IV . −L'ensemble $\mathbb{Z}$ des entiers relatifs

IV.0 . −Introduction

Même si, dans ce chapitre, nous allons montrer au paragraphe IV.3 que l'ensemble $\mathbb{Z}$ possède une structure d'anneau et même au paragraphe IV.5, une structure d'anneau euclidien nous ne considérerons dans les chapitres IV, V et VI la structure de groupe abélien de $(\mathbb{Z}, +)$. Les propriétés arithmétiques de l'anneau $\mathbb{Z}$ seront étudiées en détail au chapitre IX et plus précisément dans les paragraphes IX.2.7, IX.3.9, IX.4.2, IX.5.5, IX.6.6 et IX.7.9.

IV.1 . −Construction de l'ensemble $\mathbb{Z}$ des entiers relatifs

On cherche à définir $\mathbb{Z}$ comme l'ensemble des « différences » d'entiers naturels c'est-à-dire que, pour deux entiers p et q, il existe un entier naturel r tel que soit $q = p + r$ soit $p = q + r$ (cf. II.2.5.) Dans le dernier cas, on voudrait écrire $p - q = r$ et dans le premier cas, $p - q = -r$.

En procédant ainsi il faudra bien évidemment tenir compte du fait que plusieurs couples peuvent donner la même différence, et prendre ce dernier point en compte dans la définition des opérations sur $\mathbb{Z}$: addition et multiplication. Ce point de vue risque d'être source d'une grande quantité de disjonctions pénibles à manier et l'on sait bien que dès qu'il s'agit d'« identifier » on doit pouvoir recourir au formalisme des relations d'équivalences (cf. I.5.) On procédera donc comme suit, et l'on retrouvera l'idée initiale après avoir construit l'addition sur $\mathbb{Z}$ (cf. IV.3.10.ii) :)

Notation IV.1.1 On note :

$$Z := \mathbb{N} \times \mathbb{N} \qquad \text{IV.1.1.1}$$

l'ensemble des couples d'entiers naturels à ne pas confondre avec $\mathbb{Z}$ que nous allons définir dans cette section.

Sur l'ensemble Z, on considère la relation binaire (cf. I.2.1.iii) :) $\sim$ définie par :

$$\forall (p,q) \in Z,\ \forall (r,s) \in Z,\ (p,q) \sim (r,s) \Leftrightarrow p + s = q + r\ . \qquad \text{IV.1.1.2}$$

Ceci pourrait se réécrire, pour peu qu'on ait introduit la notation $p - q = r - s$ et correspond donc bien à l'idée qu'on se fait que l'on identifie deux couples qui donnent la même « différence ».

Proposition IV.1.2 *La relation $\sim$ est une relation d'équivalence (cf. I.2.2.v).) Pour tout $(p,q) \in Z$ on notera*

$$\overline{(p,q)} := \big\{(r,s) \in Z\ ;\ (r,s) \sim (p,q)\big\}$$

la classe du couple (p,q).

Preuve *: Voir l'exercice IV.6.1.*

IV.2 . −Entiers relatifs

Définition IV.2.1 (Entiers relatifs) On appelle *ensemble des entiers relatifs* l'ensemble des classes de Z selon $\sim$ encore appelé ensemble *quotient* $Z/\sim$ et finalement noté $\mathbb{Z}$. Un élément de $\mathbb{Z}$ est un *entier relatif*.

Notation IV.2.2 On notera :

$$\begin{array}{rccc} \pi : & Z & \to & \mathbb{Z} = Z/\sim \\ & (p,q) & \mapsto & \overline{(p,q)} \end{array} \qquad \text{IV.2.2.1}$$

la *surjection canonique* (cf. I.5.7.ii).)

Proposition IV.2.3 *Pour toute classe $\overline{(p,q)} \in \mathbb{Z}$, il existe un unique entier naturel r, tel que*

$$\overline{(p,q)} = \overline{(r,0)} \text{ ou } \overline{(0,r)} .$$

La disjonction précédente n'étant pas exclusive.

Preuve *: Pour tout couple d'entiers naturels (p,q), il existe, (cf. II.2.5) un entier naturel r tel que*

$$p + r = q \Leftrightarrow (p,q) \sim (0,r) \text{ ou } q + r = p \Leftrightarrow (p,q) \sim (r,0)$$

ce qui prouve l'existence.

Si maintenant, r et r' sont deux entiers naturels tels que, par exemple,

$$\overline{(p,q)} = \overline{(r,0)} = \overline{(r',0)} ,$$

$(r,0) \sim (r',0)$ c'est-à-dire (cf. IV.1.1.2) $r + 0 = r' + 0$ c'est-à-dire $r = r'$ ce qui assure l'unicité.

Proposition IV.2.4 *Les applications*

$$\begin{array}{rccc} i_+ : & \mathbb{N} & \to & \mathbb{Z} \\ & p & \mapsto & \overline{(p,0)} \end{array} \qquad \textit{IV.2.4.1}$$

et

$$\begin{array}{rccc} i_- : & \mathbb{N} & \to & \mathbb{Z} \\ & p & \mapsto & \overline{(0,p)} \end{array} \qquad \textit{IV.2.4.2}$$

sont injectives. (cf. I.2.7.i).)

Preuve *: Si r et r' sont deux entiers naturels tels que $i_+(r) = i_+(r')$, alors*

$$\overline{(r,0)} = \overline{(r',0)}$$

ce qui, nous l'avons déjà vu dans la démonstration de la proposition IV.2.3 implique que $r = r'$.

La vérification pour i_- est tout à fait identique.

Corollaire IV.2.5 *Les propositions IV.2.3 et IV.2.4 ont pour conséquence que :*

i) $i_+(\mathbb{N})$ *est une partie de* $\mathbb{Z}$ *en bijection (cf. I.2.7.iii)) avec* $\mathbb{N}$. *On identifiera dans la suite* $\mathbb{N}$ *à* $i_+(\mathbb{N})$ *et pour tout entier naturel* $p \in \mathbb{N}$, *on écrira aussi* $p \in \mathbb{Z}$ *pour* $\overline{(p,0)} \in \mathbb{Z}$.

ii) L'ensemble $\mathbb{Z}$ *est la réunion de* $i_+(\mathbb{N})$ *et* $i_-(\mathbb{N})$.
On notera souvent

$$\mathbb{Z}^+ \ := \ i_+(\mathbb{N}) \text{ et } \mathbb{Z}^- \ := \ i_-(\mathbb{N})$$

et l'on écrira, également $\mathbb{N} \ = \ \mathbb{Z}^+$.

iii) L'intersection de $i_+(\mathbb{N})$ *et* $i_-(\mathbb{N})$ *est la classe* $\overline{(0,0)}$ *que nous ne tarderons pas à noter simplement* 0.

Définition IV.2.6 (Entiers positifs/négatifs) On appellera $\mathbb{Z}^+$ l'ensemble des *entiers relatifs positifs* et $\mathbb{Z}^-$ l'ensemble des *entiers relatifs négatifs*.

IV.3 . −L'anneau $(\mathbb{Z}, +, *)$

Dans ce paragraphe (IV.3) l'ensemble noté Z est celui introduit en IV.1.1.1.

Notation IV.3.1 On définit une loi de composition $+_Z$ sur Z par :

$$\forall (p,q) \in Z,\ \forall (r,s) \in Z,\ (p,q) \ +_Z \ (r,s) \ := \ (p +_{\mathbb{N}} r, q +_{\mathbb{N}} s) \qquad \text{IV.3.1.1}$$

cette écriture ayant un sens puisque l'addition sur $\mathbb{N}$ est bien définie (cf. II.1.1.)

Une chose est de comprendre quelle peut être la formule qui définit la multiplication, une autre de justifier qu'elle définit bien l'opération que l'on souhaite.

Néanmoins, si l'on supposait la multiplication complètement construite, et possédant toutes les propriétés usuelles, on pourrait tout d'abord écrire tout couple d'entiers relatifs

$$(\alpha, \beta) \ = \ (\overline{(p,q)}, \overline{(r,s)}) \ .$$

Avec les notations introduites en IV.3.10.i), on aurait encore $\alpha = p - q$ et $\beta = r - s$. On écrirait alors très naturellement

$$\alpha * \beta \ = \ (p-q) * (r-s) \ = \ (pr + qs) - (qr + ps)$$

qui est la classe $\overline{(pr + qs, ps + qr)}$. Cette démarche nous montre qu'on doit pouvoir définir la multiplication dans $\mathbb{Z}$ à partir de la multiplication dans $\mathbb{N}$ et passage aux classes.

On définit donc une loi de composition $*_Z$ sur Z (pas encore sur $\mathbb{Z}$,) par :

$$\forall (p,q) \in Z,\ \forall (r,s) \in Z,\ (p,q) \ *_Z \ (r,s) \ := \ (p *_{\mathbb{N}} r +_{\mathbb{N}} q *_{\mathbb{N}} s, p *_{\mathbb{N}} s +_{\mathbb{N}} q *_{\mathbb{N}} r) \qquad \text{IV.3.1.2}$$

en utilisant les opérations $+_{\mathbb{N}}$ et $*_{\mathbb{N}}$ de $\mathbb{N}$ qui sont bien définies.

Lemme IV.3.2 *Les lois $+_Z$ et $*_Z$ définie ci-dessus sur Z sont compatibles à la relation d'équivalence $\sim$ définie en IV.1.1.2 au sens où*

$$\forall x \in Z,\ \forall y \in Z,\ \forall x' \in Z,\ \forall y' \in Z,\ \left(x \sim x' \wedge y \sim y' \ \Rightarrow\ x +_Z y \sim x' +_Z y' \text{ et } x *_Z y \sim x' *_Z y'\right).$$

Preuve *:*

i) (+)
On a, par définition (cf. IV.3.1.1,)

$$(p,q) +_Z (r,s) \ =\ (p+r, q+s) \text{ et } (p',q') +_Z (r',s') \ =\ (p'+r', q'+s').$$

Par ailleurs (cf. IV.1.1.2,) $p+q' \ =\ p'+q$ et $r+s' \ =\ r'+s$ ce qui implique que $p+q'+r+s' \ =\ p'+q+r'+s$ ce qui s'écrit encore

$$(p+r) \ +\ (q'+s') \ =\ (p'+r') \ +\ (q+s)$$

c'est-à-dire que

$$(p+r, q+s) \ \sim\ (p'+r', q'+s')$$

et prouve le résultat.

ii) (∗)
On a donc : $p+q' \ =\ p'+q$ et $r+s' \ =\ r'+s$. Il en résulte que

$$\begin{aligned} p*r + q*s + p'*s + q'*r \ &=\ (p+q')*r + (q+p')*s \\ &=\ (p'+q)*r + (p+q')*s \\ &=\ p'*r + q's + p*s + q*r \end{aligned}$$

c'est-à-dire que

$$(p,q) *_Z (r,s) \ \sim\ (p',q') *_Z (r,s).$$

En appliquant une fois encore ce raisonnement on obtient :

$$(p',q') *_Z (r,s) \ \sim\ (p',q') *_Z (r',s')$$

ce qui achève la preuve par transitivité de $\sim$.

Proposition IV.3.3 *Il existe un unique couple de lois $(+,*)$ sur $\mathbb{Z}$ tel que la surjection canonique π définie en IV.2.2.1 soit simultanément un morphisme de $(Z,+_Z)$ dans $(\mathbb{Z},+)$ et de $(Z,*_Z)$ dans $(\mathbb{Z},*)$.*

Preuve *: La compatibilité des lois $+_Z$ et $*_Z$ sur Z avec la relation déquivalence $\sim$ ayant été établie au lemme IV.3.2, le résultat découle de la proposition I.6.18.*

Proposition IV.3.4 (Le groupe $(\mathbb{Z},+)$) *Le couple $(\mathbb{Z},+)$ est un groupe abélien (cf. III.1.3.)*

***Preuve** :*

*i) (**Associativité**)*
Il faut vérifier que la loi $+$ est associative, mais en vertu de la proposition I.6.18, il suffit de vérifier que $+_Z$ est associative. Or

$$\begin{aligned}\big((p,q)+_Z(r,s)\big)+_Z(t,u) &= (p+r,q+s)+_Z(t,u)\\ &= ((p+r)+t,(q+s)+u)\\ &= (p+(r+t),q+(s+u))\\ &= (p,q)*_Z\big((r,s)+_Z(t,u)\big)\end{aligned}$$

en utilisant l'associativité de $+$ dans $\mathbb{N}$ (cf. II.1.5.i).)

*ii) (**Élément neutre**)*
On constate que

$$\forall (p,q)\in Z,\ ((p,q)+_Z(0,0)\ =\ (0,0)+_Z(p,q)\ =\ (p,q))$$

c'est-à-dire que $(0,0)$ est un élément neutre pour $+_Z$. En utilisant encore la proposition I.6.18, il s'ensuit que $\overline{(0,0)}$ est un élément neutre pour $(\mathbb{Z},+)$.

*iii) (**Symétrique**)*
Pour tout $\overline{(p,q)}\ \in\ \mathbb{Z}$,

$$\overline{(p,q)}\ +\ \overline{(q,p)}\ =\ \overline{(p+q,p+q)}\ =\ \overline{(0,0)}\,;$$

c'est-à-dire que $\overline{(q,p)}$ est un opposé à droite pour $\overline{(p,q)}$ mais l'identité ci-dessus étant vraie $\forall p,\forall q$, c'est aussi un opposé à gauche.

*iv) (**Commutativité**)*
Il est encore immédiat de constater que

$$\forall (p,q)\in Z,\ \forall (r,s)\in Z,\ \big((p,q)+_Z(r,s)\ =\ (p+r,q+s)\ =\ (r+p,s+q)\ =\ (r,s)+_Z(p,q)\big)$$

en utilisant la commutativité de $+_{\mathbb{N}}$ dans $\mathbb{N}$ (cf. II.1.5.iii).) On conclut ensuite à la commutativité de $(\mathbb{Z},+)$ une fois encore graçe à la proposition I.6.18.ii).

Les propriétés établies ci-dessus font de $(\mathbb{Z},+)$ un groupe abélien.

Remarque IV.3.5 (L'opposé dans $\mathbb{Z}$) Il convient de s'arrêter un instant sur le fait que, parmi les quatre propriétés établies dans la démonstration de la proposition IV.3.4 la seule qui ne s'obtienne pas grâce à une propriété analogue de $(\mathbb{N}, +_{\mathbb{N}})$ est l'existence du symétrique (oppposé.) Rien de surprenant à cela, puisque précisément c'est le manque de symétrique dans $\mathbb{N}$ qui conduit à construire $\mathbb{Z}$ rien d'étonnant encore qu'on ne le trouve pas avant (même dans Z) sans quoi on ne se serait peut-être pas donné le mal de construire $\mathbb{Z}$.

Proposition IV.3.6 *Étant donné un groupe $(G, \cdot)$, pour tout $x \in G$, il existe un unique morphisme de groupes*

$$\epsilon_x \,:\, \mathbb{Z} \,\to\, G$$

tel que

$$\epsilon_x(1) \,=\, x\,.$$

***Preuve** : (cf. Problème n° II, exercice A.)*

Notation IV.3.7 Avec la les notations de la proposition IV.3.6, on notera usuellement

$$x^n \,:=\, \epsilon_x(n) \text{ ou même } nx \,:=\, \epsilon_x(n) \text{ si } G \text{ est abélien }.$$

Proposition IV.3.8 (L'anneau $(\mathbb{Z}, +, *)$) *Le triplet $(\mathbb{Z}, +, *)$ est un anneau commutatif (cf. I.6.25.i).)*

***Preuve** :*

*i) (**Associativité de** $*$)*

$$\forall (p,q) \in Z,\ \forall (r,s) \in Z,\ \forall (t,u) \in Z,$$

on a :

$$\begin{aligned}\big((p,q) *_Z (r,s)\big) *_Z (t,u) &= (pr+qs, ps+qr) *_Z (t,u)\\ &= (prt+qst+psu+qru, pst+qrt+pru+qsu)\\ &= (p(rt+su)+q(st+ru), p(st+ru)+q(rt+su))\\ &= (p,q) *_Z \big((r,s) *_Z (t,u)\big)\,.\end{aligned}$$

Il suffit ensuite d'utiliser la proposition I.6.18.ii) pour assurer l'associativité de $*$ sur $\mathbb{Z}$.

ii) La démonstration des autres propriétés (élément neutre, commutativité et distributivité sur $+$) est facile et laissée en exercice. Elle se fait sur le même modèle. On pourra en particulier se rapporter au I.8.10.

Proposition IV.3.9 *Les applications i_+ et i_- étant celles introduites dans la proposition IV.2.4, pour tout couple (p, q) d'entiers naturels,*

$$i_+(p+q) \;=\; i_+(p) \;+\; i_+(q) \quad , \quad i_-(p+q) \;=\; i_-(p) \;+\; i_-(q),$$
$$i_+(p*q) \;=\; i_+(p)*i_+(q) \quad \text{et} \quad i_-(p*q) \;=\; i_-(p)*i_+(q) \;=\; i_+(p)*i_-(q)\,;$$

c'est-à-dire que i_+ est un morphisme pour $+$ et $*$ au sens de I.6.2 ; tandis que i_- en est un pour $+$ mais pas tout à fait pour $*$.

Preuve *: Voir l'exercice IV.6.2.*

Notation IV.3.10 i) **(Opposé)**

On sait (cf. IV.2.5.ii)) que pour tout entier relatif α il existe un entier naturel p, tel que $\alpha = i_+(p)$ ou $i_-(p)$ c'est-à-dire que $\alpha = \overline{(p,0)}$ ou $\alpha = \overline{(0,p)}$. On a déjà convenu, (cf. IV.2.5.i),) de noter simplement p la classe $\overline{(p,0)}$. Nous venons de plus de constater (cf. IV.3.4) que $\overline{(0,p)}$ est l'opposé de $\overline{(p,0)}$ pour la loi de composition $+$ que nous venons de définir. Traditionnellement on note $-p$ l'opposé de p, et l'on retrouve ainsi la notation usuelle.

Pour résumer, pour tout entier relatif α, il existe un unique entier naturel p tel que $\alpha = p$ ou α est l'opposé dans $\mathbb{Z}$ de p vu comme entier relatif qu'on note $-p$.

ii) Même si cette opération est définie grâce à la loi $+$ et à l'opposé dans $\mathbb{Z}$ il est commode de définir une loi de *soustraction* noté $-$ sur $\mathbb{Z}$ et définie comme la *somme* avec l'opposé c'est-à-dire que pour tout couple (p, q) d'entiers relatifs,

$$p - q \;:=\; p + (-q)\,.$$

On remarque qu'alors, pour des entiers naturels p et q,

$$p - q \;=\; \overline{(p,q)}\,.$$

Proposition IV.3.11 (Règles de calcul) *On a les propriétés suivantes :*

i) Pour tout $p \in \mathbb{Z}$, $-(-p) = p$.

ii) Pour tout $p \in \mathbb{Z}$, $p \in \mathbb{Z}^+$ si et seulement si $-p \in \mathbb{Z}^-$ (cf. IV.2.5.ii).)

iii) Pour tout couple (p, q) d'entiers relatifs,

$$-(p-q) \;=\; q - p\,.$$

On établit de manière analogue les règles usuelles :

iv)

$$(-p)*q \;=\; p*(-q) \;=\; -(p*q)$$

que l'on notera simplement $-p*q$.

v)

$$(-p) * (-q) \ = \ p * q \ .$$

vi) $(-1) * p \ = \ -p$.

Preuve *: Voir l'exercice IV.6.3.*

Proposition IV.3.12 (Intégrité) *Pour tout couple d'entiers relatifs* (p, q) $p * q = 0$ *si et seulement si* $p \ = \ 0$ *ou* $q \ = \ 0$ *c'est-à-dire que* $(\mathbb{Z}, +, *)$ *est un anneau intègre* [5]

Preuve *: On laisse le soin au lecteur de déduire cet énoncé de la proposition II.3.4.*

Corollaire IV.3.13 *Pour tout triplet* (p, q, r) *d'entiers relatifs,* $p * r \ = \ q * r$ *si et seulement si* $r = 0$ *ou* $p = q$.

Proposition IV.3.14 *Pour tout couple d'entiers relatifs* (p, q) $p * q = 1$ *si et seulement si* $(p, q) \ = \ (1, 1)$ *ou* $(p, q) \ = \ (-1, -1)$.

Preuve *:*

i) Si p *et* q *sont positifs (cf. IV.2.6,) on a* $(p, q) \ = \ (1, 1)$ *d'après la proposition II.3.7.*

ii) Si p *et* q *sont négatifs,* $-p$ *et* $-q$ *sont positifs (cf. IV.3.11.ii).) De plus,* $p * q = (-p) * (-q)$ *(cf. IV.3.9.) Il en résulte que* $(-p, -q) \ = \ (1, 1)$ *d'après le point précédent et par conséquent que* $(p, q) \ = \ (-1, -1)$.

iii) Si p *est négatif et* q *positif,* $-p$ *est positif et* $p*q \ = \ -(-p)*q$ *est négatif d'après les propositions IV.3.9 et IV.3.11.ii). Cette situation n'est donc pas possible puisque* $1 \ = \ \overline{(1, 0)} \ \in \ \mathbb{Z}^+$.

Définition IV.3.15 (Éléments inversibles) Les seuls éléments de $\mathbb{Z}$ qui ont un *inverse* sont donc 1 et -1. On dira que ce sont des éléments *inversibles* de $\mathbb{Z}$. On notera $\mathbb{Z}^\times \ := \ \{-1, 1\}$ l'ensemble des éléments inversibles de $\mathbb{Z}$.

Remarque IV.3.16 De manière analogue à ce qu'on a fait dans la remarque II.3.8, pour tout $p \in \mathbb{Z}$, on pose $p^0 \ := \ 1$ et

$$\forall n \in \mathbb{N}, \ p^{n+1} \ := \ p * p^n \ .$$

On définit ainsi la *puissance* $n^{\text{ième}}$ de l'entier relatif p. Dans l'écriture ci-dessus, l'entier n s'appelle l'*exposant*.

Il n'est pas difficile d'établir, par récurrence sur l'exposant bien entendu (cf. II.0.PA_3),) que pour tout couple (n, m) d'entiers naturels,

$$p^{n+m} \ = \ p^n \ * \ p^m \ .$$

5. Cette notion sera étudiée en plus grands détails au chapitre VII.

IV.4 . −Ordre sur $\mathbb{Z}$

On définit maintnant une relation d'ordre sur $\mathbb{Z}$ (cf. I.2.2.vi),) dont on va montrer qu'elle satisfait de « bonnes propriétés » relativement à l'addition $+$, la multiplication $*$ et les injection i_+ et i_-.

Définition IV.4.1 ($\leq$) On définit la relation $\leq$ sur $\mathbb{Z}$, par la formule :

$$\forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z},\ \big(p \ \leq\ q \ \Leftrightarrow\ \exists r \in \mathbb{N},\ (q \ =\ p + r)\big)\ . \qquad \text{IV.4.1.1}$$

Pour tout couple (p, q) d'entiers relatifs, si $p \leq q$, on dira que p est *inférieur ou égal à* q.

Proposition IV.4.2 (Ordre) *La relation $\leq$ définie ci-dessus est une relation d'ordre totale sur $\mathbb{Z}$ (cf. I.2.2.vi).)*

***Preuve** : Le fait que $\leq$ soit réflexive et transitive procède d'arguments semblables à ceux utilisés pour les propriétés analogues de la relation $\leq$ sur $\mathbb{N}$ (cf. II.2.2.)*

Pour tout couple (p, q) d'entiers relatifs, si $p \leq q$, et $q \leq p$, on a : $q - p \in \mathbb{Z}^+$ et $p - q \in \mathbb{Z}^+$. Or $p - q \in \mathbb{Z}^+$ équivaut (cf. IV.3.11.ii)) à $q - p \in \mathbb{Z}^-$. On a donc

$$q - p \ \in\ \mathbb{Z}^+ \cap \mathbb{Z}^-$$

ce qui implique (cf. IV.2.5.iii)) que $q - p \ =\ 0$ c'est-à-dire que $p \ =\ q$. La relation $\leq$ est donc antisymétrique et c'est donc une relation d'ordre.

Le fait qu'elle est totale c'est-à-dire qu'on puisse toujours comparer deux éléments, est une conséquence de IV.2.5.ii).

Remarque IV.4.3 On peut définir une relation $\geq$ de manière évidente sur $\mathbb{Z}$ qui est aussi une relation d'ordre ainsi que des relations $<$ et $>$ qui ne sont pas des relations d'ordre (cf. II.2.3.)

Proposition IV.4.4 *Pour tout couple d'entiers <u>naturels</u> (p, q), $p \leq_{\mathbb{N}} q$ au sens de la relation d'ordre sur $\mathbb{N}$ si et seulement si $i_+(p) \leq_{\mathbb{Z}} i_+(q)$ (cf. IV.2.4.1) que l'on écrira bien entendu $p \leq q$ au sens de la relation d'ordre sur $\mathbb{Z}$. Autrement dit, i_+ est un morphisme pour les relations d'ordre $\leq$ sur $\mathbb{N}$ et $\mathbb{Z}$ c'est-à-dire encore une application croissante (cf. I.2.10.)*

On pourrait encore dire que la relation d'ordre sur $\mathbb{Z}$ « prolonge » la relation d'ordre sur $\mathbb{N}$.

Proposition IV.4.5 (Propriétés de $\leq$) *i) **(Cône positif)***

Pour tout $p \in \mathbb{Z}^-$ et tout $q \in \mathbb{Z}^+$, $p \leq q$.

*ii) **(Addition et ordre)***

Pour tout quadruplet d'entiers relatifs (p, q, r, s) $p \leq q$ et $r \leq s$, implique $p + r \leq q + s$.

*iii) **(Multiplication et ordre)***

Pour tout triplet (p, q, r) d'entiers relatifs, si $p \leq q$ et $r \geq 0$, alors $r * p \leq r * q$.

Remarque IV.4.6 On laisse le soin au lecteur d'établir toutes les variantes usuelles de l'énoncé ci-dessus.

Proposition IV.4.7 *Toute partie non vide majorée (resp. minorée) de $\mathbb{Z}$ possède un plus grand élément (resp. un plus petit élément.)*

Le plus grand élément est le plus petit des majorants, tandis que le plus petit élément est le plus grand des minorants. Ceci implique, en particulier, l'unicité du plus grand (resp. du plus petit élément.)

Preuve *: On ne démontre que partiellement cette proposition, le reste de l'argument ayant la même forme.*

Étant donnée une partie non vide et majorée P de $\mathbb{Z}$,

i) si $Q := P \cap \mathbb{Z}^+ \neq \emptyset$, Q est une partie non vide majorée de $\mathbb{N}$ et possède donc un plus grand élément (cf. II.2.10.) Il est facile de voir que ce plus grand élément est encore un plus grand élément pour P.

ii) Si $P \cap \mathbb{Z}^+ = \emptyset$, il découle de la proposition IV.3.11.ii) que $P' := \{-p\ ,\ p \in P\}$, est une partie de $\mathbb{Z}^+ = \mathbb{N}$. Elle possède donc un plus petit élément ℓ d'après la proposition II.2.9. Reste à vérifier, ce qui est élémentaire, que $-\ell$ est un plus grand élément pour P.

Proposition IV.4.8 (Parties finies) *i) Une partie de $\mathbb{Z}$ est soit finie (cf. II.4.1,) soit dénombrable (cf. II.4.6.)*

ii) Une partie non vide de $\mathbb{Z}$ est finie si et seulement si elle est à la fois majorée et minorée, si et seulement si elle admet simultanément un plus grand et un plus petit élément.

Définition IV.4.9 (Valeur absolue) La proposition IV.3.11.ii) permet de définir la *valeur absolue* d'un entier relatif de la manière suivante :

i) si $p \in \mathbb{Z}^+$, on appelle valeur absolue de p et on note $|p|$ l'entier relatif p lui-même ;

ii) si $p \in \mathbb{Z}^-$, la valeur absolue $|p|$ de p est l'entier $-p \in \mathbb{Z}^+$.

De manière équivalente, on peut dire que la valeur absolue d'un entier relatif p est le plus grand des deux nombres p et $-p$:

$$|p| = \max(p, -p)\ .$$

La valeur absolue est donc une application de $\mathbb{Z}$ dans $\mathbb{N}$.

Proposition IV.4.10 (Propriétés de la valeur absolue) *La valeur absolue sur $\mathbb{Z}$ a les propriétés suivantes :*

i) $|0| = 0$;

ii)

$$\forall p \in \mathbb{Z},\ p \ \leq\ |p|\ ;$$

iii)

$$\forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z},\ |p*q| \ =\ |p|*|q|\ ;$$

iv)

$$\forall p \in \mathbb{Z},\ |-p| \ =\ |p|\ ;$$

v)

$$\forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z},\ ||p|-|q|| \ \leq\ |p+q| \ \leq\ |p| \ +\ |q|\ .$$

IV.5 . −Le théorème de la division euclidienne

Proposition IV.5.1

$$\forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z},\ \big(p|q \text{ et } q \ \neq\ 0 \ \Rightarrow\ |p| \leq |q|\big)\ .$$

Preuve *:*

$$\begin{array}{lr} \forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z}, & p|q \quad \text{et} \quad q \neq 0 \\ \Rightarrow & \exists r \in \mathbb{Z},\ q \ =\ p*r \quad \text{et} \quad r \neq 0 \\ \Rightarrow & \exists r \in \mathbb{Z},\ |r|*|p| \ =\ |q| \quad \text{et} \quad r \neq 0 \end{array}$$

Or

$$r \neq 0 \ \Rightarrow\ |r| \neq 0 \ \Rightarrow\ 1 \leq |r| \ \Rightarrow\ |p|*1 \ \leq\ |p|*|r| \ =\ |q|$$

en utilisant la proposition II.3.6.

Théorème IV.5.2 (de la division euclidienne) *Pour tout couple d'entiers relatifs* $(a,b),\ b \neq 0$, *il existe un unique couple d'entiers relatifs* (q,r) *tel que :*

$$a \ =\ b*q \ +\ r \text{ et } 0 \ \leq\ r \ <\ |b|\ . \qquad \textit{IV.5.2.1}$$

Preuve *:*

i) ***(Existence)***
Montrons d'abord l'existence du couple (q,r). *Considérons pour cela l'ensemble*

$$K \ :=\ \{a - b*k\ ,\ k \in \mathbb{Z}\}\ .$$

Lemme i).1

$$K \ \cap\ \mathbb{Z}^+ \ \neq\ \emptyset\ .$$

Preuve *: Remarquons que K n'est pas vide puisque $a = a - b * 0 \in K$. Si $K \cap \mathbb{Z}^+$ était vide, d'après la proposition IV.2.5.ii), pour tout $m \in K$, $m \leq 0$. L'ensemble K serait donc une partie non vide majorée de $\mathbb{Z}$ et posséderait donc, d'après la proposition IV.4.7, un plus grand élément $a - b * k_0$.*

Cependant, si $b > 0$,

$$a - b * (k_0 - 1) = a - b * k_0 + b > a - b * k_0$$

ce qui est contradictoire.

Si $b < 0$,

$$a - b * (k_0 + 1) = a - b * k_0 - b > a - b * k_0$$

ce qui est encore contradictoire.

Il en résulte donc que $K \cap \mathbb{Z}^+$ possède, d'après la proposition II.2.9, un plus petit élément $a - b * q$.
Reste finalement à montrer que $a - b * q < |b|$. Or $a - b * q \geq |b|$ entraîne :
— si $b > 0$, $|b| = b$ et $a - b * q \geq b$ implique $a - b * (q + 1) \geq 0$. Par ailleurs, $a - b * (q + 1) < a - b * q$ ce qui contredit la minimalité de $a - b * q$ dans $K \cap \mathbb{Z}^+$.
— Le cas $b < 0$ est laissé en exercice.

*ii) (**Unicité**)*

Supposons maintenant qu'il existe deux couples (q, r) et (q', r') satisfaisant aux conditions IV.5.2.1 du théorème. On a alors $b * q + r = b * q' + r'$ ce qui implique

$$r' - r = b * (q - q')$$

c'est-à-dire que b divise $r' - r$. Par ailleurs, on a $0 \leq r < |b|$ et $0 \leq r' < |b|$ ce qui implique que $-|b| < r' - r < |b|$. Ceci équivaut à $|r' - r| < |b|$. On en déduit, en appliquant la proposition IV.5.1 que $r' - r = 0$. Il s'ensuit que $b * (q - q') = 0$ mais comme $b \neq 0$, d'après la proposition IV.3.12, $q - q' = 0$ ce qui achève de prouver l'unicité du couple (q, r).

Définition IV.5.3 Avec les notations du théorème IV.5.2, on adopte en général la terminologie usuelle suivante : a est le *dividende* b le *diviseur* q un *quotient* et r un *reste* (cf. IX.7.1.)

On peut même, en vertu de IV.5.4.a), parler du reste et du quotient.

Remarque IV.5.4 a) On peut constater que l'énoncé IV.5.2.1 est plus précis que celui correspondant IX.7.1.1 définissant un stathme euclidien. Cet énoncé conduit à l'unicité du couple (q, r) qui n'est pas exigée dans la définition IX.7.1. Nous constaterons cependant, qu'un tel énoncé d'unicité n'est pas requis pour établir la proposition IX.7.4 dont le corollaire IV.5.5 est l'équivalent pour l'anneau $\mathbb{Z}$.

b) On laisse le soin au lecteur de justifier que, si dans la division euclidienne de a par b, a et b sont *positifs* q l'est aussi.

Corollaire IV.5.5 (Structure des sous-groupes de $(\mathbb{Z},+)$) *Pour toute partie $H \subset \mathbb{Z}$, H est un sous-groupe (cf. III.3.1,) si et seulement s'il existe $d \in \mathbb{Z}$ tel que*

$$H = d\mathbb{Z} := \{d * k \,;\, k \in \mathbb{Z}\} .$$

Preuve *:* *Voir le TD n° IV, exercice A.*

— *Si $H = \{0\}$,*

$$H = 0\mathbb{Z} = \{0z \,,\, z \in \mathbb{Z}\} .$$

— *Si $H \neq \{0\}$ il existe un entier relatif $x \neq 0$ appartenant à H. Soit $x \in \mathbb{N}^*$ soit $-x$ qui appartient également à H puisque H est un sous-groupe de $\mathbb{Z}$, appartient à $\mathbb{N}^*$ c'est-à-dire que*

$$H \cap \mathbb{N}^* \neq \emptyset .$$

Notons d le plus petit élément de $H \cap \mathbb{N}^*$ qui existe en vertu de la proposition II.2.9.

— *Remarquons tout d'abord que*

$$d\mathbb{Z} = \{dz \,,\, z \in \mathbb{Z}\} \subset H .$$

En effet, $d*0 = 0 \in H$. Pour tout entier naturel n, si $dn \in H$, $d*(n+1) = d*n+d \in H$. Il en résulte (cf. II.0.PA$_3$),) que $d\mathbb{N}^* \in H$. Par ailleurs, pour tout entier relatif n, $dn \in H$ si et seulement si

$$-dn = d*(-n) \in H .$$

Ceci, combiné avec ce qui précède montre que

$$d\mathbb{Z} \subset H .$$

— *Enfin, pour tout $n \in H$, effectuons la division euclidienne (cf. IV.5.3,) de n par $d > 0$. Il existe donc des entiers q et r tels que*

$$n = dq + r \text{ et } 0 \leq r < d .$$

Or $dq \in H$ d'après le point précédent et $n \in H$ par hypothèse, ce qui implique, H étant un sous-groupe, que

$$r = n - dq \in H .$$

L'encadrement de r et la minimalité de d, impliquent que $r = 0$ c'est-à-dire que $n = dq$. On en conclut que

$$H \subset d\mathbb{Z} .$$

Corollaire IV.5.6 (Notation de position) *Un entier naturel $b > 1$ étant fixé, pour tout entier relatif $a \neq 0$, il existe un unique entier naturel d un unique élément $\epsilon \in \mathbb{Z}^\times = \{-1; 1\}$ et un unique $d+1$-uplet $r_{i\ ,0\leq i\leq d}$ tel que*

$$a = \epsilon \sum_{i=0}^{d} r_i b^i \ ; \qquad \text{IV.5.6.1}$$

$$\forall 0 \leq i \leq d,\ 0 \leq r_i \leq b \ ; \qquad \text{IV.5.6.2}$$

$$r_d \neq 0 \ . \qquad \text{IV.5.6.3}$$

Preuve *: (voir TD n° IV, exercice D.)*

*i) (**Existence**)*

On va tout d'abord chercher à prouver l'existence des entiers d et $r_{i\ ,0\leq i\leq d}$.

a) ($a \geq 0$)

Supposons d'abord que $a > 0$. Notons A l'ensemble des entiers naturels $p > 0$ tels que pour tout $q \leq p$, il existe un entiers d_q et des entiers $r_{q,i\ ,0\leq i\leq d_q}$ tels que

$$q = \sum_{i=0}^{d_q} r_{q,i} b^i \text{ avec } 0 \leq r_{q,i} < b \text{ et } r_{q,d_q} \neq 0 \ .$$

L'entier 1 appartient à A puisque $1 = 1 + 0 * b$.

Pour $p \in A$, l'ensemble

$$B_p := \{b^k \ , \ k \in \mathbb{N} \ ; \ b^k \leq p+1\}$$

est non vide puisque $b^0 = 1 \leq p+1$ et clairement majoré par $p+1$. Il admet donc un plus grand élément (cf. IV.4.7,) b^d. Comme $b > 1$, $b^{d+1} = b * b^d > b^d$ et par maximalité de b^d on a donc

$$b^d \leq p+1 < b^{d+1} \ .$$

Notons r_d le quotient de la division euclidienne de $p+1$ par b^d et ρ son reste. On a donc,

$$0 \leq \rho < b^d \ .$$

Ceci implique, en particulier, que $r_d b^d \leq p+1 < b^{d+1}$ ce qui implique que $r_d < b$. Par ailleurs, en vertu de la remarque IV.5.4.b), on a également $r_d \geq 0$. Cependant, $r_d = 0$ signifierait que $\rho = p+1 \geq b^d$ ce qui est contradictoire. Il en résulte que

$$0 < r_d < b \ .$$

Finalement $\rho < b^d$, implique que $\rho < p+1$ c'est-à-dire que $\rho \leq p$. Grâce à l'hypothèse de récurrence faite sur p, on sait qu'il existe un entier d' et des entiers $r'_{i\ ,0\leq i\leq d'}$ tels que

$$\rho = \sum_{i=0}^{d'} r'_i b^i$$

avec $r'_{d'} \neq 0$. *Ce dernier point a en particulier pour conséquence, comme* $\rho < b^d$, *que* $d' < d$. *On a donc finalement que*

$$p+1 \;=\; r_d b^d \;+\; \sum_{i=0}^{d'} r'_i b^i$$

c'est-à-dire, sous l'hypothèse que p *appartient à* A, $p+1$ *appartient à* A. *Autrement dit* A *satisfait au principe de récurrence II.0.PA*$_3$*) et par conséquent,* A *est l'ensemble* $[1;+\infty[$ *des entiers supérieurs ou égaux à* 1.

b) $(a \leq 0)$
Si a *est négatif, on peut appliquer le résultat précédent à* $-a$ *et l'on prendra* $\epsilon = -1$.

*ii) (**Unicité**)*
On va maintenant montrer l'unicité de l'écriture précédente. Supposons que pour un entier relatif $a \neq 0$, *il existe*

$$\epsilon\ ,\ \epsilon'\ ,\ d\ ,\ d'\ ,\ r_{i\ ,0\leq i\leq d}\ \text{et}\ r'_{i\ ,0\leq i\leq d'}$$

tels que

$$a \;=\; \epsilon \sum_{i=0}^{d} r_i b^i \;=\; \epsilon' \sum_{i=0}^{d'} r'_i b^i\ .$$

a) Il est tout d'abord clair que ceci implique que $\epsilon = \epsilon'$.

b) Si $d \neq d'$, *on peut par exemple supposer que* $d > d'$. *Or on montrera en exercice que*

$$\sum_{i=0}^{d'} r'_i b^i \;<\; b^{d'+1}\ .$$

Or $d > d'$ *implique que* $d \geq d'+1$ *ce qui implique encore, comme* $r_d \neq 0$ *par hypothèse, que*

$$r_d b^d \;\geq\; b^{d'+1} \;>\; \sum_{i=0}^{d'} r'_i b^i$$

ce qui est contradictoire. On a donc $d = d'$.

c) On a par conséquent,

$$\sum_{i=0}^{d} r_i b^i \;=\; \sum_{i=0}^{d} r'_i b^i$$

ce qui implique que

$$\begin{aligned} r_0 - r'_0 \;&=\; \sum_{i=1}^{d} (r'_i - r_i) b^i \\ &=\; b * \sum_{i=1}^{d} (r'_i - r_i) b^{i-1} \end{aligned}$$

c'est-à-dire que $b|r_0 - r'_0$. *Ceci implique, par un argument déjà donné dans la preuve du théorème IV.5.2 que* $r_0 = r'_0$. *On commence ainsi un raisonnement par récurrence sur* i *compris entre* 0 *et* d, *permettant de montrer que* $r_i = r'_i$ *pour tout* $0 \leq i \leq d$. *On laisse le lecteur terminer cette preuve.*

Remarque IV.5.7 Ce corollaire justifie la notation de position c'est-à-dire qu'on peut écrire tout entier relatif en base b (usuellement en base 10 ou $2,$) comme somme de puissances de b avec des coefficients compris entre 0 et b et en utilisant également un signe $+$ ou $-$.

IV.6 . −Exercices

Exercice IV.6.1 Faire la preuve de la proposition IV.1.2.

Exercice IV.6.2 Faire la preuve de la proposition IV.3.9.

Exercice IV.6.3 Faire la preuve de la proposition IV.3.11.