Entiers naturels et relatifs

Daniel PERRIN

L'objectif de ce texte est de donner les éléments pour traiter l'exposé de CAPES numéro 9 (2006) intitulé : *Propriétés axiomatiques de* $\mathbf{N}$. *Construction de* $\mathbf{Z}$.

1 Entiers naturels : les axiomes de Peano

Ce paragraphe présente les axiomes des entiers naturels proposés par Peano en 1889 et montre comment on peut déduire de ces axiomes toutes les propriétés des entiers.

1.1 Les axiomes

1.1 Axiomes. (Axiomes de Peano) *Il existe un ensemble* $\mathbf{N}$ *dont les éléments sont appelés les entiers naturels, un élément* $0 \in \mathbf{N}$ *appelé zéro et une application* $s : \mathbf{N} \to \mathbf{N}$, *dite application successeur, vérifiant les propriétés suivantes :*
1) 0 *n'est le successeur d'aucun entier (en d'autres termes* 0 *n'est pas dans l'image de* s*),*
2) deux nombres entiers qui ont même successeur sont égaux (autrement dit, l'application s *est injective),*
3) si une partie A *de* $\mathbf{N}$ *contient* 0 *et est stable par* s *(i.e. vérifie* $s(A) \subset A$*), alors* A *est égale à* $\mathbf{N}$. *(Principe de récurrence*[1]*)*

[1]Attention à l'usage du mot principe. Dans les rapports du jury de CAPES jusqu'à 2005 inclus on trouve la phrase : *D'autre part, il est à noter que beaucoup de candidats parlent du"principe de récurrence" sans avoir conscience qu'il s'agit en fait d'un théorème dont d'ailleurs bon nombre de candidats sont difficilement capables de fournir un énoncé correct. Rappelons à ce sujet qu'une théorie mathématique ne contient pas de"principe" (contrairement à une théorie physique) mais uniquement des axiomes, des définitions et des théorèmes.* L'exemple des axiomes de Peano, où le principe de récurrence est un axiome, montre que le jury dit une bêtise en affirmant que la récurrence est un théorème (mais il faut être prudent avant de traiter les membres du jury d'imbéciles !) Par ailleurs, le mot "principe", s'agissant de la récurrence est traditionnel et des auteurs renommés comme N. Bourbaki ou J.-L. Krivine l'utilisent, sans parler des manuels. L'opprobre que le jury

On pose $1 = s(0)$, $2 = s(1)$, $3 = s(2)$, $4 = s(3)$, etc. Nous allons montrer, à partir des axiomes de Peano, les propriétés de $\mathbf{N}$. Les démonstrations sont faciles et beaucoup seront laissées au lecteur.

1.2 Proposition. *Tout entier $a \neq 0$ est le successeur d'un entier.*

Démonstration. C'est le principe de récurrence. On considère la partie $A = s(\mathbf{N}) \cup \{0\}$. On a $0 \in A$ et $A \subset \mathbf{N}$ donc $s(A) \subset s(\mathbf{N}) \subset A$. Par l'axiome 3), A est égale à $\mathbf{N}$. Si a est différent de 0, comme il est dans A, il est dans $s(\mathbf{N})$, donc est un successeur.

1.3 *Remarque.* On notera que, dans cette théorie, on ne dit pas comment est construit $\mathbf{N}$. En revanche, en théorie des ensembles on peut construire $\mathbf{N}$ à partir de la notion de cardinal. On peut même le construire uniquement à partir de l'ensemble vide[2]. Dans cette construction, les entiers sont des ensembles, précisément : $0 = \emptyset$, puis $1 = \{\emptyset\}$ (l'ensemble dont l'unique élément est l'ensemble vide), puis $2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$, $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}$, etc.

1.2 L'addition

1.2.1 Définition

1.4 Proposition-Définition. (Définition de l'addition) *Soit $n \in \mathbf{N}$. Il existe une application $m \mapsto n + m$ de $\mathbf{N}$ dans $\mathbf{N}$ définie en posant :*
• $n + 0 = n$,
• $n + s(p) = s(n + p)$ *pour tout $p \in \mathbf{N}$.*
Cette application définit une opération sur $\mathbf{N}$, c'est-à-dire une application de $\mathbf{N} \times \mathbf{N}$ dans $\mathbf{N}$ qui au couple (n, p) associe $n + p$. Cette opération est appelée **addition** *et l'entier $n + p$ est appelé* **somme** *de n et p.*

Démonstration. Il faut vérifier[3] que l'ensemble A des m pour lesquels l'application est définie est $\mathbf{N}$ tout entier. Comme A contient 0 et est stable par successeur, cela résulte du pricipe de récurrence.

1.5 *Remarque.* On a, par définition, $n + 1 = n + s(0) = s(n + 0) = s(n)$. L'application successeur est donc l'application qui consiste à ajouter 1.

---

semble jeter sur ce mot me semble donc excessif. Il indique justement que la récurrence n'a pas un statut univoque : selon la théorie elle peut être un axiome ou un théorème.

[2]Il faut disposer de deux axiomes, l'un qui assure que, si A est un ensemble, $\{A\}$ aussi et l'autre qui permet de dire que si A, B sont des ensembles, $A \cup B$ aussi.

[3]Pour des précisions sur la définition d'une application par récurrence, voir le livre d'Arnaudiès et Fraysse (Dunod).

La remarque précédente permet de reformuler le principe de récurrence :

1.6 Théorème. Principe de récurrence, deuxième forme.
Soit $P(n)$ une propriété de l'entier $n \in \mathbf{N}$. On suppose qu'on a les deux assertions suivantes :
1) $P(0)$ est vraie, (initialisation)
2) pour tout $n \in \mathbf{N}$, $P(n)$ implique $P(n+1)$, (hérédité).
Alors $P(n)$ est vraie pour tout $n \in \mathbf{N}$.

Démonstration. Il suffit d'appliquer l'axiome 3) à l'ensemble A des n qui vérifient la propriété $P(n)$.

1.2.2 Propriétés

1.7 Proposition. *On a les propriétés suivantes :*
1) L'addition est associative : on a, pour tous $a, b, c \in \mathbf{N}$, $a + (b + c) = (a + b) + c$.
2) L'addition est commutative : on a, pour tous $a, b \in \mathbf{N}$, $a + b = b + a$.
3) On a, pour tous $a, b, c \in \mathbf{N}$, $a + b = a + c \Longrightarrow b = c$ (règle de simplification).
4) Si $a + b$ est nul, a et b sont nuls.

Démonstration. Montrons 1). On fixe $a, b \in \mathbf{N}$ et on applique le principe de récurrence à c. Soit C l'ensemble des c qui vérifient la propriété. On a $0 \in C$. En effet, par définition, on a $a + (b + 0) = a + b$ et $(a + b) + 0 = a + b$. Supposons que c soit le successeur de p et que p vérifie la propriété. On a $a + (b + c) = a + (b + s(p)) = a + s(b + p) = s(a + (b + p)$ par définition de l'addition, et cette quantité est égale à $s((a + b) + p)$ puisque p est dans C. Par ailleurs, on a $(a + b) + c = (a + b) + s(p) = s((a + b) + p)$ par définition de l'addition. On voit qu'on a bien $c \in C$, de sorte que C est stable par successeur, donc égal à $\mathbf{N}$, cqfd.

Pour le point 2), on commence par montrer deux lemmes.

1.8 Lemme. *Pour tout $a \in \mathbf{N}$, on a $a + 0 = 0 + a = a$.*

Démonstration. On raisonne par récurrence sur a.

1.9 Lemme. *Pour tout $a, p \in \mathbf{N}$ on a $s(p) + a = s(p + a)$.*

Démonstration. On raisonne par récurrence sur a. Précisément, on considère l'ensemble A des a qui vérifient, pour tout $p \in \mathbf{N}$, $s(p) + a = s(p + a)$. Par définition de l'addition, 0 est dans A. Soit $q \in A$. On a donc, pour tout p, $s(p) + q = s(p + q)$. Montrons que $a = s(q)$ est aussi dans A. On

calcule $s(p) + a = s(p) + s(q) = s(s(p) + q)$ (par définition de l'addition) et c'est encore $s(s(p + q))$ par l'hypothèse de récurrence. Par ailleurs, on a $s(p + a) = s(p + s(q)) = s(s(p + q))$, par définition encore : cqfd.

On peut alors prouver le point 2). On raisonne par récurrence sur b en appelant B l'ensemble des $b \in \mathbf{N}$ qui vérifient, pour tout $a \in \mathbf{N}$, $a+b = b+a$. On a $0 \in B$ par 1.8. Supposons $p \in B$ et montrons $s(p) \in B$. On calcule $a + s(p) = s(a + p) = s(p + a) = s(p) + a$ (successivement, par définition, hypothèse de récurrence et 1.9). On a gagné.

Le point 3), après commutation, se montre par récurrence sur a.

Enfin, le point 4) est évident en raisonnant par l'absurde : si, par exemple, b n'est pas nul, c'est un successeur par 1.2, donc aussi $a + b$ par définition de l'addition et c'est absurde (axiome 1).

1.10 *Remarques.*
1) On notera qu'on a, pour tout $a \in \mathbf{N}$, $s(a) = a + 1 = 1 + a$.
2) Le premier théorème de l'arithmétique c'est : *deux et deux font quatre*, c'est-à-dire $2 + 2 = 4$. En effet, on a $4 = s(3) = 3 + 1 = (2 + 1) + 1 = 2 + (1 + 1) = 2 + 2$ en vertu de l'associativité.

1.3 La multiplication

Nous définissons maintenant la multiplication des entiers.

1.11 Proposition-Définition. *On définit une loi de multiplication sur* $\mathbf{N}$*, notée* $\times$ *(ou notée sans signe opératoire lorsqu'il n'y a pas de risque de confusion), en posant :*
• $n \times 0 = 0$ *pour tout* $n \in \mathbf{N}$*,*
• $n \times s(p) = (n \times p) + n$*.*
1) La multiplication est associative : $a \times (b \times c) = (a \times b) \times c$ *et commutative :* $a \times b = b \times a$*.*
2) La multiplication est distributive par rapport à l'addition : on a pour tous $a, b, c \in \mathbf{N}$ *:* $a \times (b + c) = a \times b + a \times c$ *et* $(a + b) \times c = a \times c + b \times c$*.*
3) On a, pour tout n*,* $n \times 1 = n$*.*
4) Si $a \times b$ *est nul,* a *ou* b *est nul.*
5) Si on a $a \times b = a \times c$ *avec* $a \neq 0$*, on a* $b = c$*.*

Démonstration. La preuve se fait essentiellement par récurrence. Elle est analogue[4] à celles de 1.4 et 1.7 et est laissée au lecteur.

[4]Mais pas tout à fait évidente. Il vaut mieux montrer 2) avant 1). Pour 5) on peut aussi utiliser l'ordre total, cf. 1.15.1.

1.4 La relation d'ordre

1.4.1 Définition

1.12 Définition. *Soient $p, q \in \mathbf{N}$. On dit que q est supérieur ou égal à p, et on écrit $q \geq p$, s'il existe $n \in \mathbf{N}$ tel que $q = n + p$. On dit que q est strictement supérieur à p si on a $q \geq p$ et $q \neq p$ et on note $q > p$.*

1.13 *Remarque.* On définit aussi les relations opposées : $p \leq q \Longleftrightarrow q \geq p$ et $p < q \Longleftrightarrow q > p$.

1.14 Proposition. *La relation $\geq$ est une relation d'ordre i.e. :*
i) elle est réflexive : on a $p \geq p$,
ii) elle est antisymétrique : si on a $p \geq q$ et $q \geq p$ on a $p = q$,
iii) elle est transitive : si on a $r \geq q$ et $q \geq p$ on a $r \geq p$.

Démonstration. Cela résulte aussitôt des propriétés de l'addition.

1.4.2 Propriétés

On a la proposition suivante :

1.15 Proposition.
1) Si p, q sont des entiers on a $p \geq q$ ou $q \geq p$ (l'ordre est total).
2) On a l'équivalence, pour tous $a, b, c \in \mathbf{N}$: $a + b \geq a + c \Longleftrightarrow b \geq c$.
3) Il n'existe pas d'entier n tel que $0 < n < 1$.
4) Il n'existe pas d'entier n supérieur à tous les autres.
5) Si on a $q \geq p$, on a $n \times q \geq n \times p$.

Démonstration. Pour le point 1), on considère, pour p fixé, l'ensemble :

$$A = \{q \in \mathbf{N} \mid q \leq p \quad \text{ou} \quad q \geq p\}$$

et on montre que cet ensemble est égal à $\mathbf{N}$ en utilisant le principe de récurrence. Il est clair que 0 est dans A car on a $0 \leq p$. Si q est dans A il y a deux cas. Si on a $q < p$, on a $p = n + q$ avec $n \neq 0$, donc $n = s(m) = m + 1$. On a alors $p = m + 1 + q = m + s(q)$, donc encore $s(q) \leq p$. Si on a $q \geq p$, on a $q = n + p$, donc $s(q) = q + 1 = n + 1 + p = (n + 1) + p$ et on a donc $s(q) \geq p$.

Le point 2) est clair en utilisant la règle de simplification.

Montrons 3). Si on a $n < 1$, cela signifie qu'il existe $p \neq 0$ avec $1 = n + p$. Comme p est non nul, il existe q tel que $p = s(q) = q + 1$ et on a donc

$1 = n + q + 1$. Par simplification on en déduit $0 = n + q$, donc $n = 0$ par 1.7.4.

Le point 4) est clair en considérant n et son successeur et la dernière assertion est évidente.

1.4.3 Le bon ordre

Les deux propriétés suivantes sont fondamentales :

1.16 Théorème.
1) Toute partie non vide de $\mathbf{N}$ *a un plus petit élément (on dit que* $\mathbf{N}$ *est* **bien ordonné***).*
2) Toute partie **finie** *non vide de* $\mathbf{N}$ *a un plus grand élément.*

Démonstration. 1) Il revient au même de montrer que si A est une partie qui n'a pas de plus petit élément, A est vide. Pour cela on montre par récurrence la propriété $P(n)$: pour tout $i \leq n$, $i \notin A$. Il est clair que $P(0)$ est vraie (sinon 0 serait le plus petit élément de A). Supposons que $P(n)$ est vraie et montrons $P(n+1)$. On sait qu'aucun des entiers $0, 1, \ldots, n$ n'est dans A et il s'agit de voir que $n+1$ n'y est pas non plus. Mais, sinon, $n+1$ serait le plus petit élément de A, contrairement à l'hypothèse.

2) On raisonne par récurrence sur le cardinal de A : $n = |A|$. Pour $n = 1$, A a un unique élément qui est bien le plus grand. Supposons la propriété établie pour $|A| = n \geq 1$ et passons à $n+1$. Soit a_0 le plus petit élément de A (qui existe par 1)) et soit $B = A - \{a_0\}$. Comme on a $|B| = n$, B admet un plus grand élément qui est aussi le plus grand élément de A, cqfd.

1.17 *Remarque.* En fait, le principe de récurrence est équivalent au bon ordre (de sorte que si l'on met celui-ci dans les axiomes la récurrence devient un théorème comme le dit le jury).

Pour le voir on utilise ce qu'on appelle un raisonnement par l'absurde et minimalité. On raisonne d'abord par l'absurde en supposant que $P(n)$ n'est pas vraie pour tous les entiers n et on considère l'ensemble des contre-exemples :

$$C = \{n \in \mathbf{N} \mid P(n) \text{ n'est pas vraie}\}.$$

Par hypothèse, C est non vide et donc, par 1.16.1, il admet un plus petit élément m (qui est donc le contre-exemple minimal : voilà la minimalité). On a $m \neq 0$ (car $P(0)$ est vraie par hypothèse). On considère alors $m-1$ qui est encore dans $\mathbf{N}$ (car m est > 0) et qui est $< m$, donc n'est plus dans C puisque m est le plus petit élément de C. Il s'ensuit que $P(m-1)$ est vraie. Mais comme on a $P(n) \Longrightarrow P(n+1)$ pour tout n, il en résulte que $P(m)$ est vraie et c'est une contradiction.

2 Construction de Z

2.1 Problématique et discussion

L'ensemble $\mathbf{N}$ muni de l'addition n'est pas un groupe, faute de l'existence d'un opposé pour chaque élément, donc d'une soustraction. On a cependant une soustraction partielle :

2.1 Lemme. *Si on a $m, n \in \mathbf{N}$ avec $n \leq m$, il existe un unique entier d tel que $n + d = m$. On note $d = m - n$.*

Démonstration. C'est la définition de la relation d'ordre.

On va maintenant plonger $\mathbf{N}$ dans un groupe $\mathbf{Z}$. Il y a pour cela deux méthodes. La construction classique consiste à construire $\mathbf{Z}$ comme un quotient de $\mathbf{N} \times \mathbf{N}$ par une certaine relation d'équivalence. Cette construction a plusieurs avantages (elle est valable dans un cadre plus général, les démonstrations sont plutôt plus simples, c'est sans doute celle que connaissent le mieux les membres du jury de CAPES) et c'est pourquoi j'ai choisi de la présenter en premier. Elle a aussi un inconvénient, c'est d'être artificielle. En effet, contrairement à ce qui se passe dans le cas des rationnels, les entiers relatifs ne sont pas de manière naturelle des couples, mais des entiers munis d'un signe et il faut – au moins – expliquer d'où proviennent les couples dans cette construction. Je propose une autre construction en annexe, plus naturelle (elle consiste simplement à adjoindre à $\mathbf{N}$ les opposés de ses éléments), mais dans laquelle les démonstrations sont plus compliquées, et surtout nécessitent souvent de distinguer plusieurs cas. Le lecteur choisira la construction qui lui convient le mieux[5].

2.2 Introduction de la construction par les couples

On part du problème des soustractions impossibles. On souhaiterait pouvoir calculer $a - b$, pour $a, b \in \mathbf{N}$, dans tous les cas, et pas seulement lorsque a est $\geq b$. Comme cela n'est pas possible dans $\mathbf{N}$ on va étendre cet ensemble en $\mathbf{Z}$ où l'on espère avoir une soustraction sans restriction, donc une application $\sigma : \mathbf{N} \times \mathbf{N} \to \mathbf{Z}$ qui à (a, b) associe $a - b$. On voit ainsi apparaître les couples (a, b) d'entiers naturels. Le problème, c'est qu'il ne faut pas confondre l'opération de soustraction et son résultat (la différence $a - b$). En effet, il y a évidemment de nombreuses soustractions différentes qui donnent le même résultat, même dans le cas des soustractions ordinaires,

[5] Attention, si l'on présente la deuxième construction, il faut se préparer à justifier ce choix.

ainsi on a $7-3=8-4=15-11=4$. Lorsqu'on a ainsi $a-b=c-d$, on en déduit $(a-b)+(b+d)=(c-d)+(b+d)$ donc $a+d=b+c$ et, si l'on reste dans $\mathbf{N}$, ces relations sont équivalentes. Cela nous conduit, dans la construction par les couples, à identifier les couples (a,b) et (c,d) qui vérifient $a+d=b+c$ autrement dit, à "passer au quotient" par cette relation.

2.3 La construction par les couples

2.3.1 Définition

On considère donc l'ensemble $E=\mathbf{N}\times\mathbf{N}$ et la relation $\mathcal{R}$ définie sur E par $(a,b)\,\mathcal{R}\,(c,d)\iff a+d=b+c$. Tout ce qui suit se comprend en pensant au couple (a,b) comme un succédané de $a-b$.

2.2 Proposition-Définition. *La relation $\mathcal{R}$ est une relation d'équivalence. On note $\mathbf{Z}$ le quotient $E/\mathcal{R}$ et $p:E\to E/\mathcal{R}$ la projection canonique qui à un élément (a,b) associe sa classe d'équivalence.*

Démonstration. La réflexivité est évidente et la symétrie résulte de la commutativité de l'addition dans $\mathbf{N}$. Pour la transitivité, si on suppose $(a,b)\mathcal{R}(c,d)$ et $(c,d)\mathcal{R}(e,f)$, on a $a+d=b+c$ et $c+f=d+e$. On ajoute f aux deux membres de la première relation, on utilise l'associativité et la commutativité de l'addition, la relation $c+f=d+e$ et la règle de simplification et on obtient $a+f=b+e$, c'est-à-dire $(a,b)\mathcal{R}(e,f)$.

2.3.2 Addition

2.3 Proposition-Définition. *L'addition définie sur $\mathbf{N}\times\mathbf{N}$ en posant, pour $x=(a,b)$ et $y=(c,d)$, $x+y=(a+c,b+d)$ induit une opération sur $\mathbf{Z}$, notée $+$, qui est commutative et associative et admet $p(0,0)$ comme élément neutre. L'élément $p(b,a)$ est l'opposé de $p(a,b)$. L'ensemble $\mathbf{Z}$ muni de la loi $+$ est un groupe abélien. L'application $\varphi:\mathbf{N}\to\mathbf{Z}$ définie par $\varphi(n)=p(n,0)$ est un homomorphisme pour les lois $+$ et envoie l'élément neutre sur l'élément neutre. On identifie désormais $\mathbf{N}$ à son image dans $\mathbf{Z}$.*

Démonstration. Dire que la loi sur $\mathbf{N}\times\mathbf{N}$ induit une loi sur $\mathbf{Z}$ signifie que l'image de $x+y$ dans le quotient ne dépend pas des représentants x et y mais seulement de leurs classes, et cela revient à montrer que, si l'on a $x\mathcal{R}x'$ et $y\mathcal{R}y'$, on a $(x+y)\mathcal{R}(x'+y')$. Posons $x=(a,b)$, $x'=(a',b')$, $y=(c,d)$, $y'=(c',d')$. On a donc $a+b'=b+a'$ et $c+d'=d+c'$ et il faut montrer $(a+c)+(b'+d')=(b+d)+(a'+c')$. C'est évident à partir des propriétés de l'addition dans $\mathbf{N}$.

Pour vérifier les propriétés d'associativité et de commutativité il suffit de le faire sur $\mathbf{N} \times \mathbf{N}$. On a à vérifier, par exemple, $\big((a,b)+(c,d)\big)+(e,f) = (a,b)+\big((c,d)+(e,f)\big)$, mais c'est clair à partir des définitions et des propriétés de $\mathbf{N}$.

Il est clair que $p(0,0)$ est neutre et, pour l'opposé, on a $(a,b)+(b,a) = (a+b, a+b)$ dans $\mathbf{N} \times \mathbf{N}$, mais cet élément est équivalent à $(0,0)$ d'où le résultat.

2.4 Proposition. *Avec l'identification précédente, tout élément de* $\mathbf{Z}$ *est soit un élément* $n \in \mathbf{N}$*, soit l'opposé d'un tel élément (noté* $-n$*). La valeur absolue de* n*, comme celle de* $-n$*, est, par définition, l'entier naturel* n*.*

Démonstration. Soit $p(a,b) \in \mathbf{Z}$, il y a deux cas. Si on a $a \geq b$, on vérifie que (a,b) est égal à $(a-b,0)$ dans $\mathbf{Z}$, c'est-à-dire à $a-b$ avec l'identification. Si on a $a < b$, (a,b) est équivalent à $(0,b-a)$ donc égal dans $\mathbf{Z}$ à l'opposé de l'élément $(b-a) \in \mathbf{N}$.

2.3.3 Multiplication

Il y a deux voies pour définir la multiplication. La première est de continuer à utiliser les couples. La définition suivante se comprend si l'on pense que (a,b) et (c,d) représentent $b-a$ et $c-d$ et qu'on les multiplie en appliquant les règles de calcul usuelles ; $(a-b)\times(c-d) = ac+bd-(bc+ad)$.

2.5 Proposition-Définition. *On définit une opération de multiplication sur* $\mathbf{Z}$ *par la formule* $(a,b)\times(c,d) = (ac+bd, bc+ad)$*. Cette opération est associative et commutative, elle est distributive par rapport à la loi* $+$ *et admet l'élément* $1 = p(1,0)$ *comme élément neutre.*

Démonstration. La plupart des vérifications sont faciles, sauf le fait que la formule définit bien une opération dans le quotient. Il s'agit de voir que si on a $(a,b)\mathcal{R}(a',b')$ et $(c,d)\mathcal{R}(c',d')$ alors on a aussi $(a,b)\times(c,d)\mathcal{R}(a',b')\times(c',d')$. La méthode la plus simple, à l'instar d'Horace, consiste à séparer les adversaires en montrant d'abord $(a,b)\times(c,d)\mathcal{R}(a',b')\times(c,d)$ puis $(a',b')\times(c,d)\mathcal{R}(a',b')\times(c',d')$.

Une autre méthode consiste à utiliser la description 2.4 (le lecteur vérifiera que pour les éléments de la forme $n = p(n,0)$ et $-n = p(0,n)$ les deux définitions coïncident) :

2.6 Définition. *Sur* $\mathbf{Z}$ *on définit une multiplication comme suit. Soient* $a, b \in \mathbf{Z}$*. Si* a, b *sont dans* $\mathbf{N}$ *la multiplication est définie comme dans* $\mathbf{N}$*. Si on a*

$a \in \mathbf{N}$ et $b = -c$ avec $c \in \mathbf{N}$, on pose $a \times (-c) = -(a \times c)$, et de même pour le produit $(-c) \times a$. Enfin, si on a $a = -c$, $b = -d$ avec $c, d \in \mathbf{N}$, on pose $(-c) \times (-d) = c \times d$.

2.7 *Remarque.* On peut encore dire que la multiplication de deux entiers est définie par la multiplication de leurs valeurs absolues et par la règle des signes : + fois + et − fois − égalent +, + fois − et − fois + égalent −. Autrefois, on justifiait cette règle en expliquant : *les amis de nos ennemis sont nos ennemis*, *les ennemis de nos ennemis sont nos amis*, etc. C'est évidemment cette règle qu'il faut faire comprendre aux élèves.

Démonstration. Pour la plupart des propriétés, c'est une vérification facile. Par exemple pour l'associativité, il suffit de vérifier l'associativité sur les valeurs absolues et sur les signes. Seule la distributivité est plus ardue. Montrons par exemple la formule : $a \times (b + c) = (a \times b) + (a \times c)$ dans le cas $a, b \in \mathbf{N}$, $c = -d$, $d \in \mathbf{N}$. Il faut distinguer deux cas : $d \leq b$ et $d > b$. Dans le premier cas on a $b = d + e$ et $b + c = b + (-d) = e$. Il faut montrer $a \times b + (-(a \times d)) = a \times e$, soit $a \times b = a \times d + a \times e$: c'est la distributivité dans $\mathbf{N}$. Dans l'autre cas, on a $d = b + e$, d'où $a \times (b + (-d)) = a \times (-e) = -a \times e$. Mais, on a aussi $a \times d = a \times b + a \times e$. On a donc $a \times b < a \times d$ et $a \times b + a \times (-d) = a \times b + (-a \times d) = -a \times e$, cqfd.

Quelle que soit la méthode employée, on a prouvé :

2.8 Théorème. *Muni des deux lois + et ×, l'ensemble* $\mathbf{Z}$ *est un anneau commutatif unitaire.*

2.4 La relation d'ordre

2.9 Proposition-Définition. *La relation $m \leq n$ définie sur* $\mathbf{Z}$ *par $n - m \in \mathbf{N}$ est une relation d'ordre total qui fait de* $\mathbf{Z}$ *un anneau ordonné (ce qui signifie que la somme et le produit de nombres positifs sont positifs).*

3 Annexe : la construction directe, un entier, un signe

3.1 La construction

On pose $\mathbf{N}^* = \mathbf{N} - \{0\}$ et on définit l'ensemble $\mathbf{Z}$ comme réunion de $\mathbf{N}$ et d'une copie Q de $\mathbf{N}^*$. L'élément de Q correspondant à $n \in \mathbf{N}^*$ est noté[6] $-n$. On parlera des éléments de $\mathbf{N}$ (resp. Q) comme des entiers positifs ou nuls (resp. des entiers négatifs).

La valeur absolue $|z|$ d'un élément z de $\mathbf{Z}$ est égale à z si z est dans $\mathbf{N}$. Si z est dans Q, donc de la forme $z = -n$ on pose $|z| = n$.

3.1.1 Construction formelle

L'axiome de réunion (pour deux ensembles non nécessairement contenus dans un troisième) fait partie des axiomes de la théorie des ensembles, mais on peut aussi construire l'ensemble $\mathbf{Z}$ de deux manières au moins, à partir des produits :

1) On considère l'ensemble $E = \mathbf{N} \times \{0, 1\}$ et on définit le sous-ensemble $\mathbf{Z}$ de E comme l'ensemble des couples $(n, 0)$, $n \in \mathbf{N}$ et $(n, 1)$, $n \in \mathbf{N}^*$. On identifie l'élément n de $\mathbf{N}$ avec le couple $(n, 0)$ de $\mathbf{Z}$ et on note $-n$ le couple $(n, 1)$. On note Q l'ensemble des couples $(n, 1)$, $n \in \mathbf{N}^*$. On a bien retrouvé $\mathbf{Z}$ comme réunion de $\mathbf{N}$ et de Q.

2) On considère $E = \mathbf{N} \times \mathbf{N}$ et on définit $\mathbf{Z}$ comme le sous-ensemble de E formé des couples $(n, 0)$ (identifiés aux éléments n de $\mathbf{N}$) et des couples $(0, n)$, pour $n \in \mathbf{N}^*$, notés $-n$. Cette construction revient à prendre le morceau utile de la construction par les couples.

3.2 L'addition

La définition de l'addition est bien naturelle et correspond à ce qu'on souhaite au final :

3.1 Définition. *Sur* $\mathbf{Z}$ *on définit une addition comme suit. Si* m, n *sont dans* $\mathbf{N}$ *la somme* $m + n$ *est prise au sens de* $\mathbf{N}$*. Si* $-m$ *et* $-n$ *sont dans* Q*, on pose* $(-m) + (-n) = -(m + n)$*. Si* m *est dans* $\mathbf{N}$ *et* $-n$ *dans* Q *il y a deux cas : si on a* $n \leq m$*, on pose* $m + (-n) = (-n) + m = m - n$ *au sens de 2.1, si on a* $m < n$ *on pose* $m + (-n) = (-n) + m = -(n - m)$*.*

3.2 Théorème. *Muni de la loi* $+$ *l'ensemble* $\mathbf{Z}$ *est un groupe abélien, d'élément neutre* 0 *et dans lequel l'opposé de* n *est* $-n$ *si* n *est dans* $\mathbf{N}^*$ *(resp. l'opposé de* $-n$ *est* n *si* $-n$ *est dans* Q*).*

[6] Pour le moment, ce signe est juste une notation. D'ailleurs, on pourrait aussi noter, comme sur les calculatrices : $\_n$ (au lieu de $-n$) avec un signe $-$ en indice.

3.3 *Remarque.* Le théorème justifie la notation $-n$ (comme opposé de n) pour les éléments de Q. On notera la formule $-(-n) = n$.

Démonstration. Seule l'associativité est non évidente et nécessite de distinguer de nombreux cas. Il s'agit de montrer, pour $a, b, c \in \mathbf{Z}$, $(a + b) + c = a+(b+c)$. Il y a des cas faciles, par exemple si a, b, c sont tous dans $\mathbf{N}$ ou tous dans Q. Regardons par exemple un cas difficile : $a, b \in \mathbf{N}$ et $c = -d \in Q$. Il faut encore distinguer trois cas de figure.

1) $d \leq b$. On a donc $b = d + e$ avec $e \in \mathbf{N}$ (et donc $e = b - d$) et donc aussi $a + b = d + (a + e)$ ce qui montre $d \leq a + b$. Par définition, on a $a + (b + c) = a + (b - d) = a + e$ et il s'agit de voir que ceci est égal à $(a + b) + c = (a + b) - d$, autrement dit qu'on a $d + (a + e) = a + b$. Mais, vu l'égalité $b = d + e$, cela résulte des propriétés de l'addition dans $\mathbf{N}$.

2) $b < d \leq a+b$. Cette fois, on a $d = b+e$ et $a+b = d+f$ avec $e, f \in \mathbf{N}$. On en déduit $d+f = b+e+f = a+b$, d'où $a = e+f$, ce qui montre $e \leq a$. Alors, on a $(a+b)+c = (a+b)+(-d) = f$ et $a+(b+c) = a+(b+(-d)) = a+(-e) = f$, d'où le résultat.

3) $a + b < d$. On a $d = a + b + e$, d'où $d - b = a + e$. On calcule alors $(a + b) + c = (a + b) + (-d) = -e$ et $a + (b + c) = a + (b + (-d)) = a + (-(a + e)) = -e$.

Les autres cas se traitent de manière analogue. On peut limiter le nombre de cas à considérer en tenant compte de la commutativité de l'addition et de la symétrie entre n et $-n$.

3.3 La multiplication

La seconde méthode utilisée dans la construction précédente permet de retrouver les mêmes résultats.