

ARITHMÉTIQUE DANS \mathbf{Z}

1. NOTIONS ÉLÉMENTAIRES

1.1. Sous-groupe de \mathbf{Z}

THÉORÈME 1.1.0.1. —

Tout sous-groupe de \mathbf{Z} est de la forme $a\mathbf{Z}$ avec $a \in \mathbf{Z}$.

DÉMONSTRATION 1.1.0.1. —

Soit G un sous-groupe de \mathbf{Z} . Si G est réduit à $\{0\}$ alors $G = 0\mathbf{Z}$.

Sinon, soit $x = |x| \in G$ l'élément minimal de G non nul (qui existe puisque $G \subset \mathbf{Z}$).

$x\mathbf{Z} \subset G$ puisque G est un groupe.

Soit $y \in G$. Par division euclidienne, il existe un unique couple $(a, b) \in \mathbf{Z} \times \{0, 1, \dots, x-1\}$ tel que $y = ax + b$. On a $y - ax \in G$ mais aussi $y - ax = b \in G$.

Or $b < x$ donc $b = 0$ et donc $y \in x\mathbf{Z}$.

On notera $x\mathbf{Z} = \mathbf{x}$.

1.2. pgcd et ppcm

DÉFINITION 1.2.0.1. —

Soient $a, b \in \mathbf{Z}$. On dit de manière équivalente :

$$a \mid b \iff \mathbf{b} \subset \mathbf{a} \iff \exists c \in \mathbf{Z}, a = cb.$$

DÉFINITION 1.2.0.2. —

Soient $a, b \in \mathbf{Z}$.

On a que $\mathbf{a} + \mathbf{b}$ est un sous-groupe de \mathbf{Z} de la forme \mathbf{d} avec $d \in \mathbf{Z}$. On note $\text{pgcd}(a, b) = d$.

$\mathbf{a} \cap \mathbf{b}$ est un sous-groupe de \mathbf{Z} de la forme \mathbf{m} avec $m \in \mathbf{N}$. On note $\text{ppcm}(a, b) = m$.

PROPOSITION 1.2.0.1. —

Soient $a, b \in \mathbf{Z}$. On a les propositions suivantes :

1. $\text{pgcd}(a, b) = d \iff (\forall x \in \mathbf{Z}, x \mid a \text{ et } x \mid b \iff x \mid d)$;
2. $\text{ppcm}(a, b) = m \iff (\forall x \in \mathbf{Z}, a \mid x \text{ et } b \mid x \iff m \mid x)$.

DÉMONSTRATION 1.2.0.2. —

Soient $a, b \in \mathbf{Z}$.

1. Soit $x \in \mathbf{Z}$. $x \mid a \text{ et } x \mid b \iff \mathbf{a} \subset \mathbf{x} \text{ et } \mathbf{b} \subset \mathbf{x} \iff \mathbf{a} + \mathbf{b} \subset \mathbf{x} \iff x \mid \text{pgcd}(a, b)$.
2. Soit $x \in \mathbf{Z}$. $a \mid x \text{ et } b \mid x \iff \mathbf{x} \subset \mathbf{a} \text{ et } \mathbf{x} \subset \mathbf{b} \iff \mathbf{x} \subset \mathbf{a} \cap \mathbf{b} \iff \text{ppcm}(a, b) \mid x$.

THÉORÈME 1.2.0.2 (Identité de Bezout). —

Si $a, b \in \mathbf{Z}$ alors il existe $u, v \in \mathbf{Z}$ tels que $au + bv = \text{pgcd}(a, b)$.

En particulier, si a et b sont premiers entre eux alors $au + bv = 1$.

2. NOTIONS MODULAIRES

2.1. Passage au quotient

DÉFINITION 2.1.0.3. —

Soit $a \in \mathbf{Z}$, \mathbf{Z}/\mathbf{a} est le sous-ensemble de \mathbf{Z} obtenu par le quotient de la relation d'équivalence $\cdot \mid \cdot$ de \mathbf{Z} par \mathbf{a} .

Si $x \in \mathbf{Z}$ alors \bar{x} est la classe d'équivalence de x dans \mathbf{Z}/\mathbf{a} .

Si $\bar{x} = \bar{y} \in \mathbf{Z}/\mathbf{a}$ alors pour x, y des représentants de leurs classes respectives :

$$x = y + ua$$

avec $u \in \mathbf{Z}$.

PROPOSITION 2.1.0.2. —

Soit $a \in \mathbf{N}$, $\mathbf{Z}/\mathbf{a} = \{\bar{0}, \bar{1}, \dots, \overline{a-1}\}$.

On étend naturellement les opérations sur \mathbf{Z} à \mathbf{Z}/\mathbf{a} .

THÉORÈME 2.1.0.3. —

\mathbf{Z}/\mathbf{p} est un groupe si, et seulement si, p est premier.

DÉMONSTRATION 2.1.0.3. —

Soit p premier et $\bar{x} \in \mathbf{Z}/\mathbf{p}$. Soit x un représentant de \bar{x} dans \mathbf{Z} .

1. Soit x est nul et c'est l'élément neutre d'inverse lui-même ;
2. Soit x est non nul et on a

$$x = ap$$

avec $a \in \mathbf{Z}^*$.

$$-ap = (-1)ap$$

et donc