoxe de Russel**. La **théorie des ensembles précise les conditions nécessaires et suffisantes pour qu'une collection soit un ensemble ou pas**. Dans le vocabulaire ensembliste **un ensemble possède des éléments et une collection des pièces**.
10. La collection définie par une proposition s'écrit de la même façon que la proposition elle-même. Exemples : $\mathcal{P}(a$ donné $,\ x)$ est une collection de paramètre a et de variable x.
11. Soient au moins deux propositions, la vérité de l'une, nommée **sortie** dépendant de celle des autres nommée **entrées**. À droite des tableaux 1, 2 et 3 on a numéroté des lignes.
12. Le tableau 2 montre les possibilité de combinaisons logiques entre une entrée et une sortie. En lignes 1 et 4 la sortie est indépendante de l'entrée. En ligne 2 la sortie suit l'entrée. En ligne 3 la sortie est la **négation** de l'entrée (tableau 1).
13. Le tableau 3 montre les possibilité de réponses d' une sortie à une deux entrées.
    En ligne 1, la sortie dit "c'est toujours faux".
    ♦ En la ligne 16, la sortie dit "c'est toujours vrai".
    ♦ En ligne 9 est **la conjonction "et"** : la sortie dit "c'est vrai" que si les deux entrées disent "c'est vrai".
    ♦ En ligne 15 est **la conjonction "ou"** :la sortie dit "c'est vrai" que si au moins une des deux entrées dit "c'est vrai".
    ♦ En ligne 7 est le **dilemme "on bien"** : la sortie dit "c'est vrai" si et seulement si une seule des deux entrées dit "c'est vrai".
    ♦ En ligne 14 (en gris) est le "**si** $\mathcal{P}$ **alors** $\mathcal{Q}$" qu'on écrit aussi $\mathcal{P} \Rightarrow \mathcal{Q}$. La sortie ne dira "c'est faux" que si l'entrée $\mathcal{P}$ dit "c'est vrai" et l'entrée $\mathcal{Q}$ dit "c'est faux". De cette ligne on extrait le tableau 4.
    La case $\mathcal{P}$ fausse , $\mathcal{Q}$ vraie et $(\mathcal{P} \Rightarrow \mathcal{Q})$ vraie n'est pas intuitive.
    Exemple : $\mathcal{P}(a$ donné, $x)$ = "x appartient à a" et $\mathcal{Q}(a$ donné, $x)$ = "x est inclus dans a" définissent la phrase $(\mathcal{P} \Rightarrow \mathcal{Q})(a$ donné, $x)$ = "Si x appartient à a alors x est inclus dans a". Si comme paramètre a on choisit l'ensemble vide, on a $(\mathcal{P} \Rightarrow \mathcal{Q})(\varnothing\ ,\ x)$ = "Si x appartient à $\varnothing$ alors x est inclus dans $\varnothing$".
    Manifestement on a $\mathcal{P}(\varnothing\ ,\ x)$ fausse, $\mathcal{Q}(\varnothing\ ,\ x)$ vraie et $(\mathcal{P} \Rightarrow \mathcal{Q})(\varnothing\ ,\ x)$ vraie.
    ♦ La ligne 12 est la ligne 14 avec inversion des rôles des deux entrées.

$\mathcal{P}$	f	v	
$\mathcal{Q}$	f	f	1
	f	v	2
	v	f	3
	v	v	4

Tableau 2
Inventaire logique pour une entrée et une sortie

$\mathcal{P}$	f	v	f	v	
$\mathcal{Q}$	f	f	v	v	
$\mathcal{R}$	f	f	f	f	1
	v	f	f	f	2
	f	v	f	f	3
	v	v	f	f	4
	f	f	v	f	5
	v	f	v	f	6
	f	v	v	f	7
	v	v	v	f	8
	f	f	f	v	9
	c	f	f	v	10
	f	v	f	v	11
	v	v	f	v	12
	f	f	v	v	13
	v	f	v	v	14
	f	v	v	v	15
	v	v	v	v	16

Tableau 3
Inventaire logique pour deux entrées et une sortie

§02 Collections et ensembles

Conventions de vocabulaire

14. Une phrase est appelée **proposition**. Elle est écrite entre deux guillemets. Si on la désigne par un signe, celui-ci sera une lettre monotype corsiva $\mathcal{MAJUSCULE}$ sans guillemets. Si on l'explicite, l'expression sera entre guillemets.
15. Une proposition admise sans démonstration est un **axiome**.
16. On ne parlera que de propositions ne pouvant qu'être vraies ou fausses.
17. Une **proposition est nullaire ou close** si sa vérité est indépendante de tout choix d'un ensemble.

Exemples : "quelque soit l'ensemble x, "$x = x$" est vraie et "$x \neq x$" est fausse".

Autre exemple : "$\forall x$, $\exists y$ tel que $\mathcal{P}(x)$".

18. Une **proposition unaire** mentionne une variable et une seule. Elle définit toujours une **collection**. Les composants d'une collection sont ses **pièces**.

Exemple : $\mathcal{P}(x)$, "$\exists x$ tel que $\forall y$ $\mathcal{P}(x , y , z)$". La variable est ici z.

Autre exemple : $\mathcal{P}(x)$, "$\exists x$ tel que $\forall y$ $\mathcal{P}(x , y , u$ donné $, z)$". Ici z est la variable et u un paramètre.

19. **Les pièces d'une collection définie par une proposition sont celles qui la rendent vraie**.
20. Par convention dans la théorie des ensembles, **les pièces d'une collection sont des ensembles**.
21. **Tout ensemble est une collection**, mais **une collection n'est pas toujours un ensemble** (page 1).
22. **Si une collection est un ensemble, elle sera un ensembles d'ensembles**.
23. L'objectif de la théorie des ensembles et de définir à quelles conditions une proposition définit une collection ou un ensemble.
24. **Les expressions et signes suivants sont réservés aux ensembles**.

$x \in a$ se dit "x **appartient** à a" ou "x est un **élément** de a" ou "a **possède** x" ou "x **est possédé** par a".

Tout les objets désignés par les lettres latines en italiques dans ce qui suit sont des ensembles. En particulier, les éléments d'un ensemble sont toujours eux-mêmes des ensembles.

25. **Inclusion**. Chez les ensembles la proposition "si x appartient à a alors x appartient à b" est codée "$a \subset b$" et se dit "a est **inclus** dans b" ou toute expression synonyme du langage courant.

Réflexivité : la proposition "si x appartient à a alors x appartient à a" est toujours vraie (proposition close, voir page 6). La proposition "$a \subset a$" est donc toujours vraie. On dit alors que **l'inclusion est réflexive**.

Transitivité : La proposition "si $a \subset b$ et si $b \subset c$ alors $a \subset c$" est toujours vraie. Il suffit de la traduire mentalement en phrases de la langue courante pour s'en convaincre. On dit alors que **l'inclusion est transitive**.

Axiomes de la théorie de Zermelo et Frænkel

26. L'appartenance n'a aucune propriété naturelle. On ne peut lui en donner qu'à partir de principes fondamentaux admis comme axiomes. Voici ceux de ZERMELO et FRÆNKEL.
27. **Axiome 1 d'égalité** : **deux ensembles possédant les mêmes éléments sont confondus**.
    Hypothèse : les propositions "si $x \in a$ alors $x \in b$" et "si $x \in b$ alors $x \in a$" sont toujours vraies.
    Postulat : $a = b$.
28. **L'inclusion est antisymétrique**.
    Démonstration. Soient deux ensembles a et b tels que $a \subset b$ et $b \subset a$. Alors "si x appartient à a alors x appartient à b" et "si x appartient à b alors x appartient à a" sont toujours vraies et on applique l'axiome ptécédent ■
29. **Axiome 2 de la réunion** : **si une collection d'ensemble est un ensemble, la réunion de ses pièces est un ensemble**.
    Hypothèse : a est un ensemble d'ensembles.
    Postulat : la phrase "$x \in$ un des y de a" est toujours un ensemble.
30. **Axiome 3 de l'ensemble des parties** : **la collection des ensembles inclus dans un ensemble donné est un ensemble**.
    Hypothèse : a est un ensemble.
    Postulat : la proposition "$x \subset a$" définit un ensemble. On le nomme **ensemble des parties** de a.
31. **Axiome 4 de substitution** :
    Hypothèse : si "$\forall$ x, y et y' [$\mathcal{E}(x , y)$ et $\mathcal{E}(x , y') \Rightarrow y = y'$]" est vraie.
    Postulat : "alors il existe x tel que $\mathcal{E}(x , y)$" définit un ensemble.
    Note : les éléments de cet ensemble sont les y. *Preuve* : x est affecté d'un "il existe".
    Cette axiome apparaît compliqué, mais c'est ce que ZERMELO et FRÆNKEL ont trouvé de plus simple pour surmonter le paradoxe de RUSSEL.

Premières démonstrations

32. **L'intersection d'une collection et d'un ensemble est un ensemble**.
Démonstration. Soit une proposition $\mathcal{A}(x)$. Il faut prouver que la proposition "$x \in a$ et $\mathcal{A}(x)$" définit un ensemble.
Définissons la proposition $\mathcal{E}(x , y)$ par "$y = x$ et $\mathcal{A}(x)$".
L'hypothèse de l'axiome de substitution est satisfaite : $\mathcal{E}(x , y)$ et $\mathcal{E}(x , y')$ est "$y = x$ et $\mathcal{A}(x)$" et "$y' = x$ et $\mathcal{A}(x)$" donc "$\mathcal{E}(x , y)$ et $\mathcal{E}(x , y') \Rightarrow y = y'$ " est toujours vraie.
L'axiome dit que la proposition "$x \in a$ et $\mathcal{A}(x)$" définit un ensemble. ■
33. **Si une collection est incluse dans un ensemble, cette collection est un ensemble**.
Démonstration. Soit la proposition "$\mathcal{A}(x) \Rightarrow x \in a$ donné". Alors $\mathcal{A}(x) \Leftrightarrow$ "$x \in a$ et $\mathcal{A}(x)$" ont la même vérité (p. 5) donc $\mathcal{A}(x)$ définit un ensemble.
34. **L'univers n'est pas un ensemble**. *La collection universelle* ou *univers* est définie par la proposition "$x = x$".
Démonstration.
Si "$x = x$" définissait un ensemble a alors $\forall x , x \in a$ serait vraie. En conséquence pour a la proposition "$x \in a$ et $\mathcal{A}(x)$" définirait un ensemble. Avec "$x \notin x$" dans le rôle de $\mathcal{A}(x)$ on pourrait conclure que "$x \notin x$" définisse un ensemble (contradiction) ■

Opérations sur les ensembles

35. **Réunion** (voir al. 16).
La phrase "a et b sont donnés et $x \in$ (a ou b) " définit un ensemble qu'on écrit $a \cup b$.
Soit un ensemble u. La phrase "u est donné et $x \in$ un des y de u" définit un ensemble qu'on écrit $\cup_{y \in u} y$.
La phrase "étant donnés une suite u et son ensemble d'indices i, $k \in i$ et x appartient à un des u_k" définit un ensemble qu'on écrit $\cup_{k \in i} u_{ik}$.
36. **Intersection** (voir al. 19)
Soit une paire d'ensembles . La phrase "$\{a , b\}$ étant donné, $x \in a$ et $x \in b$" définit une collection contenue dans au moins un ensemble (qui est a ou b), donc cette collection est un ensemble qu'on écrit $a \cap b$.
La phrase "étant donné un ensemble u, $x \in$ tous les y de u" définit une collection contenue dans au moins un ensemble (qui est un des y), donc cette collection est un ensemble qu'on écrit $\cap_{y \in u} y$.
La phrase "étant donnés une suite u et son ensemble d'indices i, x appartient à tous les $u_{k \in i}$" définit une collection contenue dans au moins un ensemble (qui est un des u_k), donc cette collection est un ensemble qu'on écrit $\cap_{k \in i} u_k$.
37. **Complémentaire**
La phrase "étant donnés a et b, $x \in a$ et $x \notin b$" définit une collection contenue dans au moins un ensemble (qui est a), donc cette collection est un ensemble qu'on écrit $a \setminus b$.

Ensembles particuliers

38. **Il existe un ensemble et un seul ne possédant aucun élément : l'ensemble vide**.
Démonstration.
La proposition "$x \in a$ et $x \neq x$" définit un ensemble (al. 19).
Cet ensemble est vide.
39. **L'ensemble vide est unique**.
40. ***Démonstration***. Soient a et b deux ensembles vides. Alors les phrases "$x \in a \Rightarrow x \in b$" et "$x \in b \Rightarrow x \in a$" sont vraies (p. 5) donc $a \subset b$ et $b \subset a$ donc (axiome de l'égalité p. 6) $a = b$ ■
41. **Note** : parce que l'ensemble vide est unique il a son symbole, $\varnothing$.
42. **Il existe des ensembles ne possédant qu'un élément**. On les appelle **singletons**.
Démonstration.
- L'axiome des parties p. 6 dit que "$x \subset \varnothing$" définit un ensemble : on l'écrit $\{\varnothing\}$. On a donc $x \in \{\varnothing\} \Leftrightarrow x \subset \varnothing$.
- L'ensemble vide est inclus dans lui-même (p. 5, "si $x \in \varnothing$ alors $x \in \varnothing$" est toujours vraie) donc $\varnothing \in \{\varnothing\}$.
- Si $x \in \{\varnothing\}$ il faut que $x \subset \varnothing$. La proposition "$y \in \varnothing \Rightarrow y \in x$" est toujours vraie (p. 5) donc $\varnothing \subset x$ donc (axiome d'égalité p. 6) $x = \varnothing$. L'ensemble $\{\varnothing\}$ ne possède donc que l'élément $\varnothing$.
- La proposition $\mathcal{E}(x , y)$ = "$x = \varnothing$ et $y = a$"est telle que "$\mathcal{E}(x , y)$ et $\mathcal{E}(x , y')$" $\Rightarrow$ (y et y') = a" est vraie.
- Conséquence : "alors il existe x tel que $\mathcal{E}(x , y)$" devient " il existe x tel que $x = \varnothing$ et $y = a$" donc, comme "il existe x tel que $x = \varnothing$" est toujours vraie $\mathcal{E}(x , y)$" est la proposition "$y = a$" qui donc définit un ensemble. On a bien $y = a \Leftrightarrow y \in \{a\}$ donc l'ensemble $\{a\}$ possède donc un unique élément qui est a. ■
Note : "$\varnothing \subset y$" est toujours vraie parce que "$x \in \varnothing \Rightarrow x \in y$" l'est toujours (p. 5).

43. **Il existe des ensembles paires**.
Démonstration.
L'axiome des parties dit que "$x \subset \{\emptyset\}$" définit un ensemble qu'on écrira $\{x , \{\emptyset\}\}$.
Pour que $x \in \{\emptyset\}$ il faut et ilsuffit que la proposition "$x \subset \{\emptyset\}$" soit vraie.
C'est le cas pour $x = \emptyset$ parce que l'ensemble vide est inclus dans n'importe quel ensemble (p. 7).
C'est le cas pour $x = \{\emptyset\}$ par réflexivité de l'inclusion.
On n'a pas d'autre cas, car si $x \in \{\emptyset\}$ alors $x \subset \{\emptyset\}$ donc si $y \in x$ alors par définition du singleton $y = \emptyset$ donc on a $x = \emptyset$.
La proposition "pour a et b donnés, $x = \emptyset$ et $y = a$ ou b" définit un ensemble qu'on écrira $\{a , b\}$. La démonstration est analogue à celle de la page 7. Cela veut dire que "$y = a$ ou b" $\Leftrightarrow$ "$x \in \{a , b\}$".

44. **Il existe des ensembles couples**.
Démonstration.
Soient a et b deux ensembles. Les paires $\{\{a\} , \{a , b\}\}$ et $\{\{b\} , \{b , a\}\}$ sont des ensembles appelés **couples** ou suites de deux. Vu leur usage très fréquent et la lourdeur des écritures, on les écrira (a , b) et (b , a).
Intérêt. À partir d'une notion non orientée qu'est la paire (la proposition "$\{a , b\} = \{b , a\}$" est toujours vraie) on en définit une autre qui est orientée (la proposition "si $a \neq b$ alors $(a , b) = (b , a)$" est toujours fausse).
Soit un couple (a , b). L'ensemble a est son **antécédent** et b est son **image**.

45. **Égalité entre couples**. Si $(a , b) = (a' , b')$ alors $a = a'$ et $b = b'$.
Démonstration.
Si $a = b$ alors
$(a , b) = \{\{a\} , \{a , a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$ et
$(a' , a') = \{\{a'\} , \{a' , a'\}\} = \{\{a'\}, \{a'\}\} = \{\{a'\}\}$.
L'égalité donne alors par définition des singletons : $\{\{a\}\} = \{\{a'\}\}$ donc $\{a\} = \{a'\}$ donc $a = a'$.
Si $a \neq b$ alors on a le choix entre deux possibilités.
Si $\{a\} = \{a'\}$ alors par définition des singletons $\{b\} = \{b'\}$ donc $a = a'$ et $b = b'$.
Si $\{a\} = \{a' , b'\}$ on a une contradiction ■

46. **Récurrence**.
On dit qu'un ensemble est une suite de un.
On a vu qu'un couple est une suite de deux.
Une suite de trois (a , b , c) est le couple $((a , b) , c)$, et on dit que la suite de quatre suit la suite de deux,
une suite de quatre (a , b , c , d) est le couple $((a , b , c) , d)$, et on dit que la suite de quatre suit la suite de trois, et ainsi de suite.
Soit alors une proposition $\mathcal{P}$. On la dit récurrente si :
initiation : on démontre que $\mathcal{P}$(une suite donnée) est vraie,
hypothèse : on postule que $\mathcal{P}$(une suite) est vraie,
hérédité : on démontre que $\mathcal{P}$(cette suite , x) est vraie.
Intérêt : si on peut répéter à volonté la démonstration de l'hérédité, la proposition est vérifiable pour toute suite de n. En conséquence, en seulement deux étapes de démonstration, on peut prouver la proposition pour n'importe quelle suite.

Relations

47. **Relations unaires** ce sont des propositions unaires (p. 7). On les appelle aussi des *domaines*.

48. **Fonction**
Un ensemble de couples dans lequel tout antécédent n'a qu'une image est une fonction.
Écritures. Si f est une fonction, c'est un ensemble de couples $(x , f(x))$. Quelque fois elle est désignée par la formule $f : x \rightarrow f(x)$.

49. **Suite**.
Dans certaines circonstances, le mot "fonction" est remplacé par "suite" et le mot "couple" par "**terme**". Dans ce cas, les antécédents sont appelés des **indices**.
Écriture. Si u est une suite. Si i est un indice, l'image est écrite u_i et la suite est un ensemble de couples (i , u_i).

50. **Relations binaires**.
On peut regarder $\mathcal{R}(x , y)$ comme des propositions unaires $\mathcal{R}((x , y))$, les valeurs de la variable étant des couples, définissant ainsi des collections de couples.

51. **Domaine de définition** : Pour une relation binaire $\mathcal{R}$ c'est "$\exists y$ tel que $\mathcal{R}(x , y)$".

52. *Relations d'équivalence* : $\mathcal{R}$ en est une si $\forall$ x et y les faits suivants sont vrais :
$\mathcal{R}(x , y) \Rightarrow \mathcal{R}(y , x)$ (*symétrie*) et
$\mathcal{R}(x , y)$ et $\mathcal{R}(y , z) \Rightarrow \mathcal{R}(x , z)$ (*transitivité*).
Note : $\mathcal{R}(x , y) \Rightarrow$ par symétrie $\mathcal{R}(y , x) \Rightarrow$ par transitivité $\mathcal{R}(x , x)$ et $\mathcal{R}(y , y)$.
Note : $\mathcal{R}(x , x)$ définit une collection qui est son *domaine de définition*.

53. *Relation d'ordre* : $\mathcal{O}$ en est une si $\forall$ x et y les faits suivants sont vrais :
♦ $\mathcal{O}(x , y) \Rightarrow \mathcal{O}(x , x)$ et $\mathcal{O}(y , y)$ (*réflexivité*),
♦ $\mathcal{O}(x , y)$ et $\mathcal{O}(y , x) \Rightarrow x = y$ (*antisymétrie*),
♦ $\mathcal{O}(x , y)$ et $\mathcal{O}(y , z) \Rightarrow \mathcal{O}(x , z)$ (*transitivité*).

54. *Relation d'ordre strict* : $\mathcal{S}$ en est une si $\forall$ x et y les faits suivants sont vrais :
♦ $\mathcal{S}(x , y) \Rightarrow \mathcal{D}(x)$ et $\mathcal{D}(y)$ (*réflexivité*),
♦ non ($\mathcal{S}(x , y)$ et $\mathcal{S}(y , x)$) (*antisymétrie stricte*) et
♦ $\mathcal{S}(x , y)$ et $\mathcal{S}(y , z) \Rightarrow \mathcal{S}(x , z)$ (*transitivité*).

55. *Relation de bon ordre* : un ordre strict $\mathcal{B}$ en est une si $\forall$ x et y les faits suivants sont vrais :
Tout *ensemble* non vide inclus dans $\mathcal{D}(x)$ a un plus petit élément au sens de $\mathcal{O}(x , y)$ = "$\mathcal{B}(x , y)$ et $\mathcal{D}(x)$ et $\mathcal{D}(y)$".
Par plus petit élément d'un ensemble a on entend un ensemble p tel que "$x \in a \Rightarrow \mathcal{O}(p , x)$.
Note : si $\mathcal{S}$ est un ordre strict alors $\mathcal{O}(x , y)$ = " $\mathcal{S}(x , y)$ ou "$\mathcal{D}(x , y)$ et $\mathcal{D}(y , z)$ et $x = y$"" est un ordre.
Fonctionnelle : $\mathcal{F}$ en est une si $\mathcal{F}(x , y)$ et $\mathcal{F}(x , y') \Rightarrow y = y'$.
Domaine de définition : c'est la collection définie par "$\exists y$ tel que $\mathcal{F}(x , y)$". Ses pièces x sont les **antécédents**.
Image : c'est la collection définie par "$\exists x$ tel que $\mathcal{F}(x , y)$". Ses pièces y sont les **images**.

Mélange des ordres

56. **Le choix entre une relation d'ordre strict et l'égalité donne une relation d'ordre**.
Démonstration. Soit la proposition "$\mathcal{P}(x , y)$ " = "$\mathcal{S}(x , y)$ ou $x = y$".
♦ $\mathcal{P}(x , y) \Rightarrow$ parce que $x = x$ et $y = y$, $\mathcal{T}(x , x)$ et $\mathcal{T}(y , y)$ (*réflexivité*),
♦ $\mathcal{P}(x , y)$ et $\mathcal{P}(y , x) \Rightarrow$ ($x \mathcal{S} y$ ou $x = y$) et ($y \mathcal{S} x$ ou $x = y$) $\Rightarrow$ parce que $\mathcal{S}(x , y)$ et $\mathcal{S}(y , x)$ est faux, $x = y$ (*antisymétrie*).
♦ $\mathcal{P}(x , y)$ et $\mathcal{P}(y , z) \Rightarrow$ ($x \mathcal{S} y$ ou $x = y$) et ($y \mathcal{S} z$ ou $x = z$) $\Rightarrow$ quatre cas donnant ($x \mathcal{S} z$ ou $x = z$) (*transitivité*).
La relation $\mathcal{P}(x , y)$ est bien une relation d'ordre ■

57. **Une relation d'ordre privée de l'égalité est une relation d'ordre strict**.
Soit la proposition "$\mathcal{T}(x , y)$ " = "$\mathcal{O}(x , y)$ et $x \neq y$" et appelons $\mathcal{D}$ un domaine contenant $\mathcal{T}$.
♦ Par réflexivité et définition du domaine, $\mathcal{T}(x , y) \Rightarrow \mathcal{O}(x , y)$ et $x \neq y \Rightarrow \mathcal{O}(x , x)$ et $\mathcal{O}(y , y)$ et $x \neq y \Rightarrow \mathcal{D}(x)$ et $\mathcal{D}(y)$ (*réflexivité*).
♦ $\mathcal{T}(x , y)$ et $\mathcal{T}(y , x) \Rightarrow \mathcal{O}(x , y)$ et $\mathcal{O}(y , x)$ et $x \neq y \Rightarrow x = y$ et $x \neq y$ (contradiction) donc on a "non $\mathcal{T}(x , y)$ et $\mathcal{T}(y , x)$" toujours vraie (*réflexivité*).
♦ $\mathcal{T}(x , y)$ et $\mathcal{T}(y , x) \Rightarrow \mathcal{O}(x , y)$ et $\mathcal{O}(y , z)$ et $x \neq y$ et $y \neq z \Rightarrow \mathcal{O}(x , z)$ et si $x = z$ alors on aurait $\mathcal{O}(x , y)$ et $\mathcal{O}(y , z)$ donc $x = y$ (contradiction) donc $\mathcal{O}(x , y)$ et $\mathcal{O}(y , z)$ et $x \neq z$ (transitivité).
La proposition $\mathcal{T}(x , y)$ est une relation d'ordre strict de domaine $\mathcal{D}$.

58. **La transitivité donne la prévalence de l'ordre strict**.
Démonstration. Soient $\mathcal{S}$ et $\mathcal{O}$ associées comme dans les al. 44 et 45.
$\mathcal{S}(x , y)$ et $\mathcal{O}(y , z)$ donne $\mathcal{O}(x , y)$ et $x \neq y$ et $\mathcal{O}(y , z)$ donc par transitivité $\mathcal{O}(x , z)$ et $y \neq y$. Si $x = z$ alors on aurait $\mathcal{O}(x , y)$ et $x \neq y$ et $\mathcal{O}(y , x)$ donc par antisymétrie $x = y$ et $x \neq y$ (contradiction).
$\mathcal{S}(x , y)$ et $\mathcal{O}(y , z)$ donnent bien $\mathcal{S}(x , z)$. La démonstration est analogue pour $\mathcal{O}(x , y)$ et $\mathcal{S}(y , z) \Rightarrow \mathcal{S}(x , z)$.

Relations binaires dans les ensembles

59. **Produit d'ensembles**.
Soit une paire d'ensembles (a , b). La phrase "$x \in a$ et $y \in b$" définit une collection C de couples (x , y).
D'autre part, on sait que $a \cup b$ est un ensemble, donc (al. 16) que l'ensemble p des parties de $a \cup b$ est un ensemble, donc que l'ensemble p des parties de p est un ensemble.
La paire {x qui $\in a$, y qui $\in b$} est une paire {x qui $\in a \cup b$, y qui $\in a \cup b$} donc une paire incluse dans $a \cup b$ donc un élément de p.
Un couple de C est une paire {{x qui $\in a$} , {x qui $\in a$, y qui $\in b$}} = {{x qui $\in a \cup b$} , un élément de p} donc une paire {un élément de p , un élément de p} donc une paire incluse dans p donc un élément de l'ensemble des parties de p.
La collection C est incluse dans un ensemble. On l'appelle produit de a par b et on l'écrit $a \times b$.

60. **Une relation binaire incluse dans un produit d'ensembles définit un ensemble de couples**.
Démonstration. Elle est immédiate (al. 19).
Cas particuliers. Pour abréger l'expression des propositions suivantes, appelons-les propositions remarquables, définissons quatre qualités de propositions : $\mathcal{F}$, $\mathcal{J}$,$\mathcal{A}(u)$ et $\mathcal{S}(v)$:
qualité $\mathcal{F}$: "chaque antécédent n'a qu'une image",
qualité $\mathcal{J}$: "chaque image n'a qu'un antécédent",
qualité $\mathcal{A}(u)$: "tout élément de u est un antécédent",
qualité $\mathcal{S}(v)$: "tout élément de v est une image".
Rappel : si les collections qu'elles définissent sont incluses dans un produit d'ensembles ce sont des ensembles de couples. On les écrira respectivement f, j , $a(u)$ et $s(v)$.
En particulier, f est une fonction.
Définissons quatre compositions de qualités *:*
La qualité *application* de u est "$\mathcal{F}$ et $\mathcal{A}(u)$",
La qualité *injection* de u est "$\mathcal{F}$ et $\mathcal{A}(u)$ et $\mathcal{J}$ ",
La qualité *surjection* sur v est "$\mathcal{F}$ et $\mathcal{S}(v)$",
La qualité *bijection* de u vers v est "$\mathcal{F}$ et $\mathcal{J}$ et $\mathcal{S}(v)$".
Conséquence : une relation qui est à la fois une injection de u et une surjection sur v est une bijection de u vers v et, parce qu'elle est incluse dans le produit $u \times v$, cette bijection est un ensemble de couples.

61. **Puissance d'un ensemble**. Soient u et v deux ensembles. La proposition "f est une application de u sur v" définit une collection incluse dans $u \times v$ donc est un ensemble (al. 19). On l'appelle "u à la puissance v" et l'écrit u^v.

62. **Produits d'ensembles**. Soit une suite donnée a d'ensembles. Soit i son ensemble d'indices. Alors a est l'ensemble des couples (k appartenant à i, a_k).
La proposition "f est une application de i sur $\cup_{n \in i} a_n$ et $k \in i \Rightarrow f(a_k) \in a_k$" définit une collection incluse dans $(\cup_{k \in i} a_k)^i$ donc un ensemble. On l'appelle produit des $a_{k \in i}$ et on l'écrit $\prod_{k \in i} a_k$.

63. **Note** : si l'application a est l'identité de l'ensemble i alors les écritures des opérations collectives changent.
$\cup_{k \in i} u_k$ (al. 21) devient $\cup_{u \in i} u$,
$\cap_{k \in i} u_k$ (al. 22) devient $\cap_{u \in i} u$, et $\prod_{k \in i} a_k$ (al. 39) devient $\prod_{a \in i} a$.

.

Relations et opérations ensemblistes

64. **Les qualités des relations binaires et l'opération réunion**.
Soient $\mathcal{R}$ une relation entre deux ensembles u et v et $\mathcal{R}'$ une autre entre u' et v'.
On entend par là que $\mathcal{R}(x , y) \Rightarrow x \in u$ et $y \in v$ et $\mathcal{R}'(x , y) \Rightarrow x \in u'$ et $y \in v'$. Autrement dit, $\mathcal{R}$ définit un ensemble r de couples (un x de u , un y de v) et $\mathcal{R}'$ définit un ensemble r' de couples (un x de u' , un y de v') donc r et r' sont disjoints.
Considérons la réunion de r et r'. Elle est définie par "$\mathcal{R}$ ou $\mathcal{R}'$".
Alors $r \cup r'$ est un ensemble de couples (un x de u ou de u' , un y de v ou de v') donc un ensemble de couples (un x de $u \cup u'$, un y de $v \cup v'$) donc une relation binaire entre $u \cup u'$ et $v \cup v'$.
♦ Si $\mathcal{R}$ et $\mathcal{R}'$ sont de qualité $\mathcal{F}$ alors un antécédent de couple de s, si il appartient à u n'a qu'une image dans r et si il appartient à u' n'a qu'une image dans r' donc dans les deux cas n'a qu'une image dans $u' \cup v'$. La réunion "$\mathcal{R}$ ou $\mathcal{R}'$ " est de qualité $\mathcal{F}$.
♦ Si $\mathcal{R}$ et $\mathcal{R}'$ sont de qualité $\mathcal{J}$ alors la réunion "$\mathcal{R}$ ou $\mathcal{R}'$" est de qualité $\mathcal{J}$ (démonstration analogue).
♦ Si $\mathcal{R}$ et $\mathcal{R}'$ sont de qualité respective $\mathcal{A}(u)$ et $\mathcal{A}(u')$ alors si x appartient à $u \cup u'$, soit $x \in u$ et alors $\mathcal{R}$, donc "$\mathcal{R}$ ou $\mathcal{R}'$" donne à x une image dans donc dans s, soit $x \in u'$ et alors $\mathcal{R}'$ donne à x une image dans s.
La réunion donne la qualité $\mathcal{A}(u \cup u')$.
♦ Si $\mathcal{R}$ et $\mathcal{R}'$ sont de qualité respective $\mathcal{S}(v)$ et $\mathcal{S}(v')$ alors la réunion donne la qualité $\mathcal{S}(v \cup v')$.

Conséquences : la réunion de deux ensembles disjoints conserve les qualités fonction, application, injection, surjection et bijection.

65. **Les qualités des relations binaires et l'inclusion**.

Soient $u \subset u'$ deux ensembles et $v = u \setminus u'$.

Soit $\mathcal{R}$ une relation binaire de u vers v.

Les couples de $\mathcal{R}$ dont les antécédents sont dans a' forment une relation binaire $\mathcal{R}'$. On a donc $\mathcal{R} \Rightarrow \mathcal{R}'$.

Les couples de $\mathcal{R}$ dont les antécédents sont hors de a' forment une relation binaire $\mathcal{C}$.

♦ Si $\mathcal{R}$ est de qualité $\mathcal{F}$ alors un antécédent de $\mathcal{R}'$ parce qu'il appartient à a' donc à a n'a qu'une image dans $\mathcal{R}$ donc qu'une image dans $\mathcal{R}'$. $\mathcal{R}'$ est de qualité $\mathcal{F}$. De même, $\mathcal{C}$ est de qualité $\mathcal{F}$.

♦ Si $\mathcal{R}$ est de qualité $\mathcal{A}(u)$ alors si $x \in u'$, $x \in u$ donc x a dans $\mathcal{R}$ une image. Comme $x \in u'$ cette image est celle d'un couple de $\mathcal{R}'$. $\mathcal{R}'$ est de qualité $\mathcal{A}(u')$. De même, $\mathcal{C}$ est de qualité $\mathcal{A}(u \setminus u')$.

Note : on peut deviner la suite en échangeant les rôles des mots antécédent et image et des lettres u et v ou x et y.

♦ Si $\mathcal{R}$ est de qualité $\mathcal{J}$, alors une image de $\mathcal{R}'$, parce qu'elle est dans v' donc dans v, est une image de $\mathcal{R}$ qui n'a qu'un antécédent qui est antécédent dans $\mathcal{R}'$. $\mathcal{R}'$ est de qualité $\mathcal{J}$. De même, $\mathcal{C}$ est de qualité $\mathcal{J}$.

♦ Si $\mathcal{R}$ est de qualité $\mathcal{A}(u)$ alors si $y \in v'$, $x \in v$ donc x a dans $\mathcal{R}$ un antécédent. . Comme $y \in v'$ cette antécédent est celui d'un couple de $\mathcal{R}'$. $\mathcal{R}'$ est de qualité $\mathcal{S}(v')$. De même, $\mathcal{C}$ est de qualité $\mathcal{S}(v \setminus v')$.

Conséquences : l'inclusion et le complémentaire de deux ensembles conserve les qualités fonction, application, injection, surjection et bijection.

66. **Les classes d'équivalence**

Soit $\mathcal{R}$ une relation d'équivalence. Pour un ensemble donné u, on appelle $u\mathcal{R}(x)$ la proposition $\mathcal{R}(u , x)$. Cette proposition définit une collection.

La proposition "a est donné et $x \in a$ est donné et $y \in a$ et $\mathcal{R}(x , y)$" = $\mathcal{C}(x$ donné , $y)$ un ensemble appelé **classe de** x **selon** $\mathcal{R}$.

67. **Une relation d'équivalence donnée dans un ensemble donné partage cet ensemble en classes deux à deux disjointes**.

Démonstration.

♦a Si $x \in a$ alors (al. 39) on a $\mathcal{C}(x$ donné , $x)$ vraie, ce qui montre que x appartient à sa propre classe.
On a donc a inclus dans la réunion des classes.

♦b Si y appartient à la réunion des classes, alors $\mathcal{C}$(un x donné , y) donc "a est donné et $x \in a$ est donné et $y \in a$ et $\mathcal{R}(x , y)$" est vraie donc $y \in a$. La réunion des classes est donc incluse dans a donc confondue avec a.

Soit "$\mathcal{C}$(un x donné , z) et $\mathcal{C}$(un y donné , z)" vraie. Alors $\mathcal{R}(x , z)$ donne $\mathcal{R}(z , x)$ qui donne par transitivité $\mathcal{R}(z , y)$ donc $\mathcal{C}$(un y donné , z). De même $\mathcal{C}$(un y donné , z) donne $\mathcal{C}$(un x donné , z). Les deux classes sont confondues ■

Opérations

68. Une **opération** est un ensemble de couples $((x , y) , z)$ dans lequel chaque antécédent n'a qu'une image. Ici, l'antécédent est le couple (x , y) et l'image, appelée aussi **résultat** est l'élément z et dans le couple antécédent, x est l'**opérande** et y l'**opérateur**.
69. Soit * une opération. Si un couple $((x , y) , z)$ lui appartient, vu qu'une fois donné l'antécédent (x , y) l'image z est unique, on peut la coder : elle est écrite $x * y$. On a donc équivalence logique entre les propositions "$((x , y) , z) \in$ *" et "$x * y = z$".
70. Une opération est **interne** à un ensemble donné si opérande, opérateur et résultat sont dans cet ensemble. Elle est **externe** dans les autres cas.
71. Une **structure** est un ensemble constitué d'un ou plusieurs ensembles et d'une ou plusieurs opérations entre leurs éléments. Exemple : l'ensemble $\mathcal{P}(\mathcal{A})$ des parties d'un ensemble donné $\mathcal{A}$ plus la réunion $\cup$, le complémentaire \ et la multiplication ensembliste $\times$ constituent la structure $\{\mathcal{P}(\mathcal{A}) ; \cup ; \setminus ; \times\}$.

Propriétés canoniques des opérations

Soient * une opération

72. Si pour toute suite $((x , y) , z)$ de l'opération on a $(x * y) * z = x * (y * z)$, l'opération est **associative**.
73. Si pour tout couple antécédent (x , y) de l'opération on a $x * y = y * x$ l'opération est **commutative**.
74. Un élément e est **neutre à droite** si pour toute antécédent (x , e) de l'opération on a $x * e =$ et
Un élément e est **neutre à gauche** si pour toute antécédent (e , x) de l'opération on a $e * x = x$.
Un élément neutre à la fois à gauche et à droite est dit **neutre**.
75. Si l'opération a un élément neutre, on appellera **éléments symétriques** un opérande x et un opérateur y tels que s'il existent $x * y = e$ et $y * x = e$.

Soient * et $\Diamond$ deux opérations

76. Si pour toute suite $(x , (y , z))$ pour laquelle (y , z) est antécédent de $\Diamond$ et $(x , (y \Diamond z))$ antécédent de * on a $x * (y \Diamond z) = (x * z) \Diamond (y * z)$ on dira que $\Diamond$ **distribue à droite** *.
Si pour toute suite $((x , y) , z)$ pour laquelle (x , y) est antécédent de * et $((x * y) , z)$ antécédent de $\Diamond$ on a $(x * y) \Diamond z = (x \Diamond z) * (y \Diamond z)$ on dira que * **distribue à gauche** $\Diamond$.

Ordinaux

1. On dit qu'un ensemble d'ensembles $\underline{u}$ est un **ordinal** si la relation binaire $x\ R\ y \Leftrightarrow$ "x et y appartiennent à $\underline{u}$ et x appartient à y" est un bon ordre de $\underline{u}$ et si tout ensemble appartenant à $\underline{u}$ est inclus dans $\underline{u}$.
   Soit $\underline{u}$ un ordinal : on a donc les quatre propriétés
   a♦ x et $y \in \underline{u} \Rightarrow x \in y$ ou $y \in x$ ou $x = y$ (ubiquité),
   b♦ x et $y \in \underline{u} \Rightarrow$ si $x \in y$ alors $y \notin x$ (antisymétrie),
   c♦ x, y et $z \in \underline{u} \Rightarrow$ si $x \in y$ et $y \in z$ alors $x \in z$ (transitivité),
   d♦ Si $v \subset \underline{u}$ alors v a un plus petit élément p, c'est-à-dire qu'il existe p appartenant à v tel que $x \in v \Rightarrow x \in p$.
   Convention d'écriture : si dans les hypothèses des propositions à démontrer il est dit qu'un ensemble est ordinal, sa lettre sera soulignée.
2. **Les ordinaux existent**. Par exemple $\varnothing$ en est un.
   Démonstration. Soit les propositions $\mathcal{P}$ = "x et $y \in \varnothing$" et Q = "$x \in y$ ou $y \in x$ ou $x = y$".
   Alors $\mathcal{P} \Rightarrow Q$ est vraie au sens de la table de vérité ci-contre car $\mathcal{P}$ est fausse. Le point a♦ est démontré.

$\mathcal{P}$	f	v	f	v
Q	f	f	v	v
$\mathcal{R}$	v	f	v	v

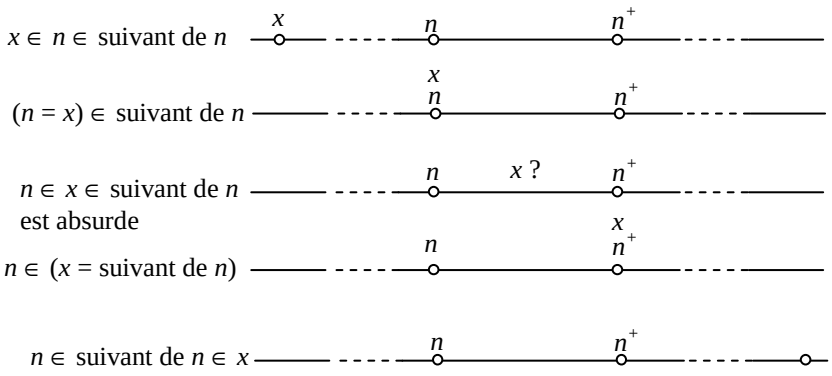
Tableau 1

   De même les points b♦ et c♦ sont aussi démontrés, ainsi que l'inclusion $\varnothing \subset \varnothing$, ce qui prouve le point d♦ ■
3. **Un segment** d'ordinal **initié** par un de ses éléments x est l'ensemble évrit S_x des éléments possédés par x.
   Exemple : $\underline{a}$ lui-même est un segment initié par $\underline{a}$.
4. **Les segment initiaux d'un ordinal sont cet ordinal et ses éléments**.
   Démonstration. Soient $\underline{a}$ un ordinal, x un de ses éléments et Sx le segment initié par x.
   a♦ $x \subset$(par définition de l'ordinal) $\underline{a}$.
   b♦ $y \in S_x \Leftrightarrow y \in x \Rightarrow$(voir a♦) $y \in \underline{a} \Rightarrow$(définition de l'intersection) $y \in x \cap \underline{a}$.
   c♦ $y \in x \cap \underline{a} \Rightarrow$(définition de l'intersection) $y \in x \Rightarrow$(définition du segment initié) $y \in S_x$.
   d♦ On a x et S_x confondus ■
5. **Tous les éléments d'un ordinal sont des ordinaux**.
   Démonstration. Soit $\underline{a}$ un ordinal et x un de ses éléments.
   a♦ $x \subset$(par définition de l'ordinal) $\underline{a}$.
   b♦ Tout bon ordre d'un ensemble est bon ordre de ses parties $\Rightarrow$(voir a♦) $\in$ est un bon ordre de x.
   c♦ y est un élément de x, $\Rightarrow$(voir a♦) y appartient à $\underline{a}$.
   d♦ $z \in y \Rightarrow$(transitivité de $\in$) $z \in x$. On conclut que $y \subset x$ ■
6. **Un ordinal ne s'appartient pas**.
   Démonstration (par l'absurde). Supposons que $\underline{a} \in \underline{a}$.
   Renommons $\underline{x}$ l'ordinal $\underline{a}$. Alors par substitution $\underline{a} \in \underline{x}$ et $\underline{x} \in \underline{a}$,ce qui contradit l'antisymétrie de $\in$ ■
7. **Soient deux ordinaux. Soit l'un appartient à l'autre, soit ils sont confondus**.
   Démonstration. Soient deux ordinaux $\underline{m}$ et $\underline{n}$. Les exclusions deux à deux des trois cas $\underline{m} \in \underline{n}$, $\underline{n} \in \underline{m}$ et $\underline{m} = \underline{n}$ viennent de l'al. 6 et de la nature des ordinaux (al. 1). Pour le reste il faut prouver que $\underline{m}$ et $\underline{n}$ étant ordinaux on a $\underline{m} \in \underline{n}$ ou $\underline{n} \in \underline{m}$ ou encore $\underline{m} = \underline{n}$.
   Comme les ordinaux sont inclus les uns dans les autres, $\underline{m} \cap \underline{n}$ est soit $\underline{m}$ soit $\underline{n}$ donc est entier naturel. En conséquence (ens al. 10 et les espaces sont volontaires)
   $\underline{m} \cap \underline{n}$ est un élément de $\underline{n}$ ou $\underline{n}$ lui-même et un élément de $\underline{m}$ ou $\underline{m}$ lui-même,
   ce qui donne quatre cas possibles :
   ♦ $\underline{m} \cap \underline{n}$ est un élément de $\underline{n}$ et de $\underline{m}$ donc $\underline{m} \cap \underline{n} \in \underline{m}$ et $\underline{m} \cap \underline{n} \in \underline{n}$ donc $\underline{m} \cap \underline{n} \in \underline{m} \cap \underline{n}$, (contradiction avec l'al. 6),
   ♦ $\underline{m} \cap \underline{n}$ est un élément de $\underline{n}$ et est $\underline{m}$ lui-même donc $\underline{m} \in \underline{n}$,
   ♦ $\underline{m} \cap \underline{n}$ est $\underline{n}$ lui-même et est un élément de $\underline{m}$ donc $\underline{n} \in \underline{m}$,
   ♦ $\underline{m} \cap \underline{n}$ est n lui-même et est $\underline{m}$ lui-même donc $\underline{m} = \underline{n}$ ■
8. **La phrase $\mathcal{P}(x)$ = "$\underline{x}$ est un ordinal" définit une collection dans laquelle l'appartenance est un bon ordre**.
   Démonstration.
   a♦ Deux ordinaux sont toujours comparables par l'appartenance (voir al. 7).
   b♦ Si entre deux ordinaux on a $\underline{a} \in \underline{b}$ on a pas $\underline{b} \in \underline{a}$ (al. 7), ce qui assure l'antisymétrie.
   c♦ Si entre trois ordinaux $\underline{a} \in \underline{b}$ et $\underline{b} \in \underline{c}$ alors $\underline{a} \subset \underline{b} \subset \underline{c}$ donc $\underline{a} \subset \underline{c}$ alors $\underline{a} \in \underline{b} \Rightarrow$(définition de l'inclusion) $\underline{a} \in \underline{c}$ (transitivité).
   d♦ Soit E un ensemble non vide d'ordinaux. Par ubiquité de l'appartenance, pour un ordinal donné $\underline{u}$ de E cet ensemble est partagé en trois parties, les $\underline{a}$ appartenant à $\underline{u}$, $\underline{u}$ lui-même et les $\underline{b}$ qui possèdent $\underline{u}$. D'autre part, $\underline{u}$ possède son plus petit élément $\underline{d}$ qui est un ordinal (al. 5), donc $\underline{d}$ appartient à $\underline{u}$ donc par définition du plus tetit élément à tous les $\underline{a}$ donc par transitivité de l'appartenance à tous les $\underline{b}$ ■
9. **Le plus petit ordinal possédant un ordinal $\underline{u}$ donné est la réunion de $\underline{u}$ avec le singleton $\{\underline{u}\}$**.
   Démonstration. Soit $\underline{a}$ un ordinal.
   a♦ On a $\underline{a} \subset \underline{a} \cup \{\underline{a}\}$.

b♦ Soit x dans $\underline{a} \cup \{\underline{a}\}$. Alors $x \in$ ($\underline{a}$ ou $\{\underline{a}\}$) donc x ($\in$ ou $= \underline{a}$). Dans les deux cas x est un ordinal.
c♦ $\underline{a} \cup \{\underline{a}\}$ est un ensemble non vide d'ordinaux donc l'appartenance est un bon ordre de $\underline{a} \cup \{\underline{a}\}$.
d♦ Si $x \in \underline{a} \cup \{\underline{a}\}$ alors ◊ ou $x \in \underline{a}$ et alors $x \subset \underline{a}$ donc $x \subset \underline{a} \cup \{\underline{a}\}$, ◊ ou $x \in \{\underline{a}\}$ donc $x = \underline{a}$ donc $x \subset \underline{a}$ donc $x \subset \underline{a} \cup \{\underline{a}\}$. On conclut que $\underline{a} \cup \{\underline{a}\}$ est un ordinal.
e♦ Si $\underline{a} \in \underline{c}$ alors $\underline{a} \subset \underline{c}$ donc $\underline{c}$ possède $\underline{a}$ et tous les éléments de $\underline{a}$ donc c contient $\underline{a} \cup \{\underline{a}\}$ donc $\underline{a} \cup \{\underline{a}\}$ est le plus petit ordinal possédant $\underline{a}$ ■

10. **Suivant d'un ordinal**. Si $\underline{a}$ est un ordinal, alors $\underline{a} \cup \{\underline{a}\}$ est appelé son suivant.
11. **Aucun ordinal ne possède son suivant**.
Démonstration. Si $n \cup \{n\} \in n$ alors $n \cup \{n\} \subset \{n\}$ donc n est inclus dans le singleton donc tout élément de n est n lui-même (contradiction avec l'al. 19) ■
12. **Il n'existe pas d'ordinal appartenant à un autre et possédant son suivant** (fig. 1).
Démonstration. Supposons $n \in x \in n \cup \{n\}$. La deuxième appartenance donne le choix entre $x \in n$ (contredit par $n \in x$ et l'al. 22) ou $x \in \{n\}$ donc par définition du singleton $x = n$ (contradiction) ■
Exemple : soit un ordinal x : on a soit $x \in \varnothing$ (absurde), soit $x = \varnothing$, soit $x = \{\varnothing\}$, soit $\{\varnothing\} \in x$.

Fig. 1



Un ordinal inclus dans un autre et distinct de cet autre lui appartient.
Démonstration. Il faut prouver que si $x \subset y$ et $x \neq y$ alors $x \in y$.
Si $y \in x$ alors $y \subset x$ (al. 18) donnerait par antisymétrie de l'inclusion $x = y$ (contradiction). Il reste donc $x \in y$ ■

13. **Borne supérieure** : par définition un ordinal $\underline{b}$ est borne supérieure d'un ensemble non vide A d'ordinaux si (tous les éléments de A) $\in \underline{b}$ et si (tous les éléments de A) $\in \underline{h} \Rightarrow \underline{b} \in \underline{h}$.
14. **Une borne supérieure, si elle existe, est unique**.
Démonstration.
Si les ordinaux $\underline{b}$ et $\underline{b'}$ sont bornes supérieures de A alors (al. 7) on a le choix entre $\underline{b} = \underline{b'}$, $\underline{b} \in \underline{b'}$ et $\underline{b'} \in \underline{b}$. Dans le 2e cas, (tous les éléments de A) $\in \underline{b} \in \underline{b'}$ donc $\underline{b'}$ ne serait pas borne supérieure de A. Dans le 3e cas le même raisonnement montre que $\underline{b'}$ ne serait pas borne supérieure de A ■
15. **Tout ensemble d'ordinaux a une borne supérieure qui est la réunion de ses éléments**.
Démonstration.
a♦ Soit A un ensemble d'ordinaux. Définissons b = réunion des $\underline{a}$ appatenant à A.
Soit x une partie non vide de b. Alors par définition de la réunion, il existe dans x un ordinal $\underline{u}$ appartenant à au moins un ordinal $\underline{a}_x$ de A. Alors $\underline{u} \in$ (x et $\underline{a}_x$) donc $x \cap \underline{a}_x$ n'est pas vide.
b♦ La réunion des $x \cap$ (un ordinal de $\underline{A}$) est x lui-même. Comme il n'est pas vide, vu que l'appartenance est un bon ordre chez les ordinaux, il a un plus petit ordinal $\underline{d}$. On conclut que b est bien ordonné par l'appartenance.
c♦ Soit x apparteant à b. Alors $x \in$ un $\underline{a}_x$ de $A \Rightarrow x \subset$ cet $\underline{a}_x$ de $A \Rightarrow x \subset$ réunion des $\underline{a}$ appatenant à $A \Rightarrow x \subset b$. On conclut que b est un ordinal ■
d♦ Si (tous les $\underline{a}$ de A) $\in \underline{h}$ alors (tous les $\underline{a}$ de A) $\subset \underline{h}$ donc (réunion des $\underline{a}$ appatenant à A) $\subset \underline{h}$.
16. **Aucun ordinal n'a l'ensemble vide comme suivant**.
Démonstration. Si n précède 0 alors on aurait $n \cup \{n\} = \varnothing$, ce qui est impossible à cause du singleton ■
17. **Deux ordinaux ayant le même suivant sont confondus**.
Démonstration. Soient les ordinaux $\underline{a}$ et $\underline{b}$ tels que $\underline{a} \cup \{\underline{a}\} = \underline{b} \cup \{\underline{b}\}$.
On a $\underline{a} \in \underline{b}$ ou $\underline{b} \in \underline{a}$ ou $\underline{a} = \underline{b}$.
Si $\underline{a} = \underline{b}$ la proposition est démontrée.
Si $\underline{a} \in \underline{b}$ et un élément de $\underline{a}$ est hors de $\underline{b}$ alors cet élément est dans $\{\underline{b}\}$ donc cet élément est $\underline{b}$ donc $\underline{b} \in \underline{a}$ (contradiction).
Le même raisonnement montre que $\underline{b}$ n'appartient pas à $\underline{a}$ ■

Ch03 Les nombres

Nombres entiers naturels

1. On a vu que l'ensemble des ordinaux contenant l'ensemble vide et des ordinaus accessibles par répétion de l'hérédité de la récurrence a une borne supérieure au sens de l'appartenance qui est leur réunion. On l'appelle $\mathbb{N}$ et ses éléments sont appelés **nombres entiers naturels** ou **entiers naturels**.
2. **Rappel :** une **proposition récurrente** est une phrase $\mathcal{P}$ qui a les propriétés suivantes :
   initiation : $\mathcal{P}$ pour l'ensemble vide est vraie, ce qu'on écrit $\mathcal{P}(\varnothing)$v,
   hypothèse : $\mathcal{P}$ pour un ordinal n est vraie, ce qu'on écrit $\mathcal{P}(n)$v,
   hérédité : alors $\mathcal{P}$ est vraie pour son suivant, ce qu'on écrit $\mathcal{P}$(suivant de n)v.

Axiomes de peanno

Peano avait proposé de définir les nombres entiers naturels comme un ensemble ayany – si il existe – les propriétés suivantes. Ces propriétés sont démontrables dans le cadre des ordinaux.

3. **Axiome 1 : il existe au moins un entier naturel, zéro** : voir ord. al.2.
4. **Axiome 2 : tout entier naturel a un suivant** : voir ord. al.9.
5. **Axiome 3 : aucun entier naturel n'a zéro comme suivant** : voir ord. al.11.
6. **Axiome 4 : deux entiers naturels ayant le même suivant sont confondus** : voir ord. al.17.
7. **Axiome 5 : si un ensemble d'entiers naturels satisfait les conditions de la récurrence, cet ensemble contient tous les entiers naturels** : voir al.1.
8.

Autres propriétés tirées de la théorie des ordinaux

9. On appelle **précédent** d'un entier naturel donné n un entier naturel qui a n comme suivant.
10. **Le précédent d'un entier naturel, si il existe, est unique** : voir al.6.
11. **L'appartenance est un bon ordre des entiers naturels** : voir ord. al.1.
12. **Il n'existe pas d'entier naturel appartenant à un autre et possédant son suivant** : voir ord. al.9.
    Exemple : soit un entier naturel x : on a soit $x \in 0$ (absurde), soit $x = 0$, soit $x = 1$ soit $1 \in x$.
13. **Un entier naturel inclus dans un autre et distinct de cet autre lui appartient** : voir ord. al.1.
14.

Nouvelles propriétés

15. **Tout ensemble d'entiers naturels inclus ou appartenant à un entier naturel donné a un premier et un dernier élément** : voir ord. al.9.
    Démonstration. Pour le premier élément c'est une conséquence du bon ordre qu'est l'inclusion.
    Étudions la phrase $\mathcal{P}(n)$ = " Si un ensemble d'entiers naturels $\underline{E}$ est inclus dans n alors $\underline{E}$ a un dernier élément ".
    Initiation : " Si un ensemble d'entiers naturels $\underline{E}$ est inclus dans 0 alors $\underline{E}$ a un dernier élément " est paradoxalement vraie. On a $\mathcal{P}(0)$v.
    Hypothèse : $\mathcal{P}(n)$v.
    Hérédité : Si un élément de $\underline{F}$ est inclus dans le suivant de n alors cet élément appartient à n ou à $\{n\}$ donc appartient à n ou est confondu avec n. Deux cas se présentent.
    ♦ Tous le éléments de $\underline{F}$ sont dans n : alors l'hypothèse dit que $\underline{E}$ a un dernier élément.
    ♦ Un élément de $\underline{F}$ est n : alors n est le dernier élément de $\underline{E}$. On a $\mathcal{P}$(suivant de n)v.
    En conséquence, tout élément de $\underline{E}$ appartenant à n étant inclus dans n a un dernier élément.
    ♦ Soit $\underline{E}$ un ensemble d'entiers naturels appartenent à un entier n donné. Alors (al. 18) ces éléments sont inclus dans n ■

$\mathcal{P}\downarrow Q\rightarrow$	f	v
f	v	v
v	f	v

Tableau 4
Vérité de
"si $\mathcal{P}$ alors Q"

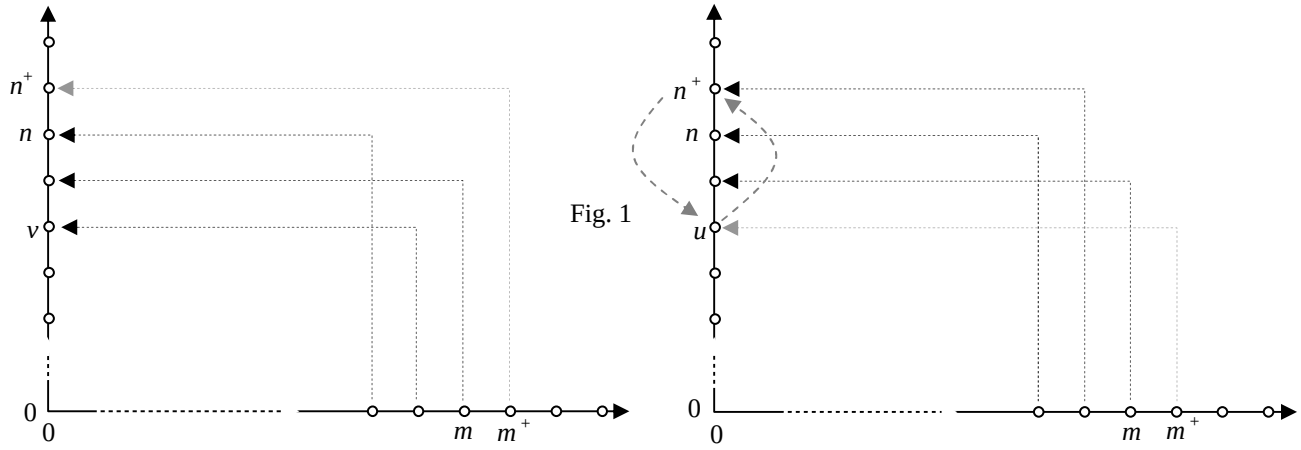
    Démonstration. Il faut prouver que si $x \subset y$ et $x \neq y$ alors $x \in y$.
    Si $y \in x$ alors $y \subset x$ (al. 18) donnerait par antisymétrie de l'inclusion $x = y$ (contradiction). Il reste donc $x \in y$ ■
16. **Toute suite strictement (dé)croissante d'entiers naturels appartenant à un entier naturel donné a au sens de l'inclusion un premier et un dernier élément**.
17. ***Démonstration***. Soit une suite croissante. C'est un ensemble de couples tels que $n \in n' \Rightarrow a_n \in a_{n'}$.
    - Le premier élément vient du caractère de bon ordre de l'inclusion (ens al. 32).
    - Nommons a_i les images de la suite et n un entier naturel donné.
    Étudions la phrase $\mathcal{P}(n)$ = " l'ensemble des images a_i majorés par n a un dernier élément ".
    Initiation ($n = 0$). La phrase "L'ensemble des a_i majorés par 0 a un dernier élément" est paradoxalement vraie.
    Hypothèse : $\mathcal{P}(n)$v.
    Hérédité : soit $\underline{F}$ l'ensemble des images a_i majorés par le suivant de n. On compare $\underline{E}$ et $\underline{F}$.
    Tous les a_i appartenent à $\underline{F}$ sont inclus dans $n \cup \{n\}$. On a deux situations.

♦ un élément de $\underline{F}$ est dans $\{n\}$ donc est n lui-même donc est le dernier élément de $\underline{F}$,
♦ aucun élément de $\underline{F}$ est dans $\{n\}$ donc tous les éléments de $\underline{F}$ sont dans n et l'hypothèse dit que $\underline{F}$ a un dernier élément.

18. **Couple** (voir ens. al. 24) **et suite de deux** : soit un couple (x , y). Les couples $(1 , x)$ et $(2 , y)$ sont les termes d'une fonction particulière dont les antécédents sont 1 et 2 et les images x et y. En faisant $x = x_1$ et $y = x_2$ les écritures (x , y) et (x_1 , x_2) sont synomymes.

Cardinal d'un ensemble

19. **Si il existe une bijection entre deux entiers naturels ils sont confondus**.
Initiation : la phrase "Si il existe une bijection entre 0 et un entier naturel celui-ci est zéro" est paradoxalement vraie.
Hypothèse la phrase "Si il existe une bijection entre m et un entier naturel celui-ci est n" est vraie.
Hérédité : soit $\mathcal{B}$ une bijection entre le suivant de m et le suivant d'un entier naturel p. Les deux suivants s'écrivent $m \cup \{m\}$ et $n \cup \{n\}$. $\mathcal{B}$ est un ensemble de couples (un élément de $m \cup \{m\}$, un élément de $n \cup \{n\}$). Chaque antécédent a une image unique et chaque image a un antécédent unique, en outre, chaque élémen $n \cup \{n\}$ est antécédent et chaque élément de $n \cup \{n\}$ est une image. Deux cas sont possibles.
♦ cas 1 (fig. 1 à gauche en gris) : $\mathcal{B}$ contient le couple (m , n) : alors $\mathcal{B}$ privé de ce couple est une bijection de m vers n donc $m = n$ par hypothèse, donc les suivants $m \cup \{m\}$ et $n \cup \{n\}$ sont égaux.
♦ cas 2(fig. 1 à droite en gris) : $\mathcal{B}$ ne contient pas le couple (m , n) : alors m, considéré comme antécédent, a comme image un élément u de $n \cup \{n\}$ qui n'est pas u donc un élément u de n. Soit alors $\mathcal{T}$ l'identité de l'ensemble $n \cup \{n\}$ à laquelle on enlève les couples (u , u) et (n^+ , n^+) et les remplace par (u , n^+) et (n^+ , u). C'est une nouvelle bijection de $n \cup \{n\}$ vers lui-même. La succession de $\mathcal{B}$ et de $\mathcal{T}$ est une bijection de $m \cup \{m\}$ vers $n \cup \{n\}$ et qui contient le couple (m , n), donc la succession de $\mathcal{B}$ et de $\mathcal{T}$ nous met dans la situation du
♦ cas 1.
Note. Soit une bijection entre $m \cup \{m\}$ et un entier naturel. Comme elle est sensée contenir au moins un couple, il faut que l'autre entier naturel ne soit pas zéro. Il est donc le suivant s d'un nombre n donc la démonstration précédente prouvant que $m \cup \{m\}$ et s sont confondus ■



20. **Cardinal** Si entre un ensemble quelconque et un entier naturel existe une bijection, alors on dira que l'entier naturel est un cardinal de E. Si $\mathcal{B}$ et $\mathcal{C}$ sont deux bijections, l'une de E vers m et l'autre de E vers n, alors la succession de la réciproque de $\mathcal{B}$ et de $\mathcal{C}$ est une bijection de m vers n donc d'après l'al. 31, $m = n$. **Le cardinal d'un ensemble si il existe est unique**. On l'écrit card E ou card(E).
21. Par définition, **un ensemble est fini et dénombrable si il a un cardinal**.

Opérations sur les nombres entiers naturels

Addition

22. **Définition**
Initiation : par définition $n + 0 = n$,
hypothèse : on a défini $n + p$,
hérédité : n + (suivant de p) est le suivant de $n + p$.

23. **Additionner 1 à un entier naturel donne son suivant**.
Démonstration. Le suivant de n, donc de $n + 0$ est n + (suivant de 0) ■

24. **Tout entier naturel autre que 0 et 1 est une série d'additions de 1**.
Démonstration. Elle est immédiate par récurrence de la proposition "$x = 0$ ou $x = 1$ ou $x = 1 \ldots + 1$" ■

25. **Toutes les règles de transformation de formules algébriques concernant l'addition apprises à l'école peuvent être démontrées** (voir structures).

26. **Si la solution x de l'équation $x + b = a$ existe elle est unique**.
Démonstration. Soit $\mathcal{D}(b)$ la phrase "si $x + b = y + b$ alors $x = y$".
Initiation : si $x + 0 = y + 0 = a$ alors x et y sont égaux donc $\mathcal{D}(0)$ est vraie.
Hypothèse : $\mathcal{D}(b)$ est vraie.
Hérédité : si x + suivant de $b = y$ + suivant de b alors suivant de $(x + b)$ = suivant de $(y + b)$ donc (al. 72) $x + b$ et $y + b$ sont égaux et on applique l'hypothèse ■

27. **Proposition**. On a toujours $a \subset a + b$.
Démonstration.
Initiation ($b = 0$) : comme $a \subset a$ la phrase "$a \subset a + 0$" est vraie.
Hypothèse : "$a \subset a + b$" est vraie.
Hérédité : Alors $a \subset a + b \subset$ (suivant de $a + b = a$ + suivant de b) donc "$a \subset a$ + suivant de b" est vraie ■

28. **Proposition**. Si $a + b = c$ alors a et b est inclus dans c.
Démonstration.
Par commutativité de l'addition, on peut refaire la démonstration en échangeant les lettres a et b ■

29. **Proposition**. Si $a \subset b$ alors il existe x tel que $x + a = b$.
Démonstration.
Initiation ($a = 0$) : la phrase "si $0 \subset b$ il existe x tel que $x + 0 = b$" est vraie, la solution x étant $x = b$.
Hypothèse : la phrase " Si $a \subset b$ alors il existe x tel que $x + a = b$ " est vraie.
Hérédité : Si (suivant de a) $\subset b$ alors (al. 69 et transitivité de l'inclusion) $a \subset b$ donc par hypothèse il existe y tel que $y + a = b$ donc $a + y = b$ donc suivant de $(a + y)$ = suivant de b donc a + (suivant de y) = suivant de b donc la phrase "Si $a \subset$ suivant de b alors existe x tel que $a + x =$ suivant de b " est vraie, la solution x étant le suivant de y ■

30. **Si une somme d'entiers naturels est nulle, ces entiers sont tous nuls**.
C'est une conséquence immédiate de l'al. 103 : $a + b = 0$ donne $a \subset 0$ et $b \subset 0$ donc a et b sont vides.
On procède ensuite par récurrence sur des sommes de 3 termes, puis 4 termes et ainsi de suite ■

31. **L'addition définit une injection de chaque entier naturel**. On l'appelle **translation croissante**.
Démonstration. On considère les qualités des relations binaires (ch 02, collections et ensembles) $\mathcal{F}$, $\mathcal{J}$,$\mathcal{A}(u)$ et $\mathcal{S}(v)$: les rappeler suffit :
Qualité $\mathcal{F}$, "chaque antécédent n'a qu'une image",
Qualité $\mathcal{J}$, "chaque image n'a qu'un antécédent",
Qualité $\mathcal{A}(u)$, "tout élément de u est un antécédent",
Qualité $\mathcal{S}(v)$, "tout élément de v est une image" □
Il reste à identifier l'ensemble des images des éléments d'un entier naturel.
De $0 \in y \in a$ vient par addition d'un même nombre aux trois membres de cette double inégalité $b \in y + b \in a + b$. Réciproquement, la soustraction de b redonne la définition de l'entier naturel a.
La translation est une bijection entre a et l'ensemble i défini par "$b \in x \in a + b$".
Note. La réunion de b avec i est l'entier naturel $a + b$.
Démonstration.
♦ $x \in b \cup i \Rightarrow x \in$ (b ou i) $\Rightarrow$(al. 24) $x \in b$ si non $x \in i$ donc $x \in a + b$.
♦ $x \in a + b \Rightarrow$ si x est hors de b alors $b \in x \in a + b$ donc $b \in i$ si non $x \in b$ donc $x \in a + b$ ■

32. **Le cardinal d'une réunion d'ensembles finis disjoints est la somme de leurs cardinaux**.
Démonstration. Soient deux ensembles A et B finis. On sait que ces cardinaux sont donnés par une bijection $\mathcal{A}$ de card(A) vers A et une autre $\mathcal{B}$ de card(B) vers B. Considérons la bijection $\mathcal{B}'$de card(A) vers l'ensemble I défini par card(B) $\in x \in$ card(A) + card(B). La succession de $\mathcal{B}' \circ \mathcal{B}$ est une bijection de I vers B donc la réunion $\mathcal{A} \cup (\mathcal{B}' \circ \mathcal{B})$ est une bijection de card(A) $\cup I$ =(al. 28) card(A) + card(B) vers $A \cup B$.

Soustraction

33. **Définition**. Si elle existe, la solution x de l'équation $x + b = a$ est unique (al. 34) donc on peut lui donner un symbole : on l'écrit $a - b$. Si donc b $\subset$ a alors (al. 102) $a - b$ est possible.
34. **On a équivalence logique entre la soustraction et l'inclusion**.
35. ***Démonstration***. $a - b$ est possible $\Rightarrow$(al. 39) il existe x tel que $x + b = a$ $\Rightarrow$(al. 37) $b \subset a$ $\Rightarrow$(al. 36) il existe x tel que $x + b = a$ $\Rightarrow$(al. 39) $a - b$ est possible ■
36. **Toutes les règles de transformation de formules algébriques concernant addition et soustraction apprises à l'école peuvent être démontrées** (voir structures).
37. **On peut additionner ou soustraire un même nombre aux deux membres d'une inclusion ou d'une appartenance**.
Démonstration.
Cela résulte des propriétés calculatoires algébriques des opérations + et – annoncées al. 42.
38. Soient deux ensembles E et F finis et dénombrables. Soient card E et card F leurs cardinaux.
39. **Le cardinal du complémentaire d'un ensemble dans un autre est la différence de leurs cardinaux**.
40. ***Démonstration***. On a $(A \setminus B) \cup B = A$ donc card$(A \setminus B)$ + card (B) = card(A) donc card$(A \setminus B)$ = card(A) – card (B) ■

Multiplication

41. **Définition**
Initiation : par définition $n \times 0 = 0$.
Hypothèse : on a défini la multiplication $n \times p$.
Hérédité : $n \times$ (suivant de p) = ($n \times p$) + p.
La phrase "$n \times p$ a été définie" est vraie quels que soient les entiers naturels n et p.
42. **Toutes les règles de transformation de formules algébriques concernant addition, soustraction et multiplication apprises à l'école peuvent être démontrées** (voir structures).
43. **Une multiplication par un entier naturel autre que 0 et 1 est égale à une série d'additions d'un même nombre**.
Démonstration : comme tout entier naturel b autre que 0 at 1 est une série d'additions de 1, on a $a\ b = a\ (1 \ldots + 1) = a \ldots + a$ ■
44. **On peut multiplier les deux membres d'une inclusion par un même nombre ou les deux membres d'une appartenance par un même nombre non nul**.
Démonstration. Si $a \subset b$ alors $a - b$ est possible alors (al. 45) $(a - b)\ m = a\ m - b\ m$ est possible et on applique l'al. 39. D'autre part $a \in b$ $\Rightarrow$(al. 80) a $\subset$ b $\Rightarrow$ $a\ m \subset b\ m$ et si $a\ m = b\ m$ alors on arrive à la contradiction $a = b$ (al. 19) ■
45. **Pour qu'un produit soit nul il faut et il suffit qu'un des multiplicateurs soit nul**.
Démonstration. Soit $\mathcal{M}(b)$ la phrase "$a\ b = 0$ si et seulement si a ou b est nul".
♦ Preuve de la nécessité :
Initiation. La phrase "$a\ 0 = 0 \Rightarrow a$ ou 0 est nul" est vraie.
Hypothèse : $\mathcal{M}(b)$v.
Hérédité : $a \times$ (suivant de b) = 0 $\Rightarrow$ $(a \times b) + a = 0 \Rightarrow$ (al. 38) $a\ b = 0$ et $a = 0 \Rightarrow a$ ou b est nul.
♦ Preuve de la suffisance : Si a ou b est nul alors $a\ b = (0\ a$ ou $0\ b) = 0$ ■
46. **Soient** b et c **deux entiers naturels, le premier étant non nul. Si elle existe, la solution** x **de l'équation** $x\ b = c$ **est unique**.
Démonstration. Soient x et x' deux solution de cette équation : alors $x\ b = x'\ b$ donc $(x - x')\ b = x\ b - x'\ b$ est nul donc (al. 47) un des facteurs $x - x'$ ou b est nul donc c'est la différence qui est nulle donc $x = x'$ ■

Division

47. **Définition** : On a vu que, si elle existe, la solution x de l'équation $x \times b = c$ est unique. Elle mérite donc un symbole : ce sera $b \div c$ ou b / c ou encore $\frac{b}{c}$ et sera appelée **quotient** de a par b, a étant appelé **dividende** et b **diviseur**.
48. **Toutes les règles calculatoires apprises en algèbre à l'école peuvent, sous réserve qu'on puisse effectuer les opérations soustraction et division, être démontrées** (voir structures).
49. **On peut diviser (si cette opération est possible) les deux membres d'une appartenance ou d'une inclusion par un même nombre non nul**.
Démonstration. si a ($\in$ ou $\subset$) b alors $a \subset b$ donc $a - b$ est possible donc si la division par m est possible on a le résultat $\frac{a}{m} - \frac{b}{m}$ qui montre que $\frac{a}{m} \subset \frac{b}{m}$. Si en plus $\frac{a}{m} = \frac{b}{m}$ une multiplication par m redonne $a = b$ ce qui est une contradiction si $a \in b$ ■

50. **Division euclidienne**. **Soient** D **et** d **deux entiers naturels, le deuxième étant autre que zéro. Il existe un couple** $(q , r \in d)$ **et un seul d'entiers naturels tel que** $D = d\ q + r$. **Dans ce cas,** D **est le dividende**, d **le diviseur**, q **le quotient et** r le **reste**. **De plus**, $d\ q \subset D \in d\ (q + 1)$ **et** r, $d\ q$ **et** q **sont inclus dans** D. Dans ce cas, on se sert de la disposition en croix ci-contre.

D	d
r	q

Disposition en croix

Démonstration.
♦a L'ensemble des multiples de d inclus dans D a un dernier élément $d\ q$. On a donc $d\ q \subset D$.
♦b Si $d\ (q + 1) \subset D$, vu que $q \in q + 1$ si d n'est pas zéro, alors (al. 51) on aurait $d\ q \in d(q + 1) \subset D$ donc $d\ q$ ne serait pas le dernier multiple de d inclus dans D. On conclut que $D \in d\ (q + 1)$.
♦c Comme $d\ q$ est unique en tent que dernier élémént unclus dans D, le reste $r = D – d\ q$ est aussi unique.
♦d Si $d \subset r =$ on aurait $D = d\ q + d = d(q + 1)$ ce qui contredit ♦b ■

51. **Note** : la division euclidienne devient une **division** si le reste est nul. Dans ce cas, on dit que le diviseur **divise** le dividende et que le dividende est un **multiple** du diviseur.

Multiples, diviseurs, base

52. **Tout entier naturel non nul est inclus dans ses multiples non nuls et contient ses diviseurs**.
53. ***Démonstration***.
♦a Soit a un entier naturel non nul. Si M est multiple de a il existe m tel que $M = m\ a$. Si m est nul, alors a est nul (contradiction). On a donc m non nul donc $1 \subset m$ (al.23) donc (al. 45) $a \subset a\ m = M$.
♦b Soit a un entier naturel non nul. Si d est diviseur de a il existe m tel que $m\ d = a$. Si m est nul, a est nul (contradiction). On a donc $1 \subset m$ donc $d \subset d\ m = a$ ■
54. **Base** : c'est un nombre entier naturel b autre que zéro et un. Alors (al. 23) $1 \in b$ donc par multiplication des deux membres par a non nul, $a \in a\ b$.
55. **Puissances d'une base** :
56. ♦aL'idée est d'écrire une multiplication $a \cdot \cdot \cdot \times a$, le nombre a étant écrit p fois, a^p. Cette idée n'est applicable en apparence que si p n'est ni zéro, ni 1, donc si $1 \subset p$. On a donc $a^p\ a = (a \dots a)\ a$ avec a écrit p fois entre parethèses, $= a \dots a\ a$ avec a écrit $p + 1$ fois, $= a^{p+1}$.
♦b Une conséquence immédiatement démontrable par récurrence de la proposition $\mathcal{P}(x) =$ "$x = 0$ ou 1 ou $a^p\ a^x = a^{p+x}$" est l'identité $a^p\ a^q = a^{p+q}$ pour p et q autres que 0 ou 1.
Initiation : si $x = 0$, "$\mathcal{P}(x)$ est vraie" est trivial.
Hypothèse : $\mathcal{P}(x)$ est vraie.
Hérédité : $a^p\ a^{\text{suivant de } x} = a^p\ (a^x\ a) = (a^p\ a^x)\ a = a^{p+x}\ a = a^{(p+x)+1} = a^{p+(x+1)} = a^{p + \text{suivant de } x}$ □
♦c **Exposant nul** : Si on souhaite conserver l'identité précédente alors il faut que $a^0\ a^q = a^q$. Si a est autre que zéro, a^q est non nul donc la résolution de cette équation d'inconnue a^0 donne en divisant les deux membres par a^q $a^0\ a^q / a^q = a^q / a^q = 1$ donc $a^0 = 1$.
♦d **Exposant unité** : le souhait de garder l'identité ♦a donne immédiatement $a^1\ a^p = a^{1+p}$ qui est $a\ a \cdot \cdot \cdot a$, le a étant écrit $p + 1$ fois, donc est $a\ (a \cdot \cdot \cdot a)$, le a étant écrit p fois entre parenthèses. On résout donc l'équation $a^1\ a^p = a\ a^p$ d'inconnue $a^1 = a$.
♦e **Division d'une puissance par une autre** : a^{p-q} est solution de l'équation $a^{p-q}\ a^q = a^p$ donc si la division est faisable avec un reste nul $a^{p-q} = a^p / a^q$.
Puissance d'une puissance : on démontre la loi $(a^m)^n = a^{m\,n}$.
Initiation : $(a^m)^0 = 1$ et $a^{m \cdot 0} = a^0 = 1$ donc $(a^m)^0 = a^{m \cdot 0}$.
Hypothèse : $(a^m)^n = a^{m\,n}$.
Hérédité : $(a^m)^{\text{suivant de } n} = (a^m)^n\ a^m = a^{m\,n+m} = a^{m \cdot \text{suivant de } n}$.
57. **La suite des puissances d'une base est strictement croissante**.
Démonstration. Soit la phrase $\mathcal{B}(n) =$ "si $m \in n$ alors $a^n \in a^m$" .
Initiation : quelque soit m on a $0^m = 0$. D'auyre part (al. donc
58. **Toute ensemble majoré de puissances d'une base a une dernière puissance incluse dans le majorant lui-même possédé par la puissance suivante de cette base**.
Démonstration. Soit b une base et a un entier naturel : il faut montrer qu'il existe un entier naturel k tel que $b^k \subset n \in b^{k+1}$.
On considère la suite des puissance d'une base b appartenant à un entier naturel donné n. Elle a un dernier élément b^k donc $b^k \subset n$. En conséquence, si on avait $b^{k+1} \subset n$ on aurait par transitivité de l'inclusion $b^{k+1} \subset b^k$ (contradiction avec l'al. 85). On a donc pas $b^{k+1} \subset n$ donc on a $n \subset b^{k+1}$ et $n \neq b^{k+1}$ donc (al. 92) l'encadrement $b^k \subset n \in b^{k+1}$■
59. Soit b une base et n un entier naturel : il existe un unique couple de nombres $(k, q \in b)$ encadrant n selon $b^k\ q \subset n \in b^k\ (q + 1)$.
Démonstration. La division euclidienne de n par b^k donne $b^k\ q \subset n \in b^k\ (q + 1)$. Associé à $b^k \subset n \in b^{k+1}$ cela donne $b^k\ q \subset n \in b^{k+1}$ donc (al 80) $b^k\ q \subset n \subset b^{k+1}$ donc par transitivité de l'inclusion $b^k\ q \subset b^k\ b$ donc (al. 116)

$q \subset b$. Si en plus $q = b$ alors on aurait $b^{k+1} \subset n \subset b^{k+1}$ donc $n = b^{k+1}$ (contradiction). On a donc q ($\subset$ et $\neq$) b donc (al. 92) $q \in b$.

60. **Écriture des entiers naturels en base** b. Elle se fait par divisions euclidiennes successives. Elle donne $n = b^k q_k + r_k$, $r_k \in b^k$, $q_k \in b$. On recommence :
$r_k = b^{k-1} q_{k-1} + r_{k-1}$, $r_{k-1} \in b^{k-1}$, $q_{k-1} \in b$ et ainsi de suite. On arrête quand $k - i$ atteint zéro, ce qui donne la décomposition $\boxed{n = b^k q_k \cdots + b^0 q_0 \text{ avec tous les } q_i \in b}$.

P.G.C.D et P.P.C.M

Compte tenu du procédé d'élaboration de cette décomposition, nous savons qu'elle est unique.

61. **Plus grand commun diviseur ou P.G.C.D.** Étant donnée une famille $\underline{E}$ d'entiers naturels non tous nuls, l'ensemble des diviseurs communs à ces nombres est une partie finie et non vide de $\mathbb{N}$:
finie, car un diviseur d'un entier non nul a est borné par le plus petit nombre de $\underline{E}$,
non vide car $\underline{E}$ contient 1.
Cet ensemble admet donc un plus grand élément d, appelé le P.G.C.D de la famille $\underline{E}$.

62. **Le P.G.C.D de deux nombres n'est pas changé si on les remplace par une de leurs combinaisons linéaires.**
Démonstration. Une combinison linéaire de a et b est une formule du genre $a\,x \pm b\,y$ où x et y sont deux entiers naturels quelconques.
Soit d un diviseur commun de a et b. Alors $a = d\,i$ et $b = d\,j$ donc $a\,x \pm b\,y = d\,i\,x \pm d\,j\,y = d\,(i\,x \pm j\,y\,)$ donc d est diviseur de $a\,x \pm b\,y$ □
Cas particulier : si la division euclidienne de a par b donne $a = b\,q + r$ et $r \in b$ et si d divise a et b alors d divise $a - b\,q$ donc r. Si d divise b et r il divise la combinaison linéaire $b\,q + r$, c'est-à-dire a. Les diviseurs communs de a et b et ceux de b et r sont les mêmes, en particulier le P.G.C.D est le même.

63. **Algorithme d'Euclide**.
Initiation. Le P.G.C.D de a et $b \in a$ est le P.G.C.D de b et du reste $r \in b$ de la division de a par b.
Après changement de symboles,
le P.G.C.D de r_0 et $r_1 \in r_0$ est le P.G.C.D de r_1 et du reste $r_2 \in r_1$ de la division de r_0 par r_1,
le P.G.C.D de r_0 et $r_{0+1} \in r_0$ est le P.G.C.D de r_{0+1} et du reste $r_{0+2} \in rr_{0+1}$ de la division de r_0 par r_{0+1}.
Hypothèse :
le P.G.C.D de r_i et $r_{i+1} \in r_i$ est le P.G.C.D de r_{i+1} et du reste $r_{i+2} \in r_{i+1}$ de la division de r_i par r_{i+1}.
Hérédité.
Le P.G.C.D de r_{i+1} et $r_{i+2} \in r_{i+1}$ est le P.G.C.D de r_{i+2} et du reste $r_{i+3} \in r_{i+2}$ de la division de r_{i+1} par r_{i+3}.
Conclusion : le P.G.C.D de r_0 et r_1, c'est-à-dire de a et b est le P.G.C.D de toutes les paires r_i , r_{i+1}.
Son arrêt : si r_{i+3} est nul alors on sait que le P.G.C.D de r_{i+1} et $r_{i+2} \in r_{i+1}$ est le P.G.C.D de r_{i+2} et de zéro et aussi le P.G.C.D de toutes les autres r_i donc est le P.G.C.D de a et b ■

64. **Plus petit commun multiple ou P.P.C.M.**
Soient a et b deux entiers naturels :
si a ou b est nul, P.P.C.M(a , b) = 0 ;
si a et b sont non nuls, considérons l'ensemble des entiers strictement positifs qui sont multiples à la fois de a et de b. Cet ensemble d'entiers naturels est non vide, car il contient $a\,b$. Il possède donc un plus petit élément, et c'est cet entier naturel que l'on appelle le P.P.C.M de a et b.

65. **Sa détermination**. Soit d le P.G.C.D de a et b, alors $a = d\,a'$, $b = d\,b'$. Définissons $m = d\,a'\,b'$. Alors à la fois m est $(d\,a')\,b' = a\,b'$ ce qui montre que m est multiple de a et $m = (d\,b')\,a' = b\,a'$ ce qui montre que m est multiple de b donc P.P.C.M(a , b) $\subset m$. Comme m est inclus dans tous ses multiples, on a $m \subset$ P.P.C.M(a , b) donc par antisymétrie de l'inclusion m = P.P.C.M(a , b).

Nombres premiers

66. Un **nombre premier** est un entier naturel qui admet exactement deux diviseurs distincts entiers. En conséquence, ces deux diviseurs sont 1 et l'entier lui-même.

67. **Chaque nombre entier naturel peut être écrit comme un produit de nombres premiers**.
Démonstration. On étudie la phrase $\mathcal{Pr}(n)$ = "tout entier inclus dans n est zéro, 1 ou une multiplication de nombres premiers".
Initiation : elle est triviale.
Hypothèse : $\mathcal{Pr}(n)$v.
Hérédité. Soit p le plus petit entier autre que zéro ou 1 et divisant le suivant de n.
a- Si p est premier, alors la démonstration est faite.
b- Si p n'est pas premier, vu qu'il divise n, on a $p\,q$ = (suivant de n) donc (q et p) $\subset$ (suivant de n). On a le choix entre (q et p) = (suivant de n) et (q et p) $\in$ (suivant de n).

c- Le premier choix donne (suivant de n) (suivant de n) = (suivant de n) donc (suivant de n) = 1 donc $n = 0$ et la démonstration est faite. Le deuxième choix donne (q et p) $\subset n$ et par hypothèse la démonstration est faite ■

68. **La décomposition précédente est unique**.

Démonstration. Nommons $\mathcal{D}(k)$ la phrase "$k = 0$ ou si les produits de nombres premiers $\prod q_{i \subset m}$ et $\prod s_{j \subset k}$ sont égaux alors leurs facteurs $q_{i \subset m}$ et $s_{j \subset k}$ sont identiques".
Initiation : elle est triviale.
Hypothèse : $\mathcal{D}(J)$v.
Hérédité. On isole les numéros particuliers m et le suivant de k nommé n.
Alors $\prod q_{i \subset m} = q_m \prod q_{i \neq m}$ et $\prod s_{j \subset n} = s_n \prod s_{j \neq n}$ (on omet dans les produits les mentions en indice $_{i \subset m}$ et $_{j \subset n}$). On a donc $q_m \prod q_{i \neq m} = s_n \prod s_{j \neq n}$. Note : $j \subset n$ et $j \neq n \Rightarrow j$ ($\subset$ et $\neq$) (suivant de k) $\Rightarrow j \subset k$.
Cas 1 : si $q_m = s_n$, on simplifie de chaque côté de l'égalité : $\prod q_{i \neq m} = \prod s_{j \neq n}$.
Cas 2 : supposons que q_m est différent de s_n. L'égalité $\prod q_i = \prod s_j$ signifie que le nombre premier q_m divise le produit des deux nombres s_n et $\prod s_{j \neq n}$ qu'on va appeler p. D'autre part, q_m ne divise pas s_n, puisque deux nombres premiers différents n'ont, par définition, pas de facteurs communs autres que 1. On conclut que q_m, divise $p = \prod s_{j \neq n}$. L'hypothèse de récurrence s'applique donc la décomposition de $\prod q_{i \neq m}$ et $\prod s_{j \neq n}$ sont identiques. Alors $q_m \prod q_{i \neq m}$ et $s_n \prod s_{j \neq n}$ sont des décompositions identiques donc $\prod q_{i \subset m}$ et $\prod s_{j \subset \text{suivant de } k}$ sont identiques ■

Théorèmes de Bezout et Gauss

69. **Dans $\mathbb{N}$, a et b étant donnés, le plus petit élément de l'ensemble des $a\,x \pm b\,y$ est le P.G.C.D de a et b.**
Démonstration.
♦a La proposition "a et b étant donnés, $\exists\, x$ et y tels que $a\,x \pm b\,y = s$" définit un ensemble $\underline{S}(a\,,\,b)$.
♦b- Cet ensemble a un plus petit élément d (al. XX). On a donc $d = a\,x \pm b\,y \subset$ tous les autres $r = a\,x' \pm b\,y'$.
♦c- Alors d divise a et b.
Preuve. Si on pouvait écrire la division euclidienne de a par d avec un reste non nul alors on aurait $a = d\,q + r$ et $r \in d$. Substituons d : on aurait $a = (a\,x \pm b\,y)\,q + r = a\,x\,q \pm b\,y\,q + r$ qui donnerait $a \pm a\,x\,q \pm b\,y\,q = r$ avec inversion du signe devant $a\,x\,q$ et $b\,y\,q$, donc $a\,(1 \pm x\,q) \pm b\,(y\,q) = r$, avec $1 \pm x\,q$ dans le rôle de x' et $y\,q$ dans celui de y', ce qui est absurde avec le point ♦b. La démonstration est analogue avec b □
d- Enfin, d est le P.G.C.D ($a\,,\,b$).
Preuve : tout diviseur de a et b divise leurs combinaisons linénaires (al XX), en particulier d donc (al XX) est inclus dans d ■

70. **Dans $\mathbb{N}$, a et b étant donnés, l'ensemble des $a\,x \pm b\,y$ est celui des multiples du P.G.C.D de a et b.**
Démonstration. Tous les entiers de $\underline{S}$ sont des multiples du P.G.C.D de a et b. Inversement, si m est un multiple du P.G.C.D de a et b, on a $m = k\,d$ donc $m = k\,(a\,x \pm b\,y) = a\,k\,x + b\,k\,y$ qui est membre de $\underline{S}$.

71. **Nombres premiers entre eux : par définition leur P.G.C.D vaut 1.**

72. **Théorème de Bezout** : **a et b sont premiers entre eux $\Leftrightarrow$ il existe u et v tels que $a\,u \pm b\,v = 1$.**

73. ***Démonstration***. P.G.C.D ($a\,,\,b$) = 1 $\Rightarrow$(al XX) il existe u et v tels que $a\,u \pm b\,v = 1$ $\Rightarrow$(al XX) 1 est multiple du P.G.C.D de a et b $\Rightarrow$ P.G.C.D de a et $b \subset 1 \Rightarrow$(aucun diviseur n'est nul) P.G.C.D de a et $b = 1$ ■

74. **Théorème de Gauss** : **Si un nombre premier avec a divise le produit $a\,b$, alors ce nombre divise b.**

75. ***Démonstration***. n est premier avec $a \Rightarrow$ il existe u et v tels que $n\,u + a\,v = 1$ donc que $b\,n\,u + b\,a\,v = b \Rightarrow$ $b\,n\,u + (b\,a)\,v = b \Rightarrow$($n$ divise $b\,a$ et $b\,n\,u$) n divise b ■

76. **Corollaire de Gauss** : **si un nombre est premier avec chacun de deux autres, il est premier avec leur produit**.
Démonstration. Si n est premier avec a et avec b, le théorème de Bézout dit qu'il il existe deux couples d'entiers ($u\,,\,v$) et ($x\,,\,y$) tels que $n\,u \pm a\,v = 1$ et $n\,x \pm b\,y = 1$, donc que $(n\,u \pm a\,v)\,(n\,x \pm b\,y) = 1$ donc que $n\,u\,n\,x \pm n\,u\,b\,y \pm a\,v\,n\,x \pm a\,v\,b\,y = 1$, donc que $n\,(u\,n\,x \pm u\,b\,y \pm a\,v\,x) \pm a\,v\,b\,y = 1$, donc que a et $b\,c$ sont premiers entre eux ■

77. **Dès qu'un de deux entiers est non nul, leur multiplication est égale à la multiplication de leur P.P.C.M par leur P.G.C.D**.
Démonstration. Soient deux entiers positifs a et b, m = P.P.C.M ($a\,,\,b$) et d = P.G.C.D ($a\,,\,b$).
Soit n un diviseur de a et b.
♦ Alors $n\,a$ et $n\,b$ divisent $a\,b$. Preuve : parce que n divise a et $b\,n\,q = a$ et $n\,r = b$ donnent $(n\,b)\,q = a\,b$ et $(n\,a)\,r = a\,b$ □
♦ Alors n divise $a\,b$. Preuve : parce que n divise de a et b on a $n\,q = a$ et $n\,r = b$ donc $n\,q = a$ et $n\,r = b$ donnent $n\,q\,n\,r = a\,b$ donc $n\,(q\,n\,r) = a\,b$ donc n divise $a\,b$ □
♦ Alors a divise $a\,b\,/\,n$. Preuve : parce que n divise a et b, $n\,q\,n\,r = a\,b$ donc $a\,r = (n\,q)\,r = a\,b\,/\,n$ donc a divise $a\,b\,/\,n$ □

♦ Alors b divise $a\ b$ / n. Preuve : la démonstration est analogue.
♦ n divise P.P.C.M(a , b) $\times$ $a\ b$ / P.G.C.D(a , b). Preuve : tous les diviseurs communs n de a et b sont tels que a et b divisent $a\ b$ / n, en particulier le plus grand donc a et b divisent $a\ b$ / P.G.C.D(a , b).
♦ Il existe donc k et l entiers naturels tels que $a\ k$ et $b\ l$ soient égaux à $a\ b$ / P.G.C.D(a , b).

Nombres entiers relatifs

78. L'idée initiale est que si la différence $a - b$ entre entiers naturels n'est pas un entier naturel, ce qui arrive si $a \in b$, elle est un nombre d'une nouvelle espèce, les **nombres entiers strictement négatifs**.
79. Il nous faut agrandir $\mathbb{Z}$ de nouveaux éléments constituant un ensemble E à définir et qu'on va renommer $\mathbb{Z}^{-}*$ de telle sorte que $\mathbb{Z}^{-}* \cup \mathbb{N}$ soit un ensemble $\mathbb{Z}$.
80. Une difficulté est que si un entier naturel est le résultat d'une soustraction, il est aussi le résultat d'une infinité d'autres soustractions.

Signes

81. Nommons $(0 , n \in \mathbb{N}*)$ le résultat supposé unique de la soustraction $0 - n$. Choisissons l'ensemble de ces couples $(0 , n)$ comme candidat $\mathbb{Z}^{-}*$.
82. Soient deux entiers naturels m et n. Parce que l'appartenance a le don d'ubiquité sur $\mathbb{N}$, on a le choix $m \in n$ ou $m = n$ ou $n \in m$ qui donne dans l'ordre $m - n \notin \mathbb{N}*$ ou $m = n$ ou $m - n \in \mathbb{N}*$. Par convention, toujours dans cet ordre le résultat $n - m$ sera dans $\mathbb{Z}^{-}*$, nul donc $m = n$, ou dans $\mathbb{N}*$, d'où la tentation de renommer $\mathbb{Z}^{+}*$ l'ensemble $\mathbb{N}*$.
On adopte aussi les définition des ensembles $\mathbb{Z}^{-}* \cup \{0\} = \mathbb{Z}^{-}$, $\{0\} \cup \mathbb{Z}^{+}* = \mathbb{Z}^{+}$ et $\mathbb{Z}^{-}* \cup \{0\} \cup \mathbb{Z}^{+}* = \mathbb{Z}$.
On a alors les identifications $\mathbb{Z}^{+} = \mathbb{N}$ et $\mathbb{Z}^{+}* = \mathbb{N}*$.
Vocabulaire : les nombres de $\mathbb{Z}^{-}$ sont des **nombres entiers négatifs**, ceux de $\mathbb{Z}^{+}$ des **nombres entiers positifs**, ceux de $\mathbb{Z}^{-}*$ des **nombres entiers strictement négatifs**, ceux de $\mathbb{Z}^{+*}$ des **nombres entiers strictement positifs**, et ceux de $\mathbb{Z}$ des **nombres entiers relatifs**.

Soustractions équivalentes

83. Dans $\mathbb{N}$, si un même entier naturel résulte des soustractions $a - b$ et $a' - b'$, alors l'égalité $a - b = a' - b'$ donne par addition de b et b' aux deux membres $a + b' = a' + b$, ce qui peut se lire *la somme des "moyens" est égale à la somme des "extrêmes"* ou "*les additions croisées sont égales*".
Inversement, si $a + b' = a' + b$, par soustraction aux deux membres de b et b', qui sont toujours possibles dans $\mathbb{N}$, on prouve que les deux soustractions $a - b$ et $a' - b'$ donneront le même entier naturel.
Par convention, si les différences ne sont pas des entiers naturels, deux d'entre elles dont la somme des extrêmes et des moyens sont égales désigneront toujours le même nombre entier relatif strictement négatif.
En particulier, (a , b) équivaut à $(0 , b - a)$ ou à $(a - b , 0)$ selon que la soustraction est dans $\mathbb{N}$ ou non.

$a - b$	$a + b'$
$a' - b'$	$a' + b$

additions croisées

Opposition

84. Opposer une différence consiste à la retourner, à permuter opérande et opérateur : l'opposée de $m - n$ est $n - m$, et est écrite $-(m - n)$. Les faits suivants sont évidents.
85. **L'opposition d'un nombre change son signe**.
86. **L'opposé de l'opposé d'un nombre est ce nombre**.
87. **Soit un entier relatif non nul. Lui-même ou son opposé est strictement positif**.
88.

opérande
* opérateur

= résultat

Opération

Valeurs absolues

89. Soit $x \in \mathbb{Z}$. Par définition, la **valeur absolue** de x est celui des deux opposés x et $-x$ qui est nul ou strictement positif. On l'écrit $|x|$. Les deux barres encadrant la lettre sont des *ornements*.
90. **Une valeur absolue est donc un entier naturel**.
91. On a $|x|$ = selon le cas $+x$ ou $-x$, ce qu'on écrit $\pm x$ et se lit "plus ou moins x".
92. En conséquence, $x = \pm |x|$.
93. On démontre immédiatement que
Si $x \in \mathbb{Z}^{+}*$ alors $|x| = x$.
Si $x \in \mathbb{Z}^{-}*$ alors $|x| = -x$, en particulier $|-1| = 1$.
Si $x = 0$, alors $|x| = 0$.
Si $x \in \mathbb{N}$ alors $|x| = x$, en particulier on a $|0| = 0$ et $|1| = 1$.

Opérations sur les entiers relatifs.

94. Dans $\mathbb{Z}$, les opérations addition, soustraction, multiplication et division ont été définies *par extension de leurs propriétés algébriques fondamentale établies dans* $\mathbb{N}$. Il s'agit
de l'associativité,
de la commutativité,
de la neutralité du zéro dans l'addition et
de la neutralité du un dans la multiplication,
de la distributivité à gauche et à droite de la multiplication par l'addition.
En conséquence, toutes les règles de transformation algébriques des formules de calcul démontrées dans $\mathbb{N}$ sont *de facto* applicables dans $\mathbb{Z}$.
La seule nouveauté est la définition de l'opposé par la soustraction à zéro : $-n = 0 - n$.
Voici, avec les démonstrations, les règles de calcul des entiers relatifs à partir d'entiers naturels a, b **et** n.

95. Additions
$a + (-b) = a + (0 - b) = (a + 0) - b = a - b$ si $a \supset b$ si non $-(b - a)$.
$(-a) + b = (0 - a) + b = 0 - (a - b) = b - a$ si $a \subset b$ si non $-(a - b)$.
$(-a) + (-b) = (0 - a) + (0 - b) = 0 + 0 - a - b = 0 - (a + b) = -(a + b)$.

96. Soustractions
$a - (-b) = a - (0 - b) = (a - 0) + b = a + b$. Soustraire un opposé, c'est l'additionner.
$(-a) - (-b) = (0 - a) + b = b + (-a) = b - a$ si $a \subset b$ si non $-(a - b)$.
$(-a) - b = (0 - a) - b = 0 - a - b = 0 - (a + b) = -(a + b)$.

97. Multiplications : on a la **règle des signes** (tableau 1).
$a\,(-b) = a\,(0 - b) = a\,0 - a\,b = 0 - a\,b = -a\,b$.
$(-a)\,(-b) = (0 - a)\,(0 - b) = 0 \cdot 0 - 0\,b - 0\,a + a\,b = 0 + 0 + 0 + a\,b = a\,b$.
$(-a)\,b = (0 - a)\,b = 0\,b - a\,b = 0 - a\,b = -a\,b$.

$x\,y$		y	
		b	$-b$
x	a	$a\,b$	$-a\,b$
	$-a$	$-a\,b$	$a\,b$

Tableau 1

98. Divisions : on a la même **règle des signes** que la multiplication.
Si $q = \frac{a}{-b}$, alors $q\,(-b) = a$ donc $(-q)\,b = a$ donc $-q = \frac{a}{b}$ donc $q = -\frac{a}{b}$ donc $\frac{a}{-b} = -\frac{a}{b}$.
Si $r = \frac{-a}{b}$, alors $r\,b = -a$ donc $(-r)\,b = a$ donc (ligne précédente) $r = -\frac{a}{b}$ donc $\frac{-a}{b} = -\frac{a}{b}$.
Si $s = \frac{-a}{-b}$, alors $s\,(-b) = -a$ donc $-s\,b = -a$ donc $s\,b = a$ donc $s = \frac{a}{b}$ donc $\frac{-a}{-b} = \frac{a}{b}$.

Inégalités entre entiers relatifs

L'usage des signes ensemblistes $\in$ et $\subset$ pour les inégalités chez les entiers naturels n'a plus de sens chez les entiers relatifs, d'où ce changement de notation : $<$ remplace $\in$ et $\leqslant$ remplace $\subset$.
Chez les ordinaux, $\subset \Leftrightarrow (\in$ ou $=)$ donc dans $\mathbb{Z}$ $\leqslant \Leftrightarrow (<$ ou $=)$.
Le modèle des inégalités sont celles dans $\mathbb{N}$: $x \in y \Leftrightarrow x - y \notin \mathbb{N}^*$ et on l'applique telle quelle dans $\mathbb{Z}$, ce qui donne la définition à $x < y \Leftrightarrow x - y \notin \mathbb{Z}^{+}{}^*$ donc $x < y \Leftrightarrow x - y \notin \mathbb{Z}^{-}{}^*$.

99. **L'opposition retourne les inégalités**.
Démonstration. $x < y \Leftrightarrow x - y \in \mathbb{Z}^{-}{}^* \Leftrightarrow$ l'opposé $-(x - y) = (-x) - (-y) \in \mathbb{Z}^{+}{}^*$ qui change le signe donne $(-y) - (-x) \in \mathbb{Z}^{-}{}^*$ qui donne $(-y) < (-x)$ ■
Cas particulier : $x < 0 \Leftrightarrow 0 < -x$. **L'opposition d'un nombre change son signe**.

100. **La multiplication par un nombre positif laisse invariantes les inégalités et la multuiplication par un nombre négatif les retournent**. C'est une conséquence immédiate de l'al. précédent et de la règle des signes de l'al. 97.

101. **On a équivalence entre**
être strictement négatif et être strictement plus petit que zéro et
être strictement positif et être strictement plus grand que zéro.
Démonstration . Soit $n \in \mathbb{Z}^{+}{}^*$: c'est un entier naturel non nul donc $0 \in n$ donne $0 < n$.
Soit $m \in \mathbb{Z}^{-}{}^*$: alors $-m \in \mathbb{Z}^{+}{}^*$ donc $0 < -m$ et par opposition on retourne l'inégalité $m < 0$ ■
Note : on a $-1 < 0 < 1$. ***Démonstration*** . On sait que dans $\mathbb{N}$, $0 \in 1$ donc $0 < 1$. Par opposition $-1 < 0$ ■

102. **Une somme d'entiers du même signe strict est de ce signe**.
Démonstration.
♦ x et $y \in \mathbb{Z}^{+}{}^* \Rightarrow x$ et $y \in \mathbb{N}^* \Rightarrow x$ et $y \in \mathbb{N} \Rightarrow x + y \in \mathbb{N} \Rightarrow$ parce que chez les entiers naturels, si une somme n'est nulle alors tous ses termes sont nuls, $x + y \in \mathbb{N}^* \Rightarrow x + y \in \mathbb{Z}^{+}{}^*$.
♦ x et $y \in \mathbb{Z}^{-}{}^* \Rightarrow -x$ et $-y \in \mathbb{Z}^{+}{}^* \Rightarrow (-x) + (-y) = -(x + y) \in \mathbb{Z}^{+}{}^* \Rightarrow x + y \in \mathbb{Z}^{-}{}^*$ ■
♦ Si deux relatifs sont du même signe strict

103. **Si une somme d'entiers relatifs de même signe est nulle chacun de ses termes est nul**.
Démonstration. Soit $x + y$ nulle. Si par exemple $x = 0$, alors il reste $y = 0$ et inversement. Si ni x ni y n'est nul on a vu que la somme est d'un signe strict ■

104. **On a la règle des signes de la multiplication ci-contre**. Le tableau 2 donne le signe strict de $x\,y$ selon les signes de x et y. ***Démonstration***.

$a\,b$		b	
		+	–
a	+	+	–
	–	–	+

Tableau 2

♦ $x > 0$ et $y > 0 \Rightarrow x$ et $y \in \mathbb{N}^* \Rightarrow x\,y \in \mathbb{Z}^{+}*$,
♦ $x > 0$ et $y < 0 \Rightarrow x$ et $-y \in \mathbb{N}^* \Rightarrow x\,(-y) \in \mathbb{Z}^{+}* \Rightarrow -x\,y \in \mathbb{Z}^{+}* \Rightarrow x\,y \in \mathbb{Z}^{-}*$,
♦ $x < 0$ et $y < 0 \Rightarrow x$ et $y \in \mathbb{Z}^{-}* \Rightarrow (-x)$ et $(-y) \in \mathbb{Z}^{+}* \Rightarrow (-x)\,(-y) = x\,y \in \mathbb{Z}^{+}*$,
♦ $x < 0$ et $y > 0 \Rightarrow -x$ et $y \in \mathbb{N}^* \Rightarrow (-x)\,y \in \mathbb{Z}^{+}* \Rightarrow -x\,y \in \mathbb{Z}^{+}* \Rightarrow x\,y \in \mathbb{Z}^{-}*$.
Si $q = a / b$, alors $q\,b = a$ d'où le tableau 2 de signes dont on déduit le tableau 3.

105. **On peut additionner ou soustraire un même nombre aux deux membres d'une inégalité sans l'inverser.**
Démonstration.
$a < b \Rightarrow a - b \in \mathbb{Z}^{-}* \Rightarrow$ si $m \in \mathbb{Z}$ et $(a + m) - (b + m)$ et $(a - m) - (b - m) = a - b \in \mathbb{Z}^{-}*$ donnent respectivement
$a + m < b + m$ et $a - m < b - m$ ■

$a\,/\,b$		b	
		+	–
a	+	+	–
	–	–	+

Tableau 3

106. **On peut additionner membre à membre deux inégalités de même sens**.
Démonstration.
$a < b$ et $x < y \Rightarrow b - a$ et $y - x \in \mathbb{Z}^{-}* \Rightarrow a - b$ et $x - y \in (\mathbb{Z}^{+}* \subset \mathbb{N}) \Rightarrow$
$(b - a) + (y - x) = (b + y) - (a + x) \in \mathbb{Z}^{+}* \Rightarrow (a + x) - (b + y) \in \mathbb{Z}^{-}* \Rightarrow (a + x) < (b + y)$ ■

107. **On peut multiplier ou diviser (si les divisions sont exactes) par un même nombre strictement positif une inégalité stricte sans l'inverser**. **Une multiplication par un nombre strictement négatif l'inverse**.
Démonstration.
♦ $a < b \Rightarrow a - b \in \mathbb{Z}^{-}* \Rightarrow$ si $m \in \mathbb{Z}^{+}*$ alors $a\,m - bm = (a - b)\,m \in \mathbb{Z}^{-}* \Rightarrow a\,m < b\,m$,
$\Rightarrow$ si $m \in \mathbb{Z}^{-}*$ alors $a\,m - bm = (a - b)\,m \in \mathbb{Z}^{+}* \Rightarrow b\,m - a\,m \in \mathbb{Z}^{-}* \Rightarrow b\,m < a\,m$.
♦ Si les divisions a / m et b / m sont exactes
$a < b \Rightarrow a - b \in \mathbb{Z}^{-}* \Rightarrow$ si $m \in \mathbb{Z}^{+}*$ alors $\frac{a}{m} - \frac{b}{m} = \frac{a-b}{m} \in \mathbb{Z}^{-}* \Rightarrow \frac{a}{m} < \frac{b}{m}$,
$\Rightarrow$ si $m \in \mathbb{Z}^{-}*$ alors $\frac{a}{m} - \frac{b}{m} = \frac{a-b}{m} \in \mathbb{Z}^{+}* \Rightarrow \frac{b}{m} - \frac{a}{m} \in \mathbb{Z}^{-}* \Rightarrow \frac{b}{m} < \frac{a}{m}$ ■

108. **Si** $1 < a < b$ **on a les encadrements** $a < a^2 < a\,b < b^2$.
Démonstration.
On a $0 < 1 < b$ donc on peut multiplier deux membres d'une inégalité par a et b.
$1 < a < b \Rightarrow a < a^2 < a\,b$ et $a\,b < b^2$ donc $a < a^2 < a\,b < b^2$ ■

109. **On peut multiplier membre à membre deux inégalités de même sens si le plus petit membre est strictement positif**.
Démonstration.
$0 < a < b$ et $0 < m < n \Rightarrow a\,m < b\,m$ et $m\,b < n\,b$ donc $a\,m < b\,n$ ■

110. **Inégalité triangulaire : la valeur absolue d'une somme est plus petite que la somme des valeurs absolues**. **Pour avoir égalité, il faut que les deux termes soient de même signe**.
Démonstration. On doit démontrer que $|x + y| \leqslant |x| + |y|$.
La définition des valeurs absolues donne
$|x + y| = |(|x|$ si $x \in \mathbb{Z}^{+}$ ou $-|x|$ si $x \in \mathbb{Z}^{-}) + (|y|$ si $y \in \mathbb{Z}^{+}$ ou $-|y|$ si $y \in \mathbb{Z}^{-})|$, ce qui donne 4 cas :
deux cas de signe contraire
♦ $\big||x| + (-|y|)\big| = \big||x| - |y|\big| =$ soit $|x| - |y|$ si la différence est positive donc est $< |x| - |y| + |y| = |x| + |y|$,
soit $-(|x| - |y|)$ si la différence est négative donc est $|y| - |x| < |y| + |x|$,
♦ $\big|(-|x|) + |y|\big| <$ par un raisonnement analogue en permutant les rôles de x et y à $|x| + |y|$.
et deux cas de même signe
♦ $\big||x| + |y|\big|$ est la valeur absolue d'une somme de deux nombres entiers naturels qui est un entier naturel, donc est cette somme $|x| + |y|$, donc on a égalité,
♦ $\big|(-|x|) + (-|y|)\big| = \big|-(|x| + |y|)\big|$ qui est la valeur absolue de l' opposée d'une somme d'entiers naturels donc est cette somme donc est $|x| + |y|$, donc on a encore égalité.
Dans les quatre cas $|x + y| \leqslant |x| + |y|$ ■

111. **La valeur absolue d'un produit ou d'un quotient est égale au produit ou au quotient des valeurs absolues**.

Démonstration. Il faut démontrer que $|x\,y| = |x|\,|y|$ et $\left|\frac{x}{y}\right| = \frac{|x|}{|y|}$.

La règle de signes du tableau 1 donne $|x\,y| = \big|\pm|x| \cdot \pm|y|\big| = \big|$un signe, peu importe lequel $|x|\,|y|\big| = |x|\,|y|$ et du tableau 3 donne $\left|\frac{x}{y}\right| = \left|\frac{\pm\,x}{\pm\,y}\right| = \Big|$un signe, peu importe lequel $\left|\frac{|x|}{|y|}\right| = \frac{|x|}{|y|}$ ■

Nombres rationnels

112. L'idée initiale est que si le quotient ($a \in \mathbb{Z}$) / ($b \in \mathbb{Z}^*$) entre entiers naturels n'est pas un entier naturel, il est un nombre d'une nouvelle espèce, les **nombres rationnels** (a / b est souvent appelé un **rapport**, en latin *ratio*).
113. Une difficulté est que si un entier relatif est le résultat d'une division, il est aussi le résultat d'une infinité d'autres divisions.
114. Dans $\mathbb{Z}$ si les deux divisions exactes a / b et a' / b' donnent le même résultat, une multiplication par $b\ b'$ donne l'*égalité entre le produit des extrêmes et le produit des moyens* $a\ b' = a'\ b$. Inversement, une division exacte de ces deux produits redonne les deux quotients égaux.
115. En particulier, $a \dfrac{b}{\text{P.G.C.D}(|a|\ ,\ |b|)} = \dfrac{a}{\text{P.G.C.D}(|a|\ ,\ |b|)}\ b$ montre l'équivalence entre $\dfrac{a}{b}$ et $\dfrac{a\ /\ \text{P.G.C.D}(|a|\ ,\ |b|)}{b\ /\ \text{P.G.C.D}(|a|\ ,\ |b|)}$.
116. Soit une division de $m \in \mathbb{Z}$ par $n \in \mathbb{Z}^*$. Si ce n'est pas un quotient exact, le résultat est une **nombre fractionnaire**, un couple $\left(\dfrac{m}{\text{P.G.C.D}(|m|\ ,\ |n|)}\ ,\ \dfrac{n}{\text{P.G.C.D}(|m|\ ,\ |n|)}\right)$.

    Note : $\mathbb{Z}^-$* a été défini comme l'ensemble des couples (0 , $n \in \mathbb{N}^*$). La confusion est donc impossible.
117. On écrira $\mathbb{Q}$ la réunion de $\mathbb{Z}$ et des nombres fractionnaires. Les nombres de $\mathbb{Q}$ sont appelés **nombres rationnels**.
118. Le P.G.C.D de 1 et de n'importe quel entier naturel est 1 donc $\left(\dfrac{1}{\text{P.G.C.D}(|1|\ ,\ |n|)}\ ,\ \dfrac{n}{\text{P.G.C.D}(|1|\ ,\ |n|)}\right)$ est (1 , n) et est appelé l'**inverse** de n et est écrit 1 / n ou $\dfrac{1}{n}$. Par convention, l'inverse de 1 / n est n lui-même.
119. Le P.G.C.D de 0 et de n'importe quel entier naturel est cet entier donc $\left(\dfrac{0}{\text{P.G.C.D}(|1|\ ,\ |n|)}\ ,\ \dfrac{n}{\text{P.G.C.D}(|1|\ ,\ |n|)}\right)$ est (0 , n / n = 1), soit le 0 / 1 ou $\dfrac{0}{1}$ de $\mathbb{Q}$, mais aussi le – 1 de $\mathbb{Z}^-$*. Pour éviter la confusion, on exclut m = 0 dans la définition de l'al. 38 des nombres fractionnaires.
120. **L'inverse de l'inverse d'un nombre est ce nombre**.
121. Une **fraction** est un couple ($a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$). On l'écrira $\dfrac{a}{b}$. Elle est dite équivalente à $\dfrac{c}{d}$ si le produit des moyens et celui des extrêmes sont égaux. En particulier, une fraction $\dfrac{p}{q}$ est équivalente au nombre rationnel $\dfrac{p\ /\ \text{P.G.C.D}(|p|\ ,\ |q|)}{p\ /\ \text{P.G.C.D}(|p|\ ,\ |q|)}$.

Opérations sur les nombres rationnels

122. Les opérations addition, soustraction, multiplication et division ont été définies telles que toutes les règles de transformation des formules de calcul soient les mêmes dans $\mathbb{Q}$ et dans $\mathbb{Z}$.
    On a donc extension des lois associativité, commutativité, neutralité du zéro en addition et du 1 en multiplication, distributivité à gauche et à droite de la multiplication par l'addition, donc toutes les règles algébriques qui en sont déductibles. La seule nouveauté est $n \dfrac{1}{n} = 1$.
123. Pour a et b et n entiers relatifs :

    On sait que, en tant qu'inverse de l'inverse $\dfrac{1}{n}$, $\dfrac{n}{1} = n$.

    Multiplications : on multiplie entre eux les numérateurs et les dénominateurs.

    L'hypothèse $q = a\ \dfrac{1}{b}$ donne $q\ b = \left(a\ \dfrac{1}{b}\right) b = a\left(\dfrac{1}{b}\ b\right) = a\ 1 = a$ et la résolution de cette équation d'inconnue q donne $q = \dfrac{a}{b}$ donc $a\ \dfrac{1}{b} = \dfrac{a}{b}$.

    Le calcul $\dfrac{1}{b}\dfrac{1}{d}\ b\ d = \dfrac{1}{b}\ b\ \dfrac{1}{d}\ d = \left(\dfrac{1}{b}\ b\right)\left(\dfrac{1}{d}\ d\right) = 1 \cdot 1 = 1$ et la résolution de cette équation $\dfrac{1}{b}\dfrac{1}{d}\ b\ d = 1$ d'inconnue $\dfrac{1}{b}\dfrac{1}{d}$ donne $\dfrac{1}{b}\dfrac{1}{d} = \dfrac{1}{bd}$.

    Le calcul $\dfrac{a}{b}\dfrac{c}{d} = \left(a\ \dfrac{1}{b}\right)\left(c\ \dfrac{1}{d}\right) = a\ c\ \dfrac{1}{b}\dfrac{1}{d} = a\ c\ \dfrac{1}{b\ d} = \dfrac{a\ c}{b\ d}$ se résume $\dfrac{a}{b}\dfrac{c}{d} = \dfrac{a\ c}{b\ d}$.

124. *Divisions* : on multiplie par la fraction inverse.
Le calcul $\frac{a}{b}\frac{d}{c}\frac{c}{d} = \frac{a}{b}\left(\frac{d}{c}\frac{c}{d}\right) = \frac{a}{b}1 = \frac{a}{b}$ et la résolution de l'équation $\frac{a}{b}\frac{d}{c}\frac{c}{d} = \frac{a}{b}$ d'inconnue $\frac{a}{b}\frac{d}{c}$ donne $\frac{a}{b}\frac{d}{c} = \frac{a}{b} / \frac{c}{d}$.
Note : $\frac{a}{b} = \frac{a}{b}\frac{n}{n} = \frac{a\,n}{b\,n}$ et $\frac{a\,/\,n}{b\,/\,n} = \frac{a\;1\,/\,n}{b\;1\,/\,n} = \frac{a\,/\,n}{b\,/\,n}$, ce qui permet de changer à volonté un dénominateur sans changer le quotient.

125. *Additions*
Le calcul $\frac{a}{n} + \frac{c}{n} = a\frac{1}{n} + b\frac{1}{n} = (a + b)\frac{1}{n} = \frac{a+b}{n}$ résumé $\frac{a}{n} + \frac{c}{n} = \frac{a+b}{n}$ montre que le dénominateur commun est distribué par l'addition.
Le calcul $\frac{a}{b} + \frac{c}{d} = \frac{a\,d}{b\,d} + \frac{c\,b}{d\,b} = \frac{a\,d}{b\,d} + \frac{b\,c}{b\,d} = \frac{a\,d + b\,c}{b\,d}$ résumé $\frac{a}{b} + \frac{c}{d} = \frac{a\,d + b\,c}{b\,d}$ montre la la règle de rédustion au même dénominateur.

126. *Soustractions* : on obtient par analogie aux additions les deux règles précédentes $\frac{a}{b} - \frac{c}{d} = \frac{a\,d - b\,c}{b\,d}$.
Note : le numérateur s'écrit parfois sous forme d'un tableau dit déterminant $\frac{a}{b} - \frac{c}{d} = \frac{\begin{vmatrix} a & c \\ b & d \end{vmatrix}}{b\,d}$.

Signes

127. C'est la règle des signes dans $\mathbb{Z}$ étendue à $\mathbb{Q}$.

Inégalités

128. Par extension de $\mathbb{Z}$ (p. 25) à $\mathbb{Q}$, les se définissent exactement comme les inégalités chez les entiers relatifs. Leurs propriétés s'en déduisent de même.
De nouvelles propriétés apparaissent.

129. Tout rationnel positif est strictement majoré par au moins un entier naturel.
Démonstration. Soit un rationnel $\frac{p}{q} > 0$. Par convention q est un entier naturel autre que zéro.
Si $1 < q$ alors $\frac{p}{q} < \frac{p}{q}\,q$ donc $\frac{p}{q} < q$ et la propriété est démontrée.
Si $q = 1$ alors $\frac{p}{q}$ est p entier naturel strictement majoré par au moins un autre et la propriété est démontrée.
On n'a pas $q < 1$, si non il faudrait que q soit zéro.

130. Tout rationnel positif est strictement majoré par au moins une puissance entière naturelle de 2.
Démonstration. Soit un rationnel $\frac{p}{q} > 0$. Il est strictement majoré par au moins un entier naturel lui-même strictement majoré par au moins une puissance entière naturelle de 2.

Intervalles

Soient $a \in \mathbb{Q}$ et $b \in \mathbb{Q}$ tels que $a \leqslant b$.

131. La phrase "(a donné ($<$ ou $\leqslant$) x ($<$ ou $\leqslant$) (b donné)" définit un ensemble nommé **intervalle** entre a et b qui en sont les **extrémités**.
132. La différence $b - a$ est la **longueur** d'un l'intervalle entre a et b.
Si sa longueur est non nulle, les extrémités sont distinctes et vice-versa.
133. Le **milieu** d'un intervalle entre a et b est un rationnel m tel que $b - m = m - a$. Il est situé à mi-distance des extrémités. La résolution de l'équation d'inconnue m donne $m = \frac{a+b}{2}$.

Définition	Adjectif	écriture
$a < x < b$	ouvert	$]a\ ,\ b[$
$a < x \leqslant b$	semi ouvert	$]a\ ,\ b]$
$a \leqslant x \leqslant b$	fermé	$[a\ ,\ b]$
$a \leqslant x < b$	semi ouvert	$[a\ ,\ b[$

134. L'**ouverture** ou la **fermeture** d'un intervalle est défini et écrit selon le tableau ci-dessus. On passe de l'un à l'autre en ajoutant ou retirant une des extrémités ou les deux.
135. **L'intersection de deux intervalles est un intervalle**.
Démonstration. Il faut faire l'inventaire des comparaisons des positions des quatre extrémités données de deux intervalles ouverrts $]a\ ,\ b[$ et $]u\ ,\ v[$ puis passer aux semi ouverts ou fermés en ajoutant ou retirant une des extrémités ou les deux.

♦ Si x est commun aux deux intervalles, alors $a < x < b$ et $u < x < v$ donc (a et u) $< x <$ (b et v).
On a $]a , b[\cap]u , v[\subset]\max(a \text{ et } u) , \min(b , v)[$.
♦ Inversement, il est immédiat que
$x \in]\max(a \text{ et } u) , \min(b , v)[\Rightarrow (a \text{ et } u) < x < (b \text{ et } v) \Rightarrow a < x < b$ et $u < x < v \Rightarrow x \in]a , b[$ et $]u , v[$ ■

136. **Entre deux rationnels donnés il y en a au moins un troisième, situé au milieu**.
Démonstration.
♦ On a $a < b \Rightarrow$ par addition du même nombre aux deux membres de l'inégalité, $a + a < a + b$ et $a + b < b + b$ donc $< 2\,a < a + b < 2\,b$ donc par division par 2 des deux membres de l'inégalité, $a < \frac{a+b}{2} <$ b donc $\frac{a+b}{2}$ appartient à $]a , b[$.
♦ Les calculs $\frac{a+b}{2} - a = \frac{a+b}{2} - \frac{2\,a}{2} = \frac{a+b-2\,a}{2} = \frac{b-a}{2}$ et $b - \frac{b-a}{2} = \frac{2\,b}{2} - \frac{b-a}{2} = \frac{2\,b-b+a}{2} = \frac{a+b}{2}$ montrent que $\frac{a+b}{2}$ est au milieu de $]a , b[$ ■

137. Une suite d'intervalles emboîtés est un ensemble de couples ($i \in \mathbb{N}$, un intervalle I_i défini par b_i et $a_i < b_i$) tel que $\forall i$ on ait $I_i \subset I_{i+1}$. Ces intervalles peuvent être ouverts, semi-ouverts ou fermés.

138. Dans des démonstrations mathématiques, on se sert souvent des suivants I_{i+1} définis à partir des précédents par a_i et $\frac{a_i + b_i}{2}$ ou par $\frac{a_i + b_i}{2}$ et b_i.

Un autre cas est l'usage des intervalles I_i définis par soit a_i et $a_i + \frac{1}{i}$ ou $b_i - \frac{1}{i}$ et b_i.

Dans les deux cas la raison est que quelque soit le rationnel $\varepsilon > 0$ dans $\mathbb{N}$ il existe k dont la valeur dépend de ε et tel que la longueur de tous les $I_{i \geqslant k}$ est moindre que ε (on dit que les longueurs sont aussi petites qu'on veut). Ces longueurs sont $1/2^i$ dans le premier exemple et $1/i$ dans le deuxième.
Une autre raison est la propriété suivante.

139. **Deux rationnels communs à des intervalles de toute taille non nulle sont confondus**.
Démonstration. Soit "$x \in \mathbb{Q}$ et $y \in \mathbb{Q}$ communs à tous les intervalles I_i d'une suite d'intervalles emboîtés d'extrémités b_i et $a_i < b_i$ dont les longueurs $b_i - a_i$ sont aussi petites qu'on veut. Par ubiquité on peut raisonner sur le cas $x < y$. Alors $\varepsilon = y - x > 0$. On a donc pour tout i de $\mathbb{N}$, $a_i < x < y < b_i$ c'est-à-dire $b_i - a_i = (b_i - y) + (y - x) + (x - a_i)$ qui est strictement plus grand que $y - x = \varepsilon$, ce qui est une contradiction ■

Rationnels et entiers relatifs

140. **Soit une fraction de numérateur et dénominateur strictement positifs.**
♦ Inverser la fraction inverse sa comparaison du rationnel avec l'unité.
♦ Si le numérateur est strictement plus petit que le dénominateur, le rationnel est dans l'intervalle ouvert]0 , 1[.
♦ Si son numérateur est strictement plus grand que le dénominateur, la rationnel est strictement plus grand que 1.
Démonstration.
♦ On a $0 < a < b \Rightarrow$ en divisant par a ou en divisant par b les trois membres on obtient $0 < 1 < \frac{b}{a}$, $0 < \frac{a}{b} < 1$ donc $0 < \frac{a}{b} < 1 < \frac{b}{a}$ ■

141. **Soit une fraction de numérateur et dénominateur strictement positifs.**
♦ Si le rationnel est dans l'intervalle]0 , 1[**alors la suite de ses puissances est strictement décroissante tout en restent dans cet intervalle**.
♦ Si le rationnel est strictement plus grand que 1 **alors la suite de ses puissances est strictement croissante et n'est pas majorée** (on dit qu'elle **tend vers + l'infini** ou $+\infty$).
***Démonstration*.**
Soit un rationnel q de l'intervalle]0 , 1[. Alors $0 < q < 1$.
♦ Par multiplication membre à membre des inégalités $0 < q^2 < 1$, puis $0 < q^3 < 1$, et ainsi de suite, en général $0 < q^n < 1$.
D'autre part, multiplier les trois membres de $0 < q < 1$ par q donne $0 < q^2 < q$ soit $0 < q^{1+1} < q^1$ généralisable par récurrence $0 < q^{n+1} < q^n$. On récapitule : quelque soit n de $\mathbb{N}$ on a $0 < q^{n+1} < q^n < 1$.
♦ De même, en multipliant les deux membres de $0 < 1 < q$ par q, il vient successivement $0 < q < q^2$, puis $q^2 < q^3$ et ainsi de suite, généralisable par récurrence en $0 < q^n < q^{n+1}$. Par transitivité, quelque soit n de $\mathbb{N}$, $0 < 1 < a^n < a^{n+1}$ ■

142. ♦ **Tout nombre rationnel positif est soit un entier naturel soit appartient à un intervalle ouvert défini par deux entiers naturels.**
♦ T**out entier naturel appartient à un intervalle ouvert défini par deux rationnels.**
♦ Autrement dit, **les ensembles $\mathbb{Z}$ et $\mathbb{Q} \setminus \mathbb{Z}$ sont enchevêtrés**.
Démonstration.

♦ Un rationnel x s'écrit $\frac{p}{q}$ avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$. Supposons $p \in \mathbb{Q}^+$. Par ubiquité on a trois cas :

$0 < p < q$ donne en divisant par q, $0 < \frac{p}{q} < 1$ donc le rationnel $\frac{p}{q}$ est dans l'intervalle $]0 , 1[\cap \mathbb{N}$.

$0 < p = q \Rightarrow \frac{p}{q}$ est l'entier naturel 1.

$0 < q < p \Rightarrow$ en divisant par q, $0 < 1 < \frac{p}{q}$.

Comme q est entier naturel non nul,

soit $q = 1$ et alors $\frac{p}{q}$ est l'entier naturel p

soit $1 < q$ et alors en multipliant les deux membres par le rationnel $\frac{p}{q}$ on trouve $\frac{p}{q} < p$ donc le rationnel $\frac{p}{q}$ est dans l'intervalle $]1 , p[\cap \mathbb{N}$.

♦ Tout entier naturel n est un rationnel $\frac{p}{q}$ avec $q \in \mathbb{N}^*$ donc $0 < \frac{1}{q}$ donc $-\frac{1}{q} < 0$ donc par addition de n aux deux membres $n - \frac{1}{q} < n$ et $n < n + \frac{1}{q}$ donc n est dans l'intervalle $]n - 1/q , n + 1/q[$ ■

143. Les bijections que sont les ensembles des couples ($m \in \mathbb{N}$, $q_m \in \mathbb{Q}$) sont des suites dont le rôle sera très important dans le conceptualisation mathématique de la physique quantique.

Bornes & intervalles chez les rationnels

144. Soient a et b deux rationnels tels que $a \leqslant b$. Les **intervalles** qu'ils définissent sont dans le tableau 1.
Soit r un rationnel. Les **intervalles infinis** qu'il définit sont dans le tableau 2.
Les intervalles semi ouverts S_r sont aussi des **sections inférieures strictes**.

Symbole	Définition	Note
$[r , +\infty[$	Ensemble des x tels que $r \leqslant x$	
$]r , +\infty[$	Ensemble des x tels que $r < x$	
$]-\infty , r]$	Ensemble des x tels que $x \leqslant r$	
$]-\infty, r[$	Ensemble des x tels que $x < r$	S'écrit aussi S_r

Tab. 1 Intervalles infinis

145. **On a l'équivalence logique** $r < r' \Leftrightarrow S_r$ ($\subset$ et $\neq$) $S_{r'}$.
Démonstration. C'est la définition même de S_r.

146. **Bornes**. Soit E un ensemble de rationnels. Une borne supérieure de E est si il existe le plus petit de ses majorants et une borne supérieure de E est si il existe le plus grand de ses minorants.

147. Soit b une borne supérieure de E. Alors (tout q de E) $\leqslant b$.

148. Soit $r < b$. Si (tout q de E) $\leqslant r$ alors r majorerait E donc on aurait $b \leqslant r$ (contradiction). On a donc $r <$ (au moins un q de E).

Symbole	Définition	Note
$[0 , +\infty[$	Ensemble des x tels que $r \leqslant x$	C'est $\mathbb{Q}^+$
$]0 , +\infty[$	Ensemble des x tels que $r < x$	C'est $\mathbb{Q}^{+*}$
$]-\infty , 0]$	Ensemble des x tels que $x \leqslant r$	C'est $\mathbb{Q}^-$
$]-\infty, 0[$	Ensemble des x tels que $x < r$	C'est $\mathbb{Q}^{-*}$
$]-\infty , +\infty[$	Ensemble des rationnels	C'est $\mathbb{Q}$

Tab. 2 Intervalles infinis particuliers

Symbole	Borne inférieure	Borne supérieure
$[a , b]$	n'existe pas	n'existe pas
$[a , b[$	n'existe pas	b
$]a , b]$	a	n'existe pas
$]a , b[$	a	b
$[r , +\infty[$	n'existe pas	n'existe pas
$]r , +\infty[$	r	n'existe pas
$]-\infty , r]$	n'existe pas	n'existe pas
$]-\infty, r[$	n'existe pas	r

Tab. 4 Intervalles bornés

Les rationnels sont dénombrables.

149. Soit E_n l'ensemble des fractions a / b où $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ telles que $|a| + b \leqslant n$. Alors séparément $|a| \leqslant n$ et $b \leqslant n$. En langage ensembliste, $|a| \in n \cup \{n\}$, donc $+a \in n \cup \{n\}$ et $-a \in n \cup \{n\}$, et $b \in n \cup \{n\}$, le cardinal de l'ensemble étant $n + 1$. L'ensemble E_n^+ des $+a$, celui E_n^- des $-a$ et celui $E_n^{\Diamond}$ des b ont chacun $n + 1$ éléments. L'ensemble des a est $E_n^+ \cup E_n^-$ donc l'ensemble des couples (a , b) est $(E_n^+ \cup E_n^-) \times E_n^{\Diamond}$.
Son cardinal est
card $(E_n^+ \cup E_n^-) \times$ card $E_n^{\Diamond}$ = (card E_n^+ + card E_n^- – card $(E_n^+ \cap E_n^-)$) $\times$ card $E_n^{\Diamond}$ donc E_n est fini et, sachant que $E_n^+ \cap E_n^- = \{0\}$, de cardinal $\big((n + 1) + (n + 1) - 1\big)\,(n + 1) = (2\,n + 1)\,(n + 1) = 2\,n^2 + 3\,n + 1$.
Mais le nombre m de rationnels définis, nommons R_n le cardinal de leur ensemble nommé F_n, à cause de la question des fractions équivalentes, est nettement inférieur à $2\,n^2 + 3\,n + 1$. Si, une fois numérotés les rationnels de F_n ceux de $F_{n+1} \setminus F_n$ peuvent à leur tour être numérotés ■

Nombres réels

Aucun carré de rationnel n'est égal à deux

150. Les mathématiciens de la Grèce antique ont découvert et démontré l'irrationalité de $\sqrt{2}$ à une époque qu'il est difficile de déterminer, au plus tard dans les premières décennies du IVe siècle av. J.-C., et vraisemblablement pas avant le Ve siècle av. J.-C. Ils montrèrent que les longueurs des côtés et celle de l'hypoténuse sont *incommensurables*, c'est-à-dire que l'on ne peut trouver de segment unité, aussi petit soit-il avec lequel on puisse mesurer de façon exacte ces deux longueurs (voir https://fr.wikipedia.org/wiki/Racine_carr%C3%A9e_de_deux#La_p%C3%A9riode_pal%C3%A9o-babylonienne).

151. Pourtant, pour satisfaire les géomètres, il a fallu admettre que ces longueurs irrationnelles existent tout comme les nombres rationnels, et c'est pourquoi on les appelle **nombres réels**.

152. Soient deux carpettes A et B, A et B les surfaces qu'elles peuvent recouvrir et S la surface du sol d'une salle. Les carpettes se recouvrent partiellement sur une surface $A \cap B$ et une partie du sol $S \setminus (A \cup B)$ n'est pas couverte. L'aire du sol est aire S = aire A + aire B – aire $(A \cap B)$ + aire $(S \setminus (A \cup B))$.
Si autant de surface du sol est couverte deux fois que découverte, aire $(A \cap B)$ = aire $(S \setminus (A \cup B))$ et alors aire S = aire A + aire B donc les carpettes recouvrent exactement le sol.
Réciproquement si les carpettes recouvrent exactement le sol, aire S = aire A + aire B alors l'équation aire A + aire B = aire A + aire B – aire $(A \cap B)$ + aire $(S \setminus (A \cup B))$ montre que la différence – aire $(A \cap B)$ + aire $(S \setminus (A \cup B))$ est nulle donc autant de surface du sol est couverte deux fois que découverte.
Appelons cette propriété le **théorème des carpettes**.

153. Exemple (fig. 1) : démonstration qu'aucun rationnel a 2 comme carré.
Les carpettes sont AHC'I et A'H'CI', le sol est ABCD et a et b sont multiples entiers naturels de l'unité de longueur.
♦a On a $b < a$. On a $a / 2 < b$.
♦b Aire recouverte = aire A'B'C'D' = $(2\,b - a)^2$.
♦c Aire non couverte = aire HBH'B' + aire ID'I'D = $2\,(a - b)^2$.
♦d La condition du théorème des carpettes, si elle est possible, est $b^2 + b^2 = a^2$. Appelons $\sqrt{2}$ un nombre dont le carré est 2. Alors $\sqrt{2}\,b = a$.
♦e La condition ♦d donne $(2\,b - a)^2 = 2\,(a - b)^2$. Alors $2\,b - a = \sqrt{2}\,(a - b)$. Le développement donne $2\,b + \sqrt{2}\,b = a + \sqrt{2}\,a \Rightarrow (2 + \sqrt{2})\,b = (2 + \sqrt{2}) \Rightarrow a = b$, en contradiction avec le point ♦d.
Sources :
http://images.math.cnrs.fr/Racines-carrees-et-nombres-rationnels.html
Au fil des maths, bulletin de l'A.P.M.E.P, ed. janvier à mars 2021

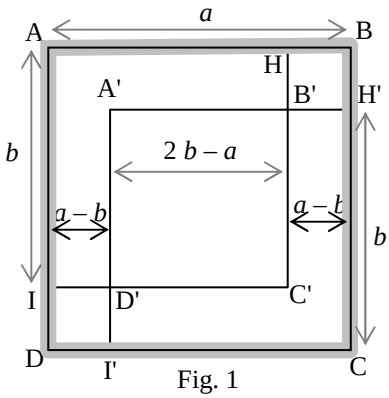


Fig. 1

Coupures de rationnels

154. On appelle **coupure** ou **section** de $\mathbb{Q}$ un ensembles S de rationnels tel que (fig. 2) :
a♦ S n'est pas vide,
b♦ $S \neq \mathbb{Q}$,
c♦ tout rationnel plus petit qu'un rationnel de S est dans S,
d♦ S n'a pas de plus grand élément.
Par convention, les rationnels sont écrits en lettres minuscule et les coupures en majuscule.

Fig. 2

155. **Si la coupure S a une borne supérieure r, alors S est confondu avec la section inférieure stricte S_r. Une telle coupure est dite rationnelle**.
Démonstration.
Par définition d'une borne supérieure, (tout q de S) $< r$. On a donc $S \subset S_r$.
Soit q de S_r. Alors $q < r$. Par définition de la borne, (au moins un q' de S) (non $\leqslant$) q donc $q <$ (ce q' de S) donc $q \in S$. On a donc $S_r \subset S$ donc $S_r = S$ ■

156. La **distance** entre S_p et $S_{q>p}$ est par définition $q - p$. La **somme** $S_p + S_q$ est $p + q$. Le **produit** $S_p\,S_q$ est S_{pq}. Le **quotient** S_p / S_q est $S_{p/q}$. On en déduit que l'**opposé** de S_p est S_{-p} et l'**inverse** de S_q est $S_{1/q}$.

157. **Tout rationnel hors d'une coupure la majore strictement**.
Si q était hors de la coupure S et plus petit qu'un de ses éléments on aurait une contradiction. Tout rationnel q hors de S la majore donc strictement ■

158. **Tout élément d'une coupure est strictement plus petit qu'au moins un autre**.

Démonstration. Soit q d'une coupure S. Si il n'existait pas de rationnel strictement plus grand que q alors tous les nombres de la coupure seraient plus petit que q qui en serait le plus grand (contradiction) ■

159. **Une coupure est la réunion des coupures rationnelles qu'elle contient**.
Démonstration. Soit une coupure S.
D'une part on a $q \in$ (réunion des $S_{r \text{ de } S}$) $\Rightarrow q \in$ (au moins un $S_{r \text{ de } S}$) $\Rightarrow q <$ (r de S) $\Rightarrow q \in S$, et
d'autre part $q \in S \Rightarrow q <$ (au moins un r de S) $\Rightarrow q \in S_{\text{ce } r \text{ de } S} \Rightarrow q \in$ (réunion des $S_{r \text{ de } S}$) ■

160. **L'inclusion stricte est un ordre total strict chez les coupures**.
Démonstration
♦ On connaît les propriétés de *réflexivité*, d'*antisymétrie* et de *transitivité* de l'inclusion.
♦ Soient S et T deux coupures distinctes. Alors un rationnel est dans l'une et pas dans l'autre.
Par exemple soit T non incluse dans S, ce qui exclut l'égalité $S = T$: alors il existe au moins un t de T hors de S.
Alors t majore S (al. 10) donc (tout s de S) $\in$ (t de T) donc par définition de la coupure T, (tout s de S) $\in T$ donc $S \subset T$ donc S ($\subset$ et $\neq$) T.
Un raisonnement analogue montre que si un rationnel est dans S et hors de T, T ($\subset$ et $\neq$) S ■

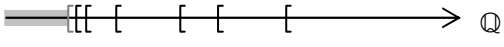
161. **Au sens de l'inclusion, entre deux coupures il en existe toujours une troisième qui leur est distincte et qui soit rationnelle**.
Démonstration. Soit les coupures S et T telles que S ($\subset$ et $\neq$) T, ce qui veut dire qu'il existe un rationnel t de T hors de S donc majorant strictement S. Alors (tous les s de S) < (r hors de S et dans T).
Comme T n'a pas de plus grand élément,
(tous les s de S) < (r hors de S et dans T) < (au moins un t de T),
donc parce qu'entre deux rationnels il en existe un troisième qui leur est distinct,
(tous les s de S) < (r hors de S et dans T) < (au moins un u) < (au moins un t de T) et
(tous les s de S) < (r hors de S et dans T) < (au moins un v) < (au moins un u) < (au moins un t de T) donc par définition des coupures
(tous les s de S) < (r hors de S et dans T) < (au moins un v de T) < (au moins un u de T) < (au moins un t de T).
Nommons S_u l'ensemble des rationnels srictement plus petits que u et S_v l'ensemble des rationnels strictement plus petits que v. On a (al. et 7) $S \subset S_r \subset S_v \subset S_u \subset T$.
Si v était dans S alors r serait dans S (contradiction).
Si S_v était confondu à T alors on aurait par transitivité S_u ($\subset$ et $\neq$) S_v (contradiction).
On a donc bien S ($\subset$ et $\neq$) $\subset S_v$ ($\subset$ et $\neq$) T ■

Théorème fondamental

162. **Tout ensemble non vide et majoré de coupures** (fig. 3, crochets en noir) **en admet une comme borne supérieure** (en gris).

Fig. 3 

Démonstration. Dans la démonstration qui suit, les ensembles de coupures seront écrites soulignées.
Soit donc $\underline{E}$ un ensemble de coupures.
♦a Si une coupure majorante M de $\underline{E}$ est dans $\underline{E}$, alors (toute classe de $\underline{E}$, y compris M) $\subset M$ donc si T majore $\underline{E}$ alors $M \subset T$ donc M est borne supérieure de $\underline{E}$ et la démonstration est faite.
♦b Ce qu'il faut prouver : si (tout coupures de $\underline{E}$) ($\subset$ et $\neq$) (une coupures donnée) alors il existe une coupures B tel que 1° (toutes les coupures de $\underline{E}$) $\subset B$ parce que B doit majorer $\underline{E}$, et 2° si (toutes les coupures de $\underline{E}$) $\subset C$ alors $B \subset C$ parce que B doit être la plus petite coupures majorant $\underline{E}$.
♦c Nommons B la réunion des coupures de $\underline{E}$.
♦d Aucune des coupures de $\underline{E}$ n'étant vide, B n'est pas vide.
♦e Soit q un rationnel de B. Alors q est dans une des coupures S de $\underline{E}$. Si $q' \leqslant q$, q' est dans cette coupure , donc dans B.
♦f Il est évident que B majore $\underline{E}$.
♦ Soit une coupure T majorant $\underline{E}$. (Tous les q des coupures de $\underline{E}$) $\in T$ donc (tous les q de la réunion des S de $\underline{E}$) $\in T$ donc $B \subset T$. B est bien la plus petite coupure majorant $\underline{E}$ ■

Fig. 4 

163. **Tout ensemble non vide et minoré de coupures en admet une comme borne inférieure** (fig. 4).
Démonstration. Soit $\underline{E}$ un ensemble non vide de coupures.
♦a Soit $\underline{F}$ l'ensemble des classes minorantes de $\underline{E}$: $S \in \underline{F} \Leftrightarrow S \subset$ (toutes les T de $\underline{E}$).
♦b Alors $\underline{F}$ est majorée par les classes de $\underline{E}$ donc à une borne supérieure B qui est la plus petite classe majorante de $\underline{F}$. On a donc (S majore $\underline{F}$) $\Rightarrow B \subset S$.
♦c Montrer que B est aussi borne inférieure de $\underline{E}$ consiste à prouver que B est la plus grand minorante de $\underline{E}$, donc que $B \in \underline{F}$ et que $S \in \underline{F} \Rightarrow S \subset B$.
♦d Comme B majore $\underline{F}$ la deuxième condition est réalisée.

♦e Si B était hors de $\underline{F}$ alors B ne minorerait pas $\underline{E}$ donc B (non $\subset$) (toutes les coupures de $\underline{E}$) donc (une coupure X de $\underline{E}$) ($\subset$ et $\neq$) B donc B ne minorerait pas $\underline{E}$ (contradiction). On a bien $B \in \underline{F}$ ■

Inégalités et intervalles

On sait que $q < q' \Leftrightarrow S_q$ ($\subset$ et $\neq$) $S_{q'}$ ce qui permet d'uniformiser l'écriture des inégalités. Ainsi : soient C et C' deux coupures : par définition, $C < C' \Leftrightarrow C$ ($\subset$ et $\neq$) C'. La définition des intervalles passe telle qu'elle chez les coupures.

Tête de coupure

164. La borne q de S_q est dans une infinité d'intervalles ouverts "à cheval" sur S_q et sur son complémantaire $\mathbb{Q}\backslash S_q$ dont les longueurs sont aussi petites qu'on veut. Généralisons.
Soit (fig. 7 en gris foncé) une coupure X. Montrons que quelque soit l'intervalle ouvert $]a\ ,\ b[$ (en gris clair) "à cheval" sur X et sur $\mathbb{Q}\backslash X$ il en existe au moins un autre $]a'\ ,\ b'[$ strictement inclus dans $]a\ ,\ b[$.

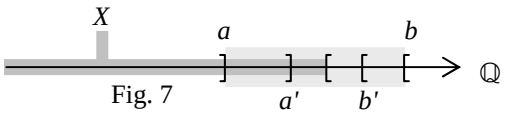


Fig. 7

Preuve. Parce que l'intervalle $]a\ ,\ b[$ est "à cheval", il existe un a' dans $]a\ ,\ b[\cap X$ et un b' dans $]a\ ,\ b[\cap (\mathbb{Q}\backslash X)$. Comme tout rationnel d'une coupure est strictement plus petit qu'un autre de son ensemble complémentaire, on a toujours $a' < b'$ donc on a bien $a < a' < b' < b$ donc S_a ($\subset$ et $\neq$) $S_{a'} \subset X \subset S_{b'}$ ($\subset$ et $\neq$) S_b □

165. **Intervalles chez les coupures** : la définition est la même que chez les rationnels (p. 31) à condition de remplacer les symboles $\leqslant$ et $<$ par respectivement $\subset$ et ($\subset$ et $\neq$). Ensuite, par commodité, chez les coupures on remettra les symboles inégalitaires.
En conséquence, chez les coupures, on peut dire que quelque soit l'intervalle $]S_a\ ,\ S_b[$ contenant X, il existe un autre $]S_{a'}\ ,\ S_{b'}[$ inclus dans $]S_a\ ,\ S_b[$.

166. Appelons **tête de la coupure** X l'ensemble des intervalles $]a\ ,\ b[$ "à cheval" sur X et sur $\mathbb{Q}\backslash X$ et étendons ce vocabulaire aux intervalles correspondants $]S_a\ ,\ S_b[$.
On a donc (tous les a) < (tous les b) et (tous les $S_{a \in X}$) < (une coupure unique qui est X) <(tous les $S_{b \notin X}$).

167. Réciproquement, **un ensemble d'intervalles ouverts de rationnels dont toutes les bornes inférieures sont plus petites que toutes les bornes supérieures et dont la longueur est aussi petite qu'on veut est la tête d'une coupure unique**.
La double inégalité chez les rationnels donne $b' - a' < b - a$ ce qui prouve que dans $\mathbb{Q}$ la distance entre les bornes inférieures et supérieures des intervalles de la tête de X est nulle. Par extension de langage, $b - a$ sera aussi la longueur de l'intervalle $]S_a\ ,\ S_b[$.
Soit Y une autre coupure contenue dans tous les intervalles de la tête de X. Supposons Y distinct de X. Par ubiquité, raisonnons par exemple dans le cas $X < Y$. Le théorème fondamental dit qu'il existe une coupure rationnelle S_m tel que $X < S_m < Y$. Alors quel que soit l'intervalle $]S_a\ ,\ S_b[$ de la tête de X on aurait $S_a < X < S_m < Y < S_b$ donc $]S_a\ ,\ S_m[$ et $]S_m\ ,\ S_b[$ seraient "à cheval" et plus courts que $]S_a\ ,\ S_b[$ et ne contenant pas Y (contradiction).

Opérations sur les coupures

168. **Usage des têtes de coupure pour définir les opérations analogues à celles chez les rationnels** : soit * l'une d'elles : c'est un ensemble de couples de rationnels dans lequel chaque antécédent $(q\ ,\ q')$ n'a qu'une image qui s'écrit $q * q'$. Soient alors X et X' deux coupures.
Nommons respectivement $]a\ ,\ b[$ et $]a'\ ,\ b'[$ les intervalles de leurs têtes respectives. Il faut examiner trois critères.
Premier critère : pour $]a\ ,\ b[$ et $]a'\ ,\ b'[$ donnés l'ensemble des $(x \in\ ]a\ ,\ b[) * (x' \in\ ]a'\ ,\ b'[)$ est toujours un intervalle $]r\ ,\ s[$.
Deuxième critère : (tous les r) < (tous les s).
Troisième critère : la longueur $s - r$ des $[r\ ,\ s]$ soit aussi petite qu'on veut.

169. Alors une coupure R unique est commune à tous les $]S_r\ ,\ S_s[$. Cette coupure sera considérée comme le résultat de l'opération $X * X'$.

Addition

Premier critère. $a < x < b$ et $a' < x' < b' \Rightarrow a + a' < x + x' < b + b'$ montre que pour $]a\ ,\ b[$ et $]a'\ ,\ b'[$ donnés l'ensemble des $(x \in\ ]a\ ,\ b[) + (x' \in\ ]a'\ ,\ b'[)$ est toujours un intervalle $]a + a'\ ,\ b + b'[$.
Deuxième critère. Parce que (tous les a) < (tous les b) et (tous les a') < (tous les b') on a (tous les $a + a'$) < (tous les $b + b'$).
Troisième critère. La longueur des $]a + a'\ ,\ b + b'[$ est $(b - a) + (b' - a')$ aussi petite qu'on veut.
L'unique coupure S commune à tous les $]S_{a+a'}\ ,\ S_{b+b'}[$ sera la somme $X + X'$.

Soustraction

170. *Premier critère.* $a < x < b$ et $a' < x' < b' \Rightarrow -b' < x' < -a' \Rightarrow a - b' < x - x' < b - a'$ montre que pour $]a\ ,\ b[$ et $]a'\ ,\ b'[$ donnés l'ensemble des $(x \in\ ]a\ ,\ b[) - (x' \in\ ]a'\ ,\ b'[)$ est toujours un intervalle $]a - b'\ ,\ b - a'[$.
Deuxième critère.
Parce que (tous les a) < (tous les b) et (tous les a') < (tous les b') $\Rightarrow$ (tous les $a - b'$) < (tous les $b - a'$).
Troisième critère. La longueur des $]a - b'\ ,\ b - a'[$ est $(b - a') - (a - b') = (b - a) + (b' - a')$ aussi petite qu'on veut.
L'unique coupure D commune à tous les $]S_{a-b'}\ ,\ S_{b-a}[$ sera la différence $X - X'$.

Multiplication

171. La **règle des signes** de cette opération dans $\mathbb{Q}$ complique la situation, parce qu'on procède par multiplication des membres des inégalités par un même nombre, parce que si ce nombre est positif les inégalités sont invariantes alors que si ce nombre est négatif les inégalités se retournent (p. 29 et 25).
Premier critère. Dans les démonstrations qui suivent, les couleurs de surlignage ou celle des caractères indiquent les applications de la transitivité, les conclusions sont surlignées en gris et les chiffres en exposant numérotent les inégalités.
Soient $x \in\ ]a\ ,\ b[$ et $x' \in\ ]a'\ ,\ b'[$. Selon que zéro appartienne ou non aux intervalles, deux groupes de cas sont à envisager.

Premier groupe :

172. C'est le cas où aucun intervalle de tête de X et de X' ne contient zéro.
Zéro est hors de tous les intervalles qui y sont inclus. Ni X ni X' n'est S_0.
Hypothèse : $]a\ ,\ b[\subset \mathbb{Q}^+$ et $]a'\ ,\ b'[\subset \mathbb{Q}^+$. Les numéros des formules suivantes servent à choisir l'application de la transitivité.
(1ere ligne) $a < x < b$ [1] $\quad a\,a' < x\,a' < b\,a'$ [2] $\quad a\,x' < x\,x' < b\,x'$ [3] $\quad a\,b' < x\,b' < b\,b'$ [4]
(2e ligne) $a' < x' < b'$ [5] $\quad a'\,a < a\,x' < b'\,a$ [6] $\quad a'\,x < x\,x' < b'\,x$ [7] $\quad a'\,b < b\,x' < b'\,b$ [8]
donnent par transitivité
[2] et [7] $\Rightarrow a\,a' < x\,x'$ $\quad$ [3] et [8] $\Rightarrow x\,x' < b\,b'$ $\quad$ donc $\quad a\,a' < x\,x' < b\,b'$.
$a\,a'$ est dans le rôle de r et $b\,b'$ est dans celui de s.
Hypothèse : $]a\ ,\ b[\subset \mathbb{Q}^+$ et $]a'\ ,\ b'[\subset \mathbb{Q}^-$.
Par rapport à la première hypothèse les inégalités de la première ligne se retournent donc $b\,a' < x\,x' < a\,b'$.
La distance entre les bornes est $a\,b' - a'\,b = a\,(b' - a') - (a' - b')\,b - (b\,b' - a\,a')$.
$a\,b'$ est dans le rôle de r et $a'\,b$ est dans celui de s.
Hypothèse : $]a\ ,\ b[\subset \mathbb{Q}^-$ et $]a'\ ,\ b'[\subset \mathbb{Q}^+$.
Par rapport à la première hypothèse les inégalités de la deuxième ligne se retournent donc $a\,b' < x\,x' < b\,a'$.
La distance entre les bornes est encore $a\,(b' - a') - (a' - b')\,b - (b\,b' - a\,a')$.
$a\,b'$ est dans le rôle de r et $b\,a'$ est dans celui de s.
Hypothèse : $]a\ ,\ b[\subset \mathbb{Q}^-$ et $]a'\ ,\ b'[\subset \mathbb{Q}^-$.
Par rapport à la première hypothèse les inégalités des deux lignes se retournent donc $b\,b' < x\,x' < a\,a'$.
La distance entre les bornes est $(a\,a' - b\,b')$. $b\,b'$ est dans le rôle de r et $a\,a'$ est dans celui de s.

Deuxième groupe :

173. ***Hypothèse*** : tous les intervalles de tête de X ou tous ceux de X' contiennent le rationnel zéro.
Note : X ou X' est donc S_0.
L'ensemble des $(x \in\ ]a\ ,\ b[) \times (x' \in\ ]a'\ ,\ b'[)$ contient zéro, parce que par exemple, (0 de $]a\ ,\ b[$) $\times$ (x' de $]a'\ ,\ b'[$) est zéro.
Les inégalités $a < 0 < b$ et $a' < x' < b'$ donnent, vu que a est négatif, $b\,a' < 0 < a\,a'$. La longueur de $]b\,a'\ ,\ a\,a'[$ est $(a - b)\,a'$. $b\,a'$ est dans le rôle de r et $a\,a'$ est dans celui de s.
Un raisonnement analogue donne $a < x < b$ et $a' < 0 < b'$ donne $b'\,a < 0 < a'\,a$ et la longueur $(a' - b')\,a$. $b'\,a$ est dans le rôle de r et $a'\,a$ est dans celui de s.
La coupure commune à tous les $]S_r\ ,\ S_s[$ est donc S_0.
Deuxième critère. il est satisfait dans chacun des cinq cas. Par exemple, dans le deuxième cas si $]a_1\ ,\ b_1[$ est inclus dans $]a_2\ ,\ b_2[$ avec x commun et $]a'_1\ ,\ b'_1[$ est inclus dans $]a'_2\ ,\ b'_2[$ avec x' commun alors à la fois $b_1\,a'_1 < x\,x' < a_1\,b'_1$ et $b_2\,a'_2 < x\,x' < a_2\,b'_2$ donc ($b_1\,a'_1$ et $b_2\,a'_2$) < ($a_1\,b'_1$ et $a_2\,b'_2$).
Troisième critère. Dans les deux groupes de cas, $x\,x'$ appartient à un intervalle ouvert aussi court qu'on veut.

Dans tous les cas, l'unique coupure commune à tous les intervalles ext considérée comme le résultat de la multiplication de X par X'.

Division

174. On procède comme avec la multiplication, sauf que toutes les inégalités sont retournées et que le deuxième groupe est exclu.

175. **Propriétés algébriques des opérations** : toutes celles dans $\mathbb{Q}$ sont transmissibles immédiatement aux coupures. Exemple : dans $\mathbb{Q}$ la multiplication est commutative. En conséquence, les $x\,x'$ et les $x'\,x$ forment les mêmes ensembles, en particulier les coupures, donc $X\,X' = X'\,X$.
Il en résulte qu'aucun calcul numérique n'est faisable directement sur les coupures, mais seulement avec les rationnels définissant les sections aussi proches qu'on veut d'elles.

Numération des coupures

176. Les divisions euclidiennes entre rationnels donnent toutes des quotients dont les décimales sont périodiques à partir d'un certain rang. Si on cherche à écrire une coupure avec les mêmes chiffres que les rationnels, deux cas se présentent :
- soit la coupure est une section définie par un rationnel, alors on l'écrit avec les chiffres de sa borne supérieure rationnelle,
- soit la coupure est irrationnelle et alors dans son écriture chiffrée les décimales ne sont jamais périodiques.

177. **Signe**. Soit une coupure X. Son signe strict est défini selon le tableau ci-contre.

X strictement positive	S_0 ($\subset$ et $\neq$) X
X nulle	$X = S_0$
X strictement négative	X ($\subset$ et $\neq$) S_0

Tableau 5 : signe d'une coupure

Ensemble $\mathbb{R}$ des nombres réels

178. **Agrandissement de $\mathbb{Q}$**
L'ensemble $\mathbb{R}$ des nombres réels est la réunion de $\mathbb{Q}$ et de l'ensemble $\mathbb{R}^{irr}$ des coupures irrationnelles.
Les opérations * se définissent ainsi :
entre rationnels x et x' ce sont les $x * x'$,
entre un rationnel x et une coupure irrationnelle X', c'est la coupure $S_x * X'$,
entre une coupure irrationnelle X et un rationnel x' c'est la coupure $X * S_{x'}$,
entre deux coupures irrationnelles X et X' c'est la coupure $X * X'$.

179. **Inégalités** : elles se définissent à partir des signes et des soustractions comme chez les rationnels. Elles en possèdent donc exactement les mêmes propriétés.

Équations du deuxième degré

1. La formule générale est $a\,x^2 + b\,x + c = 0$.
2. Hypothèse : $a \neq 0$.
3. Mise en forme canonique : une multuplcation par $4\,a$ donne $4\,a^2\,x^2 + 4\,a\,b\,x + 4\,a\,c = 0$. Une factorisation donne $(2\,a\,x)^2 + 2\,(a\,x)\,b + 4\,a\,c = 0$. En tête on reconnaît deux termes de l'identité remarquable $(2\,a\,x + b)^2 = (2\,a\,x)^2 + 2\,(a\,x)\,b + b^2$ donc l'équation devient $(2\,a\,x + b)^2 - b^2 + 4\,a\,c = 0$ soit $(2\,a\,x + b)^2 - (b^2 - 4\,a\,c) = 0$.
4. La forme canonique annoncée est $(\alpha\,x + b)^2 - \Delta = 0$ avec $\alpha = 2\,a$ et $\Delta = b^2 - 4\,a\,c$.
5. La quantité Δ est appelée *discriminant*. En effet, son signe décide de la solvabilité de l'équation.
6. Si $\Delta > 0$, sa racine carrée existe : $\Delta = \sqrt{\Delta}^2$ donc avec une identité remarquable l'équation devient $\left[(\alpha\,x + b) - \sqrt{\Delta}\right]\left[(\alpha\,x + b) - \sqrt{\Delta}\right] = 0$, ce qui revient à annuler un produit de deux facteurs :
soit $\alpha\,x + b - \sqrt{\Delta} = 0$ donc $x = \dfrac{-b + \sqrt{\Delta}}{\alpha}$,
soit $\alpha\,x + b + \sqrt{\Delta} = 0$ donc $x = \dfrac{-b - \sqrt{\Delta}}{\alpha}$.
En remplaçant α et β, on conclut que
$\boxed{\text{si } b^2 - 4\,a\,c > 0 \text{ alors } x = \dfrac{-b \pm \sqrt{b^2 - 4\,a\,c}}{2\,a}}$.
7. Si $\Delta = 0$, la démarche précédente ne donne qu'une solution $x = \dfrac{-b}{\alpha}$, soit $x = \dfrac{-b}{2\,a}$ donc
En remplaçant α et β, on conclut que
$\boxed{\text{si } b^2 - 4\,a\,c = 0 \text{ alors } x = \dfrac{-b}{2\,a}}$.
8. Enfin, si $\Delta < 0$, l'égalité $(\alpha\,x + b)^2 - \Delta = 0$, équivalente à $(\alpha\,x + b)^2 = \Delta$ n'est jamais vraie quelque soit x.
En remplaçant α et β, on conclut que
$\boxed{\text{si } b^2 - 4\,a\,c < 0 \text{ alors } a\,x^2 + b\,x + c = 0 \text{ n'est jamais vraie}}$.

Ch 4 Fonctions à valeurs réelles définies sur des réels

Objet : il s'agit d'une catégorie d'ensembles de couples dont les antécédents et le simages sont des nombres réels.

Fonctions continues

180. **Fonction continue**. La fonction f est **continue** en X si et seulement si
♦ elle est définie en X (c'est **très important**),
♦ tout intervalle ouvert J contenant $f(X)$ a comme ensemble d'antécédents un intervalle ouvert I (fig. 5 et 6).

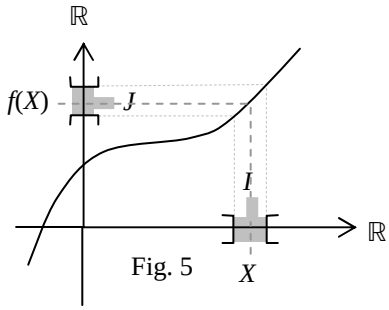


Fig. 5

181. **Théorème des valeurs intermédiaires** (fig. 5). Soit f une fonction continue au moins sur un intervalle $I =]A , B[$ et J l'intervalle $[f(A) , f(B)]$ si $f(A) < f(B)$ ou $[f(B) , f(A)]$ si $f(B) < f(A)$. Alors toute équation $f(X) = C$ avec $C \in J$ a au moins une solution dans I.
Démonstration. Raisonnons dans le cas $f(A) < f(B)$. Alors $]f(A) , f(B)[$ a l'intervalle ouvert $]A , B[$ comme ensemble d'antécédents. Comme C est dans $]f(A) , f(B)[$, il a un antécédent situé dans $]A , B[$ ■

182. **Une fonction continue sur un intervalle fermé atteint ses bornes**.

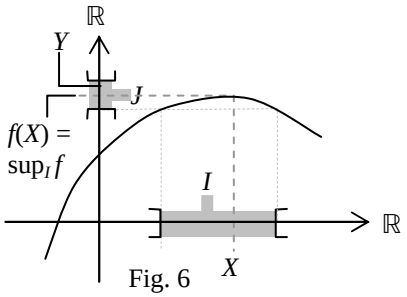


Fig. 6

a- Si la fonction f est définie et majorée sur un intervalle I (fig. 6) elle a une borne supérieure $\sup_I f$, c'est-à-dire que dès que $Y < \sup_I f$ il existe au moins une image f (un X de $[A , B]$) dans l'intervalle $]Y , \sup_I f[$.
b- Supposons qu'il n'existe pas de réel de $[A , B]$ solution de l'équation d'inconnue X : $f(X) = \sup_I f$.
c- L'ensemble de ces images $f(X)$ a quand-même sa borne supérieure B. Si $\sup_I f < B$ par définition de la borne B il existerait au moins un X' de $[A , B]$ tel que $\sup_I f < f(X') < B$, ce qui contredit la définition de $\sup_I f$.
d- On aurait donc $B < \sup_I f$.
e- Comme il existe des $f(X) < B$ et des X' tels que $B < f(X') < \sup_I f$, l'ensemble des antécédents des Y de $]f(X) , f(X')[$ serait, à cause de la continuité de f, un intervalle ouvert défini par deux coupures C' et $C < C'$.
f- Alors B serait l'image d'un nombre E de $]C , C'[$. L'équation d'inconnue E : $f(E) = B$ aurait au moins une solution.
e- Pour finir, en répétant le raisonnement *c*-, on trouverait la conclusion de *d*- inversée $\sup_I f < B = f(E)$ (contradiction).
f- La démonstration est analogue si les $f(X \in I)$ étaient minorés ■

Dérivée et intégrale

1. **L'aire sous une courbe représentative, née au moyen âge, induisit une révolution intellectuelle fondamentale au XVIIe siècle : le calcul différentiel et intégral, dus à Newton et Lebniz**

2. Soit (fig. 7) une fonction f' (la présence du "prime" sera justifié plus loin) définie au moins sur un intervalle $[a , b]$ et continue sur ce segment. On sait qu'elle atteint sa borne supérieure $\max_{[a , b]} f$ et inférieure $\min_{[a , b]} f$. Entre les deux, le théorème des valeurs intermédiaires dit que toute équation d'inconnue x : $f'(x) = y$ a au moins une solution.
L'aire du rectangle $ABC_{max}D_{max}$ de largeur $b - a$ et de hauteur $\max_{[a , b]} f'$ est $S_{max} = (b - a) \max_{[a , b]} f'$.
L'aire du rectangle $ABC_{max}D_{min}$ de largeur $b - a$ et de hauteur $\min_{[a , b]} f'$ est $S_{min} = (b - a) \min_{[a , b]} f'$.
L'aire du rectangle ABCD de largeur $b - a$ et de hauteur f'(un x de $[a , b]$) est $S = (b - a) f'(x)$.
$S - S_{min}$ est l'aire
Sur la représentation graphique on a l'encadrement $S_{min} \leqslant S \leqslant S_{max}$. Ce sont les aires de trois rectangles de même largeur $b - a$.
L'aire exacte de $ABC_{max}D_{min}$ est S_e encadrée aussi par S_{max} et S_{min} : $S_{min} \leqslant S_e \leqslant S_{max}$.

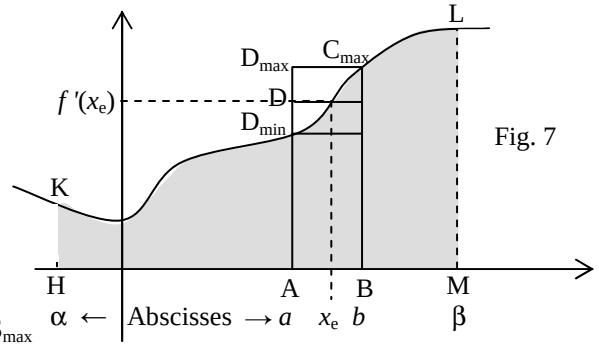


Fig. 7

Par continuité de f', l'équation $S(x) = S_e$ d'inconnue x a au moins une solution x_e appartenant à $[a , b]$.
Note : en cas de décroissance ou d'extrémum de f' sur $[a , b]$, le lettrage de la figure 7 reste le même.

3. Leibniz avait proposé plusieurs nouveaux codes d'écriture mathématiques :
$f(x)$ et y pour les images d'une fonction f, ∂x pour l'écart $b - a$ entre deux abscisses (la lettre ∂ remplace d pour éviter de confondre avec une multiplication d'un nombre d par x), ∂S et $f'(x_e)\, \partial x$ pour l'aire exacte de $ABC_{max}D_{min}$. Cette aire elle-même peut être vue comme la variation de l'aire S de la surface $HAD_{min}K$ définie par l'axe des abscisses, deux parallèles à l'axe des ordonnées d'abscisses m et a et la courbe représentative de la fonction f'.

4. L'aire S (en gris) est donc une fonction f distincte de f' dont les antécédents sont les couples de valeurs de (α , β). Cette aire S s'écrit donc $f(\alpha , \beta)$. Comme elle est la somme des aires de figures comme ABML, la lettre S allongée et garnie des bornes α et β donne notre symbole d'intégrale $f(\beta) - f(\alpha) = \int_{\alpha}^{\beta} f'(x)\, \partial x$.

5. Pour des raisons pratiques, le ∂ de Leibniz est remplacé par le "d" ordinaire : $f(\beta) - f(\alpha) = \int_{\alpha}^{\beta} f'(x)\, \mathrm{d}x$.

L'aire de $ABC_{max}D_{min}$ s'écrit donc $\mathrm{d}f = f'(x_e)\, \mathrm{d}x$. Une algèbre donne $\frac{\mathrm{d}f}{\mathrm{d}x} = f'(x_e)$ et la formule intégrale $f(\beta) = \int_{\alpha}^{\beta} \frac{\mathrm{d}f}{\mathrm{d}x}\, \mathrm{d}x + f(\alpha)$. La fonction ensemble des couples $(\beta , f(\beta))$ est donc connue à une constante près, la **constante d'intégration** $f(\alpha)$.

6. L'indice e de x_e dans les formules est presque toujours omis quand on écrit par exemple $\frac{\mathrm{d}f}{\mathrm{d}x} = f'(x)$, avec la convention que la valeur de x est justement celle qui rend $\mathrm{d}f$ exactement égal à l'aire de $ABC_{max}D_{min}$.

7. Si les images d'une fonction dépend de plusieurs variables, par exemple si f est l'ensemble des couples $((x , y , z) , f(x , y , z))$, une variation de f due à celles des trois variables x, y et z à la fois on l'écrira $\mathrm{d}f$ alors que par exemple, si on fixe les valeurs de x et z, la variation de f due à la seule variation $\mathrm{d}y$ de y s'écrira ∂f. On aura donc $\frac{\partial f}{\partial y} = f'(x , y_e , z)$ avec $y \leqslant y_e \leqslant y + \mathrm{d}y$.

8. Leibniz invanta aussi des termes de vocabulaire mathématique nouveaux, toujours employé aujourd'hui comme *fonction* pour f ou f', *coordonnée* pour x et y et *différentielle* – nommée *fluxion* chez newton – pour $\mathrm{d}f$ ou ∂f.

Calcul de dérivée par passage à la limite

183. Soit une fonction f définie au moins sur un intervalle $[a , b]$. Pour chaque $x \in]a , b[$ et h tel que $x + h \in]a , b[$ considérons la fonction ensemble q des couples $\left(h , q(h) = \frac{f(x+h) - f(x)}{h}\right)$. Manifestement, le couple $(0 , q(0))$ n'est pas défini. Si il existe un nombre r tel que la réunion de la fonction q et du couple $(0 , r)$ soit une fonction continue en h, alors r est nommé **nombre dérivé**. Comme pour connaître r il faut d'abord choisir x, ce nombre sera écrit comme une nouvelle fonction f' ensemble de couples $(x , f'(x))$, appelée **dérivée de** f.
Exemple : soit la fonction f ensemble des couples (x , x^2). On a $f(x) = x^2$. Le quotient dépendant de h est une fonction q ensemble des couples $\left(h , q(h) = \frac{f(x+h) - f(x)}{h}\right)$ donc tant que $h \neq 0$ on peut simplifier :
$q(h) = \frac{f(x+h) - f(x)}{h} = \frac{(x+h)^2 - x^2}{h} = \frac{2\,h\,x + h^2}{h} = 2\,x + h$. Pour assurer la continuité de la fonction q en $h = 0$,

on adjoint à q le couple $(0 , 2\,x)$, ce qui s'écrit $\lim_{h \to 0} q(h) = 2\,x$.
En pratique, une fois les simplifications faites, on remplace h par zéro.
Par ce procédé, on démontre les formules classiques de dérivées.

Fonction	Note	$\frac{f(x+h) - f(x)}{h}$	Dérivée	Démonstration
$x \to K$	Fonction constante	$\frac{K - K}{h} = 0$ (indépendant de h)	$x \to 0$	1
$x \to x^n$	Puissance d'une fonction	$\frac{(x+h)^n - x^n}{h}$	$n\,x^{n-1}$	2
$1 / x$	Fonction inverse	$\frac{-1}{x\,(x+h)}$	$\frac{-1}{x^2}$	3
$\sqrt{x}$	Fonction racine carrée	$\frac{\sqrt{x+h} - \sqrt{x}}{h} = \frac{1}{\sqrt{x+h} + \sqrt{x}}$	$\frac{1}{2\sqrt{x}}$	4
$K\,f$	Produit par une constante	$\frac{K\,f(x+h) - K\,f(x)}{h}$	$K\,f'(x)$	5

$f+g$	Somme de fonctions	$\frac{[f(x+h)+g(x+h)]-[f(x)+g(x)]}{h}$	$f'+g'$	6
$f-g$	Différence de fonctions	$\frac{[f(x+h)-g(x+h)]-[f(x)-g(x)]}{h}$	$f'-g'$	7
$\sum_{i\in I} f_i(x)$	Somme de fonctions	$\frac{\sum_{i\in I} f_i(x+h)-\sum_{i\in I} f_i(x)}{h}$	$\sum_{i\in I} f_i'(x)$	8
$f\times g$	Produit de fonctions	$\frac{f(x+h)\,g(x+h)-f(x)\,g(x)}{h}$	$f'(x)\,g(x)+f(x)\,g'(x)$	9
$\frac{f}{g}$	Quotient de fonctions	$\frac{f(x+h)/g(x+h)-f(x)/g(x)}{h}$	$\frac{\begin{vmatrix} f'(x) & g'(x) \\ f(x) & g(x)\end{vmatrix}}{g^2(x)}$	10

Démonstration 2 : le binôme de Newton donne $\frac{\sum_0^n \frac{n!}{k!(n-k)!}x^k h^{n-k}-x^n}{h}=\sum_0^n \frac{n!}{k!(n-k)!}\frac{x^k h^{n-k}}{h}-\frac{x^n}{h}$

$=\frac{n!}{n!(n-n)!}\frac{x^n h^{n-n}}{h}+\sum_0^{n-1}\frac{n!}{k!(n-k)!}\frac{x^k h^{n-k}}{h}-\frac{x^n}{h}=\sum_0^{n-1}\frac{n!}{k!(n-k)!}x^k h^{n-k-1}$

et tous ces termes sont nuls quand $h=0$ sauf si $n-k-1=0$ donc si $k=n-1$, donc il reste

$\frac{n!}{(n-1)!(n-(n-1))!}x^{n-1}=\frac{n!}{(n-1)!\,1!}x^{n-1}=\frac{n(n-1)!}{(n-1)!}x^{n-1}=n\,x^{n-1}$.

Démonstration 3 : $\frac{\frac{1}{x+h}-\frac{1}{x}}{h}=\frac{x-(x+h)}{(x+h)\,x}\frac{1}{h}=\frac{-h}{x\,(x+h)}\frac{1}{h}=\frac{-1}{x\,(x+h)}=\frac{-1}{x^2}$

Démonstration 4 : $\frac{\sqrt{x+h}-\sqrt{x}}{h}=\frac{\sqrt{x+h}-\sqrt{x}}{h}\frac{\sqrt{x+h}+\sqrt{x}}{\sqrt{x+h}+\sqrt{x}}=\frac{x+h-x}{h}\frac{1}{\sqrt{x+h}+\sqrt{x}}=\frac{1}{\sqrt{x+h}+\sqrt{x}}$

Démonstration 5 : $\frac{K\,f(x+h)-K\,f(x)}{h}=K\,\frac{f(x+h)-f(x)}{h}$

Démonstration 6 : $\frac{[f(x+h)+g(x+h)]-[f(x)+g(x)]}{h}=\frac{[f(x+h)-f(x)]-[g(x+h)-g(x)]}{h}$

$=\frac{f(x+h)-f(x)}{h}+\frac{g(x+h)-g(x)}{h}$

Démonstration 7 : analogue à la précédente

Démonstration 8 : $\frac{\sum_{i\in I} f_i(x+h)-\sum_{i\in I} f_i(x)}{h}=\frac{\sum_{i\in I}[f_i(x+h)-f_i(x)]}{h}=\sum_{i\in I}\frac{f_i(x+h)-f_i(x)}{h}$

Démonstration 9 : un artifice de calcul donne $\frac{f(x+h)\,g(x+h)-f(x)\,g(x+h)+f(x)\,g(x+h)-f(x)\,g(x)}{h}$ qui se décompose

$\frac{f(x+h)\,g(x+h)-f(x)\,g(x+h)}{h}+\frac{f(x)\,g(x+h)-f(x)\,g(x)}{h}$ et se factorise

$\frac{f(x+h)-f(x)}{h}\,g(x+h)+f(x)\,\frac{g(x+h)-g(x)}{h}$, puis le passage à la limite donne directement $f'(x)\,g(x)+f(x)\,g'(x)$.

Démonstration 10 : nommons $q(x)$ le quotient $\frac{f(x)}{g(x)}$. Alors $q(x)\,g(x)=f(x)$. Prenant la dérivée des deux membres, $q'(x)\,g(x)+q(x)\,g'(x)=f'(x)$. Substituons $q(x)$: $q'(x)\,g(x)+\frac{f(x)}{g(x)}\,g'(x)=f(x)$. Multiplions par $g(x)$: $q'(x)\,g^2(x)+f(x)\,g'(x)=f'(x)\,g(x)$. Soustrayons $f(x)\,g'(x)$: $q'(x)\,g^2(x)=f'(x)\,g(x)-f(x)\,g'(x)$. Multiplions par l'inverse du carré de $g(x)$: $q'(x)=[f'(x)\,g(x)-f(x)\,g'(x)]\frac{1}{g^2(x)}$. Utilisons l'écriture du déterminant :

$q'(x)=\frac{1}{g^2(x)}\begin{vmatrix} f'(x) & g'(x) \\ f(x) & g(x)\end{vmatrix}$.

Note : cas particulier : le numérateur est constant : $q'(x) = \frac{1}{g^2(x)} \begin{vmatrix} 0 & g'(x) \\ K & g(x) \end{vmatrix} = \frac{-K\,g'(x)}{g^2(x)}$.

La formule de Taylor

9. La dérivée de x^n est $n\,x^{n-1}$.
Celle de $b - x$ est -1.
On a $\frac{d}{dx}(b-x)^n = \frac{d}{d(x-b)}(b-x)^n \cdot \frac{d}{dx}(b-x) = (-1)\,n\,(b-x)^{n-1}$.

10. On sait que la dérivée d'une multiplication de fonctions est $\frac{d}{dx}[f(x)\,g(x)] = \frac{df}{dx}g(x) + f(x)\frac{dg}{dx}$.

On sait que $\int_a^b u(x)\,dx = u(b) - u(a)$ qu'on a coutume d'écrire $\left| u(x) \right|_a^b$.

On a donc $\int_a^b \frac{d}{dx}[f(x)\,g(x)]\,dx = \left| f(x)\,g(x) \right|_a^b$ donc $\left| f(x)\,g(x) \right|_a^b = \int_a^b \frac{df}{dx} g(x)\,dx + \int_a^b f(x)\frac{dg}{dx}\,dx$ donc

$\boxed{\int_a^b f(x)\frac{dg}{dx}\,dx = \left| f(x)\,g(x) \right|_a^b - \int_a^b \frac{df}{dx} g(x)\,dx}$ qui est la formule d'intégration par parties. On peut écrire

$\int_a^b f(x) \cdot (\text{dérivée de } g)\,dx = \left| f(x)\,g(x) \right|_a^b - \int_a^b (\text{dérivée de } f) \cdot g(x)\,dx$.

11. Si on prend $f(x)$ = la n-ième dérivée de $u(x)$, écrite $u^{(n)}(x)$, et $g(x) = (b-x)^{k+1}$, la dérivée de f est la $n+1$ ème dérivée de u, écrite $u^{(n+1)}(x)$ et la dérivée de g est $-(k+1)(b-x)^k$ donc on trouve

$\int_a^b u^{(n)}(x) \cdot [(-1)(k+1)(b-x)^k]\,dx = \left| u^{(n)}(x)\,(b-x)^{k+1} \right|_a^b - \int_a^b u^{(n+1)}(x) \cdot (b-x)^{k+1}\,dx$.

On sort les constantes : $(-1)(k+1)\int_a^b u^{(n)}(x) \cdot (b-x)^k\,dx = \left| u^{(n)}(x)\,(b-x)^{k+1} \right|_a^b - \int_a^b u^{(n+1)}(x) \cdot (b-x)^{k+1}\,dx$.

$\left| u^{(n)}(x)\,(b-x)^{k+1} \right|_a^b = u^{(n)}(b)\,(b-b)^{k+1} - u^{(n)}(a)\,(b-a)^{k+1} = -u^{(n)}(a)\,(b-a)^{k+1}$.

12. Conclusion : $(-1)(k+1)\int_a^b u^{(n)}(x) \cdot (b-x)^k\,dx = -u^{(n)}(a)\,(b-a)^{k+1} - \int_a^b u^{(n+1)}(x) \cdot (b-x)^{k+1}\,dx$ donc

$\int_a^b u^{(n)}(x) \cdot (b-x)^k\,dx = \frac{1}{k+1}u^{(n)}(a)\,(b-a)^{k+1} + \frac{1}{k+1}\int_a^b u^{(n+1)}(x) \cdot (b-x)^{k+1}\,dx$

13. *Initiation*

Cas $k = 0$ et $n = 1$: $\int_a^b u^{(1)}(x) \cdot (b-x)^0\,dx = \frac{1}{0+1}u^{(1)}(a)\,(b-a)^{0+1} + \frac{1}{0+1}\int_a^b u^{(1+1)}(x) \cdot (b-x)^{0+1}\,dx$

$\int_a^b (\text{dérivée de } u)\,dx = u^{(1)}(a)\,(b-a) + \int_a^b u^{(2)}(x) \cdot (b-x)\,dx$ donc

$u(b) - u(a) = u^{(1)}(a)\,(b-a) + \int_a^b u^{(2)}(x) \cdot (b-x)\,dx$ donc $u(b) = u(a) + u^{(1)}(a)\,(b-a) + \int_a^b u^{(2)}(x) \cdot (b-x)\,dx$.

14. Pour écrire l'intégrale de sorte qu'on puisse appliquer l'al.4 avec $k = 1$ et $n = 2$, écrivons-la $\int_a^b u^{(2)}(x) \cdot (b-x)^1\,dx$, ce qui donne $\frac{1}{1+1}u^{(2)}(a)\,(b-a)^{1+1} + \frac{1}{1+1}\int_a^b u^{(2+1)}(x) \cdot (b-x)^{1+1}\,dx$ soit

$\frac{1}{2}u^{(2)}(a)\,(b-a)^2 + \frac{1}{2}\int_a^b u^{(3)}(x) \cdot (b-x)^2\,dx$. Intégrée dans la formule de l'al.5 :

$u(b) = u(a) + u^{(1)}(a)\,(b-a) + \frac{1}{2}u^{(2)}(a)\,(b-a)^2 + \frac{1}{2}\int_a^b u^{(3)}(x) \cdot (b-x)^2\,dx$.

15. Pour deviner la formule récurrente, on recommence sur l'intégrale, ce qui donne $k = 2$, $n = 3$ et

$\int_a^b u^{(3)}(x) \cdot (b-x)^2\,dx = \frac{1}{2+1}u^{(3)}(a)\,(b-a)^{2+1} + \frac{1}{2+1}\int_a^b u^{(3+1)}(x) \cdot (b-x)^{2+1}\,dx$

$= \frac{1}{3}u^{(3)}(a)\,(b-a)^3 + \frac{1}{3}\int_a^b u^{(4)}(x) \cdot (b-x)^3\,dx$. Intégrée dans la formule de l'al.6

$u(b) = u(a) + u^{(1)}(a)\,(b-a) + \frac{1}{2}u^{(2)}(a)\,(b-a)^2 + \frac{1}{2}\left[\frac{1}{3}u^{(3)}(a)\,(b-a)^3 + \frac{1}{3}\int_a^b u^{(4)}(x) \cdot (b-x)^3\,dx\right]$. Le

développement donne deux multiplications $\frac{1}{2}$ par $\frac{1}{3}$ qui donne $\frac{1}{2\times 3} = \frac{1}{3!}$, ce qui induit la tentation d'introduire les factorielles particulières $0! = 1$, $1! = 1$ et $2! = 2$:

$u(b) = \frac{1}{0\,!}u^{(0)}(a) + \frac{1}{1\,!}u^{(1)}(a)\,(b-a)^1 + \frac{1}{2\,!}u^{(2)}(a)\,(b-a)^2 + \frac{1}{3\,!}u^{(3)}(a)\,(b-a)^3 + \frac{1}{3\,!}\int_a^b u^{(4)}(x)\cdot(b-x)^3\,dx.$

16. *Hypothèse* : $\boxed{u(b) = \sum_{k=0}^{n}\frac{1}{k\,!}u^{(k)}(a)\,(b-a)^k + \text{[résidu] avec [résidu]} = \frac{1}{n\,!}\int_a^b u^{(n+1)}(x)\cdot(b-x)^n\,dx}$.

C'est la formule de Taylor.

Hérédité : on reprend l'intégrale : $\int_a^b u^{(n+1)}(x)\cdot(b-x)^n\,dx$, lue comme $\int_a^b f(x)\cdot(\text{dérivée de } g)\,dx$ devenue

$\int_a^b u^{(n+1)}(x)\cdot\left(\text{dérivée de }\frac{1}{n+1}(b-x)^{n+1}\right)dx$ égale à

$\left|u^{(n+1)}(x)\frac{1}{n+1}(b-x)^{n+1}\right|_b^a - \int_a^b\left(\text{dérivée de } u^{(n+1)}(x)\right)\frac{1}{n+1}(b-x)^{n+1}\,dx$ égale à

$\frac{1}{n+1}\left|u^{(n+1)}(x)\;(b-x)^{n+1}\right|_b^a - \frac{1}{n+1}\int_a^b\left(\text{dérivée de } u^{(n+1)}(x)\right)(-1)\,(b-x)^{n+1}\,dx$.

On trouve le coefficient $\frac{1}{n\,!}\frac{1}{n+1} = \frac{1}{(n+1)\,!}$ et le terme entre barres $u^{(n+1)}(b)\;(b-b)^{n+1} - u^{(n+1)}(a)\;(b-a)^{n+1}$

donc la formule $\sum_{k=0}^{n}\frac{1}{k\,!}u^{(k)}(a)\,(b-a)^k + \frac{1}{(n+1)\,!}u^{(n+1)}(a)\,(b-a)^{n+1} = \sum_{k=0}^{n+1}\frac{1}{k\,!}u^{(k)}(a)\,(b-a)^k$ et on retrouve l'analogue de la formule de l'al. XX

$u(b) = \sum_{k=0}^{n+1}\frac{1}{k\,!}u^{(k)}(a)\,(b-a)^k + \text{[résidu] avec [résidu]} = \frac{1}{(n+1)\,!}\int_a^b u^{((n+1)+1)}(x)\cdot(b-x)^{n+1}\,dx.$

17. Le résidu permet d'estimer la limite extrême de l'erreur de calcul si on le néglige. Imaginons que les points de coordonnées $\begin{pmatrix} x \\ u^{(n+1)}(x)\end{pmatrix}$ soit tous dans un rectangle de hauteur $M - m$ où $m = \inf u^{(n+1)}(x \in [a\,,\,b])$ et $M = \sup u^{(n+1)}(x \in [a\,,\,b])$ alors $m \leqslant u^{(n+1)}(x) \leqslant M$ donne $m\,(b-x)^n \leqslant u^{(n+1)}(x)\cdot(b-x)^n \leqslant M\,(b-x)^n$.
Comme $a \leqslant x \leqslant b$, on a $a - b \leqslant x - b \leqslant 0$ donc $0 \leqslant b - x \leqslant b - a$ donc $0 \leqslant (b-x)^n \leqslant (b-a)^n$ et $a - x \leqslant 0 \leqslant b - x$ donc $0 \leqslant (b-x)^n$
On a donc par transitivité des inégalités $0 \leqslant u^{(n+1)}(x)\cdot(b-x)^n \leqslant M\,(b-a)^n$ et par intégration

$0 \leqslant \int_a^b u^{(n+1)}(x)\cdot(b-x)^n\,dx \leqslant M\int_a^b(b-a)^n\,dx$ donc $\boxed{0 \leqslant \text{[résidu]} \leqslant \frac{1}{n\,!}M\,(b-a)^{n+1}}$.

Le logarithme népérien

1. **Etymologie** : le mot "logarithme" vient de AL KWARISMI né dans le *Kwarezm*, une province de l'empire arabe du VIIIe siècle : c'est donc le surnom d'un mathématicien perse de cette époque. Le mot "népérien" vient de NEPER ou NAPIER, mathématicien britannique du XVIIe siècle.
2. Le logarithme de u est (figure 10a) l'aire de ABCD. Le nom de cette figure se lit en tournant dans le sens positif comme en trigonométrie. Le logarithme de v est l'aire de AEFD. Le nom de cette figure se lit en tournant dans le sens négatif comme en trigonométrie.
3. Exemples sur le figure 10a : l'aire jaune foncé est le **logarithme népérien de 4**, écrit ln 4. L'aire jaune clair est ln $\frac{1}{3}$. L'aire ln 4 est positive alors que l'aire ln $\frac{1}{3}$ est négative.
4. Le logarithme de 1 est l'aire du rectangle aplati ADDA donc $\boxed{\ln 1 = 0}$ (formule 10a).
5. Sur la figure 10b on lit immédiatement $\boxed{\frac{d\ln x}{dx} = \frac{1}{x}}$. On dit que **la dérivée de la fonction logarithme est la fonstion inverse**.
6. En conséquence, par cumul des variations $\int_1^b\frac{1}{x}\,dx = \ln x - \ln 1$ d'où $\boxed{\int_1^b\frac{1}{x}\,dx = \ln x}$.

7. On a $\frac{\mathrm{d}\ln(a\,x)}{\mathrm{d}x} = \frac{\mathrm{d}\ln(a\,x)}{\mathrm{d}(a\,x)}\frac{\mathrm{d}(a\,x)}{\mathrm{d}x}$. La première dérivée est $\frac{1}{a\,x}$ et la deuxième est la fonction constante égale à a donc $\frac{\mathrm{d}\ln(a\,x)}{\mathrm{d}x} = \frac{1}{x}$ donc $\ln(a\,x)$ et $\ln x$ ont la même dérivée, donc diffèrent d'une fonction constante K :
$\ln(a\,x) - \ln x = K$. En choisissant 1 pour x on trouve $\ln a - \ln 1 = K$ d'où l'identificaation $K = \ln a$ et on retient $\boxed{\ln a\,x = \ln a + \ln x}$. **C'est la propriété fondamentale du logarithme : il transforme une multiplication en addition**.
8. Par récurrence on démontre que $\ln(a \ldots m) = \ln a \ldots + \ln m$.
9. Cas particulier : si n est un entier naturel $\boxed{\ln a^n = n \ln a}$.
10. Si q est le quotient a/b on a $q\,b = a$ donc $\ln q\,b = \ln a$ donc $\ln q = \ln a - \ln b$ donc $\boxed{\ln a/b = \ln a - \ln b}$.
11. La formule de l'al. 5 montre que si $\mathrm{d}x$ et x sont positifs $\mathrm{d}\ln x$ est positif, donc que **le logarithme est une fonction uniformément croissante**.
12. **Le logarithme croît uniformément de $-\infty$ à $+\infty$ quand son antécédent va de zéro à $+\infty$.**
♦ Soit $a > 1$. Alors $\ln a > 0$. Supposons tous les logarithmes majorés par un réel unique : alors ils seraient bornés supérieurement par un réel M, et il existerait un entier naturel N tel que $N \ln a > M$, donc tel que $\ln a^N > M$ (contradiction).
♦ Soit a appartenant à l'intervalle $]0\ ,\ 1[$. 1. Alors $\ln a < 0$. Supposons tous les logarithmes minorés par un réel unique : alors ils seraient bornés inférieurement par un réel m, et il existerait un entier naturel N tel que $N \ln a < m$, donc tel que $\ln a^N < m$ (contradiction).
13. **Quelque soit le nombre réel** donné y **l'équation** $\ln x = y$, **a une solution unique**. En effet, quand x croît de zéro à $+\infty$ son logarithme croît de $-\infty$ à $+\infty$ strictement et uniformément.
Il existe alors deux logarithmes $\ln a$ et $\ln b$ encadrant $\ln y$ donc en vertu du théorème des valeurs intermédiaires un $\ln x$ exactement égal à y et, parce que la croissance du logarithme est uniforme et stricte, unique.
Cas particulier : l'équation d'inconnue e : $\boxed{\ln e = 1}$ a une solution unique. Ce nombre est appelé **base népérienne des logarithmes**.

Autres logarithmes

14. Par définition, $\boxed{\lg_a x = \frac{\ln x}{\ln a}}$. Deux cas particuliers sont très utilisés : $\lg_{10}$, couramment écrit lg ou log pour les calculs numériques et en chimie pour définir le pH = – log [concentration des ions H^+ en mole/litre] et les lois régissant les réactions en équilibre, et $\lg_2$ par les développeurs en informatique.
15. $\boxed{\lg_a a = 1 \text{ et } \lg_a a^x = x}$. En particulier $\log 10^n = n$. La deuxième formule vient de $\lg_a a^x = \frac{\ln a^x}{\ln a} = \frac{x \ln a}{\ln a}$.

Les exponentielles

16. **Généralisation de la notion de puissance** : si a et x sont deux réels, alors l'équation d'inconnue y : $\ln y = x \ln a$ a une solution unique. Par analogie avec le formule de l'al. 9, y sera écrit a^x. On a donc $\boxed{\ln y = x \ln a \Leftrightarrow y = a^x}$.
17. Cas particulier : si $a = e$ alors $\boxed{\ln y = x \Leftrightarrow y = e^x}$.
La fonction ensemble des couples $(x\ ,\ a^x)$ est appelée **exponentielle de base** a. La fonction ensemble des couples $(x\ ,\ e^x)$ est appelée **exponentielle**, ses images e^x sont aussi écrites $\exp x$: $\boxed{e^x = \exp x}$.
18. Avec les définitions précédentes, $\boxed{\ln \exp y = y}$ et $\boxed{\exp \ln x = x}$.
19. Conséquence : $\exp \ln y = \exp(x \ln a)$ donne $\boxed{a^x = \exp(x \ln a)}$.
sa dérivée sont confondues.
20. Parce que $\ln \exp a = a$ et $\ln \exp b = b$ on a $\ln(\exp a \times \exp b) = \ln \exp a + \ln \exp b = a + b$ et
$\ln(\exp a \times \exp b) = a + b$ donne $\exp a \times \exp b = \exp(a + b)$ donc **un produit d'exponentielles est l'exponentielle d'une somme** : $\boxed{\exp(a + b) = \exp a \exp b}$.
Cette propriété justifie le nom d'exponentielle donné à la fonction ensemble des couples $(x\ ,\ \exp x)$.
Parce que $\ln \exp(a\,x) = \ln \exp a\,x = a\,x$ et $\ln(\exp x)^a = a \ln \exp x = a\,x$, par identification $\boxed{\exp(a\,x) = (\exp x)^a}$.
21. **Dérivée de l'exponentielle de base** e. Soient $x = \ln y$. Alors $\exp x = y$ donc
$\mathrm{d}\ln y = \frac{1}{y}\mathrm{d}y \Leftrightarrow \mathrm{d}x = \frac{1}{\exp x}\mathrm{d}\exp x \Leftrightarrow \exp x\,\mathrm{d}x = \mathrm{d}\exp x \Leftrightarrow \boxed{\exp x = \frac{\mathrm{d}\exp x}{\mathrm{d}x}}$ donc **l'exponentielle de base** e **et sa dérivée sont confondues**.

22. **Intégrale d'une exponentielle** : parce que $\int_a^b \frac{\mathrm{d}\exp x}{\mathrm{d}x}\,\mathrm{d}x = \exp b - \exp a$, on retient

$$\boxed{\int_a^b \exp x\,\mathrm{d}x = \exp b - \exp a}.$$

23. **Exponentielle d'une fonction** : $\frac{\mathrm{d}}{\mathrm{d}x}\exp f(x) = \frac{\mathrm{d}\exp f(x)}{\mathrm{d}f(x)}\frac{\mathrm{d}f(x)}{\mathrm{d}x} = \frac{\mathrm{d}f}{\mathrm{d}x}\exp f(x)$ et on retient

$$\boxed{\frac{\mathrm{d}}{\mathrm{d}x}\exp f(x) = \frac{\mathrm{d}f}{\mathrm{d}x}\cdot\exp f(x)}.$$

24. On en déduit l'intégrale $\boxed{\exp f(b) - \exp f(a) = \int_a^b \frac{\mathrm{d}f}{\mathrm{d}x}\exp f(x)\,\mathrm{d}x}$.

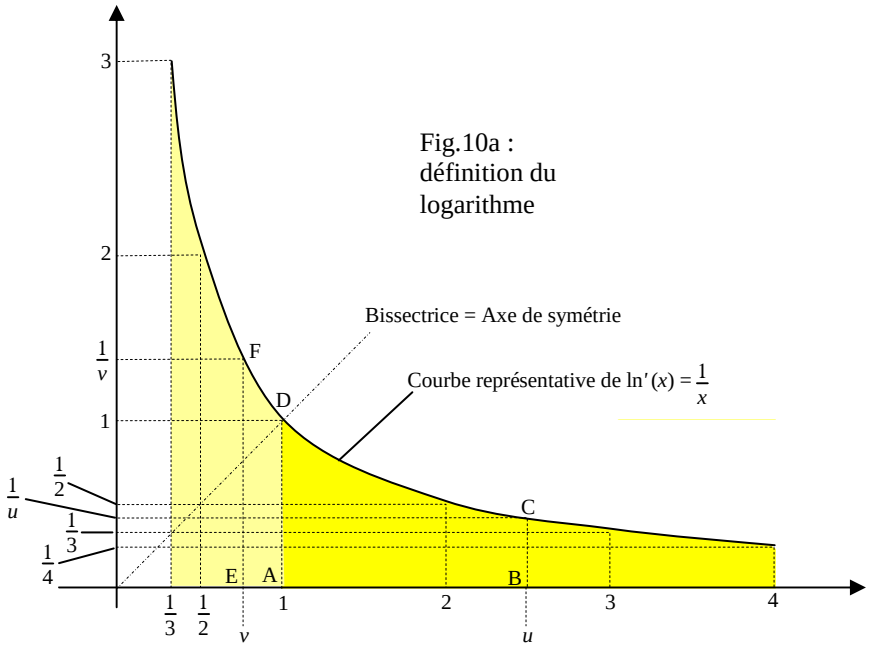


Fig.10a :
définition du
logarithme

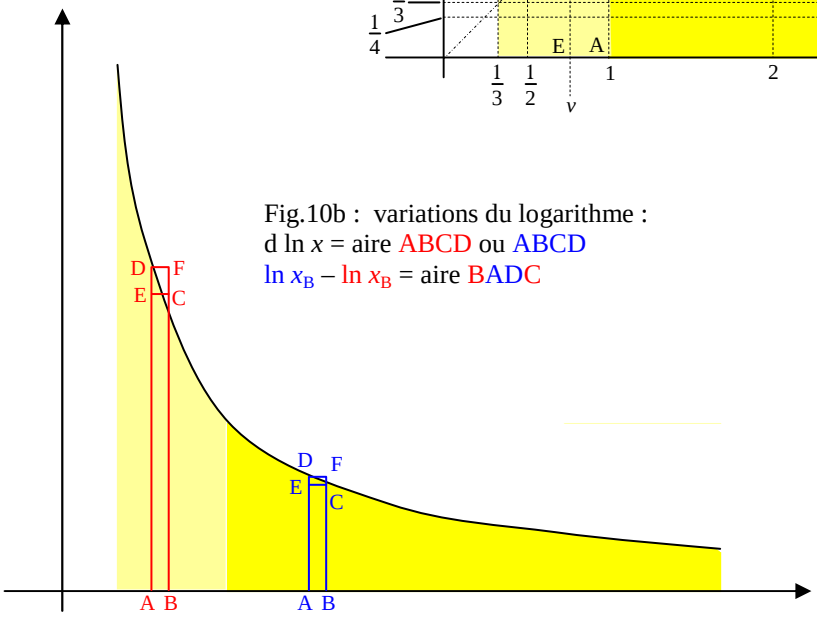


Fig.10b : variations du logarithme :
d ln x = aire ABCD ou ABCD
ln x_B – ln x_B = aire BADC

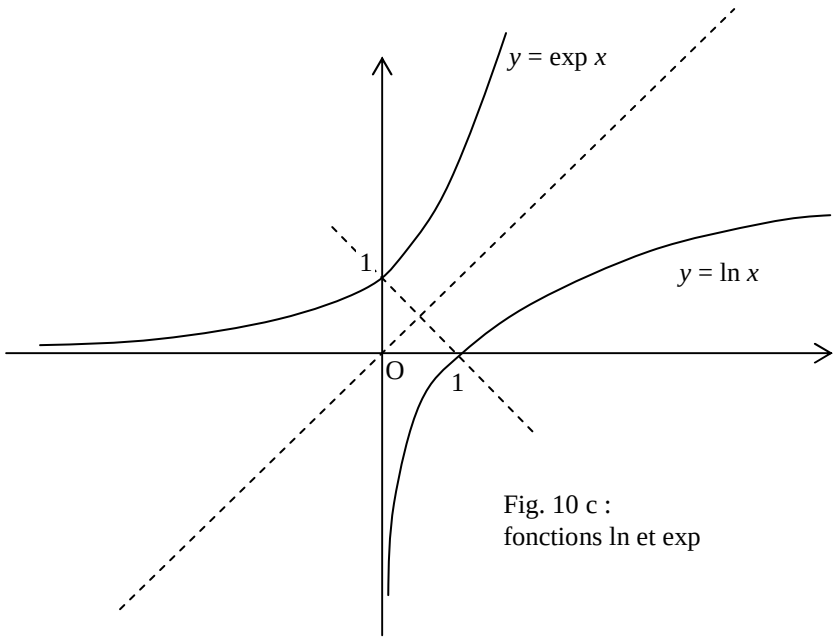


Fig. 10 c :
fonctions ln et exp

Équations différentielles du premier ordre

18. Par définition ce sont des équations dont les inconnues ne sont plus de simples nombres, mais des fonctions, c'est-à-dire des ensembles de couples $\big(x\ ,\ f(x)\big)$ dans lesquels chaque antécédent n'a qu'une seule image.
Vocabulaire : **résoudre une équation différentielle s'appelle l'intégrer**.

19. **Exemple** : la résolution de $\frac{\mathrm{d}f}{\mathrm{d}x} = 0$ dont l'inconnue est la fonction f. Dans chaque intervalle de longueur dx on a df, en tant que variation de f sur cet intervalle, nul : $\mathrm{d}f = 0\ \mathrm{d}x$. En conséquence, f est une fonction constante.

> Les solutions de $\frac{\mathrm{d}f}{\mathrm{d}x} = 0$ sont toutes les fonctions constantes.

Soient deux fonctions f et g qui ont même dérivée : la dérivée de la différence érant la différence des dérivées, on a $\frac{\mathrm{d}}{\mathrm{d}x}(f - g) = 0$ donc la différence $f - g$ est une fonction constante : **deux fonctions de même dérivée diffèrent d'une fonction constante**.

20. **Équation monôme** : soit à résoudre $\frac{\mathrm{d}f}{\mathrm{d}x} = a\,x^n$. D'une part on sait que la dérivée de $k\,x^{n+1}$ est $(n + 1)\,k\,x^n$ et d'autre part les solutions diffèrent entre elles d'une fonction constante ensemble des couples $(x\ ,\ C)$. On procède par identification : a doit être égal à $(n + 1)\,k$ et une algèbre donne $k = \frac{a}{n+1}$. On conclut que les solutions sont les fonctions $f(x) = \frac{a}{n+1}\,x^{n+1} + C$: > Les solutions de $\frac{\mathrm{d}f}{\mathrm{d}x} = a\,x^n$ sont les $\frac{a}{n+1}\,x^{n+1} + C$.

21. **Équation** $\frac{\mathrm{d}f}{\mathrm{d}x} = a\,f(x)$: une division par $f(x)$ donne $\frac{1}{f(x)}\frac{\mathrm{d}f}{\mathrm{d}x} = a$. À gauche on reconnaît la dérivée de $\ln f(x)$ et à droite celle de $a\,x$: les deux fonctions $\ln f(x)$ et $a\,x$ diffèrent d'une fonction constante ensemble des couples $(x\ ,\ C)$ qu'on va appeler C : $\ln f(x) = a\,x + C$. On prend l'exponentielle des deux membres : $f(x) = \exp(a\,x + C)$ ou encore $f(x) = \exp(a\,x) \cdot \exp C$.
Note : si x est nul, il reste $f(0) = \exp C$ qui est strictement positive, donc on retient :

> Les solutions de $\frac{\mathrm{d}f}{\mathrm{d}x} = a\,f(x)$ sont les $f(0) \cdot \exp f(x)$ où $f(0)$ est une valeur strictement positive quelconque.

Fonctions trigonométriques

22. On sait que $\cos^2 x + \sin^2 x = 1$. On allège les écritures en renommant c la fonction cosinus et s la fonction sinus : $c^2(x) + s^2(x) = 1$.
23. Ici, x est la longueur d'un arc du cercle trigonométrique et non les coordonnées d'un point de ce cercle. Aussi est-il sage de la renommer l et écrire $c^2(l) + s^2(l) = 1$.
24. En dérivant ; $2\,c\,\frac{\mathrm{d}c}{\mathrm{d}l} + 2\,s\,\frac{\mathrm{d}s}{\mathrm{d}l} = 0$. On allège les écritures en renommant c' et s' les dérivées : $c\,c' + s\,s' = 0$. Les deux flèches de coordonnées $\begin{pmatrix} c \\ s \end{pmatrix}$ et $\begin{pmatrix} c' \\ s' \end{pmatrix}$ sont orthogonales.
25. La longueur dl d'un arc du cercle trigonométrique est assimilable – s'il est assez petit – à une petite corde, un petit segment de droite sur lequel on applique le théorème de Pythagore $\mathrm{d}l^2 = \mathrm{d}x^2 + \mathrm{d}y^2 = \mathrm{d}c^2 + \mathrm{d}s^2$ donc $1 = \left(\frac{\mathrm{d}c}{\mathrm{d}l}\right)^2 + \left(\frac{\mathrm{d}s}{\mathrm{d}l}\right)^2$ et on retrouve $1 = c'^2 + s'^2$. Les deux dérivées recherchées sont cosinus et sinus d'un angle à identifier.
26. Vu l'orthogonalité précedente, on peut donc écrire $c = \cos l$; $s = \sin l$; $c' = \cos(l \pm \pi/2)$ et $s' = \sin(l \pm \pi/2)$.
27. Pour connaître le signe, il suffit de se souvenir que quand l augmente de dl à partir de la valeur zéro, le sinus augmente et le cosinus diminue, donc $\left[c'(l=0) = \cos(\pm\pi/2)\right]\mathrm{d}l < 0$ et $\left[s'(l=0) = \sin(\pm\pi/2)\right]\mathrm{d}l > 0$, ce qui n'est possible que si le signe devant $\pi/2$ est +. La conclusion est que $c' = \cos(l + \pi/2)$ et $s' = \sin(l + \pi/2)$:

$\boxed{\frac{\mathrm{d}}{\mathrm{d}l}\cos l = \cos(l + \pi/2) \text{ et } \frac{\mathrm{d}}{\mathrm{d}l}\sin l = \sin(l + \pi/2)}$. **Dériver une fonction sinus ou cosinus consiste à ajouter** $\pi/2$ **à son argument**.

28. On a $\tan l = \frac{\sin l}{\cos l}$ dont le modèle est $\frac{f(x)}{g(x)}$ de dérivée $\frac{\begin{vmatrix} f'(x) & g'(x) \\ f(x) & g(x) \end{vmatrix}}{g^2(x)}$, ce qui donne $\frac{1}{\cos^2 l}\begin{vmatrix} \sin(l+\pi/2) & \cos(l+\pi/2) \\ \sin l & \cos l \end{vmatrix} = \begin{vmatrix} \cos l & -\sin l \\ \sin l & \cos l \end{vmatrix}$. Le résultat est $\frac{1}{\cos^2 l}(\cos^2 l + \sin^2 l) = \frac{1}{\cos^2 l}$ ou $1 + \frac{\sin^2 l}{\cos^2 l}$ soit $1 + \tan^2 l$. On retient : $\boxed{\frac{\mathrm{d}}{\mathrm{d}l}\tan l = \frac{1}{\cos^2 l} = 1 + \tan^2 l}$.
29. **Trigonométrie d'une fonction**. On a On a $\frac{\mathrm{d}}{\mathrm{d}x}\sin l(x) = \frac{\mathrm{d}\sin l(x)}{\mathrm{d}l(x)} \cdot \frac{\mathrm{d}\,l(x)}{\mathrm{d}x} = \sin(\mathrm{l} + \pi/2) \cdot \frac{\mathrm{d}\,l(x)}{\mathrm{d}x}$ et par analogie $\frac{\mathrm{d}}{\mathrm{d}x}\cos l(x) = \cos(\mathrm{l} + \pi/2) \cdot \frac{\mathrm{d}\,l(x)}{\mathrm{d}x}$. Le même raisonnement avec la tangente donne $\frac{\mathrm{d}}{\mathrm{d}x}\tan l(x) = \frac{1}{\cos^2 l(x)}\frac{\mathrm{d}\,l(x)}{\mathrm{d}x}$ ou encore $(1 + \tan^2 l)\frac{\mathrm{d}\,l(x)}{\mathrm{d}x}$. On retient :

$\boxed{\frac{\mathrm{d}}{\mathrm{d}x}\sin l(x) = \sin(\mathrm{l} + \pi/2) \cdot \frac{\mathrm{d}\,l}{\mathrm{d}x}}$, $\boxed{\frac{\mathrm{d}}{\mathrm{d}x}\cos l(x) = \cos(\mathrm{l} + \pi/2) \cdot \frac{\mathrm{d}\,l}{\mathrm{d}x}}$ et

$\boxed{\frac{\mathrm{d}}{\mathrm{d}x}\tan l(x) = \frac{1}{\cos^2 l(x)}\frac{\mathrm{d}\,l(x)}{\mathrm{d}x} = (1 + \tan^2 l)\frac{\mathrm{d}\,l(x)}{\mathrm{d}x}}$.

Équations différentielles du deuxième ordre

30. Ce sont des équations différentielle contenant au moins une dérivée du deuxième ordre.
31. **Équation** $\frac{\mathrm{d}^2 f}{\mathrm{d}x^2} + a\,f(x) = 0$ avec $a > 0$. On multiplie par la dérivée première : $\frac{\mathrm{d}^2 f}{\mathrm{d}x^2}\frac{\mathrm{d}f}{\mathrm{d}x} + a\,\frac{\mathrm{d}f}{\mathrm{d}x}f(x) = 0$. On renomme f' la dérivée $\frac{\mathrm{d}f}{\mathrm{d}x}$ dans le premier terme : $\frac{\mathrm{d}f'}{\mathrm{d}x}f'(x) + a\,\frac{\mathrm{d}f}{\mathrm{d}x}f(x) = 0$. On multiplie par 1/2 : $\frac{1}{2}\frac{\mathrm{d}f'}{\mathrm{d}x}f'(x) + \frac{1}{2}a\,\frac{\mathrm{d}f}{\mathrm{d}x}f(x) = 0$. On sait que la dérivée de $f^2(x)$ est $2\,\frac{\mathrm{d}f}{\mathrm{d}x}f(x)$, donc par analogie que $2\,\frac{\mathrm{d}f'}{\mathrm{d}x}f'(x)$ est celle de $f'^2(x)$. Le membre de gauche de l'équation énoncée est donc la dérivée de $f'^2(x) + a\,f^2(x)$ et sa nullité montre que cette quantité est une fonction constante C.
32. Comme C est de signe positif, donc peut être écrite comme le carré d'un nombre réel positif K : $f'^2(x) + a\,f^2(x) = K^2$. Comme a aussi est le carré d'un réel positif A, $f'^2(x) + A^2 f^2(x) = K^2$.

33. Vu la règle $\left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2}$ on déduit $\left(\frac{f'}{K}\right)^2 + \left(\frac{A f}{K}\right)^2 = 1$, ce qui montre que $\frac{f'}{K}$ et $\frac{a f}{K}$ sont cosinus et sinus d'un même angle l : $\frac{f'}{K} = \cos l$ et $\frac{A f}{K} = \sin l$.

34. Ici, l est une certaine fonction de x : par dérivation, $\frac{A f'}{K} = \frac{\mathrm{d} \sin l}{\mathrm{d} l} \cdot \frac{\mathrm{d} l}{\mathrm{d} x} = \cos l \cdot l'(x) = \frac{f'}{K} l'(x)$. L'équation $\frac{A f'}{K} = \frac{f'}{K} l'(x)$ donne $A = l'(x)$ dont la solution générale est $l(x) = A x + B$ où B est une fonction constante.

35. Conclusion : $\frac{A f}{K} = \sin (A x + B)$ donne $f(x) = \frac{K}{A} \sin (A x + B)$. ici, $\frac{K}{A}$ peut être lu comme l'amplitude F d'une fonction sinusoïdale $f(x) = F \sin (A x + B)$. On a par identification $A = \sqrt{a}$ et on retient que

si $a > 0$ … … la solution générale de l'équation $\frac{\mathrm{d}^2 f}{\mathrm{d} x^2} + a f(x) = 0$ est $f(x) = F \sin \left(\sqrt{a} x + B\right)$ …

… où F est une constante positive nommée **amplitude**.