Construction de $\mathbb{Z}$

8

Introduction

Quand a et b sont des entiers naturels, on rappelle que la notation $a \leqslant b$ abrège « $\exists k \in \mathbb{N}, b = a + k$ » (dans l'axiomatique de Peano). On sait par ailleurs qu'il en existe un et un seul. L'unique entier naturel k vérifiant l'égalité $b = a + k$ se note $b - a$ et ainsi, on a l'égalité $b = a + (b - a)$.

Donc certaines soustractions sont possibles dans $\mathbb{N}$.

Mais pour a et b fixés dans $\mathbb{N}$, l'équation d'inconnue x : $a + x = b$ n'admet jamais de solution dans $\mathbb{N}$ si $b < a$.
On souhaiterait alors construire un ensemble tel que l'équation précédente admette toujours une solution.

Prérequis

- Axiomatisation de $\mathbb{N}$ (**chapitre 7**)

Objectifs du chapitre

- Définir l'ensemble $\mathbb{Z}$ à l'aide d'une relation d'équivalence
- Démontrer les propriétés liées à l'addition dans $\mathbb{Z}$
- Démontrer les propriétés liées à la multiplication dans $\mathbb{Z}$
- Démontrer les propriétés liées à l'ordre dans $\mathbb{Z}$
- Immerger $\mathbb{N}$ dans $\mathbb{Z}$

Le cours du chapitre 8

1 Généralités

A Motivation

Soient a et b deux entiers naturels.
On s'intéresse à l'équation dans $\mathbb{N}$ d'inconnue x :

$$x + a = b \ (*).$$

C'est le cas si $a \leqslant b$.

Cette équation n'admet pas toujours une solution.
Quand $a \leqslant b$, l'entier x est identifié par le couple (a, b). Le souci, c'est que deux couples distincts peuvent être associés au même entier x.

Par exemple, pour l'équation : $x + 10 = 4$, les couples $(4, 10)$, $(3, 9)$ et plus généralement $(k, k+6)$ avec $k \in \mathbb{N}$ sont tous associés à x.

Cherchons alors à quelle condition deux couples d'entiers naturels (a, b) et (c, d) définissent le même entier x.
Quand x est une solution de l'équation $(*)$, les égalités $x + a = b$ et $x + c = d$ entraînent que :

$$b + (x + c) = (x + a) + d \text{ , soit } b + c = a + d .$$

Nous allons donc définir une relation entre les couples d'entiers naturels et faire en sorte que cette dernière soit une relation d'équivalence.

B Définition des entiers relatifs

On définit la relation $\mathcal{R}$ dans $\mathbb{N}^2$ par :

$$\forall (a, b), (c, d) \in \mathbb{N}^2, (a, b) \mathcal{R} (c, d) \Leftrightarrow a + d = b + c .$$

Théorème 1

La relation $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{N}^2$.

Preuve

Soient $(a, b), (c, d), (e, f) \in \mathbb{N}^2$.

Réflexivité

L'addition étant commutative dans $\mathbb{N}$, on a $a + b = b + a$ d'où $(a, b) \mathcal{R} (a, b)$.

Symétrie

On dispose des implications suivantes : $(a, b) \mathcal{R} (c, d) \Rightarrow a + d = b + c \Rightarrow c + b = d + a \Rightarrow (c, d) \mathcal{R} (a, b)$.

Transitivité

On dispose des implications suivantes : $\begin{cases} (a, b) \mathcal{R} (c, d) \\ (c, d) \mathcal{R} (e, f) \end{cases} \Rightarrow \begin{cases} a + d = b + c \\ c + f = d + e \end{cases} \Rightarrow (a + d) + (c + f) = (b + c) + (d + e)$

$$\begin{aligned} &\Rightarrow (a + f) + (d + c) = (b + e) + (c + d) \\ &\Rightarrow a + f = b + e \\ &\Rightarrow (a, b) \mathcal{R} (e, f) . \end{aligned}$$

Ainsi $\mathcal{R}$ est bien une relation d'équivalence sur $\mathbb{N}^2$. □

Remarques

1. L'ensemble-quotient $\mathbb{N}^2 / \mathcal{R}$ est noté usuellement $\mathbb{Z}$.

Pour $(a, b) \in \mathbb{N}^2$, on note naturellement $\overline{(a, b)} = \{(c, d) \in \mathbb{N}^2, (a, b) \mathcal{R} (c, d)\}$.

On préférera cette notation plutôt que la notation $\mathrm{Cl}((a, b))$.

2. Les éléments de $\mathbb{Z}$ sont appelés **entiers relatifs**.

Exemple

Par la relation $\mathcal{R}$, les couples $(1, 4)$, $(2, 5)$ et $(0, 3)$ sont en relation.
Plus généralement, ce sont tous des représentants d'une même classe : $\overline{(1, 4)} = \{(k, k + 3), k \in \mathbb{N}\}$.

L'entier relatif $(1, 4)$ est donc un ensemble composé d'une infinité de couples d'entiers naturels.

C Représentant canonique

Pour un entier relatif désigné, il existe une infinité d'écritures possibles. C'est dérangeant. On aimerait bien, parmi tous les représentants possibles d'un même entier relatif en désigner qu'un seul. Cela permettra d'utiliser par la suite ce représentant qui sera bien plus pratique.
On peut remarquer que parmi les représentants d'un même entier relatif, il y en a qu'un seul comportant un entier naturel nul. C'est ce qui motive le théorème suivant :

Théorème 2 — **Représentant canonique d'un entier relatif**

Soit α un entier relatif.

Il existe un unique entier naturel m tel que $\alpha = \overline{(m,0)}$ ou $\alpha = \overline{(0,m)}$.

Preuve

Soit α un nombre relatif (on notera $\alpha = \overline{(a,b)}$ où $(a,b) \in \mathbb{N}^2$).

Existence

On va distinguer deux cas :

- si $a \geqslant b$, l'entier naturel $a-b$ qu'on notera m est tel que $m+b=0+a$, donc $(m,0)\mathcal{R}(a,b)$;
- si $a \leqslant b$, l'entier naturel $b-a$ qu'on notera m est tel que $a+m=b+0$, donc $(a,b)\mathcal{R}(0,m)$.

La relation $\leqslant$ étant totale dans $\mathbb{N}$, on se retrouve dans l'une au moins des deux situations.

Unicité

Soient m et n deux entiers naturels tels que $\overline{(m,0)} = \overline{(n,0)}$.

Alors (**théorème 12-2** du **chapitre 2**) $(m,0)\mathcal{R}(n,0)$, c'est-à-dire $m+0=0+n$, soit $m=n$.

De même, si $\overline{(0,m)} = \overline{(0,n)}$, on obtient $m=n$. □

Définition 1

Soit α un entier relatif.

1) S'il existe un entier naturel m tel que $\alpha = \overline{(m,0)}$, on dit alors que α est un **entier positif**.

2) S'il existe un entier naturel m tel que $\alpha = \overline{(0,m)}$, on dit alors que α est un **entier négatif**.

Compte tenu du **théorème 2**, l'existence de cet entier naturel est toujours garantie.

Remarque

1. On note $\mathbb{Z}_+$ (resp. $\mathbb{Z}_-$) l'ensemble des entiers positifs (resp. négatifs).
2. De ce qui précède, il est clair que $\mathbb{Z}_+ \cup \mathbb{Z}_- = \mathbb{Z}$.
3. L'intersection $\mathbb{Z}_+ \cap \mathbb{Z}_- = \{\overline{(0,0)}\}$ est simple à établir (à faire par le lecteur en exercice).
4. En reprenant les hypothèses du **théorème 2**, l'entier naturel m est la **valeur absolue** de α et est notée $|\alpha|$.

Indice : quand une somme de deux entiers naturels est nulle, c'est que ces deux entiers le sont aussi.

2 Opérations dans Z

A Addition

Sur $\mathbb{N}^2$, on définit une opération d'addition par :

$$\forall (a,b),(c,d) \in \mathbb{N}^2, (a,b)+(c,d) = (a+c,b+d)\,.$$

On va montrer que la relation d'équivalence $\mathcal{R}$ est compatible avec l'addition. C'est-à-dire que :

$$\forall (a,b),(a',b'),(c,d),(c',d') \in \mathbb{N}^2, \begin{cases}(a,b)\mathcal{R}(a',b') \\ (c,d)\mathcal{R}(c',d')\end{cases} \Rightarrow (a+c,b+d)\mathcal{R}(a'+c',b'+d')\,.$$

Supposons alors que $(a,b)\mathcal{R}(a',b')$ et $(c,d)\mathcal{R}(c',d')$.

On a alors $a+b'=b+a'$ et $c+d'=d+c'$, soit en additionnant membre à membre :

$$(a+b')+(c+d') = (b+a')+(d+c')\,.$$

Par les propriétés de l'addition, il vient que $(a+c)+(b'+d') = (b+d)+(a'+c')$, ce qui correspond bien en utilisant la relation $\mathcal{R}$ à $(a+c,b+d)\mathcal{R}(a'+c',b'+d')$.

On peut alors définir sans crainte l'addition de deux entiers relatifs.

Définition 2

Soient α et β deux entiers relatifs désignés respectivement par les classes $\overline{(a,b)}$ et $\overline{(c,d)}$.

On définit la **somme** des entiers relatifs α et β en posant :

$$\alpha + \beta = \overline{(a+c,b+d)}\,.$$

On sous-entend évidemment que les lettres a, b, c et d sont des entiers naturels.

La compatibilité de la relation d'équivalence $\mathcal{R}$ avec l'addition permet de rendre cohérente la définition.

En effet, l'entier relatif $\overline{(a+c,b+d)}$ ne dépend pas du choix des représentants des classes α et β .

Exemple

Donnons la somme des entiers relatifs $\overline{(7,1)}$ et $\overline{(2,5)}$.

En passant par les représentants canoniques, on a $\overline{(7,1)} = \overline{(6,0)}$ et $\overline{(2,5)} = \overline{(0,3)}$.

Donc : $\overline{(7,1)} + \overline{(2,5)} = \overline{(6,0)} + \overline{(0,3)} = \overline{(6,3)} = \overline{(3,0)}$.

On vient d'ajouter 6 et -3 !

Le cours du chapitre 8

Remarque
Par définition, $(\mathbb{Z},+)$ est un magma.

Le **théorème 3** affirme que la somme de deux entiers positifs et positive et que la somme de deux entiers négatifs est négative.

Théorème 3

$$1)\ \ \forall(\alpha,\beta)\in\mathbb{Z}_+\times\mathbb{Z}_+, \alpha+\beta\in\mathbb{Z}_+ \qquad 2)\ \ \forall(\alpha,\beta)\in\mathbb{Z}_-\times\mathbb{Z}_-, \alpha+\beta\in\mathbb{Z}_- .$$

Preuve

Les entiers α et β sont positifs.

1) Notons $\alpha=\overline{(m,0)}$ et $\beta=\overline{(n,0)}$ où $(m,n)\in\mathbb{N}^2$.

On a : $\alpha+\beta=\overline{(m,0)}+\overline{(n,0)}=\overline{(m+n,0)}$, donc $\alpha+\beta\in\mathbb{Z}_+$.

Les entiers α et β sont négatifs.

2) Notons $\alpha=\overline{(0,m)}$ et $\beta=\overline{(0,n)}$ où $(m,n)\in\mathbb{N}^2$.

On a : $\alpha+\beta=\overline{(0,m)}+\overline{(0,n)}=\overline{(0,m+n)}$, donc $\alpha+\beta\in\mathbb{Z}_-$. □

Autrement dit, l'addition dans $\mathbb{Z}$ est associative.

Théorème 4 **Associativité de l'addition dans $\mathbb{Z}$**

$$\forall(\alpha,\beta,\gamma)\in\mathbb{Z}^3, \alpha+(\beta+\gamma)=(\alpha+\beta)+\gamma .$$

Preuve

Notons $\alpha=\overline{(a,b)}$, $\beta=\overline{(c,d)}$ et $\gamma=\overline{(e,f)}$ où toutes les lettres a, b, c, d, et f sont des entiers naturels.

Utilisation de l'associativité de l'addition dans $\mathbb{N}$.

$$\begin{aligned}\alpha+(\beta+\gamma)=\overline{(a,b)}+[\overline{(c,d)}+\overline{(e,f)}]=\overline{(a,b)}+\overline{(c+e,d+f)}=\overline{(a+(c+e),b+(d+f))}&=\overline{((a+c)+e,(b+d)+f)}\\&=\overline{(a+c,b+d)}+\overline{(e,f)}\\&=[\overline{(a,b)}+\overline{(c,d)}]+\overline{(e,f)}\\&=(\alpha+\beta)+\gamma .\end{aligned}$$ □

Remarque
On a montré que le couple $(\mathbb{Z},+)$ est un demi-groupe.

On va prouver que l'entier relatif $\overline{(0,0)}$ est neutre pour l'addition.

Théorème 5 **Elément neutre de l'addition dans $\mathbb{Z}$**

$$\forall\alpha\in\mathbb{Z}, \exists\varepsilon\in\mathbb{Z}, \alpha+\varepsilon=\varepsilon+\alpha=\alpha .$$

Preuve

Notons $\alpha=\overline{(a,b)}$ où a et b sont des entiers naturels.

On a : $\overline{(a,b)}+\overline{(0,0)}=\overline{(a+0,b+0)}=\overline{(a,b)}$ et $\overline{(0,0)}+\overline{(a,b)}=\overline{(0+a,0+b)}=\overline{(a,b)}$.

Ainsi, l'entier relatif $\overline{(0,0)}$ est neutre pour l'addition dans $\mathbb{Z}$. □

Remarque
On a montré que le couple $(\mathbb{Z},+)$ est un monoïde.

Autrement dit, l'addition dans $\mathbb{Z}$ est commutative.

Théorème 6 **Commutativité de l'addition dans $\mathbb{Z}$**

$$\forall(\alpha,\beta)\in\mathbb{Z}^2, \alpha+\beta=\beta+\alpha .$$

Preuve

Notons $\alpha=\overline{(a,b)}$ et $\beta=\overline{(c,d)}$ où a, b, c et d sont des entiers naturels.

Utilisation de la commutativité de l'addition dans $\mathbb{N}$.

On a : $\alpha+\beta=\overline{(a,b)}+\overline{(c,d)}=\overline{(a+c,b+d)}=\overline{(c+a,d+b)}=\overline{(c,d)}+\overline{(a,b)}=\beta+\alpha$. □

Autrement dit, tout entier relatif admet un opposé pour l'addition.

Théorème 7 **Eléments symétrisables pour l'addition dans $\mathbb{Z}$**

$$\forall\alpha\in\mathbb{Z}, \exists\beta\in\mathbb{Z}, \alpha+\beta=\overline{(0,0)} .$$

Preuve

Notons $\alpha=\overline{(a,b)}$ et $\beta=\overline{(b,a)}$ où a et b sont des entiers naturels.

La commutativité de l'addition dans $\mathbb{Z}$ montre aussi que $\beta+\alpha=\overline{(0,0)}$.

On a : $\alpha+\beta=\overline{(a,b)}+\overline{(b,a)}=\overline{(a+b,b+a)}=\overline{(0,0)}$.

Ainsi, tout entier relatif admet un opposé pour l'addition. □

Le cours du chapitre 8

Remarques

1. On a montré (**théorème 6** et **7**) que le couple $(\mathbb{Z},+)$ est un groupe commutatif.

On rappelle que dans un groupe, tout élément est régulier.

2. De ce qui précède, tous les entiers relatifs sont réguliers pour l'addition.

3. Pour tout entier relatif α, on notera par commodité $-\alpha$ l'opposé de α.
Il vient alors que pour tout entier relatif α, $-(-\alpha)=\alpha$.

4. Pour α et β dans $\mathbb{Z}$, l'entier relatif $\alpha+(-\beta)$ sera noté $\alpha-\beta$ et s'appelle **différence** de α et β.

Théorème 8

1) $\forall\alpha\in\mathbb{Z}_+, -\alpha\in\mathbb{Z}_-$ 2) $\forall\alpha\in\mathbb{Z}_-, -\alpha\in\mathbb{Z}_+$.

Preuve

L'entier α est positif.

1) Notons $\alpha=\overline{(m,0)}$ avec m un entier naturel.
Comme $-\alpha=\overline{(0,m)}$, il vient que $-\alpha\in\mathbb{Z}_-$.

L'entier α est négatif.

2) Notons $\alpha=\overline{(0,m)}$ avec m un entier naturel.
Comme $-\alpha=\overline{(m,0)}$, il vient que $-\alpha\in\mathbb{Z}_+$. □

Théorème 9

$$\forall\alpha\in\mathbb{Z}, |\alpha|=|-\alpha|.$$

Preuve

Soit m un entier naturel.
En notant $\alpha=\overline{(m,0)}$, on a $-\alpha=\overline{(0,m)}$ et par définition de la valeur absolue, $m=|\alpha|=|-\alpha|$. □

Remarque

Nous sommes enfin capables de résoudre totalement l'équation d'inconnue x dans $\mathbb{Z}$: $\alpha+x=\beta$ où α et β sont des entiers relatifs fixés.

Utilisation des propriétés de l'addition dans $\mathbb{Z}$.

En effet, on a les équivalences suivantes : $\alpha+x=\beta \Leftrightarrow (\alpha+x)+(-\alpha)=\beta+(-\alpha) \Leftrightarrow x=\beta-\alpha$.

B Multiplication

Sur $\mathbb{N}^2$, on définit une opération de multiplication par :

Contrairement à l'addition, la multiplication est définie de manière moins naturelle.

$$\forall(a,b),(c,d)\in\mathbb{N}^2, (a,b)\times(c,d)=(ac+bd, ad+bc).$$

On va montrer que la relation d'équivalence $\mathcal{R}$ est compatible avec la multiplication. C'est-à-dire que :

$$\forall(a,b),(a',b'),(c,d),(c',d')\in\mathbb{N}^2, \begin{cases}(a,b)\,\mathcal{R}\,(a',b')\\(c,d)\,\mathcal{R}\,(c',d')\end{cases} \Rightarrow (ac+bd, ad+bc)\,\mathcal{R}\,(a'c'+b'd', a'd'+b'c').$$

Supposons alors que $(a,b)\,\mathcal{R}\,(a',b')$ et $(c,d)\,\mathcal{R}\,(c',d')$.

Alors $a+b'=b+a'$ et $c+d'=d+c'$.

Multiplication par c' et d'.

D'une part, $ac'+b'c'=bc'+a'c'$ et $ad'+b'd'=bd'+a'd'$.

Multiplication par a et b.

D'autre part, $ac+ad'=ad+ac'$ et $bc+bd'=bd+bc'$.

Il vient alors que :

$$(ac'+b'c')+(ad'+b'd')+(ac+ad')+(bc+bd')=(bc'+a'c')+(bd'+a'd')+(ad+ac')+(bd+bc').$$

En simplifiant, on trouve :

$$(ac+bd)+(a'd'+b'c')=(ad+bc)+(a'c'+b'd').$$

Cette dernière égalité revient à dire que $(ac+bd, ad+bc)\,\mathcal{R}\,(a'c'+b'd', a'd'+b'c')$.

On est maintenant en mesure de définir le produit de deux entiers relatifs.

Définition 3

On sous-entend évidemment que les lettres a, b, c et d sont des entiers naturels.

Soient α et β deux entiers relatifs désignés respectivement par les classes $\overline{(a,b)}$ et $\overline{(c,d)}$.
On définit le **produit** des entiers relatifs α et β en posant :

$$\alpha\times\beta=\overline{(ac+bd, ad+bc)}.$$

La compatibilité de la relation d'équivalence $\mathcal{R}$ avec la multiplication permet de rendre cohérente la définition.
En effet, l'entier $\overline{(ac+bd, ad+bc)}$ ne dépend pas du choix des représentants des classes α et β.

Exemple

Multiplions les entiers relatifs $\overline{(2,3)}$ et $\overline{(4,1)}$.

Le cours du chapitre 8

Pour éviter de lourds calculs, on va passer par les représentants canoniques.

On a multiplié les entiers -1 et 3 !

On a : $\overline{(2,3)}\times\overline{(4,1)}=\overline{(0,1)}\times\overline{(3,0)}=\overline{(0,3)}$.

Remarques

1. Par définition, $(\mathbb{Z},\times)$ est un monoïde.

2. Pour α et β dans $\mathbb{Z}$, on notera par commodité $\alpha\beta$ le produit de α par β au lieu de $\alpha\times\beta$.

Théorème 10

1) $\forall(\alpha,\beta)\in\mathbb{Z}_+\times\mathbb{Z}_+, \alpha\beta\in\mathbb{Z}_+$ 2) $\forall(\alpha,\beta)\in\mathbb{Z}_-\times\mathbb{Z}_-, \alpha\beta\in\mathbb{Z}_+$ 3) $\forall(\alpha,\beta)\in\mathbb{Z}_+\times\mathbb{Z}_-, \alpha\beta\in\mathbb{Z}_-$.

Preuve

Les entiers α et β sont positifs.

1) Notons $\alpha=\overline{(m,0)}$ et $\beta=\overline{(n,0)}$ où $(m,n)\in\mathbb{N}^2$.

On a : $\alpha\beta=\overline{(m,0)}\times\overline{(n,0)}=\overline{(mn,0)}$, donc $\alpha\beta\in\mathbb{Z}_+$.

Les entiers α et β sont négatifs.

2) Notons $\alpha=\overline{(0,m)}$ et $\beta=\overline{(0,n)}$ où $(m,n)\in\mathbb{N}^2$.

On a : $\alpha\beta=\overline{(0,m)}\times\overline{(0,n)}=\overline{(mn,0)}$, donc $\alpha\beta\in\mathbb{Z}_+$.

L'entier α est positif et l'entier β est négatif.

3) Notons $\alpha=\overline{(0,m)}$ et $\beta=\overline{(n,0)}$ où $(m,n)\in\mathbb{N}^2$.

On a : $\alpha\beta=\overline{(m,0)}\times\overline{(0,n)}=\overline{(0,mn)}$, donc $\alpha\beta\in\mathbb{Z}_-$. □

Théorème 11 **Associativité de la multiplication dans $\mathbb{Z}$**

Autrement dit, la multiplication dans $\mathbb{Z}$ est associative.

$$\forall(\alpha,\beta,\gamma)\in\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}, \alpha(\beta\gamma)=(\alpha\beta)\gamma.$$

Preuve

Notons $\alpha=\overline{(a,b)}$, $\beta=\overline{(c,d)}$ et $\gamma=\overline{(e,f)}$ où toutes les lettres a, b, c, d, et f sont des entiers naturels.

On a d'une part :

$\alpha(\beta\gamma)=\overline{(a,b)}\times[\overline{(c,d)}\times\overline{(e,f)}]=\overline{(a,b)}\times\overline{(ce+df,cf+de)}=\overline{(ace+adf+bcf+bde,acf+ade+bce+bdf)}$.

D'autre part, on a :

$(\alpha\beta)\gamma=[\overline{(a,b)}\times\overline{(c,d)}]\times\overline{(e,f)}=\overline{(ac+db,ad+bc)}\times\overline{(e,f)}=\overline{(ace+dbe+adf+bcf,acf+dbf+ade+bce)}$.

Donc $(\alpha\beta)\gamma=\alpha(\beta\gamma)$. □

Remarque

On a montré que le couple $(\mathbb{Z},\times)$ est un demi-groupe.

Théorème 12 **Elément neutre de la multiplication dans $\mathbb{Z}$**

On va prouver que l'entier relatif $\overline{(1,0)}$ est neutre pour la multiplication.

$$\forall\alpha\in\mathbb{Z}, \exists\varepsilon\in\mathbb{Z}, \alpha\varepsilon=\varepsilon\alpha=\alpha.$$

Preuve

Notons $\alpha=\overline{(a,b)}$ où a et b sont des entiers naturels.

On a : $\overline{(a,b)}\times\overline{(1,0)}=\overline{(a+0,0+b)}=\overline{(a,b)}$ et $\overline{(1,0)}\times\overline{(a,b)}=\overline{(a+0,b+0)}=\overline{(a,b)}$.

L'entier relatif $\overline{(1,0)}$ est donc neutre pour la multiplication dans $\mathbb{Z}$. □

Remarque

On a montré que le couple $(\mathbb{Z},\times)$ est un monoïde.

Théorème 13 **Commutativité de la multiplication dans $\mathbb{Z}$**

Autrement dit, la multiplication dans $\mathbb{Z}$ est commutative.

$$\forall(\alpha,\beta)\in\mathbb{Z}\times\mathbb{Z}, \alpha\beta=\beta\alpha.$$

Preuve

Notons $\alpha=\overline{(a,b)}$ et $\beta=\overline{(c,d)}$ où a, b, c et d sont des entiers naturels.

On a d'une part : $\alpha\beta=\overline{(a,b)}\times\overline{(c,d)}=\overline{(ac+bd,ad+bc)}$.

D'autre part, on a : $\beta\alpha=\overline{(c,d)}\times\overline{(a,b)}=\overline{(ca+db,cb+da)}$.

La commutativité de l'addition et de la multiplication dans $\mathbb{N}$ montre que $\alpha\beta=\beta\alpha$. □

Le cours du chapitre 8

Théorème 14 Distributivité de la multiplication sur l'addition

$$\forall(\alpha,\beta,\gamma)\in\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z},\begin{cases}\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma\\(\beta+\gamma)\alpha=\beta\alpha+\gamma\alpha\end{cases}.$$

Autrement dit, la multiplication est distributive sur l'addition.

Preuve

Notons $\alpha=\overline{(a,b)}$, $\beta=\overline{(c,d)}$ et $\gamma=\overline{(e,f)}$ où toutes les lettres a, b, c, d, et f sont des entiers naturels.

On a d'une part :

$\alpha(\beta+\gamma)=\overline{(a,b)}\times[\overline{(c,d)}+\overline{(e,f)}]=\overline{(a,b)}\times\overline{(c+e,d+f)}=\overline{(ac+ae+bd+bf,ad+af+bc+be)}$.

D'autre part, on a :

$\alpha\beta+\alpha\gamma=\overline{(a,b)}\times\overline{(c,d)}+\overline{(a,b)}\times\overline{(e,f)}=\overline{(ac+bd,ad+bc)}+\overline{(ae+bf,af+be)}=\overline{(ac+bd+ae+bf,ad+bc+af+be)}$.

Ainsi, $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$.

L'égalité $(\beta+\gamma)\alpha=\beta\alpha+\gamma\alpha$ découle de la commutativité de la multiplication dans $\mathbb{Z}$. □

Remarque

Nous avons établi que le triplet $(\mathbb{Z},+,\times)$ est un anneau commutatif.

C Ordre dans Z

Définition 4

Soient α et β deux entiers relatifs.

Dire que l'entier α est **inférieur ou égal** à β signifie que $\beta-\alpha\in\mathbb{Z}_+$.

Remarques

1. On écrit $\alpha\leqslant\beta$ pour signifie que α est inférieur ou égal à β.
2. Quand $\alpha\leqslant\beta$ avec de plus $\alpha\neq\beta$, on écrit $\alpha<\beta$.
3. La relation réciproque de la relation $\leqslant$ (resp. $<$) est notée $\geqslant$ (resp. $>$).

Exemple

L'entier relatif $\overline{(2,3)}$ est inférieur à l'entier relatif $\overline{(7,3)}$ car $\overline{(7,3)}-\overline{(2,3)}=\overline{(7,3)}+\overline{(3,2)}=\overline{(10,5)}$ et $\overline{(10,5)}=\overline{(5,0)}$.

Théorème 15 Relation d'ordre dans $\mathbb{Z}$

Le couple $(\mathbb{Z},\leqslant)$ est un ensemble ordonné.

Preuve

Réflexivité

Pour tout entier relatif α, on a : $\alpha-\alpha=\alpha+(-\alpha)=\overline{(0,0)}$.

Comme $\overline{(0,0)}\in\mathbb{Z}_+$, il vient que $\alpha\leqslant\alpha$.

Antisymétrie

Soient α et β deux entiers relatifs tels que $\alpha\leqslant\beta$ et $\beta\leqslant\alpha$.

Alors $\beta-\alpha\in\mathbb{Z}_+$ et $\alpha-\beta\in\mathbb{Z}_+$, d'où $\beta-\alpha=-(\alpha-\beta)\in\mathbb{Z}_-$.

Ainsi, $\beta-\alpha=\overline{(0,0)}$ et $\beta=\alpha$.

On rappelle que $\mathbb{Z}_+\cap\mathbb{Z}_-=\{\overline{(0,0)}\}$.

Transitivité

Soient α, β et γ des entiers relatifs tels que $\alpha\leqslant\beta$ et $\beta\leqslant\gamma$.

Alors $\beta-\alpha\in\mathbb{Z}_+$ et $\gamma-\beta\in\mathbb{Z}_+$.

Ainsi, $(\beta-\alpha)+(\gamma-\beta)=\gamma-\alpha\in\mathbb{Z}_+$, d'où $\gamma\leqslant\alpha$. □

Somme de deux entiers positifs.

Théorème 16 Relation d'ordre totale dans $\mathbb{Z}$

Le couple $(\mathbb{Z},\leqslant)$ est un ensemble totalement ordonné.

Preuve

On sait déjà que le couple $(\mathbb{Z},\leqslant)$ est un ensemble ordonné. Il reste à montrer que : $\forall(\alpha,\beta)\in\mathbb{Z}^2,(\alpha\leqslant\beta)\vee(\beta\leqslant\alpha)$.

Comme $\mathbb{Z}=\mathbb{Z}_+\cup\mathbb{Z}_-$, il suffit de considérer l'entier relatif $\beta-\alpha$ (avec α et β des entiers relatifs). □

Le lecteur terminera la démonstration.

Remarques

1. Il est clair que : $\forall \alpha \in \mathbb{Z}_+, \overline{(0,0)} \leqslant \alpha$.

2. Il est clair que : $\forall \alpha \in \mathbb{Z}_-, \alpha \leqslant \overline{(0,0)}$.

3. On note $\mathbb{Z}_+^*$ (resp. $\mathbb{Z}_-^*$) l'ensemble des entiers positifs non nuls (resp. l'ensemble des entiers négatifs non nuls).

Il est aussi clair que $\mathbb{Z}_-^* \cap \mathbb{Z}_+^* = \varnothing$.

Il vient alors que : $\forall (\alpha, \beta) \in \mathbb{Z}^2, \alpha < \beta \Leftrightarrow \beta - \alpha \in \mathbb{Z}_+^*$.

Théorème 17

Autrement dit, tout entier négatif est inférieur à tout entier positif.

$$\forall \alpha \in \mathbb{Z}_-, \forall \beta \in \mathbb{Z}_+, \alpha \leqslant \beta \, .$$

Preuve

Soient α un entier positif et β un entier négatif.

On a donc $\alpha \leqslant 0$ et $0 \leqslant \beta$, soit par transitivité de la relation d'ordre $\leqslant$, $\alpha \leqslant \beta$. □

Théorème 18 Compatibilité de la relation d'ordre avec l'addition

Autrement dit, la relation $\leqslant$ est compatible avec l'addition.

$$\forall (\alpha, \beta, \gamma) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}, \alpha \leqslant \beta \Rightarrow \alpha + \gamma \leqslant \beta + \gamma \, .$$

Preuve

Supposons que $\alpha \leqslant \beta$.

On a : $(\beta + \gamma) - (\alpha + \gamma) = \beta + \gamma - \alpha - \gamma = \beta - \alpha$.

Comme $\alpha \leqslant \beta$ par hypothèse, il vient que $\beta - \alpha \in \mathbb{Z}_+$ et donc que $\alpha + \gamma \leqslant \beta + \gamma$. □

Théorème 19

Le **théorème 19** est une conséquence immédiate du **théorème 18**.
On peut additionner membre à membre des entiers relatifs dans des inégalités.

$$\forall (\alpha, \beta, \gamma, \delta) \in \mathbb{Z}^4, \begin{cases} \alpha \leqslant \beta \\ \gamma \leqslant \delta \end{cases} \Rightarrow \alpha + \gamma \leqslant \beta + \delta \, .$$

Preuve

Supposons que $\alpha \leqslant \beta$ et $\gamma \leqslant \delta$.

D'une part, l'inégalité $\alpha \leqslant \beta$ entraîne que $\alpha + \gamma \leqslant \beta + \gamma$, d'autre part l'inégalité $\gamma \leqslant \delta$ entraîne que $\gamma + \beta \leqslant \delta + \beta$.

Par transitivité de la relation d'ordre $\leqslant$, on a $\alpha + \gamma \leqslant \beta + \delta$. □

Théorème 20 Régularité de la multiplication dans $\mathbb{Z}$

Autrement dit, tous les entiers relatifs non nuls sont réguliers pour la multiplication.
Comme la multiplication est commutative, il n'y a qu'une implication à démontrer.

$$\forall \alpha \in \mathbb{Z}^*, \forall (\beta, \gamma) \in \mathbb{Z} \times \mathbb{Z}, \alpha\beta = \alpha\gamma \Rightarrow \beta = \gamma \, .$$

Preuve

Supposons que $\alpha\beta = \alpha\gamma$.

Pour des questions de commodité, nous avons noté 0 au lieu de $\overline{(0,0)}$. Ceci sera justifié lorsqu'on aura « plongé » l'ensemble $\mathbb{N}$ dans $\mathbb{Z}$.

Alors, $\alpha\beta - \alpha\gamma = \alpha(\beta - \gamma) = 0$.

$\mathbb{Z}$ étant un anneau intègre (voir l'**exercice 1**), on a nécessairement $\alpha = 0$ ou $\beta = \gamma$. Mais l'entier α est supposé non nul, donc $\beta = \gamma$. □

Théorème 21

Attention à l'inégalité en 2).

1) $\forall (\alpha, \beta) \in \mathbb{Z} \times \mathbb{Z}, \forall \gamma \in \mathbb{Z}_+, \alpha \leqslant \beta \Rightarrow \alpha\gamma \leqslant \beta\gamma$ 2) $\forall (\alpha, \beta) \in \mathbb{Z} \times \mathbb{Z}, \forall \gamma \in \mathbb{Z}_-, \alpha \leqslant \beta \Rightarrow \beta\gamma \leqslant \alpha\gamma$.

Preuve

1) Supposons que $\alpha \leqslant \beta$.

Alors $\beta - \alpha \in \mathbb{Z}_+$ et comme $\gamma \in \mathbb{Z}_+$, on a (**théorème 10-1**) $(\beta - \alpha)\gamma \in \mathbb{Z}_+$, c'est-à-dire $\beta\gamma - \alpha\gamma \in \mathbb{Z}_+$, soit encore $\alpha\gamma \leqslant \beta\gamma$.

2) Supposons que $\alpha \leqslant \beta$.

Alors $\beta - \alpha \in \mathbb{Z}_+$ et comme $\gamma \in \mathbb{Z}_-$, on a (**théorème 10-3**) $(\beta - \alpha)\gamma \in \mathbb{Z}_-$, c'est-à-dire $\beta\gamma - \alpha\gamma \in \mathbb{Z}_-$, soit encore $\beta\gamma \leqslant \alpha\gamma$. □

On a utilisé l'équivalence suivante : $\forall (\alpha, \beta) \in \mathbb{Z}^2, \beta - \alpha \in \mathbb{Z}_- \Leftrightarrow \beta \leqslant \alpha$.
Elle s'établit facilement en remarquant que $-(\beta - \alpha) \in \mathbb{Z}_+$.

La propriété d'Archimède vue avec $\mathbb{N}$ reste encore valable dans $\mathbb{Z}$:

Le cours du chapitre 8

Théorème 22 **Propriété d'Archimède pour $\mathbb{Z}$**

$$\forall \alpha \in \mathbb{Z}, \forall \beta \in \mathbb{N}^*, \exists n \in \mathbb{N}, \alpha \leqslant \beta n\,.$$

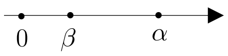
Autrement dit, on peut dépasser n'importe quel entier relatif à partir d'un entier naturel non nul en l'ajoutant un certain nombre de fois.

Preuve

Traitons deux cas suivant le signe de α.

- Supposons que $\alpha \leqslant 0$.

Alors comme $\beta > 0$, on a $\alpha < \beta$ et 1 comme valeur de n convient.



- Supposons que $\alpha > 0$.

Comme $\mathbb{N}$ est archimédien, le résultat en découle immédiatement. □

3 Plongement de N dans Z

Il est maintenant temps de manipuler les entiers relatifs avec des écritures telles qu'on les attendait depuis le début de ce chapitre.

Nous avons écrit par commodité $0 = \overline{(0,0)}$. Mais la notation 0 désigne aussi l'entier naturel 0. On aimerait bien considérer les entiers naturels comme des cas particuliers d'entiers relatifs.

Mais il y a un problème de taille ! Tous les entiers relatifs se voient comme des ensembles de couples d'entiers naturels. Il est donc théoriquement impossible, du point de vue de notre construction d'établir l'inclusion $\mathbb{N} \subset \mathbb{Z}$.

Rien n'est perdu pour autant comme on va le voir.

A Plongement de l'addition

Montrons que la somme de deux entiers naturels est la même que ceux-ci soient considérés comme des éléments de $\mathbb{N}$ ou de $\mathbb{Z}$.

Théorème 23

L'application $f : \begin{array}{l} \mathbb{N} \longrightarrow \mathbb{Z} \\ n \mapsto \overline{(n,0)} \end{array}$ est un morphisme injectif de $(\mathbb{N},+)$ dans $(\mathbb{Z},+)$.

On parle aussi de **monomorphisme** au lieu de morphisme injectif.

Preuve

Soient n et m deux entiers naturels.

On a : $f(n+m) = \overline{(n+m,0)} = \overline{(n,0)} + \overline{(m,0)} = f(n) + f(m)$.

Donc f est bien un morphisme de $(\mathbb{N},+)$ dans $(\mathbb{Z},+)$.

Puis, $f(n) = f(m) \Rightarrow \overline{(n,0)} = \overline{(m,0)} \Rightarrow (n,0)\,\mathcal{R}\,(m,0) \Rightarrow n = m$.

Donc f est injective. □

L'application f ainsi définit est un « plongement de $\mathbb{N}$ dans $\mathbb{Z}$ » en ce sens qu'elle permet d'identifier $\mathbb{N}$ et son image $f\langle\mathbb{N}\rangle$ en écrivant pour tout entier naturel m, $m = \overline{(m,0)}$.

L'égalité $\overline{(n+m,0)} = \overline{(n,0)} + \overline{(m,0)}$ montre qu'ajouter les entiers naturel n et m revient à ajouter les entiers relatifs n et m et donne dans les deux cas le même résultat.

De plus, on sait que l'opposé de m est $\overline{(0,m)}$ qui se note $-m$.

B Plongement de la multiplication

Montrons que le produit de deux entiers naturels est le même que ceux-ci soient considérés comme des éléments de $\mathbb{N}$ ou de $\mathbb{Z}$.

Théorème 24

L'application $f : \begin{array}{l} \mathbb{N} \longrightarrow \mathbb{Z} \\ n \mapsto \overline{(n,0)} \end{array}$ est un morphisme injectif de $(\mathbb{N},\times)$ dans $(\mathbb{Z},\times)$.

Preuve

Soient n et m deux entiers naturels.

On a : $f(nm) = \overline{(nm,0)} = \overline{(n,0)} \times \overline{(m,0)} = f(n) \times f(m)$.

De même, l'égalité : $\overline{(nm,0)} = \overline{(n,0)} \times \overline{(m,0)}$, montre que multiplier les entiers naturel n et m revient à multiplier les entiers relatifs n et m et donne dans les deux cas le même résultat.

Donc f est bien un morphisme de $(\mathbb{N},+)$ dans $(\mathbb{Z},+)$.

L'injectivité de f s'établit comme plus haut. □

C Plongement de la relation d'ordre

Montrons enfin que deux entiers naturels et les deux entiers relatifs auxquels ils sont « égaux » sont rangés dans le même ordre.

Théorème 25

$$\forall (n, m) \in \mathbb{N}^2, n \leqslant m \Leftrightarrow \overline{(n, 0)} \leqslant \overline{(m, 0)} .$$

Notez que comme pour l'addition et la multiplication, la relation d'ordre $\leqslant$ n'est pas théoriquement la même si on la considère dans $\mathbb{N}$ (membre de gauche dans l'équivalence) ou si on la considère dans $\mathbb{Z}$ (membre de droite de l'équivalence).
Bien heureusement, avec les différents plongements, il n'y a pas à faire de distinctions.

Preuve

Soient n et m deux entiers naturels.

On dispose des équivalences suivantes :

$$\begin{aligned}
\overline{(n, 0)} \leqslant \overline{(m, 0)} \Leftrightarrow \overline{(m, 0)} - \overline{(n, 0)} \in \mathbb{Z}_+ &\Leftrightarrow \overline{(m, 0)} + \overline{(0, n)} \in \mathbb{Z}_+ \\
&\Leftrightarrow \overline{(m, n)} \in \mathbb{Z}_+ \\
&\Leftrightarrow \exists k \in \mathbb{N}, \overline{(m, n)} = \overline{(k, 0)} \\
&\Leftrightarrow \exists k \in \mathbb{N}, m = n + k \\
&\Leftrightarrow n \leqslant m .
\end{aligned}$$

□

Les exercices du chapitre 8

1 Démonstrations supplémentaires du cours

1) Montrer que :

$$\forall(\alpha,\beta)\in\mathbb{Z}\times\mathbb{Z}, |\alpha\beta| = |\alpha|\times|\beta|\,.$$

2) En déduire que :

$$\forall(\alpha,\beta)\in\mathbb{Z}\times\mathbb{Z}, \alpha\beta = 0 \Rightarrow (\alpha=0)\vee(\beta=0)\,.$$

Ainsi, $(\mathbb{Z},+,\times)$ *est un anneau intègre.*

2 Démonstrations supplémentaires du cours

Montrer que : $\forall(\alpha,\beta)\in\mathbb{Z}\times\mathbb{Z}, \alpha<\beta \Leftrightarrow \alpha+1\leqslant\beta$.

3 Démonstrations supplémentaires du cours

Montrer qu'entre deux entiers relatifs consécutifs, il n'existe aucun entier relatif.

4 Démonstrations supplémentaires du cours

1) Montrer que toute suite croissante (resp. décroissante) et majorée (resp. minorée) de $\mathbb{Z}$ est stationnaire.
2) Montrer que toute partie non vide et majorée (resp. minorée) de $\mathbb{Z}$ admet un plus grand élément (resp. un plus petit élément).

5 ★★ Equation diophantienne

Montrer que l'équation diophantienne d'inconnue (x,y) :

$$x^2+(x+1)^2 = y^2\,,$$

admet une infinité de solutions entières strictement positives.

6 ★★ Equation diophantienne

Déterminer les entiers naturels non nuls et distincts $x_1,\dots,x_n$ solutions de l'équation :

$$1+1x_1+2x_1x_2+3x_1x_2x_3+\dots+(n-1)x_1x_2\dots x_{n-1} = x_1x_2\dots x_n\,.$$

7 ★★ Comme aux olympiades !

Déterminer les triplets (x,y,z) d'entiers strictement positifs solutions de l'équation :

$$(x+y)^2+3x+y+1 = z^2\,.$$

8 ★★ Comme aux olympiades !

Montrer que, pour tout entier naturel n, il existe n entier(s) naturel(s) $x_1,\dots,x_n$ tels que :

$$x_1+\dots+x_n = x_1\times\dots\times x_n\,.$$

9 ★ Equation diophantienne

Résoudre dans $\mathbb{N}^2$ l'équation d'inconnue (x,y) :

$$y^3 = x^3+8x^2+7x+10\,.$$

10 ★ Equation diophantienne

Résoudre dans $\mathbb{N}^2$ l'équation d'inconnue (x,y) :

$$y^3 = x^3+8x^2-6x+8\,.$$

11 ★ Equation diophantienne

Trouver tous les quadruplets $(n,p,q,r)\in\mathbb{N}^4$ tels que :

$$n!+p!+q! = r!\,.$$

12 ★ Equation diophantienne

Résoudre dans $\mathbb{N}^2$ l'équation d'inconnue (x,y) :

$$3x^3+xy+4y^3 = 349\,.$$

13 ★ Equation diophantienne

Résoudre dans $(\mathbb{N}^*)^3$ l'équation d'inconnue (x,y,z) :

$$xyz = 1+x+y+z\,.$$

14 ★ Utiliser un théorème de récurrence

Soit x un nombre réel tel que $x+\dfrac{1}{x}\in\mathbb{Z}$.

Montrer que :

$$\forall n\in\mathbb{N}, x^n+\frac{1}{x^n}\in\mathbb{Z}\,.$$

15 ★ Equation diophantienne

Montrer que l'équation d'inconnue (x,y) :

$$4x(x+1) = y(y+1)\,,$$

n'admet aucune solution dans $\mathbb{N}^2\setminus\{(0,0)\}$.