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* sont une réalité riche d'intérêt.
Un ensemble comme {a , a , a , a , a , a , a} ou les 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 – à tout habitant de notre terre.

Disons " 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 ∅ …
Mais si ∅ ne contient rien, ∅ est un objet et on conçoit un ensemble contenant cet objet et que cet objet et qu'on écrit {∅}, 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 {∅ , {∅}} 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 IIIII 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. Ce n'est possible que par 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.

Collectivités d'objets

Peut-on définir un ensemble par une phrase ?
Une phrase a un sujet, c'est-à-dire 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. 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. Alors parce que cette phrase est vraie x est dans A et à cause de ce que dit la phrase x est hors de A !
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.
Cette collectivité sera en mathématiques appelée *collection*.
Dans le langage commun *ensemble* et *collection* sont synonymes, 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 il existe bien plus d'ordinaux que de nombres.
La récurrence définit le premier lot d'ordinaux, leur commencement.
La réunion des nombres vus comme ordinaux est un ordinal : elle est l'ensemble des entiers naturels !

Ch01 Théorie des ensembles

§01 Les propositions en mathématiques

1. Une **proposition** est une phrase affirmant quelque chose. 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".

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

Tableau 1 : négation

2. Une **proposition décidable** peut être 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.
3. Un **argument logique** est le sujet d'une proposition. Par exemple 10 est l'argument de $\mathcal{P}(10)$.
4. Selon le choix de valeur d'un argument logique appelé **paramètre logique** la vérité d'une proposition selon un autre argument appelé **variable logique** peut changer.
   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 d'un paramètre et 5 et 8 deux valeurs d'une variable.
   Généralisons : "pour b donné $\mathcal{P}(x\ ,\ b)$" est une propositipn qui a x comme **variable** et b comme **paramètre**.
5. Une **table de vérité** donne les vérités possibles d'une combinaison de propositions des variables.
6. La **négation** d'une proposition consiste à inverser sa vérité (tableau 1).
7. Une **proposition** sans variable est dite **close** ou **nulaire**. Exemple : $\mathcal{P}$ = "il existe un ensemble qui ne possède pas d'élément". Une proposition **unaire** a une variable, **binaire** deux variables, etc.
8. La **théorie des ensembles** sépare le sens des deux mots **ensemble** et **collection** qui sont synonymes dans la langue courante. Elle est motivée par le **paradoxe de Russel**. La proposition $\mathcal{P}(x) = (x \notin x)$ a cette propriété étrange : appelons A l'ensemble – si il existe – des x pour lesquels $\mathcal{P}$ soit vraie. Alors $(x \notin x)$ vraie $\Rightarrow x \in A$ parce que $\mathcal{P}(x)$ est vraie et $x \notin A$ parce que $\mathcal{P}(x)$ dit que x n'est pas dans A. La collection des x tels que $\mathcal{P}(x)$ vraie ne peut pas être un ensemble. La **théorie des ensembles précise les conditions nécessaires et suffisantes pour qu'une collection soit un ensemble ou pas**. Vocabulaire ensembliste : **un ensemble possède des éléments et une collection des pièces**.

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

Tableau 2 Inventaire logique pour une entrée et une sortie

9. 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 valeurs de x.
10. Soient au moins deux propositions, la vérité de l'une, nommée **sortie** dépendant de celle des autres nommée **entrées**. À droite des tableaux 2 et 3 on a numéroté des lignes.
11. Le tableau 2 montre les possibilité de combinaisons logiques entre une entrée et une sortie. Lignes 1 et 4 la sortie est indépendante de l'entrée. Ligne 2 la sortie suit l'entrée. Ligne 3 la sortie est la **négation** de l'entrée.
12. Le tableau 3 montre les possibilité de réponse entre une deux entrées et une sortie. Ligne 1, la sortie dit "c'est toujours faux".
    ♦ La ligne 16, la sortie dit "c'est toujours vrai".
    ♦ La ligne 9 est **la conjonction "et"** : la sortie dit "c'est vrai" que si les deux entrées disent "c'est vrai".
    ♦ La ligne 15 est **la conjonction "ou"** :la sortie dit "c'est vrai" que si au moins une des deux entrées dit "c'est vrai".
    ♦ La 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".
    ♦ La ligne 14 (en gris) est le "**si** $\mathcal{P}$ **alors** Q" qu'on écrit aussi $\mathcal{P} \Rightarrow Q$. La sortie ne dira "c'est faux" que si l'entrée $\mathcal{P}$ dit "c'est vrai" et l'entrée Q dit "c'est faux". De cette ligne on extrait le tableau 4.
    La case $\mathcal{P}$f , Qv ou Qf et $(\mathcal{P} \Rightarrow Q)$v n'est pas intuitive.
    Exemple : $\mathcal{P}(a\ ,\ x)$ = "x appartient à a" et $Q(a\ ,\ x)$ = "x est inclus dans a" définissent la phrase $(\mathcal{P} \Rightarrow Q)(a\ ,\ x)$ = "Si x appartient à a alors x est inclus dans a". Si comme paramètre a on choisit l'ensemble vide, on a $(\mathcal{P} \Rightarrow Q)(\varnothing\ ,\ x)$ = "Si x appartient à $\varnothing$ alors x est inclus dans $\varnothing$".
    Manifestement on a $\mathcal{P}(\varnothing\ ,\ x)$f, $Q(\varnothing\ ,\ x)$f mais $(\mathcal{P} \Rightarrow Q)(\varnothing\ ,\ x)$v.
    ♦ La ligne 12 est la ligne 14 avec inversion des rôles des deux entrées.

$\mathcal{P}$	f	v	f	v	
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

1. 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.
2. Une proposition admise sans démonstration est un **axiome**.
3. Une proposition ne pourra être que vraie ou fausse.
4. Une **proposition nullaire** ou **close** si sé vérité est indépendante du 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 $\mathcal{P}(x)$".
5. 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 z désigne une pièce de collection.
   Autre exemple : $\mathcal{P}(x)$, "$\exists x$ tel que $\forall y\ \mathcal{P}(x\ ,\ y\ ,\ u$ donné $,\ z)$".
6. **Les pièces d'une collection définie par une proposition sont celles qui la rendent vraie**.
7. Par convention dans la théorie des ensembles, **les pièces d'une collection sont des ensembles**.
8. **Tout ensemble est une collection**, mais **une collection n'est pas toujours un ensemble**.
9. **Si elle est un ensemble, une collection d'ensemble sera un ensembles d'ensembles**.
10. L'objectif de la théorie des ensembles et de définir à quelles conditions une proposition définit une collection ou un ensemble.
11. **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 eux-mêmes des ensembles.
12. **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 "b est **contenu dans** a" ou "b est **une partie** de a".
    Réflexivité : la proposition "si x appartient à a alors x appartient à a" est toujours vraie. 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**.

Pourquoi une théorie des ensembles ?

13. **Un paradoxe logique a induit la séparation des notions d'ensemble et de collection**.
    Rappel de l'al. 8 : *Le paradoxe de Russel* est la proposition "$x \notin x$". Soit – si il existe – l'ensemble a rendant cette proposition vraie. À cause de cette vérité, x appartient à a et, à cause de ce que dit la proposition, x n'appartient pas à a.

Axiomes de la théorie de Zermelo et Frænkel

14. 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.
15. **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 : $a = b$.
16. **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 ■
17. **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.
18. **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.
19. **Axiome 4 de substitution** :
    Hypothèse : "$\mathcal{E}(x\ ,\ y)$ et $\mathcal{E}(x\ ,\ y') \Rightarrow y = y'$ " est toujours vraie.

Postulat : la proposition "dans tout ensemble a il existe un x tel que $\mathcal{E}(x , y)$" définit un ensemble.
Note (al. 4) : les éléments de cet ensemble sont les y. Critère : a est affecté d'un "pour tout" et x 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

20. **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 "dans tout ensemble a il existe un x tel que $\mathcal{A}(x)$" 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.
Le postulat de l'axiome dit que la proposition "dans tout ensemble a, "$x \in a$ et $\mathcal{A}(x)$"" définit un ensemble ■
21. **Si une collection est incluse dans un ensemble, cette collection est un ensemble**.
Démonstration. Elle est immédiate.
22. **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

23. **Réunion** (voir al. 17).
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 $\cup_{k \in i} u_{ik}$.
24. **Intersection** (voir al. 21)
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 $\cap_{k \in i} u_k$.
25. **Complémentaire** (voir al. 19)
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

26. **Il existe un ensemble et un seul ne possédant aucun élément : l'ensemble vide**.
Démonstration. Ici, "$x \neq x$" joue le rôle de $\mathcal{A}(x)$.
Pour tout ensemble a la proposition unaire "dans a il existe un x tel que $x \neq x$" définit un ensemble.
Cet ensemble est vide.
Note : une proposition comme "x appartient à un ensemble vide $\Rightarrow \mathcal{P}(x)$" est toujours vraie quelle que soit la phrase $\mathcal{P}$.
27. **L'ensemble vide est unique**.
28. ***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 donc (axiome de l'égalité al. 15) $a = b$ ■
29. **Note** : parce que l'ensemble vide est unique il a son symbole, $\varnothing$.
30. **Il existe des ensembles ne possédant qu'un élément**. On les appelle **singletons**.
Démonstration.
L'axiome des parties dit que "$x \subset \varnothing$" définit un ensemble u.
L'ensemble vide est inclus dans lui-même donc $\varnothing \in u$.

Si $x \in u$ il faut que $x \subset \varnothing$, ce qui , vu que l'esemble vide est inclus dans n'importe quel ensemble, donne $x = \varnothing$.
L'ensemble u ne possède que l'élément $\varnothing$.
La proposition "pour a donné, $x = \varnothing$ et $y = a$", la partie après la virgule jouant dans al. 20 le rôle de $\mathcal{A}$, définit un ensemble v.
Si $y = a$ alors $y \in v$.
Si $y \in v$ alors $y = a$.
L'ensemble v possède donc un unique élément qui est a, ce qu'on écrit $u = \{a\}$. ■

31. **Il existe des ensembles paires**.
Démonstration.
L'axiome des parties dit que "$x \subset \{\varnothing\}$" définit un ensemble w.
Pour que $x \in w$ il faut que la proposition "$x \subset \{\varnothing\}$" soit vraie.
C'est le cas pour $x = \varnothing$ parce que l'ensemble vide est inclus dans n'importe quel ensemble.
C'est le cas pour $x = \{\varnothing\}$ par réflexivité de l'inclusion.
On n'a pas d'autre cas, car si $x \in w$ alors $x \subset \{\varnothing\}$ donc si $y \in x$ alors par définition du singleton $y = \varnothing$ donc on aurait $x = \varnothing$.
La proposition "pour a et b donnés, $x = \varnothing$ et $y = a$ ou b" qui joue le rôle de $\mathcal{A}$, définit un ensemble h.
Si $y = a$ ou b alors $x \in h$.
Si $x \in h$ alors $x = a$ ou b.
C'est pourquoi h est écrit$\{a , b\}$ ■

32. **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**.

33. **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 ■

34. **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

35. **Relations unaires** ce sont des propositions unaires (al. 7). On les appelle aussi des *domaines*.
36. **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 $f : x \rightarrow f(x)$.
37. **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).

38. **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.

39. **Domaine** : $\mathcal{R}$ est incluse dans le domaine $\mathcal{D}$ si "$\exists y$ tel que $\mathcal{R}(x , y) \Rightarrow \mathcal{D}(x)$" est toujours vraie.

40. *Relations d'équivalence* : $\mathcal{R}$ en est une si
$\mathcal{R}(x , y) \Rightarrow \mathcal{R}(y , x)$ (*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 $\mathcal{R}(y , y)$.
$\mathcal{R}(x , x)$ définit une collection qui est son *domaine de définition*.

41. *Relation d'ordre* : $\mathcal{O}$ en est une si
♦ $\mathcal{O}(x , y) \Rightarrow \mathcal{O}(x , x)$ 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*).

42. *Relation d'ordre strict* :
♦ $\mathcal{S}(x , y) \Rightarrow \mathcal{D}(x)$ 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*).

43. *Relation de bon ordre* : un ordre strict $\mathcal{B}$ de domaine $\mathcal{D}$ en est un si
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

44. **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 ■

45. **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 $\mathcal{D}$.

46. **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

47. **Produit d'ensembles**.
Soit une paire d'ensembles (a , b). La phrase "$x \in a$ et $y \in b$" définit une collection $\mathcal{C}$ 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 $\mathcal{C}$ 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 $\mathcal{C}$ est incluse dans un ensemble. On l'appelle produit de a par b et on l'écrit $a \times b$.

48. **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.

49. **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.

50. **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 $\prod_{k \in i} a_k$.

51. **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 entre ensembles

52. **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.

53. **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.

54. **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** $\mathcal{R}$.

55. **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

56. Une **opération** est un ensemble de couples $((x , y) , z)$ dans lequel chaque antécédent n'a qu'une image. Ici, l'antécédent de $((x , y) , z)$ est le couple (x , y) et l'image, appelée aussi **résultat** est zet dans l'antécédent (x , y), x est l'**opérande** et y l'**opérateur**.
57. 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 "$x * y = z$".
58. Une opération est **interne** à l'ensemble a si opérande, opérateur et résultat sont dans a. Elle est **externe** dans les autres cas.
59. Une **structure** est un ensemble ou ensemble d'ensembles dotés d'opérations. Exemple : l'ensemble des parties d'un ensemble donné doté de la réunion, du complémentaire et de la multiplication.

Soient * une opération

60. Si pour tout x, y et z de a et z de b on a $(x * y) * z = x * (y * z)$ l'opération est **associative**.
61. Si pour tout x et y de a on a $x * y = y * x$ l'opération est **commutative** sur a.
62. Un élément e est **neutre** sur a si pour tout x de a on a $e * x = x$ et $x * e = x$.
63. Soit e un élément neutre de a. Un élément y de a est **symétrique** de x par rapport à e si $x * y = e$ et $y * x = e$.

Soit * et ◊ deux opérations

64. Si pour tout x de a et tout y et z de b on a $x * (y \lozenge z) = (x * z) \lozenge (y * z)$ l'opération ◊ **distribue à droite** l'opération *.
65. Si pour tout x et y de a tout et z de b on a $(x * y) \lozenge z = (x \lozenge z) * (y \lozenge z)$ l'opération * **distribue à gauche** l'opération ◊.

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

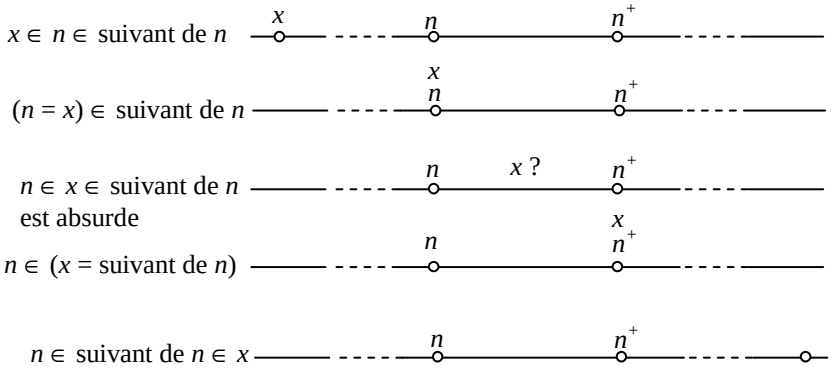
Tableau 1

   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 $\Diamond$ ou $x \in \underline{a}$ et alors $x \subset \underline{a}$ donc $x \subset \underline{a} \cup \{\underline{a}\}$, $\Diamond$ 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.

Autres propriétés tirées de la théorie des ordinaux

8. On appelle **précédent** d'un entier naturel donné n un entier naturel qui a n comme suivant.
9. **Le précédent d'un entier naturel, si il existe, est unique** : voir al.6.
10. **L'appartenance est un bon ordre des entiers naturels** : voir ord. al.1.
11. **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 $1 \in x$.
12. **Un entier naturel inclus dans un autre et distinct de cet autre lui appartient** : voir ord. al.1.

Nouvelles propriétés

13. **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 $x \in y$ ■
14. **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**.
15. ***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.
16. **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

17. **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 ■

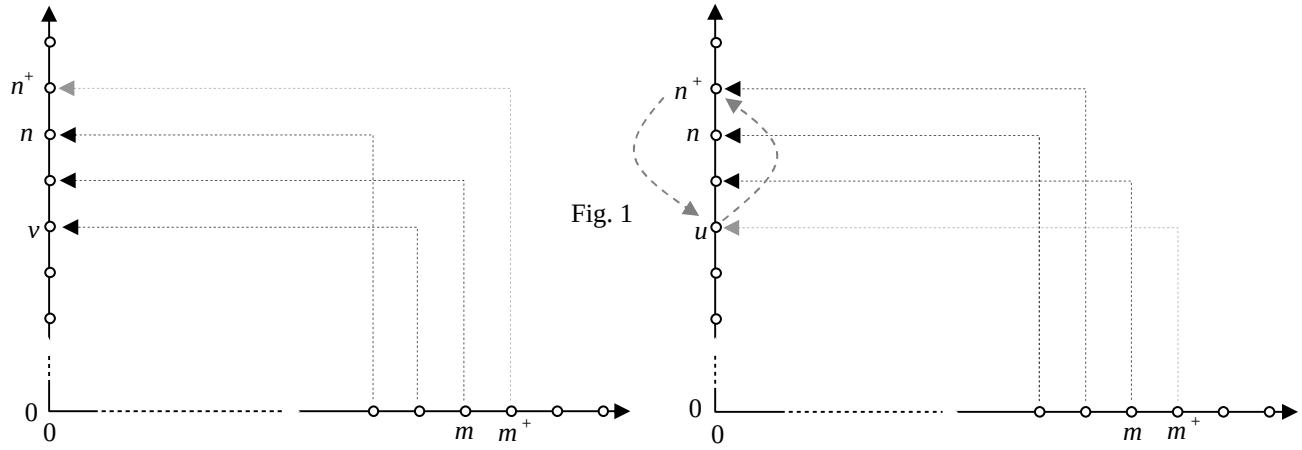


Fig. 1

18. **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).
19. Par définition, **un ensemble est fini et dénombrable si il a un cardinal**.

Opérations sur les nombres entiers naturels

Addition

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

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

22. **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 $x = 1 \ldots + 1$" ■

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

24. **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 ■

25. **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 ■

26. **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 ■

27. **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 ■

28. **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 ■

29. **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 $x \in a + b$ ■

30. **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

31. **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.
32. **On a équivalence logique entre la soustraction et l'inclusion**.
33. ***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 ■
34. **Toutes les règles de transformation de formules algébriques concernant addition et soustraction apprises à l'école peuvent être démontrées** (voir structures).
35. **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.
36. Soient deux ensembles E et F finis et dénombrables. Soient card E et card F leurs cardinaux.
37. **Le cardinal du complémentaire d'un ensemble dans un autre est la différence de leurs cardinaux**.
38. ***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

39. **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.
40. **Toutes les règles de transformation de formules algébriques concernant addition, soustraction et multiplication apprises à l'école peuvent être démontrées** (voir structures).
41. **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 … + 1) = a … + a ■
42. **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) ■
43. **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 ■
44. **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

45. **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**.
46. **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).
47. **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 $a \in b$ ■

48. **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 ■

49. **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 et diviseurs

50. **Tout entier naturel non nul est inclus dans ses multiples non nuls et contient ses diviseurs**.
51. ***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 $d \subset d\ m = a$ ■
52. **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, $a \in a\ b$.
53. **Puissances d'une base** :
54. ♦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 : $(a^m)^{\text{suivant de } n} = (a^m)^n\ a^m = a^{m\,n+m} = a^{m \cdot \text{suivant de } n}$.
55. **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
56. **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 $b^k \subset n \in b^{k+1}$■
57. 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) $q \in b$.

58. **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 $\boxed{n = b^k q_k \cdots + b^0 q_0 \text{ avec tous les } q_i \in b}$.
Compte tenu du procédé d'élaboration de cette décomposition, nous savons qu'elle est unique.

59. **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 $\underline{E}$.

60. **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.

61. **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 ■

62. **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.

63. **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

64. 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.

65. **Chaque nombre entier naturel peut être écrit comme un produit de nombres premiers**.
Démonstration. On étudie la phrase $\mathcal{P}r(n)$ = "tout entier inclus dans n est zéro, 1 ou une multiplication de nombres premiers".
Initiation : elle est triviale.
Hypothèse : $\mathcal{P}r(n)$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 ■

66. **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

67. **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 ■
68. **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 $\underline{S}$.
69. **Nombres premiers entre eux : par définition leur P.G.C.D vaut 1.**
70. **Théorème de Bezout** : a **et** b **sont premiers entre eux ⇔ il existe** u **et** v **tels que** $a\,u \pm b\,v = 1$.
71. ***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 $b = 1$ ■
72. **Théorème de Gauss** : **Si un nombre premier avec** a **divise le produit** $a\,b$**, alors ce nombre divise** b.
73. ***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 ■
74. **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 ■
75. **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$(a\,,\,b)$.

Une source sur la Toile

http://uel.unisciel.fr/mathematiques/arithmetique/arithmetique_ch03/co/apprendre_ch3_02.html

Bibliographie

Jean-Louis Krivine, *Théorie des ensembles*, Cassini, Paris, 1998
Daniel Perrin, *Nombres, mesure et géométrie*, Cassini, paris, 2011