6. Construction de $\mathbb{Z}$ comme extension de $\mathbb{N}$

1. $(\mathbb{Z}, +, 0)$ comme symétrisé du monoïde $(\mathbb{N}, +, 0)$
2. Propriété universelle et unicité de $(\mathbb{Z}, +, 0)$
3. L'anneau $(\mathbb{Z}, +, 0, \cdot, 1)$
4. Propriété universelle et unicité de $(\mathbb{Z}, +, 0, \cdot, 1)$
5. Les congruences de Gauss
6. Première définition de $\mathbb{Z}/n\mathbb{Z}$ comme anneau

1. $(\mathbb{Z}, +, 0)$ comme symétrisé du monoïde $(\mathbb{N}, +, 0)$

Objectif : "plonger" le monoïde $(\mathbb{N}, +, 0)$ (commutatif, régulier) dans un groupe $(G, +, 0)$ "le plus petit possible" ...

Heuristique :

1. $G = \mathbb{N} \cup (-\mathbb{N})$ mais comment définir $n + (-n')$??
2. Il faut assurer $n_1 + (-n'_1) = n_2 + (-n'_2)$ dès que $n_1 + n'_2 = n_2 + n'_1$

Construction :

• (on fait de la place pour les symétriques ...) à partir du monoïde commutatif régulier $(\mathbb{N}, +, 0)$, on construit le monoïde produit $(\mathbb{N} \times \mathbb{N}, +, (0, 0))$ par :

$$(n_1, n_2) + (n'_1, n'_2) \overset{\text{déf.}}{=} (n_1 + n'_1, n_2 + n'_2)$$

construction de $(\mathbb{Z}, +, 0)$ (2)

• (. . . et on ajuste par un "quotient idoine") on définit une relation d'équivalence sur $\mathbb{N} \times \mathbb{N}$ par :

$$(n_1, n_2)\mathcal{R}(n_1', n_2') \overset{\text{déf.}}{\iff} n_1 + n_2' = n_2 + n_1'$$

et on considère l'ensemble quotient $\boxed{G \overset{\text{déf.}}{=} \mathbb{N} \times \mathbb{N}/\mathcal{R}}$ et la projection canonique $\pi : \mathbb{N} \times \mathbb{N} \to G$.

• (il reste à faire de G un groupe . . .) on définit une opération sur G, encore notée $+$ par :

$$\begin{array}{rcl} + : G \times G & \longrightarrow & G \\ (x, x') & \longmapsto & x + x' \overset{\text{déf.}}{=} \pi\left((n_1, n_2) + (n_1', n_2')\right) \end{array}$$

où $x = \pi\left((n_1, n_2)\right)$ et $x = \pi\left((n_1', n_2')\right)$.

construction de $(\mathbb{Z}, +, 0)$ (3)

Exercices :

1. Vérifier que cette définition ne dépend pas des représentants choisis pour x et x'.
2. Montrer que $+$ est une loi de groupe sur G, d'élément neutre $\pi((0,0))$, et de symétrique $-x = \pi((n_2, n_1))$ si $x = \pi((n_1, n_2))$.

- (simplifions les notations) on pose :

$$\begin{aligned}
0 &\overset{\text{notation}}{=} \pi((0,0)) = \pi((1,1)) = \cdots = \pi((n,n)) \ , \qquad \forall n \in \mathbb{N} \\
n &\overset{\text{notation}}{=} \pi((n,0)) = \pi((n+k,k)) \ , \qquad \forall n,k \in \mathbb{N} \\
-n &\overset{\text{notation}}{=} \pi((0,n)) = \pi((k,n+k)) \ , \qquad \forall n,k \in \mathbb{N}
\end{aligned}$$

et on notera $(\mathbb{Z}, +, 0)$ le groupe ainsi construit.

2. Propriété universelle et unicité de $(\mathbb{Z}, +, 0)$

Bilan de la construction précédente :

- La construction précédente donne en particulier un morphisme de monoïde injectif.

$$\begin{array}{rccl} j : \mathbb{N} & \longrightarrow & \mathbb{Z} & \\ n & \longmapsto & n & \overset{\text{notation}}{=} \pi((n,0)) \end{array}$$

  C'est le (?) plongement désiré.

- Avec des notations évidentes, on a l'égalité (ensembliste)

$$\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$$

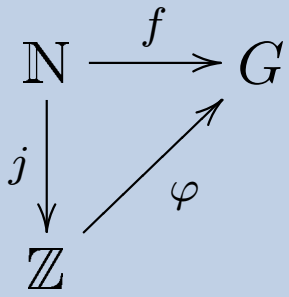
  et $\mathbb{Z}$ apparaît donc comme le (?) "plus petit" groupe qui symétrise $\mathbb{N}$.

Propriété universelle vérifiée par $(\mathbb{Z}, j)$

- Par ailleurs, le couple $(\mathbb{Z}, j)$ vérifie la propriété universelle :

Propriété universelle de $(\mathbb{Z}, j)$

Pour tout couple (G, f), où G est un groupe et $f : \mathbb{N} \to G$ est un morphisme de monoïde, il existe un unique morphisme de groupe $\varphi : \mathbb{Z} \to G$ qui rende commutatif le diagramme



Démonstration : φ doit vérifier :

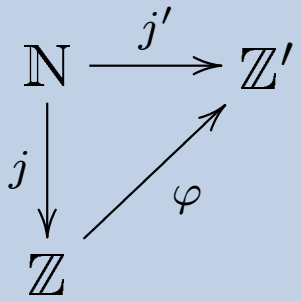
1. $\forall n \in \mathbb{N}, \quad \varphi(n) = f(n)$ (pour que $\varphi \circ j = f$)
2. $\forall n \in \mathbb{N}, \quad \varphi(-n) = \varphi(n)^{-1}$

Il reste à montrer que φ est un morphisme de groupe (exercice). □

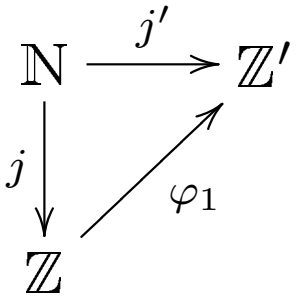
unicité à isomorphisme unique près de $\mathbb{Z}$

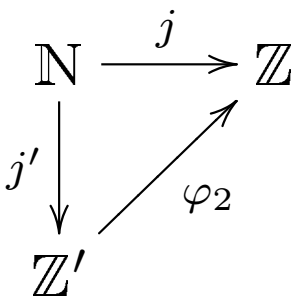
Théorème

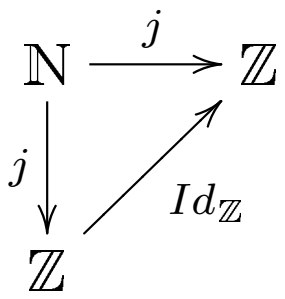
Si $(\mathbb{Z}', j')$, où $\mathbb{Z}'$ est un groupe et $j' : \mathbb{N} \to \mathbb{Z}'$ un morphisme de monoïde, vérifie aussi la propriété universelle de $(\mathbb{Z}, j)$, alors il existe un unique isomorphisme de groupe $\varphi : \mathbb{Z} \to \mathbb{Z}'$ qui rende commutatif le diagramme

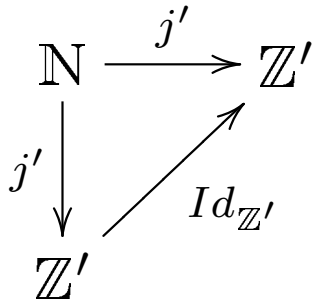


Démonstration :









□

3. L'anneau $(\mathbb{Z}, +, 0, \cdot, 1)$

On définit sur $\mathbb{Z}$ une multiplication

$$\begin{array}{rcl} \cdot : \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ (x, x') & \longmapsto & x \cdot x' \end{array}$$

par les règles : $(\forall n, n' \in \mathbb{N})$

$$\begin{cases} n \cdot n' & \overset{\text{déf.}}{=} & n \cdot n' \\ n \cdot (-n') & \overset{\text{déf.}}{=} & -(n \cdot n') \\ (-n) \cdot n' & \overset{\text{déf.}}{=} & -(n \cdot n') \\ (-n) \cdot (-n') & \overset{\text{déf.}}{=} & n \cdot n' \end{cases}$$

Théorème

$(\mathbb{Z}, +, 0, \cdot, 1)$ *est un anneau commutatif.*

Démonstration : exercice. □

4. Propriété universelle et unicité de $(\mathbb{Z}, +, 0, \cdot, 1)$

Propriété universelle de l'anneau $\mathbb{Z}$

Pour tout anneau A, il existe un unique morphisme d'anneau $\varphi : \mathbb{Z} \to A$.

Démonstration : φ doit vérifier :

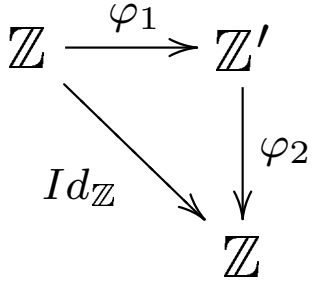
1. $\varphi(1) = 1_A$
2. $(\forall n \in \mathbb{Z}) \qquad \varphi(n) = n1_A$ (préciser cette notation !)

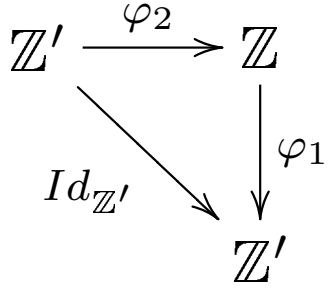
Il reste à montrer que φ est un morphisme d'anneau (exercice). □

Théorème (unicité à isomorphisme unique près de l'anneau $\mathbb{Z}$)

Si $\mathbb{Z}'$ est un anneau qui vérifie aussi la propriété universelle de $\mathbb{Z}$, alors il existe un unique isomorphisme d'anneau $\varphi : \mathbb{Z} \to \mathbb{Z}'$.

Démonstration :





□

5. Les congruences de Gauss

Soit $n \in \mathbb{N}$, $n \geq 2$. Posons $n\mathbb{Z} \overset{\text{déf}}{=} \{nx \ : \ x \in \mathbb{Z}\}$

Proposition (congruence)

On définit une relation d'équivalence sur $\mathbb{Z}$ par

$$(\forall a, b \in \mathbb{Z}) \quad a = b \ [n] \quad \overset{déf}{\Longleftrightarrow} \quad a \ et \ b \ ont \ même \ reste \ dans \ la \ division \ euclidienne \ par \ n$$
$$\Longleftrightarrow \quad a - b \in n\mathbb{Z}$$

On dit que a est congru à b modulo n. Si on effectue une division euclidienne de a par n, *i.e.* $a = qn + r$, on dit que a est réduit à r modulo n, ou que r est le résidu de a modulo n.

Exercices :

1. Démontrer la proposition.
2. Montrer que la congruence est compatible avec l'addition et la multiplication de $\mathbb{Z}$.
3. 123456789 est-il divisible par 9 ? (suite en TD)

6. Première définition de $\mathbb{Z}/n\mathbb{Z}$ comme anneau

Posons $\boxed{\mathbb{Z}/n\mathbb{Z} \overset{\text{déf}}{=} \mathbb{Z}/=_{[n]}}$, ensemble quotient de $\mathbb{Z}$ par la relation (d'équivalence) de congruence modulo n.
$\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ désigne la projection canonique associée.
On pose habituellement :

$$\begin{cases} \overline{0} & \overset{\text{déf}}{=} & \pi(0) = \pi(n) = \cdots & = & n\mathbb{Z} \\ \overline{1} & \overset{\text{déf}}{=} & \pi(1) = \pi(1+n) = \cdots & = & 1 + n\mathbb{Z} \\ & \vdots & & & \\ \overline{n-1} & \overset{\text{déf}}{=} & \pi(-1) = \pi(n-1) = \cdots & = & (n-1) + n\mathbb{Z} = -1 + n\mathbb{Z} \end{cases}$$

de sorte que :

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}; \overline{1}; \ldots; \overline{n-1}\right\}$$

Chaque classe d'équivalence est désignée par le résidu modulo n de l'un (quelconque) de ses représentants.

Puisque la congruence modulo n est compatible avec l'addition et la multiplication de $\mathbb{Z}$, ces deux opérations "passent au quotient" et font de $\mathbb{Z}/n\mathbb{Z}$ un anneau :

$$\left(\mathbb{Z}/n\mathbb{Z}, +, \overline{0}, \cdot, \overline{1}\right)$$

L'addition $+$ sur $\mathbb{Z}/n\mathbb{Z}$ est définie par

$$\begin{array}{rccl} + : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \\ (\overline{x}, \overline{x'}) & \longmapsto & \overline{x} + \overline{x'} & \overset{\text{déf}}{=} \pi(x + x') \end{array}$$

Exercices :

1. Montrer que cette définition est licite et que $\left(\mathbb{Z}/n\mathbb{Z}, +, \overline{0}\right)$ est un groupe abélien.
2. Définir de même la multiplication dans $\mathbb{Z}/n\mathbb{Z}$, et montrer que $\left(\mathbb{Z}/n\mathbb{Z}, +, \overline{0}, \cdot, \overline{1}\right)$ est un anneau commutatif.