Division euclidienne dans $\mathbb{Z}$

Christian CYRILLE

30 mai 2017

"Il ne s'agit ni de rire, ni de pleurer mais de comprendre"
Spinoza

1 Notion de multiple

Soit $n \in \mathbb{Z}$. Soit $m \in \mathbb{Z}$.
On dit que n divise m (qu'on notera $n \mid m$) ou que m est un multiple de n lorsque

$$\exists k \in \mathbb{Z} \quad m = n\,k$$

L'ensemble des multiples de n est $\{n\,k / k \in \mathbb{Z}\}$ qu'on notera $n\mathbb{Z}$.

1.1 Exemples

1. $0\mathbb{Z} = \{0\}$
2. $1\mathbb{Z} = \mathbb{Z}$
3. $(-1)\mathbb{Z} = \mathbb{Z}$
4. $2\mathbb{Z} =$ l'ensemble des entiers relatifs pairs.

1.2 Théorème

$\forall n \in \mathbb{Z} \qquad n\mathbb{Z}$ est un sous groupe du groupe $(\mathbb{Z}, +)$

1.2.1 Démonstration

1. $n\mathbb{Z} \subset \mathbb{Z}$.
2. $0 \in n\mathbb{Z}$ car $0 = n \times 0$ donc $n\mathbb{Z} \neq \emptyset$
3. Soit $m_1 \in n\mathbb{Z}$ et $m_2 \in n\mathbb{Z}$.
   Alors $\exists (k_1, k_2) \in \mathbb{Z}^2$ tel que $m_1 = k_1 n$ et $m_2 = k_2 n$.
   Donc $m_1 - m_2 = nk_1 - nk_2 = n(k_1 - k_2) = nk$ où $k = k_1 - k_2 \in \mathbb{Z}$.
   Par conséquent, $m_1 - m_2 \in n\mathbb{Z}$

1.3 Relation de divisibilité dans $\mathbb{Z}$

La relation de divisibilité dans $\mathbb{Z}$:

- est réflexive
- est transitive
- n'est pas antisymétrique car

$$a \mid b \text{ et } b \mid a \Longrightarrow a = b \text{ ou } a = -b$$

Donc " $\mid$ " n'est pas une relation d'ordre dans $\mathbb{Z}$.

1.3.1 Démonstration

- Soit $a \in \mathbb{Z}$ alors $a = 1 \times a$ alors $a \mid a$ donc " $\mid$ " est réflexive
- Soit $(a, b, c) \in \mathbb{Z}^3$ tel que $a \mid b$ et $b \mid c$.
  Alors $\exists k_1 \in \mathbb{Z}\ b = k_1 a$ et $\exists k_2 \in \mathbb{Z}\ c = k_2 b$.
  Donc $c = k_2 k_1 a = ka$ où $k = k_1 k_2 \in \mathbb{Z}$ donc $ca \mid c$. Par conséquent, " $\mid$ " est transitive.
- Soit $(a, b) \in \mathbb{Z}^2$ tel que $a \mid b$ et $b \mid a$.
  Alors $\exists k_1 \in \mathbb{Z}\ b = k_1 a$ et $\exists k_2 \in \mathbb{Z}\ a = k_2 b$.
  Par conséquent $a = k_2 k_1 a$ d'où $a(1 - k_2 k_1) = 0$.
  - ou bien $a \neq 0$ donc $1 - k_2 k_1 = 0$ donc $k_2 k_1 = 1$.
    Or les seuls éléments inversibles de $\mathbb{Z}$ sont -1 et 1.
    Par conséquent, ou $k_2 = k_1 = -1$ ou $k_2 = k_1 = 1$ donc $a = b \text{ ou } a = -b$
  - ou bien $a = 0$ mais alors $b = 0$ donc $a = b \text{ ou } a = -b$

  On a donc " $\mid$ " qui n'est pas antisymétrique car

$$a \mid b \text{ et } b \mid a \Longrightarrow a = b \text{ ou } a = -b$$

1.4 Remarque

Dans $\mathbb{N}$ par contre, la relation de divisibilité " $\mid$ " est une relation d'ordre partiel
car elle est :

- réflexive
- transitive
- antisymétrique

Mais cette relation d'ordre n'est pas une relation d'ordre total. Cet ordre est partiel car $\exists (x, y) \in \mathbb{N}^2 \quad x$ ne divise pas y *et* y ne divise pas x : par exemple 2 ne divise pas 3 et 3 ne divise pas 2

1.5 Théorème

Soit $(a, b) \in \mathbb{Z}^2$ alors : $\quad a \mid b \iff b\mathbb{Z} \subset a\mathbb{Z}$

1.5.1 Démonstration

- $\Longrightarrow$:
  Supposons que $a \mid b$.
  soit $n \in b\mathbb{Z}$ donc $\exists k_1 \in \mathbb{Z} \quad n = k_1 b$. Or $a \mid b$ donc $\exists k_2 \in \mathbb{Z} \quad b = k_2 a$.
  Par conséquent $n = k_1 b = k_1 k_2 a = ka$ où $k = k_1 k_2 \in \mathbb{Z}$ donc $n \in a\mathbb{Z}$.
  On a donc $b\mathbb{Z} \subset a\mathbb{Z}$. CQFD.

- $\Longleftarrow$:
  Supposons que $b\mathbb{Z} \subset a\mathbb{Z}$.
  Or $b \in b\mathbb{Z}$ donc $b \in a\mathbb{Z}$. Par conséquent, $\exists k \in \mathbb{Z} \quad b = ak$ donc $a \mid b$. CQFD.

2 Division euclidienne dans $\mathbb{Z}$

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

2.0.1 Démonstration

1. ou bien $a \in \mathbb{N}$
   Alors d'après le théorème sur la division euclidienne dans $\mathbb{N}$
   Comme $(a,b) \in \mathbb{N} \times \mathbb{N}^*$ $\exists!(q,r) \in \mathbb{N} \times \mathbb{N}$ $a = bq + r$ *et* $0 \leq r < b$
2. ou bien $a \in \mathbb{Z} - \mathbb{N}$
   (a) ou bien $b \mid a$
   Dans ce cas $\exists k \in \mathbb{Z}$ tel que $a = kb$.
   k est unique car si l'on suppose qu'il existe aussi $k' \in \mathbb{Z}$ tel que $a = k'b$ alors $kb = k'b$ donc $kb - k'b = 0$ d'où $(k - k')b = 0$.
   Or $b \neq 0$ donc $k - k' = 0$. Par conséquent $k = k'$.
   On en déduit $\exists!(q,r) \in \mathbb{N} \times \mathbb{N}$ $a = bq + r$ *avec* $(q,r) = (b,0)$
   (b) ou bien b ne divise pas a.
   On s'intéresse à $\mid a \mid$ qui appartient à $\mathbb{N}$.
   En utilisant la division euclidienne dans $\mathbb{N}$ et le fait que $b \not| a$ on obtient donc que :
   $\exists! q' \in \mathbb{N}$ tel que $bq' <\mid a \mid< b(q'+1)$
   c'est-à-dire que $bq' < -a < b(q'+1)$ d'où $-bq' > a > -b(q'+1)$.
   On a donc $b(-q'-1) < a < b(-q')$.
   En posant $q = -q'$ on obtient que $bq < a < b(q+1)$
   Par conséquent $\exists!(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ avec
   $$\begin{cases} q = -q' - 1 \\ r = a - b(-q' - 1) \end{cases}$$

3 Sous groupes de $(\mathbb{Z}, +)$

Les seuls sous groupes du groupe $(\mathbb{Z}, +)$ sont les $(n\mathbb{Z}, +)$ où $n \in \mathbb{N}$

3.1 Démonstration

1. On sait déjà que tous les $n\mathbb{Z}$ sont des sous groupes de $(\mathbb{Z}, +)$.
2. Reste donc à prouver que si H est un sous groupe de $(\mathbb{Z}, +)$
   alors $\exists n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.
   (a) **unicité de** n :
   Supposons que $H = n\mathbb{Z}$ et que $H = n'\mathbb{Z}$ où $(n, n') \in \mathbb{N}^2$.
   Par conséquent, $n\mathbb{Z} = n'\mathbb{Z}$ donc $n\mathbb{Z} \subset n'\mathbb{Z}$ et $n'\mathbb{Z} \subset n\mathbb{Z}$.
   On en déduit que $n' \mid n$ et que $n \mid n'$ donc $n = n'$ ou $n = -n'$.
   Mais n et n' sont des entiers naturels donc $n = n'$.

(b) **existence de** n :
Soit H un sous groupe de $(\mathbb{Z}, +)$.

i. **ou bien** $H = \{0\}$
Alors $H = \{0\} = 0\mathbb{Z}$. CQFD.

ii. **ou bien** $H \neq \{0\}$
Alors $\exists a \in H$ avec $a \neq 0$. Par conséquent $-a \in H$. De toutes façons $\mid a \mid \in H$ avec $\mid a \mid \neq 0$.
Soit l'ensemble $F = H \cap \mathbb{N}$. Alors F est un sous ensemble d'entiers naturels non vide donc F admet un plus petit élément n.
Nous allons maintenant démontrer que $H = n\mathbb{Z}$

- $n\mathbb{Z} \subset H$?
soit $x \in n\mathbb{Z}$ donc $\exists k \in Z$ tel que $x = nk$
donc $\mid x \mid = n \mid k \mid = n + n + \cdots + n$ (ceci $\mid k \mid$ fois).
Or $n \in H$ et H est un sous groupe additif donc $\mid x \mid \in H$.
Par conséquent, $x \in H$. CQFD.
- $H \subset n\mathbb{Z}$?
Soit $x \in H$. Comme $n \in \mathbb{N}^*$ alors d'après la division euclidienne
$\exists!(q, r) \in (\mathbb{Z} \times \mathbb{N})$ tel que $x = nq + r$ et $0 \leq r < n$
Alors

— supposons que $0 < r < n$.
Or $r = x - nq$ où $x \in H$ et $nq \in n\mathbb{Z}$.
Or $n\mathbb{Z} \subset H$ donc $nq \in H$.
Comme H est un sous groupe additif et que $x \in H$ et $nq \in H$
alors $x - nq \in H$.
Par conséquent, $r \in H$.
Donc $H \cap \mathbb{N}^*$ aurait comme plus petit élément r et non n. Ceci n'est pas possible.

— donc forcément $r = 0$
Donc $x = nq$ donc $x \in n\mathbb{Z}$. CQFD.