§ 5. Ensembles finis et nombres entiers

Il est évidemment impossible de faire quoi que ce soit en Mathématiques sans utiliser la théorie des nombres entiers, et avant l'invention de la théorie des ensembles on la considérait comme le point de départ des Mathématiques : « Dieu nous a donné les nombres entiers, tout le reste est l'œuvre de l'homme », disait Kronecker.

On peut en fait aujourd'hui, à l'aide de la théorie des ensembles, construire les nombres entiers sans invoquer aucune divinité; l'idée de base, qu'on a de toute façon toujours enseignée aux enfants, est que les nombres entiers servent à « compter » les éléments des ensembles « finis », et que deux tels ensembles ont le même nombre d'éléments lorsqu'il existe une *bijection* du premier sur le second, et dans ce cas seulement (dans l'enseignement élémentaire on ne parle pas de « bijection » — on aligne les pommes au dessous des poires de façon à associer une pomme à chaque poire et vice-versa, ce qui est une méthode concrète simple pour construire une application bijective). Autrement dit, la notion d'entier est ce qui subsiste de la notion d'ensemble fini lorsque l'on considère comme identiques deux ensembles *équipotents* au sens du § 4, *Exemple* 3.

Lorsqu'il a commencé à édifier la théorie des ensembles, Cantor s'est aussitôt et principalement intéressé à cette question, mais sous un angle beaucoup plus général et difficile, à savoir celui qui consiste à « compter » les éléments d'un ensemble arbitraire, *fini ou non*, ce qui l'a conduit aux *nombres transfinis* qui permettent de distinguer les différentes espèces d'ensembles infinis. Ces « nombres » sont rarement utilisés dans la pratique élémentaire, mais il est difficile d'exposer raisonnablement la théorie des entiers ordinaires sans parler en même temps des autres.

La plupart des résultats énoncés dans ce § le seront sans démonstration, afin de réduire la longueur du texte (et parce que les démonstrations de certains théorèmes aux énoncés fort simples sont malheureusement difficiles, même dans le cadre « élémentaire » de la théorie des entiers ordinaires). Ce § n'est donc qu'un cadre dans lequel on pourrait, si on le désirait, insérer une étude complète et rigoureuse des nombres entiers.

Notons enfin que les entiers dont il s'agit ici sont des *objets mathématiques* au sens du § 0 (leur définition complète ferait intervenir les signes τ et $\square$ du n° 9 du § 0) qui servent de modèles abstraits aux nombres « concrets » avec lesquels on ne doit pas les confondre.

1. Ensembles équipotents

Rappelons (§ 4, *Exemple* 3) qu'un ensemble X est *équipotent* à un ensemble Y s'il existe une bijection de X sur Y. La relation

$$\text{X est équipotent à Y,}$$

qu'on note parfois

$$\text{Eq (X, Y),}$$

est une *relation d'équivalence.*

Cette relation possède un certain nombre de propriétés simples vis-à-vis des opérations de la théorie des ensembles.

Soient X, Y, X′, Y′ quatre ensembles, et supposons X équipotent à Y et X′ équipotent à Y′. Alors l'ensemble $X \times X'$ est équipotent à l'ensemble $Y \times Y'$ (car si f et f' sont des bijections de X sur Y et de X′ sur Y′, il est clair que $f \times f'$ est une bijection de $X \times X'$ sur $Y \times Y'$); de même l'ensemble

$$X^{X'}$$

des applications de X′ dans X (§ 2, *Remarque* 3) est équipotent à l'ensemble $Y^{Y'}$ des applications de Y′ dans Y; enfin, $X \cup X'$ est équipotent à $Y \cup Y'$ *pourvu que* X et X′ soient disjoints, ainsi que Y et Y′ : si f est une bijection de X sur Y, et f' une bijection de X′ sur Y′, on définit une bijection g de $X \cup X'$ sur $Y \cup Y'$ en posant

$$g(x) = \begin{cases} f(x) & \text{si} \quad x \in X \\ f'(x) & \text{si} \quad x \in X'. \end{cases}$$

A côté de ces propriétés d'énoncé simple et de démonstration immédiate, il existe d'autres résultats, d'énoncé également fort simple mais de démonstration incomparablement plus difficile; le plus frappant est le suivant, qui exprime intuitivement qu'étant donnés deux ensembles quelconques X et Y, on peut toujours « comparer » le « nombre » (sic) d'éléments de X au « nombre » d'éléments de Y :

THÉORÈME 1. *Soient* X *et* Y *deux ensembles. L'une au moins des deux assertions suivantes est vraie :*

X est équipotent à une partie de Y
Y est équipotent à une partie de X.

En outre, si ces deux assertions sont vraies simultanément, X *et* Y *sont équipotents.*

Bien que Cantor ait conjecturé cet énoncé dès ses premières recherches, la seconde partie de celui-ci n'a été démontrée qu'en 1897, par Bernstein, et la première, beaucoup plus difficile, qu'en 1904, par Zermelo. On trouvera le raisonnement de Bernstein dans l'*Exercice* 5 de ce §. Ajoutons que le Théorème 1 est non trivial (bien qu'intuitivement évident) même lorsque X et Y sont des ensembles finis; on conseille vivement au lecteur d'y réfléchir pour s'en convaincre (étant entendu qu'il s'agit de *démontrer* le résultat en question et non pas seulement de le rendre plausible).

2. *Le cardinal d'un ensemble*

Pour étendre au cas général la notion « de nombre » d'éléments d'un ensemble « fini », on a été amené avec Georg Cantor à attacher à chaque ensemble X un nouvel objet mathématique qu'on note

$$\text{Card}(X),$$

qu'on appelle le **cardinal** ou la **puissance** de X, et qui est défini de telle sorte que la condition suivante soit vérifiée : *pour que deux ensembles* X *et* Y *soient équipotents, il faut et il suffit que* Card (X) = Card (Y).

¶¶ *Remarque* 1. S'il existait un *ensemble* Ω dont les éléments soient tous les ensembles, il suffirait de prendre pour Card (X) la classe de X pour la relation d'équivalence Eq(X, Y). Mais on sait (§ 1, *Remarque* 5) qu'un tel ensemble Ω n'existe pas, en sorte qu'on ne peut utiliser ici les constructions du § 4. En fait, le cardinal d'un ensemble X est défini par la relation

$$\text{Card}(X) = \tau_Y(\text{Eq}(X, Y))$$

qui utilise les considérations du § 0, n° 9.

On dit qu'un objet mathématique x est un **nombre cardinal** s'il existe un ensemble X tel que $x = \text{Card}(X)$.

Parmi les nombres cardinaux figurent les suivants, qu'on désigne par les symboles 0, 1, 2,... mais qui ne sont naturellement pas les nombres 0, 1, 2,... « usuels » ou « naïfs » (en ce sens que les entiers « usuels » sont des idées métaphysiques déduites de l'expérience concrète, tandis que les entiers « mathématiques » sont des objets théoriquement définissables à l'aide des procédés du § 0) :

$$0 = \text{Card}(\emptyset), \tag{1}$$

cardinal de l'ensemble vide,

$$1 = \text{Card}(\{\emptyset\}), \tag{2}$$

cardinal de l'ensemble $\{\emptyset\}$ réduit au seul élément ∅,

$$2 = \text{Card}(\{\emptyset, \{\emptyset\}\}), \tag{3}$$

cardinal de l'ensemble dont les seuls éléments sont l'ensemble vide ∅ et l'ensemble $\{\emptyset\}$ dont le seul élément est l'ensemble vide ∅, etc... Étant donné un ensemble X, dire que Card (X) = 0 signifie que X est vide; dire que Card (X) = 1 signifie que X est un ensemble à un élément (i.e. que X est non vide et que les relations $x \in X$ et $y \in X$ impliquent $x = y$); dire que Card (X) = 2 signifie que X est un ensemble à deux éléments (i.e. qu'il existe $x \in X$ et $y \in X$ tels que l'on ait $x \neq y$ et tels que la relation $z \in X$ signifie $z = x$ ou $z = y$), etc... On reviendra plus loin (n° 4) sur ces nombres cardinaux particuliers.

Soient x et y deux nombres cardinaux; on écrit

$$x \leqslant y$$

lorsqu'il existe des ensembles X et Y tels que $x = \text{Card}(X)$, $y = \text{Card}(Y)$, et tels que X soit équipotent à une partie de Y — s'il en est ainsi pour un choix particulier de X et Y il en sera évidemment de même pour tout autre choix. Le Théorème 1 exprime alors que quels que soient x et y, on a toujours

$$x \leqslant y \quad \text{ou} \quad y \leqslant x; \tag{4}$$

et qu'en outre

$$x \leqslant y \quad \text{et} \quad y \leqslant x \quad \text{implique} \quad x = y. \tag{5}$$

Il est clair d'autre part que si x, y, z sont trois cardinaux, alors

$$x \leqslant y \quad \text{et} \quad y \leqslant z \quad \text{implique} \quad x \leqslant z; \tag{6}$$

car s'il existe une injection f d'un ensemble X dans un ensemble Y, et une injection g de Y dans un ensemble Z, il existe une injection de X dans Z, à savoir $g \circ f$.

La principale propriété de la relation $x \leqslant y$ entre cardinaux est exprimée par l'énoncé suivant (que nous admettrons) :

THÉORÈME 2. *Soit* E *un ensemble de cardinaux. Il existe un et un seul cardinal* a *possédant les propriétés suivantes:*

(i) *on a* $x \leqslant a$ *(resp.* $x \geqslant a$*) pour tout* $x \in E$;

(ii) *si un cardinal* b *est tel que l'on ait* $x \leqslant b$ *(resp.* $x \geqslant b$*) pour tout* $x \in E$, *on a* $b \geqslant a$ *(resp.* $b \leqslant a$*).*

Ce Théorème exprime que lorsqu'on a un *ensemble* E de cardinaux, il existe des cardinaux supérieurs (resp. inférieurs) à tous les éléments de E, et de plus que, parmi tous les cardinaux qui sont supérieurs (resp. inférieurs) à tous les éléments de E il en existe un qui est inférieur (resp. supérieur) à tous les autres. C'est donc le *plus petit* (resp. plus grand) cardinal a vérifiant $a \geqslant x$ (resp. $a \leqslant x$) pour tout $x \in E$. On l'appelle la **borne supérieure** (resp. la **borne inférieure**) de l'ensemble E, et on le désigne généralement par la notation

$$\sup(E) \qquad (\text{resp. } \inf(E))$$

ou une notation analogue.

Remarque 2. Le fait que dans l'énoncé précédant la lettre E désigne un *ensemble* de cardinaux est d'autant plus essentiel qu'il n'existe pas d'ensemble contenant tous les cardinaux (pas plus qu'il n'existe d'ensemble contenant tous les ensembles). Du reste, s'il existait un tel ensemble, le Théorème 2 appliqué à cet ensemble montrerait qu'il existe un cardinal a supérieur à *tous* les cardinaux — or c'est impossible, car on peut démontrer que pour tout cardinal a on a l'inégalité stricte

$$a < 2^a.$$

On voit donc, ici encore, que si l'on attribue au mot « ensemble » sa signification intuitive, on s'expose à des contradictions logiques.

Notons d'autre part que si E est un ensemble de cardinaux, les cardinaux $\sup(E)$ et $\inf(E)$ n'appartiennent pas nécessairement à E. Si par exemple on prend pour E l'ensemble $\mathbf{N}$ de tous les cardinaux finis (voir plus loin), $\sup(E)$ n'est autre que la puissance du dénombrable (n° 5) et par suite n'est pas dans E.

Cependant, lorsque E est un ensemble de cardinaux *finis* i.e. d'entiers naturels (cette notion sera définie au n° 4), on a toujours $\inf(E) \in E$. En effet comme $\inf(E)$ est inférieur à tout $x \in E$ il est clair que $\inf(E)$ est fini; si $\inf(E)$ n'appartenait pas à E, on aurait $\inf(E) < x$ et donc

$$\inf(E) + 1 \leqslant x$$

pour tout $x \in E$, de sorte que d'après la propriété (ii) du Théorème 2 on aurait la relation

$$\inf(E) + 1 \leqslant \inf(E),$$

ce qui est impossible puisque $\inf(E)$ est fini.

En d'autres termes, *si* E *est un ensemble d'entiers naturels il existe un élément de* E *qui est plus petit que tous les autres*, résultat qu'on utilise constamment dans la pratique.

3. *Opérations sur les cardinaux*

Soient x et y deux nombres cardinaux, et posons $x = \mathrm{Card}(X)$, $y = \mathrm{Card}(Y)$; on appelle **produit** de x par y le nombre cardinal

$$xy = \mathrm{Card}(X \times Y); \tag{7}$$

il est clair qu'il ne change pas si l'on remplace X (resp. Y) par un ensemble équipotent à X (resp. Y).

Cette opération vérifie les identités que voici :

$$xy = yx; \qquad x(yz) = (xy)z; \qquad 0x = 0; \qquad 1x = x. \tag{8}$$

Pour démontrer la seconde par exemple, il suffit d'observer que, si X, Y et Z sont trois ensembles, alors $X \times (Y \times Z)$ est équipotent à $(X \times Y) \times Z$, ce qui est clair si l'on associe à chaque élément $(a, (b, c))$ du premier l'élément $((a, b), c)$ du second.

¶ *Remarque* 3. Malgré ce qu'indique l'intuition, *il est faux* que

$$xz = yz \quad \text{implique} \quad x = y$$

même si $z \neq 0$. Pour obtenir un contre-exemple, admettons (voir plus loin) l'existence d'un ensemble $\mathbf{N}$ dont les éléments sont les entiers 0, 1, 2,...; prenons $z = \mathrm{Card}(\mathbf{N})$, $x = 1$, $y = 2$, en sorte que x est le cardinal d'un ensemble X réduit à un élément a, et y le cardinal d'un ensemble Y réduit à deux éléments

b et c. Tout revient à construire une *bijection* f de $X \times \mathbf{N}$ sur $Y \times \mathbf{N}$; pour cela, on pose

$$f(a, n) = \begin{cases} (b, p) & \text{si } n = 2p \text{ est pair} \\ (c, p) & \text{si } n = 2p + 1 \text{ est impair.} \end{cases}$$

Bien entendu, le fait que

$$xz = yz \quad \text{implique} \quad x = y \quad \text{si} \quad z \neq 0$$

est cependant vrai si x, y, z sont des entiers « naturels » (voir plus loin).

Soient maintenant x et y deux cardinaux, et choisissons deux ensembles *disjoints* X et Y tels que $x = \mathrm{Card}(X)$, $y = \mathrm{Card}(Y)$; on appelle **somme** de x et y le cardinal

$$x + y = \mathrm{Card}(X \cup Y) \qquad (\text{pour } X \cap Y = \emptyset); \tag{9}$$

on vérifie aussitôt qu'il ne dépend pas du choix de X et Y. On a les identités suivantes :

$$x + y = y + x; \qquad x + (y + z) = (x + y) + z; \qquad 0 + x = x. \tag{10}$$

La dernière par exemple exprime que, pour tout ensemble X, l'ensemble X est équipotent à $X \cup \emptyset$, ce qui est d'autant moins surprenant qu'on a même

$$X = X \cup \emptyset \ldots$$

Remarque 4. La définition de $x + y$ donnée ci-dessus suppose établi qu'on peut toujours trouver des ensembles X et Y *disjoints* tels que $x = \mathrm{Card}(X)$, $y = \mathrm{Card}(Y)$. Pour cela, posons $x = \mathrm{Card}(X')$, $y = \mathrm{Card}(Y')$, et prenons

$$X = X' \times \{a\}, \qquad Y = Y' \times \{b\}$$

avec $a \neq b$; alors X et Y sont équipotents à X' et Y', et disjoints car la relation $(x, a) = (y, b)$ exige $a = b$.

¶ *Remarque* 5. Ici encore, *il est faux* que la relation

$$x + z = y + z \qquad \text{implique} \qquad x = y;$$

par exemple, on peut fort bien avoir à la fois

$$x + x = x \qquad \text{et} \qquad x \neq 0;$$

pour cela, prenons $x = \mathrm{Card}(\mathbf{N})$ où $\mathbf{N}$ est l'ensemble (voir plus loin) des entiers 0, 1, 2,...; alors $x + x = \mathrm{Card}(Y)$ où Y est l'ensemble des couples (n, u) avec $n \in \mathbf{N}$ et $u = 0$ ou $u = 1$; on obtient une bijection f de Y sur $\mathbf{N}$ en posant

$$f(n, u) = \begin{cases} 2n & \text{si } u = 0 \\ 2n + 1 & \text{si } u = 1, \end{cases}$$

ce qui montre qu'on a bien $x + x = x$ dans ce cas...

On a d'autre part entre l'addition et la multiplication la relation de « distributivité »

$$x(y+z) = xy + xz; \tag{11}$$

elle signifie qu'étant donnés trois ensembles X, Y, Z, alors $X \times (Y \cup Z)$ est équipotent à $(X \times Y) \cup (X \times Z)$, ce qui est évident « géométriquement ».

Considérons enfin deux cardinaux x et y, et posons $x = \mathrm{Card}(X), y = \mathrm{Card}(Y)$; on pose alors

$$x^y = \mathrm{Card}(X^Y), \tag{12}$$

cardinal de l'ensemble de toutes les applications de Y dans X. Cette opération, appelée **exponentiation** des cardinaux, satisfait aux identités que voici :

$$x^{y+z} = x^y . x^z; \qquad (xy)^z = x^z y^z; \qquad (x^y)^z = x^{yz}; \qquad x^0 = 1; \qquad x^1 = x. \tag{13}$$

Pour établir par exemple la première, posons $x = \mathrm{Card}(X)$, $y = \mathrm{Card}(Y)$, $z = \mathrm{Card}(Z)$ et supposons Y et Z dispoints, de sorte que $y + z = \mathrm{Card}(Y \cup Z)$. Alors tout revient à montrer que les ensembles

$$X^{Y \cup Z} \qquad \text{et} \qquad X^Y \times X^Z$$

sont équipotents, i.e. à construire une bijection f du premier sur le second; pour cela soit u un élément du premier ensemble, i.e. une application de $Y \cup Z$ dans X; soient u_Y et u_Z ses restrictions à Y et Z; on pose alors $f(u) = (u_Y, u_Z)$, et le lecteur vérifiera facilement (en utilisant l'hypothèse que Y et Z sont disjoints) que f est bijective.

Remarque 6. Considérons un ensemble A à deux éléments, par exemple $A = \{0, 1\}$, et soit f une application d'un ensemble X dans A; pour déterminer f, il suffit évidemment de connaître l'ensemble

$$f^{-1}(0) \subset X$$

des x où $f(x) = 0$; on vérifie aussitôt que l'application $f \to f^{-1}(0)$ de A^X dans $\mathfrak{P}(X)$ ainsi définie est *bijective*. Il s'ensuit que

$$\mathrm{Card}(\mathfrak{P}(X)) = 2^{\mathrm{Card}(X)}.$$

Remarque 7. On peut montrer que, pour tout cardinal x, on a

$$x < 2^x$$

(i.e. $x \leq 2^x$ et $x \neq 2^x$). En particulier, si X est un ensemble, $\mathfrak{P}(X)$ *n'est pas* équipotent à X. Voir *Exercice* 1.

¶ *Remarque* 8. On peut définir non seulement la somme ou le produit de *deux* nombres cardinaux, mais plus généralement la somme ou le produit d'une

famille quelconque (même « infinie ») de tels nombres. On procède comme suit.

Tout d'abord soit $(X_i)_{i \in I}$ une famille d'ensembles; on appelle **produit cartésien** des X_i l'ensemble, noté

$$\prod_{i \in I} X_i,$$

dont les éléments sont toutes les familles $(x_i)_{i \in I}$ pour lesquelles on a $x_i \in X_i$ pour tout $i \in I$; cette notion généralise évidemment celle du § 2, n° 2, car si $I = \{1, 2\}$ et si l'on identifie une famille $(x_i)_{i \in I}$ au couple (x_1, x_2) on voit qu'on peut identifier le produit des X_i, $i \in I$, à l'ensemble $X_1 \times X_2$.

Cela dit, si $(x_i)_{i \in I}$ est une famille quelconque de cardinaux, et si l'on choisit pour chaque $i \in I$ un ensemble X_i tel que $x_i = \mathrm{Card}(X_i)$, on pose par définition

$$\prod_{i \in I} x_i = \mathrm{Card}\left(\prod_{i \in I} X_i\right).$$

Le cardinal ainsi obtenu s'appelle le **produit de la famille de nombres cardinaux** $(x_i)_{i \in I}$.

On définit de même la **somme de la famille de nombres cardinaux** $(x_i)_{i \in I}$ comme étant le cardinal noté

$$\sum_{i \in I} x_i$$

et défini par la relation

$$\sum_{i \in} x_i = \mathrm{Card}\left(\bigcup_{i \in I} X_i\right)$$

à condition que les ensembles X_i choisis soient *deux à deux disjoints* bien entendu.

Supposons par exemple $x_i = 1$ pour tout $i \in I$; on peut alors prendre $X_i = \{i\}$ pour tout $i \in I$, et la réunion de ces ensembles est I; on a donc

$$\mathrm{Card}(I) = \sum_{i \in I} x_i \qquad \text{avec} \qquad x_i = 1 \quad \text{pour tout} \quad i \in I; \tag{14}$$

intuitivement, cela signifie que tout nombre cardinal est une somme (généralement « infinie » ...) de termes tous égaux à 1, propriété bien connue des entiers usuels.

4. *Ensembles finis et entiers naturels*

Le résultat suivant est fondamental :

THÉORÈME 3. *Soit* X *un ensemble. Les propriétés suivantes sont équivalentes:*

a) Le seul ensemble contenu dans X *et équipotent à* X *est* X *lui-même.*

b) On a $\mathrm{Card}(X) \neq \mathrm{Card}(X) + 1$.

Supposons Card (X) = Card (X) + 1; en désignant par a un objet n'appartenant pas à X, il existe donc une bijection f de l'ensemble $X \cup \{a\}$ sur l'ensemble X; l'image de X par f est évidemment équipotente à X et strictement contenue dans X.

Supposons inversement X équipotent à une ensemble X′ strictement contenu dans X. On a alors, puisque $X = X' \cup (X - X')$,

$$\text{Card}(X) = \text{Card}(X) + \text{Card}(X - X');$$

mais Card $(X - X') \geqslant 1$ puisque $X - X'$ est non vide; il vient donc

$$\text{Card}(X) \geqslant \text{Card}(X) + 1 \geqslant \text{Card}(X)$$

et par suite Card (X) = Card (X) + 1 d'après le Théorème 1, ce qui achève la démonstration du Théorème 3.

On dit qu'un ensemble X est **fini** s'il possède les propriétés *a*) et *b*) de l'énoncé ci-dessus, et **infini** dans le cas contraire. De même, un cardinal x est **fini** si $x \neq x + 1$, et **infini** si $x = x + 1$. Un cardinal fini s'appelle aussi un **entier naturel**, et un cardinal infini un **nombre transfini.**

Les entiers naturels possèdent des propriétés fort simples (et que tout le monde connaît...). Tout d'abord, *si x et y sont des entiers naturels, il en est de même des cardinaux $x + y$, xy et x^y*; plus généralement, si $(x_i)_{i \in I}$ est une famille *finie* d'entiers naturels (on dit qu'une famille $(x_i)_{i \in I}$ est **finie** lorsque l'ensemble d'indices I est fini), alors les cardinaux (*Remarque* 8)

$$\prod_{i \in I} x_i \quad \text{et} \quad \sum_{i \in I} x_i$$

sont encore finis.

Si x est un entier naturel, tout cardinal y tel que $y \leqslant x$ est encore fini (autrement dit, *toute partie d'un ensemble fini est un ensemble fini*); et il existe alors un cardinal z et un seul tel que

$$x = y + z;$$

z est fini, s'appelle la **différence** entre x et y, et se note

$$z = x - y;$$

si $x = \text{Card}(X)$ et $y = \text{Card}(Y)$ avec $Y \subset X$, on a évidemment $z = \text{Card}(X - Y)$.

Enfin, quand il s'agit de cardinaux finis, les circonstances pathologiques examinées dans les *Remarques* 3 et 5 ne peuvent pas se produire; de façon précise, la relation

$$x + z = y + z \quad \text{implique} \quad x = y \quad \text{si } z \text{ est fini,}$$

et de même la relation

$$xz = yz \quad \text{implique} \quad x = y \quad \text{si } z \text{ est fini et non nul.}$$

Il va de soi que les cardinaux 0, 1, 2, ... définis plus haut sont finis.

On a fréquemment besoin de la propriété suivante :

THÉORÈME 4. *Soient* X *un ensemble et* f *une application de* X *dans* X. *Les propriétés suivantes sont équivalentes :*

a) *f est injective.*

b) *f est surjective.*

c) *f est bijective.*

Il suffit évidemment de montrer l'équivalence de *a*) et *b*). Si f est injective, f est une bijection de X sur une partie de X, à savoir $f(X)$, qui est donc équipotente à X; si X est fini on a donc $f(X) = X$, en sorte que *a*) implique *b*).

Supposons f surjective; il existe alors (§ 2, Théorème 4) une application h de X dans X telle que $f \circ h = j_X$, application identique; évidemment h est injective, donc surjective puisqu'on a déjà établi que *a*) implique *b*), donc bijective, et par suite f est l'application réciproque de h, et est donc injective, d'où le Théorème.

5. L'ensemble N des entiers naturels

Les considérations précédentes rendent évidente l'existence d'ensembles finis, puisque les ensembles

$$\emptyset, \quad \{\emptyset\}, \quad \{\emptyset, \{\emptyset\}\}, \quad \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots$$

sont finis — c'est du reste à ce moment précis qu'on voit les Mathématiques acquérir de la substance, en dépit du fait que tout repose sur la notion d'ensemble vide...

Par contre, l'*existence d'ensembles infinis* n'est pas claire, et l'est même si peu qu'en fait c'est l'un des *axiomes* des Mathématiques. Le lecteur qui trouverait ce point de vue étrange et contraire à l'intuition fera bien de se rappeler du fait qu'en Mathématiques on se propose de *démontrer logiquement* des assertions, et qu'en particulier le mot « existence » n'y a pas du tout le même sens qu'en Physique ou en Théologie.

THÉORÈME 5. *Soit* X *un ensemble infini. Tout ensemble fini est équipotent à une partie de* X.

Tout revient à montrer qu'on a $y \leqslant x$ pour tout cardinal fini y et tout cardinal infini x. Mais s'il n'en était pas ainsi on aurait $y \geqslant x$, et x serait fini comme on l'a vu au n° précédent.

THÉORÈME 6. *Il existe un ensemble* N *et un seul tel que la relation*

$$x \in \mathbf{N}$$

soit équivalente à la relation

$$x \text{ est un entier naturel.}$$

L'ensemble N *est infini.*

L'unicité de N est évidente d'après le Théorème 2 du § 1. L'existence de N provient du fait que, si l'on choisit un cardinal infini a (ce qui est possible en vertu de l'existence d'ensembles infinis), alors tout entier naturel x vérifie la relation $x < a$ comme on vient de le voir; il suffit donc de montrer que, pour tout cardinal a,

les cardinaux x tels que $x < a$ sont les éléments d'un *ensemble*, ce que nous admettrons (*).

Supposons enfin $\mathbf{N}$ fini, et pour chaque $n \in \mathbf{N}$ choisissons un ensemble X_n tel que Card $(X_n) = n$; puisque $\mathbf{N}$ et chaque X_n sont finis, il en est de même de

$$X = \bigcup_{n \in \mathbf{N}} X_n,$$

et comme chaque X_n est contenu dans X on voit donc que, si $\mathbf{N}$ était fini, il existerait un entier naturel $x = \text{Card}\,(X)$ tel que l'on ait $n \leqslant x$ pour tout n fini; mais alors, puisque x est fini, il en est de même de $x + 1$, on a donc $x + 1 \leqslant x$, mais aussi $x \leqslant x + 1$, donc $x = x + 1$, ce qui contredit le fait que x est fini. On aboutit donc à une contradiction en supposant $\mathbf{N}$ fini, ce qui achève la démonstration (sic).

On voit en résumé que les deux assertions suivantes :

il existe un ensemble infini

. il existe un ensemble dont les éléments sont les entiers naturels

sont *équivalentes*.

Le cardinal

$$\text{Card}\,(\mathbf{N})$$

s'appelle la **puissance du dénombrable** et on dit qu'un ensemble X est **dénombrable** s'il est équipotent à $\mathbf{N}$, autrement dit s'il existe une *bijection*

$$n \mapsto x_n$$

de l'ensemble des entiers naturels sur l'ensemble des éléments de X.

Exemple 1. L'ensemble des nombres fractionnaires (on suppose cette notion déjà acquise) est dénombrable. Il suffit pour le voir de montrer qu'on peut écrire les nombres fractionnaires (qui *à priori* dépendent de *deux* entiers) sous forme d'une suite illimitée contenant chacun de ces nombres une fois et une seule. On procède comme suit :

$$\frac{0}{1}\,;\quad \frac{1}{1}\,;\quad \frac{1}{2},\ \frac{2}{1}\,;\quad \frac{1}{3},\ \frac{3}{1}\,;\quad \frac{1}{4},\ \frac{2}{3},\ \frac{3}{2},\ \frac{4}{1}\,;\quad \frac{1}{5},\ \frac{5}{1}\,;\quad \ldots$$

on écrit d'abord les nombres p/q tels que $p + q = 1$, puis ceux pour lesquels $p + q = 2$ et qui n'ont pas déjà été écrits, puis ceux pour lesquels $p + q = 3$ et qui n'ont pas déjà été écrits, etc...

L'idée qu'il n'existe « pas plus » de nombres fractionnaires que de nombres entiers est à première vue contraire au bon sens; mais c'est précisément l'une des plus grandes réussites de Cantor que d'avoir pu disqualifier l'emploi du « bon sens » en Mathématiques.

Remarque 8. Le cardinal

$$2^{\text{Card}(\mathbf{N})}$$

(*) Posant $a = \text{Card}\,(A)$, les $x \leqslant a$ sont en « correspondance biunivoque » avec les classes d'équivalence dans $\mathfrak{P}(A)$ pour la relation Eq (X, Y) du n° 1; c'est ce qui explique (sic) pourquoi ces x restent dans un *ensemble*.

de l'ensemble $\mathfrak{P}(\mathbf{N})$ est strictement plus grand que Card $(\mathbf{N})$ d'après la *Remarque* 7; on l'appelle la **puissance du continu**. On peut démontrer que

$$2^{\text{Card}(\mathbf{N})} = \text{Card}\,(\mathbf{R})$$

où $\mathbf{R}$ est l'ensemble des nombres réels (ou des points d'une droite).

Depuis le début du siècle, on a cherché en vain à établir l'*hypothèse du continu*, à savoir que toute partie infinie de $\mathbf{R}$ est équipotente à $\mathbf{N}$ ou à $\mathbf{R}$. On a pu démontrer en 1939 (K. Gödel) que l'hypothèse du continu, comme l'axiome du choix (voir p. 64), était compatible avec les autres axiomes de la théorie des ensembles. Plus récemment (P. Cohen, 1963), on a en outre établi que l'hypothèse du continu et l'axiome du choix sont des assertions indépendantes l'une de l'autre (autrement dit : les axiomes de la théorie des ensembles, axiome du choix inclus, n'impliquent pas l'hypothèse du continu qui, de son côté, n'implique pas non plus l'axiome du choix). On trouvera un excellent exposé de ces questions dans P. Cohen, *Set Theory and the Continuum Hypothesis* (Benjamin, New York, 1966). Noter qu'en dépit de ces résultats impressionnants la question de la non-contradiction de la théorie des ensembles reste toujours ouverte.

6. *Le raisonnement par récurrence*

Le raisonnement par récurrence est fondé sur l'assertion que voici :

THÉORÈME 6. *Soit* R$\{n\}$ *une relation contenant une variable* $n \in \mathbf{N}$. *Supposons que la relation* R$\{0\}$ *soit vraie, et que la relation*

$$\text{R}\{n\} \quad \text{implique} \quad \text{R}\{n + 1\}$$

soit vraie pour tout $n \in \mathbf{N}$. *Alors la relation* R$\{n\}$ *est vraie pour tout* $n \in \mathbf{N}$.

Soit en effet E l'ensemble des $n \in \mathbf{N}$ tels que R$\{n\}$ soit vraie; on doit montrer que E $= \mathbf{N}$ ou, ce qui revient au même, que $F = \mathbf{N} - E$ est vide. Mais supposons F non vide; alors (*Remarque* 2) il existe un $a \in F$ tel que l'on ait $a \leqslant n$ pour tout $n \in F$; comme R$\{0\}$ est vraie par hypothèse, on a $0 \in E$ et par conséquent $a \geqslant 1$; donc $a = n + 1$ pour un $n \in \mathbf{N}$, et comme $n < a$ on ne peut avoir $n \in F$, de sorte que R$\{n\}$ est vraie; mais comme R$\{n\}$ implique R$\{n + 1\}$ par hypothèse, il s'ensuit que R$\{n + 1\}$, i.e. R$\{a\}$, est vraie, ce qui contredit le fait que $a \in F$. D'où le Théorème.

Dans la pratique on utilise fréquemment des variantes du Théorème 6, et en particulier celle qui consiste à remplacer l'hypothèse que R$\{n\}$ implique R$\{n + 1\}$ par la suivante :

$$\text{la conjonction des relations R}\{1\}, \ldots, \text{R}\{n\} \text{ implique R}\{n + 1\}$$

(il peut en effet arriver que, pour établir R$\{n + 1\}$, on ait à se servir non seulement de R$\{n\}$ mais de *toutes* les assertions précédant R$\{n + 1\}$).

Exemple 2. Pour tout entier n, notons E_n l'ensemble des entiers x tels que $x \leqslant n$; nous allons démontrer, en raisonnant par récurrence sur n, que l'on a

$$\text{Card}\,(E_n) = n + 1$$

pour tout n. En effet, pour $n = 0$ on a $E_n = \{0\}$ et par suite Card $(E_0) = 1$.

Il reste donc à établir que l'assertion relative à l'entier n implique l'assertion relative à l'entier $n+1$. Or soit $x \leqslant n+1$; on a soit $x \leqslant n$, et alors $x \in E_n$, soit

$$n < x \leqslant n+1,$$

et alors $x = n+1$ (voir ci-dessous). Donc $E_{n+1} = E_n \cup \{n+1\}$, en sorte que

$$\text{Card}\,(E_{n+1}) = \text{Card}\,(E_n) + 1;$$

cela montre évidemment que la relation $\text{Card}\,(E_n) = n+1$ implique, comme annoncé, la relation $\text{Card}\,(E_{n+1}) = n+2$. On a donc bien $\text{Card}\,(E_n) = n+1$ pour tout n.

On a fait usage ci-dessus du fait que la relation

$$n < x \leqslant n+1 \quad \text{implique} \quad x = n+1.$$

On l'établit par exemple comme suit. Soit A un ensemble tel que

$$\text{Card}\,(A) = n+1;$$

comme $x \leqslant n+1$, il existe un ensemble X tel que $x = \text{Card}\,(X)$ et $X \subset A$; comme $n < x$, il existe un ensemble B tel que

$$n = \text{Card}\,(B), \qquad B \subset X, \qquad B \neq X.$$

On a

$$n+1 = \text{Card}\,(A) = \text{Card}\,(B) + \text{Card}\,(A - B) = n + \text{Card}\,(A - B)$$

et donc $\text{Card}\,(A - B) = 1$, en sorte que le complément de B dans A se réduit à un élément. Comme X contient B et est distinct de B, on a donc $X = A$, et par suite $x = n+1$ comme annoncé.

7. *Analyse combinatoire*

Dans ce qui suit, étant donné un entier naturel n, on appelle **ensemble à n éléments** tout ensemble X tel que $\text{Card}\,(X) = n$.

THÉORÈME 7 (Principe des bergers). *Soit f une application d'un ensemble X dans un ensemble Y. On suppose que Y est un ensemble à q éléments, que pour tout $y \in Y$ l'ensemble $f^{-1}(y) \subset X$ est à p éléments, et que f est surjective. Alors X est un ensemble à pq éléments.*

Désignons par F un ensemble à p éléments choisi une fois pour toutes, et, pour chaque $y \in Y$, choisissons une bijection u_y de l'ensemble F sur l'ensemble $f^{-1}(y)$. Définissons une application

$$u : Y \times F \to X$$

en posant

$$u(y, z) = u_y(z) \quad \text{pour} \quad y \in Y \quad \text{et} \quad z \in F;$$

on vérifie aussitôt (en tenant compte du fait que f est surjective) que u est bijective. Donc

$$\text{Card}\,(X) = \text{Card}\,(Y \times F) = \text{Card}\,(Y).\text{Card}\,(F) = qp,$$

ce qui achève la démonstration.

THÉORÈME 8. *Soient X un ensemble à p éléments et Y un ensemble à q éléments. Alors l'ensemble des applications de Y dans X est à p^q éléments.*

Ce Théorème est en fait (n° 3) la définition de p^q. Bien entendu, pour lui donner tout son intérêt, il faut vérifier que, lorsqu'il s'agit d'entiers naturels, l'exponentiation des cardinaux se réduit à l'opération que tout le monde connait. Or les formules (13) du n° 3 montrent entre autres que

$$n^1 = n, \qquad n^0 = 1, \qquad n^{p+q} = n^p n^q;$$

on a donc

$$n^2 = n^{1+1} = n^1 n^1 = n.n; \qquad n^3 = n^{2+1} = n^2 n^1 = n.n.n, \quad \text{etc...}$$

Remarque 9. Prenons pour Y l'ensemble des entiers i tels que $1 \leqslant i \leqslant q$; une application de Y dans X est encore une famille $(x_i)_{i \in Y}$ d'éléments de X; une telle famille s'écrit souvent sous la forme

$$(x_i)_{1 \leqslant i \leqslant q},$$

et s'appelait autrefois un **arrangement des éléments de X pris q à q**. Le Théorème 8 affirme donc que, si X est à p éléments, le nombre de ces arrangements est p^q.

THÉORÈME 9. *Soient X un ensemble à p éléments et Y un ensemble à q éléments. Supposons $p \leqslant q$. Alors le nombre des injections de X dans Y est*

$$\frac{q!}{(q-p)!}$$

où, pour tout entier naturel n, on pose

$$n! = 1.2.3\ldots n \quad \text{si } n \neq 0, \qquad \text{et} \qquad n! = 1 \quad \text{si } n = 0.$$

Si $p = 0$, l'ensemble X est vide, et il y a une seule injection de X dans Y, de sorte que le Théorème est vrai dans ce cas. Il reste donc (Théorème 6) à montrer que s'il est vrai pour un entier p il est aussi vrai pour $p+1$.

Supposons donc $\text{Card}\,(X) = p+1$ et $\text{Card}\,(Y) = q \geqslant p+1$. Choisissons une fois pour toutes un $a \in X$ et posons $X' = X - \{a\}$, de sorte que X' possède p éléments. Soit I l'ensemble des injections de X dans Y. On peut définir une application

$$u : I \to Y$$

en posant

$$u(f) = f(a) \quad \text{pour toute} \quad f \in I,$$

et il est clair que cette application de I dans Y est surjective (autrement dit, pour tout $b \in Y$ il existe une application *injective* f de X dans Y telle que $f(a) = b$). Pour un $b \in Y$ donné, considérons les $f \in I$ telles que $f(a) = b$; posant $Y' = Y - \{b\}$, une telle f induit évidemment une injection f' de X' dans Y', et réciproquement toute injection f' de X' dans Y' peut être complétée en une injection f de X dans Y telle que $f(a) = b$. On voit donc, en utilisant l'hypothèse de récurrence, que le nombre de $f \in I$ telles que $u(f)$ soit donné est

$$\frac{(q-1)!}{[(q-1)-(p-1)]!} = \frac{(q-1)!}{(q-p)!};$$

comme u applique I *sur* l'ensemble Y à q éléments, le principe des bergers montre donc que

$$\text{Card (I)} = q \cdot \frac{(q-1)!}{(q-p)!},$$

et comme

$$q! = q.(q-1)!$$

la démonstration est achevée.

COROLLAIRE. *Le nombre des permutations d'un ensemble* X *à n éléments est n !*

Une permutation est une bijection de X dans X (§ 2, n° 8), mais comme X est fini les permutations de X sont aussi les injections de X dans X (Théorème 4). Il reste alors à appliquer le Théorème en prenant $Y = X$, et $p = q = n$, et à observer que

$$(n-n)! = 0! = 1.$$

Le nombre n ! se lit **factorielle** n. On a les relations

$$0! = 1, \quad 1! = 1, \quad 2! = 2, \quad 3! = 6, \quad 4! = 24, \quad 5! = 120, \quad \ldots$$

THÉORÈME 10. *Soient* X *un ensemble à n éléments et p un entier inférieur ou égal à n. Le nombre d'ensembles à p éléments contenus dans* X *est*

$$\frac{n(n-1)\ldots(n-p+1)}{p!} = \frac{n!}{p!\,(n-p)!}.$$

Soit E un ensemble à p éléments choisi une fois pour toutes. Désignons par I l'ensemble des injections de E dans X, et par P l'ensemble des parties à p éléments de X.

Pour toute $f \in$ I, il est clair que f(E) est une partie à p éléments de X. On peut donc définir une application

$$u : \text{I} \to \text{P}$$

en posant

$$u(f) = f(\text{E}).$$

Cette application est *surjective*, car toute partie Y à p éléments de X est équipotente à E, donc est l'image de E par une application injective de E dans X.

Nous allons maintenant compter les $f \in$ I telles que f(E) = Y soit une partie donnée de X. Si f_0 est une telle application, on obtient les autres en composant f_0 avec une permutation arbitraire de l'ensemble E : si $f(\text{E}) = f_0(\text{E})$, alors pour tout $x \in$ E il existe un et un seul $s(x) \in$ E tel que $f(x) = f_0(s(x))$, et s est évidemment une permutation de E. Ainsi, en associant à chaque permutation s de E l'application $f = f_0 \circ s$ de E dans X, on obtient une *bijection* de l'ensemble des permutations de E sur l'ensemble des $f \in$ I telles que f(E) = Y.

Les $f \in$ I telles que f(E) = Y soit donné sont donc au nombre de p ! (Corollaire du Théorème 9). D'après le principe des bergers, on a donc

$$\text{Card (I)} = p! \text{ Card (P)};$$

donc

$$\text{Card (P)} = \frac{\text{Card (I)}}{p!} = \frac{n!}{p!\,(n-p)!}$$

d'après le Théorème 9, et ceci achève la démonstration.

On pose habituellement

$$\frac{n!}{p!\,(n-p)!} = \binom{n}{p}$$

et on appelle ces entiers les **coefficients du binôme** pour des raisons qui apparaîtront plus loin (§ 8, n° 4).

Remarque 10. Une partie à p éléments d'un ensemble X est aussi ce qu'on appelait autrefois une **combinaison des éléments de** X **pris** p **à** p. Les ouvrages traditionnels définissent une telle combinaison comme étant une « suite »

$$x_1, \cdots, x_p$$

d'éléments de X, deux à deux distincts, et en convenant qu'on regarde comme identiques deux telles suites lorsqu'elles ne diffèrent que par l'ordre des facteurs. Il est naturellement beaucoup plus clair d'utiliser le langage de la théorie des ensembles.

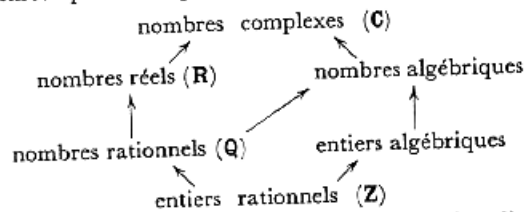
8. *Entiers rationnels* (*)

En plus des entiers naturels, on a besoin en Mathématiques des entiers « de signe quelconque » ou **entiers rationnels**. Nous allons indiquer sommairement comment on peut les définir.

(*) Ce n° a pour but de justifier des résultats avec lesquels le lecteur est déjà familier; il peut donc être négligé en première lecture.

Indiquons en passant que les entiers de signe quelconque (que nous appelons, comme le font tous les mathématiciens, des *entiers rationnels*) sont généralement appelés, dans l'enseignement secondaire français, des « entiers algébriques » (de même qu'on y appelle « nombres algébriques » les nombres de signe quelconque, entiers ou non, que nous appelons, à nouveau comme tous les mathématiciens, des *nombres réels*). Ces divergences de terminologie n'auraient aucune importance si les mathématiciens n'utilisaient déjà dans un tout autre sens les expressions « entier algébrique » et « nombre algébrique » que l'on définira plus loin (§ 11, *Exemple* 11 ainsi que les *Exercices* du § 26).

Les relations d'inclusion entre les diverses notions de nombre qu'on rencontre le plus souvent sont schématisées par le diagramme suivant



où chaque flèche indique que l'ensemble de départ est contenu dans l'ensemble d'arrivée.

L'idée fondamentale est que, si x et y sont deux entiers naturels, il existe un entier rationnel z tel que

$$x + z = y$$

— c'est précisément pour rendre la soustraction possible dans tous les cas qu'on a inventé les entiers négatifs. Si donc on suppose déjà construit l'ensemble $\mathbf{Z}$ des entiers rationnels on peut définir une application

$$D : \mathbf{N} \times \mathbf{N} \to \mathbf{Z},$$

d'ailleurs *surjective*, par

$$D(x, y) = x - y.$$

Il est clair de plus que la relation

$$D(x,y) = D(x',y') \quad \text{équivaut à} \quad x + y' = x' + y.$$

Ces remarques expliquent la construction qui suit (et dans laquelle nous ne supposerons plus, évidemment, le problème résolu...).

Pour construire l'ensemble $\mathbf{Z}$ des entiers rationnels, on part de l'ensemble $\mathbf{N} \times \mathbf{N}$ des couples d'entiers naturels; et, sur cet ensemble, on définit une *relation d'équivalence* R en déclarant que deux couples (x, y) et (x', y') d'entiers naturels sont équivalents mod R si et seulement si l'on a

$$x + y' = x' + y;$$

la vérification du fait que R est une relation d'équivalence est triviale, et laissée au lecteur. Ceci fait, on pose, par définition,

$$\mathbf{Z} = (\mathbf{N} \times \mathbf{N})/\mathrm{R},$$

et on appelle **entier rationnel** tout élément de l'ensemble $\mathbf{Z}$.

Il faut encore, bien entendu, définir les opérations algébriques sur les entiers rationnels, et montrer comment on peut considérer les entiers naturels comme des entiers rationnels particuliers. Notons pour cela D l'application canonique (§ 4, n° 2) de $\mathbf{N} \times \mathbf{N}$ sur $\mathbf{Z}$; pour définir la **somme** et le **produit** de deux entiers rationnels z et z', on choisit des couples (x, y), $(x', y') \in \mathbf{N} \times \mathbf{N}$ tels que

$$z = D(x, y), \qquad z' = D(x', y'),$$

et on pose (*)

$$z + z' = D(x + x', y + y')$$
$$zz' = D(xx' + yy', xy' + x'y);$$

on peut aussi, si l'on préfère, appliquer le Théorème 3 du § 4 en prenant, dans les

(*) Cette construction s'explique par le fait qu'on désire parvenir finalement aux relations

$$(x - y) + (x' - y') = (x + x') - (y + y'),$$
$$(x - y).(x' - y') = (xx' + yy') - (xy' + x'y).$$

notations du Théorème 3 en question,

$$X = Y = Z = \mathbf{N} \times \mathbf{N}, \qquad R = S = T,$$

et pour application $f : X \times Y \to Z$ soit celle qui est donnée par

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

soit celle qui est donnée par

$$f((x, y), (x', y')) = (xx' + yy', xy' + x'y).$$

Il faut vérifier la condition *a*) du Théorème 3; cela veut dire qu'on doit prouver que les relations

$$(x, y) \equiv (u, v) \bmod R \qquad \text{et} \qquad (x', y') \equiv (u', v') \bmod R$$

impliquent

$$(x + x', y + y') \equiv (u + u', v + v') \bmod R$$

et

$$(xx' + yy', xy' + x'y) \equiv (uu' + vv', uv' + u'v) \bmod R$$

Vu la définition de R, on est donc ramené à établir que, quels que soient les entiers naturels $x, y, x', y', u, v, u', v'$, les relations

$$x + v = y + u \qquad \text{et} \qquad x' + v' = y' + u'$$

impliquent les relations

$$x + x' + v + v' = y + y' + u + u'$$

et

$$xx' + yy' + uv' + u'v = xy' + x'y + uu' + vv',$$

ce qui est évidemment facile.

La somme et le produit étant définis dans l'ensemble $\mathbf{Z}$, on établit ensuite les propriétés fondamentales de ces opérations, à savoir :

(I) on a $x + y = y + x$, $x + (y + z) = (x + y) + z$ quels que soient $x, y, z \in \mathbf{Z}$, et il existe un élément 0 de $\mathbf{Z}$ et un seul tel que $x + 0 = x$ pour tout $x \in \mathbf{Z}$.

(II) quels que soient $x, y \in \mathbf{Z}$, il existe un $z \in \mathbf{Z}$ et un seul tel que $x + z = y$.

(III) on a $xy = yx$, $x(yz) = (xy)z$ quels que soient $x, y, z \in \mathbf{Z}$, et il existe un élément 1 de $\mathbf{Z}$ tel que $1x = x$ pour tout x.

(IV) on a $x(y + z) = xy + xz$ quels que soient $x, y, z \in \mathbf{Z}$.

Montrons par exemple comment on établit (IV). On choisit dans $\mathbf{N} \times \mathbf{N}$ des couples tels que

$$x = D(x', x''), \qquad y = D(y', y''), \qquad z = D(z', z'');$$

on a alors

$$x(y+z) = \mathrm{D}(x', x'').\mathrm{D}(y'+z', y''+z'') \\ = \mathrm{D}[x'(y'+z') + x''(y''+z''), x'(y''+z'') + x''(y'+z')]$$

et

$$xy + xz = \mathrm{D}(x'y' + x''y'', x'y'' + x''y') + \mathrm{D}(x'z' + x''z'', x'z'' + x''z') \\ = \mathrm{D}(x'y' + x''y'' + x'z' + x''z'', x'y'' + x''y' + x'z'' + x''z'),$$

et on obtient (IV) en comparant les résultats obtenus.

Il reste enfin à identifier chaque entier naturel n à un entier rationnel — à savoir à l'entier rationnel

$$\mathrm{D}(n, 0);$$

on vérifie facilement que l'application $n \to \mathrm{D}(n, 0)$ de **N** dans **Z** ainsi définie est *injective*, et compatible avec les opérations algébriques définies sur les entiers naturels d'une part, et sur les entiers rationnels d'autre part. De cette façon, il n'y a aucun inconvénient à considérer **N** comme une partie de **Z**.

Ceci fait, on observe que, quels que soient les entiers naturels x et y, on a

$$\mathrm{D}(x, y) = \mathrm{D}(x, 0) - \mathrm{D}(y, 0)$$

(la **différence** $a - b$ entre deux entiers rationnels a et b étant, par définition, l'unique entier rationnel c tel que $a = b + c$: voir la propriété (II) ci-dessus) ; en effet

$$\mathrm{D}(x, y) + \mathrm{D}(y, 0) = \mathrm{D}(x + y, y)$$

en sorte que tout revient à vérifier que $\mathrm{D}(x + y, y) = \mathrm{D}(x, 0)$, i.e. que

$$(x + y) + 0 = y + x,$$

ce qui est clair. En convenant de poser dorénavant

$$\mathrm{D}(x, 0) = x \quad \text{pour tout } x \in \mathbf{N},$$

la relation précédente s'écrit donc

$$\mathrm{D}(x, y) = x - y$$

et montre que *tout entier rationnel est différence de deux entiers naturels.*

Soit z un entier rationnel; l'entier rationnel $0 - z$ se note

$$-z$$

et s'appelle l'**opposé** de z; il est donc caractérisé par la relation

$$z + (-z) = 0,$$

et il est clair que

$$-z = y - x \quad \text{si} \quad z = x - y.$$

Ceci dit, écrivons $z = x - y$ avec $x, y \in \mathbf{N}$; deux cas sont possibles.

Il peut arriver que $x \geqslant y$; alors il existe un $z' \in \mathbf{N}$ tel que $x = y + z'$ et comme cette relation est aussi valable dans **Z** on voit, en vertu de l'unicité de la soustraction dans **Z**, que l'on a dans ce cas $z = z'$, autrement dit $z \in \mathbf{N}$.

Dans le cas où l'on a au contraire $y \geqslant x$, la relation $-z = y - x$ montre que $-z \in \mathbf{N}$.

Autrement dit, *pour tout entier rationnel z, on a soit $z \in \mathbf{N}$, soit $-z \in \mathbf{N}$.* Les entiers rationnels z tels que $z \in \mathbf{N}$ sont dits **positifs,** les autres sont dits **négatifs.** Si x et y sont deux entiers rationnels, on écrit

$$x \leqslant y$$

lorsque $y - x$ est positif, de sorte que les $z \in \mathbf{Z}$ positifs sont caractérisés par la relation

$$z \geqslant 0.$$

On démontre facilement que, dans l'ensemble **Z**, la relation $x \leqslant y$ possède les propriétés « évidentes », à savoir que les relations

$$x \leqslant y \quad \text{et} \quad y \leqslant z \quad \text{impliquent} \quad x \leqslant z,$$

que la relation

$$x = y \quad \text{équivaut à} \quad x \leqslant y \quad \text{et} \quad y \leqslant x,$$

que quels que soient x et y on a

$$\text{soit } x \leqslant y \text{ soit } y \leqslant x,$$

que la relation

$$x \leqslant y \quad \text{équivaut à} \quad x + z \leqslant y + z,$$

et que la relation

$$x \leqslant y \quad \text{équivaut à} \quad xz \leqslant yz \quad \text{si} \quad z > 0, \quad \text{à} \quad xz \geqslant yz \quad \text{si} \quad z < 0.$$

Il nous arrivera parfois par la suite d'utiliser d'autres propriétés de **Z** que celles que nous venons d'énoncer; nous les démontrerons complètement toutes les fois qu'elles ne seront pas « évidentes ». Pour le moment, on conseille au lecteur de ne pas trop chercher à approfondir les considérations du présent n° : elles n'ont pour but que de justifier des résultats avec lesquels il est déjà familier, et sans lesquels il ne saurait être question de faire des Mathématiques. C'est quand il voudra approfondir sa compréhension des théories exposées dans cet ouvrage que le lecteur aura intérêt à écrire en détail toutes les démonstrations que nous avons escamotées dans le présent n°.

9. *Nombres rationnels*

Après avoir construit des entiers naturels, puis des entiers rationnels, il est nécessaire de construire les **nombres rationnels** i.e. les quotient p/q de deux entiers rationnels p et q, avec $q \neq 0$. L'ensemble de ces entiers rationnels se note

Q.

Toutefois, nous n'exposerons pas ici la construction de $\mathbf{Q}$ à partir de $\mathbf{Z}$; elle s'effectue par des méthodes analogues à celles qu'on a utilisées pour passer de $\mathbf{N}$ à $\mathbf{Z}$; mais surtout, la construction de $\mathbf{Q}$ à partir de $\mathbf{Z}$ est un cas particulier d'un procédé beaucoup plus général, qui sera exposé en détail au § 29, et dont nous aurons de toute façon besoin dans d'autres cas.

On conseille donc au lecteur, soit de prendre pour argent comptant les propriétés « évidentes » des nombres rationnels (qui du reste n'interviendront jamais dans le présent ouvrage qu'à titre d'exemple), soit de passer directement au § 29 après avoir lu les §§ 6, 7 et 8 qui sont indispensables à la compréhension du § 29. Il va de soi que, pour le débutant, il sera de beaucoup préférable d'utiliser la première méthode, à condition de ne pas se faire d'illusions (i.e. de ne pas considérer comme triviales des propriétés qu'on ne sait pas démontrer immédiatement).

Groupes, anneaux, corps

Tout le monde sait que faire de l'Algèbre, c'est *calculer*; mais alors que l'Algèbre classique consistait à calculer sur des nombres, le développement des Mathématiques aux XIX^e^ et XX^e^ siècles a obligé de plus en plus les mathématiciens (et les physiciens) à calculer sur des objets mathématiques de nature extrêmement variée, et à isoler des situations qu'on rencontre constamment. On a ainsi été conduit aux notions « abstraites » de groupe, d'anneau et de corps. La première s'est présentée en Géométrie (groupes de transformations : rotations, translations, transformations homographiques, etc...), en Arithmétique (étude par Gauss, Dirichlet, Hermite des « unités des formes quadratiques » — il s'agit, un polynôme homogène du second degré à coefficients entiers étant donné, de trouver toutes les substitutions linéaires à coefficients entiers qu'on peut effectuer sur les variables sans changer la forme du polynôme en question), en Algèbre (groupes de Galois dans la théorie des équations algébriques) et en Analyse (groupes de Lie, fonctions automorphes), sans parler de la Physique (groupe de Lorentz); c'est dire que la notion de groupe, actuellement, n'est guère moins importante en Mathématiques que celles d'ensemble ou de fonction. Quant aux notions de corps et d'anneau, c'est avant tout l'étude au siècle dernier de la théorie des nombres algébriques qui a conduit les mathématiciens (et principalement Dedekind) à les formuler, mais on les utilise maintenant dans toutes les branches de l'Algèbre et de l'Arithmétique, et dans certaines branches de l'Analyse où elles permettent bien souvent l'emploi d'une terminologie commode.

On trouvera ensuite un § sur les « nombres complexes », dont l'importance en Algèbre proprement dite est minime, mais sans lesquels il est pratiquement impossible de faire quoi que ce soit en Analyse. La méthode choisie pour les introduire sert, en Algèbre « supérieure », à effectuer des constructions formidablement plus générales, et c'est sa principale justification.

EXERCICES

Il est parfaitement utopique d'espérer apprendre des Mathématiques, si élémentaires ou si supérieures soient-elles, sans résoudre des Exercices.

Les Exercices qu'on trouvera dans ce livre sont de trois sortes. Certains sont des illustrations pratiques ou même numériques des théories exposées dans le texte; le lecteur débutant ne pourra pas acquérir la technique du calcul sans résoudre une partie appréciable des Exercices de ce genre. D'autres apportent au texte des compléments théoriques élémentaires; en les étudiant, le lecteur s'habituera à manipuler le langage et les modes de raisonnements utilisés dans le texte; ceux de ces Exercices qui ne sont pas *très* faciles sont précédés d'un signe ¶. Enfin, la dernière catégorie est constituée par des Exercices qui apportent au texte des compléments importants et difficiles; ils sont destinés uniquement aux étudiants déjà avancés qui s'intéressent vraiment aux Mathématiques; ces Exercices sont précédés de deux ou même trois signes ¶.

Nous ne saurions trop insister enfin sur le fait que résoudre un Exercice ne consiste pas seulement à se convaincre, à l'aide d'un « brouillon » fait à la hâte, du fait qu'on en a à peu près compris la solution; si cette méthode est admissible pour les Exercices de calcul numérique, il faut par contre s'efforcer de *rédiger intégralement* les Exercices plus théoriques, où l'on doit construire de véritables démonstrations. De cette façon, et uniquement de cette façon, l'étudiant parviendra à acquérir un langage clair et correct, et à utiliser les termes techniques dans leur sens propre, ce qui, en Mathématiques, est le signe le plus certain de la compréhension d'un sujet.

¶ **1.** Soient X un ensemble et f une application de X dans l'ensemble $\mathfrak{P}(X)$ des parties de X. On note A l'ensemble des $x \in X$ vérifiant la relation $x \notin f(x)$. Montrer qu'il n'existe aucun $x \in X$ tel que $A = f(x)$. En déduire qu'il n'existe aucune application *surjective* de X dans $\mathfrak{P}(X)$, et que par suite on a

$$x < 2^x$$

pour tout nombre cardinal x (G. Cantor).

¶ **2.** Soit $(f_n)_{n \in \mathbf{N}}$ une suite d'applications de l'ensemble **N** dans lui-même; on définit une application f de **N** dans **N** en posant

$$f(n) = f_n(n) + 1 \quad \text{pour tout } n \in \mathbf{N}.$$

Montrer qu'il n'existe aucun entier $p \in \mathbf{N}$ tel que $f = f_p$. En déduire que l'ensemble de toutes les applications de **N** dans **N** est non dénombrable (G. Cantor).

¶ **3.** La réunion d'une infinité dénombrable d'ensembles dénombrables est un ensemble dénombrable (s'inspirer de la méthode utilisée dans l'*Exemple* 1 du n° 5).

4. Soit I l'ensemble des nombres réels compris entre 0 et 1; on représentera chaque $x \in I$ par un développement décimal illimité (pouvant se terminer par une infinité de chiffres 0). Soit $(x_n)_{n \in \mathbf{N}}$ une suite d'éléments de I; on forme un nombre $x \in I$ comme suit: la n^e décimale de x est égale à 1 si la n^e décimale de x_n est différente de 1, et est égale à 2 si la n^e décimale de x_n est égale à 1. Montrer qu'on a $x \neq x_n$ pour tout n. En conclure que l'ensemble I (et *à fortiori* l'ensemble **R** de tous les nombres réels) est non dénombrable (G. Cantor).
Préciser l'analogie entre ce raisonnement et celui de l'*Exercice* 2 ci-dessus.

¶¶ **5.** Soient f une bijection d'un ensemble X sur une partie Y_1 d'un ensemble Y, et g une bijection de Y sur une partie X_1 de X; on se propose de montrer que X et Y sont équipotents (Bernstein). Pour cela, on définit des parties A_n de X et B_n de Y en posant

$$A_0 = X - X_1, \qquad B_1 = f(A_0), \qquad A_1 = g(B_1), \qquad B_2 = f(A_1), \qquad A_2 = g(B_2), \ldots$$

puis on définit une application h de X dans Y comme suit : étant donné un $x \in X$, on prend

$$h(x) = f(x) \quad \text{si} \quad x \in \bigcup_{n \in \mathbf{N}} A_n,$$

et dans le cas contraire (de sorte qu'alors $x \in X_1$) on prend

$$h(x) = g^{-1}(x).$$

Montrer que h est une bijection de X sur Y.

6. Soient E un ensemble fini à h éléments, et n un entier naturel. On considère les applications f de E dans **N** telles que la somme des h nombres $f(x)$, $x \in E$, soit au plus égale à n. Montrer que les applications f considérées sont en nombre égal à

$$\binom{n+h}{h}.$$

7. Montrer que, pour entier n, la somme des coefficients du binôme $\binom{n}{p}$ est égale à 2^n.

¶ **8.** Démontrer la relation

$$\binom{n}{0}\cdot\binom{n}{p} + \binom{n}{1}\cdot\binom{n-1}{p-1} + \binom{n}{2}\cdot\binom{n-2}{p-2} + \cdots + \binom{n}{p}\cdot\binom{n-p}{0} = 2^p \cdot \binom{n}{p}.$$

(On cherchera d'abord, dans un ensemble X à n éléments, combien il existe de parties à p éléments qui contiennent un ensemble à k éléments donné d'avance).

¶ **9.** Soient p et n des entiers tels que $1 \leqslant p \leqslant n$, et $S_{n,p}$ le nombre des applications surjectives de l'ensemble $\{1, 2, \ldots, n\}$ dans l'ensemble $\{1, 2, \ldots, p\}$. Montrer qu'on a

$$p^n = S_{n,p} + \binom{p}{1} S_{n,p-1} + \binom{p}{2} \cdot S_{n,p-2} + \cdots + \binom{p}{p-1}.$$

En déduire que

$$S_{n,p} = p^n - \binom{p}{1}\cdot(p-1)^n + \binom{p}{2}\cdot(p-2)^n - \cdots + (-1)^{p-1}\binom{p}{p-1}.$$

Simplifier ce résultat pour $p = 2, 3$.

¶¶¶ **10.** Soient E et F deux ensembles finis, et $x \mapsto A(x)$ une application de E dans l'ensemble des parties de F. Pour qu'il existe une *injection* f de E dans F vérifiant

$$f(x) \in A(x) \qquad \text{pour tout } x \in E,$$

il faut et il suffit qu'on ait

$$\text{Card}\left(\bigcup_{x \in H} A(x)\right) \geqslant \text{Card}\,(H)$$

pout toute partie H de E. (Ce résultat est généralement connu sous le nom de *lemme des mariages*).

11. En utilisant le fait que, dans tout ensemble (fini ou infini) d'entiers naturels, il existe un entier plus petit que tous les autres, démontrer les résultats classiques que voici :

a) Tout entier $n \geqslant 2$ possède au moins un diviseur premier (on rappelle qu'un **nombre premier** est un entier $p \geqslant 2$ n'admettant pas d'autres diviseurs positifs que 1 et p).

b) Étant donnés deux entiers naturels a et b, avec $b \geqslant 1$, il existe des entiers naturels q et r tels que

$$a = bq + r, \qquad r < b,$$

et les entiers q et r sont uniques (**division euclidienne**, ou division avec reste, de a par b).

12. Démontrer que l'ensemble des nombres premiers est infini.

¶ **13.** L'ensemble des nombres premiers de la forme $4n - 1$ (resp. $6n - 1$) est infini.
[Ce résultat est un cas particulier du *théorème de la progression arithmétique* de Dirichlet, à savoir que si a et b sont des entiers premiers entre eux, il existe une infinité de nombres premiers de la forme $an - b$. La démonstration générale du théorème de Dirichlet, l'un des plus célèbres de toute la Théorie des Nombres, ne peut pas se faire à l'heure actuelle par des procédés purement arithmétiques; toutes les démonstrations connues (à commencer par celle de Dirichlet lui-même, qu'on n'a pas pu substantiellement simplifier) utilisent des méthodes appartenant à l'Analyse, ou qui s'en inspirent directement.]

14. (Numération de base q). On choisit un entier naturel $q \geqslant 2$.

a) Soit x un entier naturel non nul. Montrer qu'il existe un et un seul entier $n \geqslant 0$ tel que

$$q^n \leqslant x < q^{n+1},$$

puis un et un seul entier a_n vérifiant

$$0 \leqslant a_n \leqslant q - 1, \qquad a_n q^n \leqslant x < (a_n + 1)q^n.$$

b) Montrer que, pour tout entier naturel x, il existe une et une seule suite d'entiers $a_0, a_1, \ldots, a_r, \ldots$ vérifiant les conditions suivantes :

1) on a $0 \leqslant a_r \leqslant q - 1$ pour tout $r \geqslant 0$.

2) les entiers r tels que $a_r \neq 0$ sont en nombre fini.

3) on a

$$x = a_0 + a_1 q + a_2 q^2 + \cdots + a_r q^r + \cdots$$

[la dernière somme, qui comporte en apparence une infinité de termes, a un sens à cause de la condition (2) imposée aux a_r]. Montrer que l'entier n de la question *a*) est le plus grand entier tel que $a_n \neq 0$, et que le nombre a_n défini à la question *a*) est égal au nombre a_n de la question *b*). La suite

$$a_n a_{n-1} \ldots a_0$$

(il ne s'agit pas d'un produit !) s'appelle le **développement de x dans le système de numération de base q**.

c) Trouver le développement du nombre 718 dans le système de numération binaire (i.e. à base $q = 2$).

d) Soit x un nombre rationnel positif, non nécessairement entier. Montrer qu'il existe une et une seule suite de nombres entiers

$$\ldots, a_n, a_{n-1}, \ldots, a_0, a_{-1}, a_{-2}, \ldots$$

vérifiant les conditions suivantes :

1) on a $0 \leqslant a_r \leqslant q - 1$ pour tout $r \in \mathbf{Z}$.

2) les entiers *positifs* r tels que $a_r \neq 0$ sont en nombre fini.

3) pour tout $r \in \mathbf{Z}$, on a

$$a_r q^r + a_{r+1} q^{r+1} + \cdots \leqslant x < q^r + a_r q^r + a_{r+1} q^{r+1} + \cdots$$

On dit alors que

$$a_n a_{n-1} \ldots a_0, a_{-1} a_{-2} \ldots a_{-r} \ldots$$

(où n est le plus petit entier naturel tel que l'on ait $a_r = 0$ pour tout $r > n$) est le développement de x dans le système de numération de base q.

e) Pour qu'une famille d'entiers a_n ($n \in \mathbf{Z}$) vérifiant les conditions 1) et 2) de la question précédente constitue le développement d'un nombre rationnel dans le système de numération de base q, il faut et il suffit qu'il existe un entier rationnel r et un entier naturel $k \geqslant 1$ tels que l'on ait

$$a_{n-k} = a_n \qquad \text{pour tout } n \leqslant r$$

(périodicité des développements des nombres rationnels)

15. Le développement de la Recherche Spatiale purement pacifique lui ayant permis de réaliser quelques différences intéressantes, le Président-Directeur-Général de la *Société Anonyme pour l'Exploitation Financière de la Physique Purement Théorique*, Commandeur de la Légion d'Honneur, achète en Basse-Normandie un domaine de 200 hectares à raison de 8 000 F l'hectare. Inspiré par cet exemple, un ouvrier plombier-zingueur attaché à l'établissement en question, et gagnant 800 F par mois, décide de placer chaque année un dixième de son salaire en Bons du Trésor rapportant 4 % l'an. Combien d'années devra-t-il travailler avant d'être en mesure d'acquérir en Basse-Normandie un domaine de 200 hectares pour y finir paisiblement ses jours ? (On tiendra compte des intérêts composés mais on négligera l'effet des dévaluations possibles de la monnaie).

16. D'après le journal *Le Monde* du 21 Juillet 1954, les dépenses occasionnées par la guerre d'Indochine sont fournies par le tableau suivant (il s'agit de milliards d'anciens francs) :

1946 :	101,8	1949 :	177,3	1952 :	427,6
1947 :	131,3	1950 :	258,3	1953 :	403,5
1948 :	136,3	1951 :	321	1954 :	428.

Vérifier sur cet exemple les propriétés fondamentales de l'addition (associativité et commutativité).

17. En Novembre 1954, on comptait en Algérie 1 230 000 Européens et 8 300 000 indigènes. A la même date, l'Université d'Alger comptait 4 548 étudiants européens et 557 indigènes. Calculer, à une unité près par défaut, le rapport entre les chances d'un Européen et celles d'un indigène d'accéder à l'Enseignement Supérieur.