Entiers relatifs

1 Définition

On définit, sur l'ensemble $\mathbb{N} \times \mathbb{N}$, la relation binaire $\mathfrak{R}$ par :

$$(a,b)\mathfrak{R}(c,d) \iff a+d = b+c$$

On vérifie sans peine que $\mathfrak{R}$ est bien une relation d'équivalence :

- La réflexivité découle de la commutativité de l'addition sur $\mathbb{N}$.
- Idem pour la symétrie.
- La transitivité n'est guère plus compliquée : soient (a,b), (c,d) et (e,f) tels que $(a,b)\mathfrak{R}(c,d)$ et $(c,d)\mathfrak{R}(e,f)$. On a alors

  $$a+d = b+c \quad \text{et} \quad c+f = d+e$$

  donc
  $$(a+d)+(c+f) = (b+c)+(d+e)$$

  En utilisant l'associativité et la commutativité de l'addition sur $\mathbb{N}$, il vient :

  $$(a+f)+(c+d) = (b+e)+(c+d)$$

  Comme tous les éléments de $\mathbb{N}$ sont réguliers pour l'addition, on obtient l'égalité $a+f = b+e$, c'est-à-dire le résultat voulu $(a,b))\mathfrak{R}(e,f)$.

Définition Un *entier relatif* α est une classe d'équivalence pour la relation $\mathfrak{R}$. Si (a,b) est dans la classe α, on note $\alpha = \overline{(a,b)}$. Enfin, on note $\mathbb{Z}$ l'ensemble des entiers relatifs ($\mathbb{Z} = \mathbb{N}^2/\mathfrak{R}$).

N.B. $\mathbb{Z}$ est donc dénombrable, grâce au théorème de Cantor-Bernstein ($\mathbb{Z}$ se plonge dans $\mathbb{N}^2$, lui-même dénombrable). Il est d'ailleurs on ne peut plus élémentaire de construire une bijection de $\mathbb{N}$ sur $\mathbb{Z}$.
Remarque Pour tout entier relatif α, il existe un unique représentant (c,d) de α (*i.e.* un unique élément de la classe α) tel que $c = 0$ ou $d = 0$. Celui-ci est appelé *représentant canonique* de α.

En effet, si $\alpha = \overline{(a,b)}$, on peut distinguer deux cas :

- $a \geq b$: L'entier naturel $m = a - b$ est alors bien défini, et l'on a $a + m = b + 0$, donc $(m,0)$ est aussi un représentant de α, d'où l'existence.
  Si (c,d) est un représentant de α vérifiant $c = 0$ ou $d = 0$, alors $c = m+d$, donc $d = 0$ (sinon $c \geq d > 0$), et donc $c = m$, d'où l'unicité.
- $a < b$: Là aussi, en posant $m = b - a$, on a $a + m = b$ donc $\alpha = \overline{(0,m)}$. L'unicité se prouve exactement de la même manière.

Définition Si α est de la forme $\overline{(m,0)}$, on dit que α est un entier *positif*. Si α est de la forme $\overline{(0,m)}$, on dit que α est un entier *négatif*.

On note $\mathbb{Z}_+$ (resp. $\mathbb{Z}_-$) l'ensemble des entier positifs (resp. négatifs). Dans tous les cas, l'entier naturel m est appelé *valeur absolue* du relatif α, notée $|\alpha|$.

Il est temps de revenir aux notations standards pour les entiers relatifs, pour éviter trop de lourdeur. Rappelons toutefois que, pour l'instant, ce n'est qu'une notation...

Notation : Lorsque α est de la forme $\overline{(m,0)}$, on identifie α et m. Et lorsque α est de la forme $\overline{(0,m)}$, on le note $-m$.

2 Addition dans $\mathbb{Z}$

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

$$(a,b)+(c,d)=(a+c,b+d)$$

Montrons que cette opération est compatible avec la relation d'équivalence $\mathfrak{R}$. Soient $(a,b)\mathfrak{R}(a',b')$ et $(c,d)\mathfrak{R}(c',d')$. Alors par définition de $\mathfrak{R}$, on a :

$$a+b'=b+a' \quad \text{et} \quad c+d'=d+c'$$

soit par sommation $(a+c)+(b'+d')=(b+d)+(a'+c')$

c'est-à-dire que l'on a bien $(a+c,b+d)\mathfrak{R}(a'+c',b'+d')$. Notre addition sur $\mathbb{N}^2$ passe donc au quotient (on peut définir la somme de deux classes), et induit donc une opération sur $\mathbb{Z}$:

Définition Si $\alpha=\overline{(a,b)}$ et $\beta=\overline{(c,d)}$, on définit leur somme $\alpha+\beta$ par :

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

Remarques

- Si $\alpha\in\mathbb{Z}_+$ et $\beta\in\mathbb{Z}_+$, alors $\alpha+\beta\in\mathbb{Z}_+$. En effet, α est de la forme $\overline{(m,0)}$ et β de la forme $\overline{(n,0)}$, et alors $\alpha+\beta=\overline{(m+n,0)}$ est encore dans $\mathbb{Z}_+$.
- De la même façon, si $\alpha\in\mathbb{Z}_-$ et $\beta\in\mathbb{Z}_-$, alors $\alpha+\beta\in\mathbb{Z}_-$.

Théorème 2.1 $(\mathbb{Z},+)$ *est un groupe commutatif.*

Démonstration : La commutativité découle immédiatement de la commutativité de l'addition sur $\mathbb{N}$, tout comme l'associativité découle de l'associativité de l'addition sur $\mathbb{N}$. On vérifie également sans difficulté que $\overline{(0,0)}$, noté 0, est un élément neutre pour l'addition sur $\mathbb{Z}$.

Reste à montrer que tout élément est symétrisable. Soit donc $\alpha=\overline{(a,b)}\in\mathbb{Z}$. En posant $\beta=\overline{(b,a)}$, on vérifie que :

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

On note $-\alpha$ ce symétrique (appelé ici *opposé*) de α.

□

Remarques

- Si $\alpha\in\mathbb{Z}_+$, alors $-\alpha\in\mathbb{Z}_-$. (en effet l'opposé de $\overline{(m,0)}$ est $\overline{(0,m)}$ d'après ce qui précède.) De même, si $\alpha\in\mathbb{Z}_-$, alors $-\alpha\in\mathbb{Z}_+$.
- Pour tout entier relatif α, on a $-(-\alpha)=\alpha$. (immédiat par la structure de groupe.)
- Pour tout entier relatif α, on a $|-\alpha|=|\alpha|$.

Notation : L'entier $\beta+(-\alpha)$ est noté $\beta-\alpha$, et appelé *différence* de β et α.

3 Relation d'ordre dans $\mathbb{Z}$

Définition On définit la relation binaire $\leq$ sur $\mathbb{Z}$ par :

$$\alpha \leq \beta \Longleftrightarrow \beta - \alpha \in \mathbb{Z}_+$$

Théorème 3.1 *$\leq$ est une relation d'ordre total sur $\mathbb{Z}$.*

Démonstration :

- Réflexivité : Pour tout $\alpha \in \mathbb{Z}$, on a $\alpha - \alpha = 0 \in \mathbb{Z}_+$, donc $\alpha \leq \alpha$.
- Antisymétrie : Si $\alpha \leq \beta$ et $\beta \leq \alpha$, alors $\beta - \alpha \in \mathbb{Z}_+$ et $\alpha - \beta \in \mathbb{Z}_+$, donc $\beta - \alpha = -(\alpha - \beta) \in \mathbb{Z}_-$.
  Nous avons donc $\beta - \alpha \in \mathbb{Z}_+ \cap \mathbb{Z}_- = \{0\}$, donc $\beta = \alpha$.
- Transitivité : Soient α, β et γ tels que $\alpha \leq \beta$ et $\beta \leq \gamma$. Alors $\beta - \alpha \in \mathbb{Z}_+$ et $\gamma - \beta \in \mathbb{Z}_+$.
  Donc $\gamma - \alpha = (\gamma - \beta) + (\beta - \alpha) \in \mathbb{Z}_+$, c'est-à-dire que $\alpha \leq \gamma$.
- Ordre total : Soient α et β deux entiers relatifs. On a $\mathbb{Z}_+ \cup \mathbb{Z}_- = \mathbb{Z}$, donc l'entier relatif $\beta - \alpha$ est forcément dans $\mathbb{Z}_+$ ou dans $\mathbb{Z}_-$. si $\beta - \alpha \in \mathbb{Z}_+$, alors $\alpha \leq \beta$. sinon, $\beta - \alpha \in \mathbb{Z}_-$ donc $\alpha - \beta \in \mathbb{Z}_+$ et donc $\beta \leq \alpha$.

□

Remarques

- $\alpha \in \mathbb{Z}_+ \Longleftrightarrow 0 \leq \alpha \quad$ et $\quad \alpha \in \mathbb{Z}_- \Longleftrightarrow \alpha \leq 0$
- $(\alpha \in \mathbb{Z}_- \quad$ et $\quad \beta \in \mathbb{Z}_+) \Longrightarrow \alpha \leq \beta$
- $\leq$ est compatible avec l'addition sur $\mathbb{Z}$: si $\alpha \leq \beta$ et $\gamma \leq \delta$, alors $\beta - \alpha \in \mathbb{Z}_+$ et $\delta - \gamma \in \mathbb{Z}_+$, donc $\beta - \alpha + \delta - \gamma \in \mathbb{Z}_+$, et donc
$$\alpha + \gamma \leq \beta + \delta$$

Notation : On notera $\alpha < \beta$ pour ($\alpha \leq \beta$ et $\alpha \neq \beta$). C'est-à-dire que $<$ est l'ordre strict associé à $\leq$.

On note également $\mathbb{Z}_+^*$ l'ensemble des entiers relatifs strictement positifs, soit $\mathbb{Z}_+ \setminus \{0\}$. (et $\mathbb{Z}_-^*$ l'ensemble des entiers relatifs strictement négatifs, soit $\mathbb{Z}_- \setminus \{0\}$)

Avec ces notations, on a l'équivalence $\alpha < \beta \Longleftrightarrow \beta - \alpha \in \mathbb{Z}_+^*$.

De plus on a, pour tous relatifs α et β, $\alpha \leq \beta$ ou $\beta < \alpha$. En effet, le relatif $\beta - \alpha$ est soit dans $\mathbb{Z}_+$, soit dans $\mathbb{Z}_-^*$.

4 Multiplication dans $\mathbb{Z}$

Soit dans $\mathbb{N}^2$ la multiplication définie par :

$$(a, b) \times (c, d) = (ac + bd, ad + bc)$$

Montrons que cette multiplication est compatible avec la relation $\mathfrak{R}$. Posons $(a, b)\mathfrak{R}(a', b')$ et $(c, d)\mathfrak{R}(c', d')$. On doit montrer que :

$$(ac + bd, ad + bc)\mathfrak{R}(a'c' + b'd', a'd' + b'c')$$

soit
$$ac + bd + a'd' + b'c' = ad + bc + a'c' + b'd' \qquad \textbf{(1)}$$

Supposons (par exemple) $c \geq d$. Alors il exite un entier nature m tel que $c = d + m$. On a aussi la relation $c' = d' + m$. Donc l'égalité **(1)** équivaut à :

$$\begin{aligned} a(d+m)+bd+a'd'+b'(d'+m) &= ad+b(d+m)+a'(d'+m)+b'd' \\ &\iff am+b'm = bm+a'm \\ &\iff (a+b')m = (b+a')m \end{aligned}$$

Cette dernière égalité est assurée par la relation $a+b' = b+a'$.

Cette compatibilité permet alors de définir une multiplication sur $\mathbb{Z}$:

Définition Si $\alpha = \overline{(a,b)}$ et $\beta = \overline{(c,d)}$ on pose :

$$\alpha \times \beta = \overline{(a,c)\times(b,d)} = \overline{(ac+bd, ad+bc)}$$

(on note encore ce produit $\alpha.\beta$ ou $\alpha\beta$)

Remarques

- $\alpha, \beta \in \mathbb{Z}_+ \Rightarrow \alpha\beta \in \mathbb{Z}_+$
  En effet $[\alpha = \overline{(m,0)}$ et $\beta = \overline{(n,0)}] \Longrightarrow \alpha\beta = \overline{(mn,0)}$
- $\alpha, \beta \in \mathbb{Z}_- \Rightarrow \alpha\beta \in \mathbb{Z}_+$
  En effet $\overline{(0,m)} \times \overline{(0,n)} = \overline{(mn,0)}$.
- $[\alpha \in \mathbb{Z}_+$ et $\beta \in \mathbb{Z}_-] \Rightarrow \alpha\beta \in \mathbb{Z}_-$
  En effet $\overline{(m,0)} \times \overline{(0,n)} = \overline{(0,mn)}$ (résultat analogue avec $\alpha \in \mathbb{Z}_-$ et $\beta \in \mathbb{Z}_+$)
- De plus, cette distinction de cas montre que :

$$\forall \alpha, \beta \in \mathbb{Z}, \quad |\alpha\beta| = |\alpha|\,|\beta|$$

Théorème 4.1 $(\mathbb{Z}, +, \times)$ *est un anneau commutatif unitaire*

Démonstration : Puisqu'on connaît déjà la structure de groupe commutatif pour $(\mathbb{Z}, +)$ il ne reste qu'à démontrer les propriétés relatives à l'opération $\times$:

- Commutativité :
  Si $\alpha = \overline{(a,b)}$ et $\beta = \overline{(c,d)}$, alors :

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

  et

$$\beta\alpha = \overline{(ca+db, cb+da)}$$

  donc

$$\alpha\beta = \beta\alpha$$

- Associativité :
  Soient $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ et $\gamma = \overline{(e,f)}$. Alors :

$$\begin{aligned} \alpha(\beta\gamma) &= \overline{(a,b)\times(ce+df, cf+de)} \\ &= \overline{(a(ce+df)+b(cf+de), a(cf+de)+b(ce+df))} \end{aligned}$$

  et

$$\begin{aligned} (\alpha\beta)\gamma &= \overline{(ac+bd, ad+bc)\times(e,f)} \\ &= \overline{((ac+bd)e+(ad+bc)f, (ac+bd)f+(ad+bc)e)} \end{aligned}$$

  donc

$$\alpha(\beta\gamma) = (\alpha\beta)\gamma$$

- Distributivité sur l'addition : (On sait que $\times$ est commutative)
  Soient $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ et $\gamma = \overline{(e,f)}$. On a :

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

  et

$$\begin{aligned} \alpha\beta+\alpha\gamma &= \overline{(ac+bd, ad+bc)} + \overline{(ae+bf, af+be)} \\ &= \overline{(ac+bd+ae+bf, ad+bc+af+be)} \end{aligned}$$

donc $$\alpha\beta + \alpha\gamma = \alpha(\beta + \gamma)$$

– $\overline{(1,0)}$ est élément neutre : (on le note 1)
$\times$ est commutative. Soit $\alpha = \overline{(a,b)}$. Alors :
$$\alpha \cdot 1 = \overline{(a,b)} \times \overline{(1,0)} = \overline{(a,b)} = \alpha$$

□

Remarques

– $\mathbb{Z}$ est un anneau intègre : $\alpha\beta = 0 \Longleftrightarrow (\alpha = 0 \text{ ou } \beta = 0)$
En effet :
$\boxed{\Rightarrow}$ découle du fait que :
$\alpha\beta = 0 \Longrightarrow |\alpha\beta| = |0| \Longrightarrow |\alpha|\,|\beta| = 0 \Longrightarrow [|\alpha| = 0 \text{ ou } |\beta| = 0]$ (propriété vue dans $\mathbb{N}$)
$\boxed{\Leftarrow}$ est immédiat.

– α est inversible (i.e. symétrisable pour $\times$) si et seulement si $\alpha = 1$ ou $\alpha = -1$:
1 est inversible car son propre inverse, et -1 également.
Réciproquement, soit α inversible. Alors il existe β tel que $\alpha\beta = 1$; donc $|\alpha|\,|\beta| = 1$.
Nécessairement $|\alpha| \neq 0$ et $|\beta| \neq 0$, donc $|\alpha| \geq 1$ et $|\beta| \geq 1$.
Si $|\alpha| > 1$, alors $|\alpha|\,|\beta| \geq |\alpha| > 1$, contradiction.
Donc $|\alpha| = 1$, soit $\alpha = 1$ ou $\alpha = -1$.

Propriété 4.2 $$\forall \gamma \in \mathbb{Z}_+, \quad (\alpha \leq \beta \Longrightarrow \alpha\gamma \leq \beta\gamma)$$

et $$\forall \gamma \in \mathbb{Z}_-, \quad (\alpha \leq \beta \Rightarrow \alpha\gamma \geq \beta\gamma)$$

Démonstration : Soit $\gamma \in \mathbb{Z}_+$ et $\alpha \leq \beta$. Alors $\beta - \alpha \in \mathbb{Z}_+$, donc $\gamma(\beta - \alpha) \in \mathbb{Z}_+$, et donc $\gamma\beta - \gamma\alpha \in \mathbb{Z}_+$, c'est-à-dire $\gamma\alpha \leq \gamma\beta$.

De même, soit $\gamma \in \mathbb{Z}_-$ et $\alpha \leq \beta$. Alors $\beta - \alpha \in \mathbb{Z}_+$ donc $\gamma(\beta - \alpha) \in \mathbb{Z}_-$, et l'on obtient cette fois $\gamma\beta \leq \gamma\alpha$

□

Propriété 4.3 *La multiplication dans $\mathbb{Z}_+$ est compatible avec $\leq$.*

Démonstration :

En effet, soient $0 \leq \alpha \leq \beta$ et $0 \leq \gamma \leq \delta$. On a, d'après la propriété précédente, $\alpha\gamma \leq \beta\gamma$ et $\beta\gamma \leq \beta\delta$, donc par transitivité :
$$\alpha\gamma \leq \beta\delta$$ □

Ayant défini les opérations $+$ et $\times$ sur $\mathbb{Z}$, ainsi que la relation d'ordre $\leq$, nous sommes en mesure d'étudier le :

Plongement de $\mathbb{N}$ dans $\mathbb{Z}$:

On a vu que $\mathbb{Z}_+$ est stable pour les opérations $+$ et $\times$. Nous allons montrer qu'en fait, $(\mathbb{Z}_+, +, \times, \leq)$ est isomorphe à $(\mathbb{N}, +, \times, \leq)$.

Soit f l'application de $\mathbb{N}$ dans $\mathbb{Z}_+$ définie par :
$$f : m \longmapsto \overline{(m,0)}$$

f est bien sûr surjective, mais aussi injective car pour tout entier naturel n :

$$\begin{aligned} f(m) = \overline{(n,0)} &\iff \overline{(m,0)} = \overline{(n,0)} \\ &\iff m = n \end{aligned}$$

Donc f est une bijection de $\mathbb{N}$ sur $\mathbb{Z}_+$. D'autre part, il découle de la définition des opérations $+$ et $\times$ dans $\mathbb{Z}$ que pour tout couple (m,n) d'entier naturels, on a $f(m+n) = f(m) + f(n)$ et $f(mn) = f(m)f(n)$. Enfin, on a

$$\begin{aligned} f(m) \leq f(n) &\iff \overline{(m,0)} \leq \overline{(n,0)} \\ &\iff \overline{(n,0)} - \overline{(m,0)} \in \mathbb{Z}_+ \\ &\iff m \leq n \end{aligned}$$

f est donc un isomorphisme de $(\mathbb{N}, +, \times, \leq)$ sur $(\mathbb{Z}_+, +, \times, \leq)$. Ceci justifie l'identification entre un relatif positif $\alpha = \overline{(m,0)}$ et l'entier naturel m correspondant.

5 Division euclidienne et divisibilité

Théorème 5.1 $\forall (a,b) \in \mathbb{Z} \times \mathbb{N}^*, \exists ! (q,r) \in \mathbb{Z} \times \mathbb{Z}, \quad (a = bq + r \text{ et } 0 \leq r < b)$

Démonstration : Le cas $a \geq 0$ a déjà été étudié dans le texte sur les entiers naturels. Supposons donc $a < 0$.

- Existence de (q,r)
  $-a > 0$ donc $-a = bq' + r'$ avec $q' \in \mathbb{N}$ et $0 \leq r' < b$.
  Donc $a = b(-q') - r' = b(-q'-1) + b - r'$. Et $0 < b - r' \leq b$.
  Si $r' = 0$, alors on avait en réalité $a = b(-q')$. On prend pour q et r le couple $(-q', 0)$.
  Sinon, $r' > 0$ donc $0 < b - r' < b$. On prend le couple $(-q'-1, b-r')$.
- Unicité de (q,r)
  Supposons $a = bq + r = bq' + r'$ avec $0 \leq r < b$ et $0 \leq r' < b$.
  Alors $b(q-q') = r' - r$ donc $b\,|q-q'| = |r'-r|$
  Si $q \neq q'$, alors $|q-q'| \geq 1$ donc $|r'-r| \geq b$.
  Or $r' - r < b$ (sinon $r' \geq b + r \geq b$) ; et $r - r' < b$ (sinon $r \geq b + r' \geq b$).
  Donc $|r'-r| < b$, contradiction.
  Donc $q = q'$ ce qui entraîne également $r = r'$.

□

En particulier, $\mathbb{Z}$ est donc un anneau euclidien (*i.e.* muni d'une division euclidienne, sic), donc principal. C'est-à-dire que tous les idéaux de $\mathbb{Z}$ sont de la forme $a\mathbb{Z}$, avec a un entier. (cf le texte d'introduction aux idéaux)

Définition Soient a et b deux entiers relatifs. On dit que b *divise* a (noté $b|a$) si il existe un entier q tel que $a = bq$; c'est-à-dire si le reste de la division euclidienne de a par b est 0. a est alors un *multiple* de b.

Théorème 5.2 *Soient a et b deux entiers. On a l'équivalence :*

$$b|a \iff a\mathbb{Z} \subset b\mathbb{Z}$$

Démonstration :

$\boxed{\Rightarrow}$ Si $b|a$, alors il existe q tel que $a = bq$. Mais alors, pour tout élément $x = ak$ de $a\mathbb{Z}$, on a $x = bqk$, soit $x \in b\mathbb{Z}$; et donc $a\mathbb{Z} \subset b\mathbb{Z}$.

$\boxed{\Leftarrow}$ Si $a\mathbb{Z} \subset b\mathbb{Z}$, alors en particulier $a \in b\mathbb{Z}$ (puisque $a = a \times 1 \in a\mathbb{Z}$). Et donc il existe un entier q tel que $a = bq$, c'est-à-dire que $b|a$.

□

6 Arithmétique dans $\mathbb{Z}$, PGCD, PPCM

6.1 Multiples communs, PPCM

Théorème 6.1 *Soient a et b dans $\mathbb{Z}$. Alors il existe un unique entier positif μ qui vérifie :*

$$\forall n \in \mathbb{Z}, \quad a|n \text{ et } b|n \Longleftrightarrow \mu|n$$

Démonstration :

– Existence de μ :
$a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de $\mathbb{Z}$, donc un idéal principal. Donc

$$\exists \mu \in \mathbb{Z}, \quad a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$$

On peut prendre $\mu \in \mathbb{N}$ car $\mu\mathbb{Z} = (-\mu)\mathbb{Z}$. Alors

$$(a|x \text{ et } b|x) \Longleftrightarrow x \in a\mathbb{Z} \cap b\mathbb{Z} \Longleftrightarrow x \in \mu\mathbb{Z} \Longleftrightarrow \mu|x$$

– Unicité de μ :
Soient μ_1 et μ_2 qui conviennent. alors $\mu_1\mathbb{Z} = \mu_2\mathbb{Z}$. En particulier, il existe deux entiers naturel k et l tels que $\mu_1 = k\mu_2$ et $\mu_2 = l\mu_1$, soit encore $\mu_1 = kl\mu_2$.
Or $kl = 1$ entraîne $k = l = \pm 1$, et donc $\mu_1 = \pm\mu_2$. Comme μ_1 et μ_2 sont positifs, on a $\mu_1 = \mu_2$.

□

Remarque Les multiples communs à a et b sont donc exactement les multiples de μ. C'est le cas en particulier de μ lui-même, qui est le plus petit.
Définition L'entier μ est appelé *plus petit multiple commun* de a et b (ou PPCM), et noté $a \vee b$.
Remarque Pour tous a, b et c, on a $(a \vee b) \vee c = a \vee (b \vee c)$. Également, on a $a \vee b = b \vee a$. C'est-à-dire que $\vee$ définit une loi de composition interne sur $\mathbb{Z}$ (à valeurs dans $\mathbb{Z}_+$) associative et commutative.

Propriété 6.2 *Pour tous entiers a, b et c, on a la relation :*

$$(ac) \vee (bc) = |c| \cdot (a \vee b)$$

Démonstration : En effet l'entier naturel $n = (ac) \vee (bc)$ est l'entier qui vérifie $n\mathbb{Z} = ac\mathbb{Z} \cap bc\mathbb{Z}$. Or, l'on vérifie aisément que :

$$ac\mathbb{Z} \cap bc\mathbb{Z} = c\,(a\mathbb{Z} \cap b\mathbb{Z})$$

Si m est un élément de $ac\mathbb{Z} \cap bc\mathbb{Z}$, alors m s'écrit sous la forme acu ou bcv, avec u et v deux entiers, vérifiant donc $au = bv$. Donc ce terme $au = bv$ est dans $a\mathbb{Z} \cap b\mathbb{Z}$, c'est-à-dire que m est bien dans l'idéal $c\,(a\mathbb{Z} \cap b\mathbb{Z})$.

Réciproquement, tout élément m de $c\,(a\mathbb{Z} \cap b\mathbb{Z})$ est de la forme ck, avec $k \in a\mathbb{Z} \cap b\mathbb{Z}$ donc de la forme au et de la forme bv. On conclue de la même façon que $m \in ac\mathbb{Z} \cap bc\mathbb{Z}$.

Mais alors, comme $c\,(a\mathbb{Z} \cap b\mathbb{Z}) = |c|\,(a\mathbb{Z} \cap b\mathbb{Z}) = |c|\,(a \vee b)\mathbb{Z}$, on obtient comme annoncé :

$$(ac) \vee (bc) = |c| \cdot (a \vee b) \qquad \square$$

Enfin, on vérifie aisément que $a \vee 1 = |a|$ et $a \vee 0 = 0$, ainsi que

$$a, b \in \mathbb{Z} \backslash \{0\} \Longrightarrow a \vee b \in \mathbb{Z}_+^*$$

6.2 Diviseurs communs, PGCD

Théorème 6.3 *Soient $a, b \in \mathbb{Z}$. Alors il existe un unique entier naturel δ tel que :*

$$\forall d \in \mathbb{Z}, \quad (d|a \text{ et } d|b) \Longleftrightarrow d|\delta$$

Démonstration :

– Existence de δ :
$a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$, donc

$$\exists \delta \in \mathbb{N}, \quad a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$$

$\boxed{\Rightarrow}$ Soit d tel que $d|a$ et $d|b$. On a alors $a = da_1$ et $b = db_1$ (avec $a_1, b_1 \in \mathbb{Z}$). Et :

$$\begin{aligned} x \in a\mathbb{Z} + b\mathbb{Z} &\Longrightarrow \exists k, h \in \mathbb{Z}, \quad x = ka + hb \\ &\Longrightarrow \exists k, h \in \mathbb{Z}, \quad x = d(ka_1 + hb_1) \\ &\Longrightarrow x \in d\mathbb{Z} \end{aligned}$$

Donc $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$ donc $\delta\mathbb{Z} \subset d\mathbb{Z}$, et finalement $d|\delta$.
$\boxed{\Leftarrow}$ Soit d tel que $d|\delta$. Alors $a\mathbb{Z} \subset \delta\mathbb{Z}$ donc $\delta|a$, donc $d|a$; de même $d|b$.

– Unicité de δ : Soient δ_1 et δ_2 ayant la propriété du théorème. Alors pour tout d dans $\mathbb{Z}$:

$$(d \mid \delta_1 \Longleftrightarrow d \mid \delta_2)$$

donc $\delta_2 = k\delta_1$ et $\delta_1 = l\delta_2$ $(k, l \in \mathbb{N})$; donc $\delta_1 = kl\delta_1$ donc $kl = 1$ donc $\delta_1 = \delta_2$.

$\square$

L'entier δ ainsi défini divise lui-même a et b, c'est le plus grand entier naturel vérifiant cette propriété. D'où la :

Définition L'entier δ est appelé *plus grand commun diviseur* de a et b (ou PGCD), et noté $a \wedge b$.

L'ensemble des diviseurs communs à a et b est exactement l'ensemble des diviseurs de leur PGCD. Tout comme pour le PPCM, $\wedge$ définit sur $\mathbb{Z}$ une loi de composition interne (à valeurs dans $\mathbb{Z}_+^*$) associative et commutative.

On a également, pour tout entier a, les relations $a \wedge 1 = 1$ et $a \wedge 0 = |a|$. Enfin, on a le :

Propriété 6.4 *Soient a, b et c trois entiers. Alors*

$$(ac) \wedge (bc) = |c| \cdot (a \wedge b)$$

Démonstration : On a $ac\mathbb{Z}+bc\mathbb{Z} = c\,(a\mathbb{Z}+b\mathbb{Z}) = |c|\cdot(a\wedge b)\mathbb{Z}$, donc $(ac)\wedge(bc) = |c| \times (a \wedge b)$.

□

6.3 Primalité

Définition Deux entiers a et b sont dits premiers entre eux si et seulement si ils vérifient $a \wedge b = 1$.
Remarque $a \wedge b = 1 \iff a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$

Théorème 6.5 (Bezout) *Pour tous entiers a et b, on a :*

$$a \wedge b = 1 \iff \exists u, v \in \mathbb{Z}, \quad au + bv = 1$$

Démonstration : $\boxed{\Rightarrow}$ $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ et $1 \in \mathbb{Z}$, d'où le résultat.
$\boxed{\Leftarrow}$ $a \wedge b | a$ et $a \wedge b | b$, donc $a \wedge b | au + bv = 1$, et donc $a \wedge b = 1$.

□

Théorème 6.6 (Lemme de Gauss) $(a|bc \text{ et } a \wedge b = 1) \Longrightarrow a|c$

Démonstration : Soient u et v tels que $au + bv = 1$. Multipliant cette égalité par c, on obtient :

$$acu + bcv = c$$

Or a divise acu et bcv (par hypothèse), donc a divise la somme c.

□

Théorème 6.7 *Soient a et b dans $\mathbb{Z}^*$. Alors*

$$\delta = a \wedge b \iff \exists a_1, b_1 \neq 0, \quad (a = \delta a_1 \text{ et } b = \delta b_1 \text{ et } a_1 \wedge b_1 = 1) \text{ et } \delta > 0$$

Démonstration :
$\boxed{\Rightarrow}$ Soient a_1 et b_1 tels que $a = \delta a_1$ et $b = \delta b_1$. Soit d un diviseur commun de a_1 et b_1. Alors le produit $d\delta$ divise a et b, donc δ, et donc $d = 1$. D'où $a_1 \wedge b_1 = 1$.
$\boxed{\Leftarrow}$ $a \wedge b = (\delta a_1) \wedge (\delta b_1) = \delta(a_1 \wedge b_1) = \delta$.

□

Théorème 6.8 $(a|c \text{ et } b|c \text{ et } a \wedge b = 1) \Longrightarrow ab|c$

Démonstration : a divise c donc il existe un entier q tel que $c = aq$. Mais alors, b divise le produit aq tout en étant premier avec a. D'après le lemme de Gauss, on a alors $b|q$. C'est-à-dire que q est de la forme bk, avec k un entier. Et donc $c = abk$, c'est-à-dire que le produit ab divise bien c.

□

Théorème 6.9 *Pour tous entiers a et b, on a la relation :*

$$|ab| = (a \wedge b) \cdot (a \vee b)$$

Démonstration : Soient $\delta = a \wedge b$ et $\mu = a \vee b$. L'entier μ est multiple commun de a et b, donc il existe deux entiers u et v tels que

$$\mu = ua = vb$$

D'autre part, d'après le théorème 6.7, on sait qu'il existe deux entiers a_1 et b_1 premiers entre eux, et tels que $a = \delta a_1$ et $b = \delta b_1$. Remplaçant ceci dans l'égalité précédente, on obtient :

$$u\delta a_1 = v\delta b_1 \quad \text{soit} \quad ua_1 = vb_1$$

D'après le théorème de Gauss, a_1 étant premier à b_1, on sait que a_1 divise v. Donc μ est multiple du produit $|\delta a_1 b_1|$. Comme bien sûr $|\delta a_1 b_1|$ est multiple commun de a et b, c'est leur PPCM. On a montré :

$$\mu = \delta\,|a_1| \cdot |b_1| \quad \text{donc} \quad \mu\delta = |\delta a_1| \cdot |\delta b_1|$$

soit encore $$(a \wedge b) \cdot (a \vee b) = |ab|$$ □