ARITHMÉTIQUE DANS Z

1. NOTIONS ÉLÉMENTAIRES

1.1. Sous-groupe de 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 $(a, b) \in \mathbf{Z} \times \{0, 1, \ldots, x-1\}$ 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 $x\mathbf{Z} = \boldsymbol{x}$.

1.2. pgcd et ppcm

DÉFINITION 1.2.0.1. —
Soient $a, b \in \mathbf{Z}$. On dit de manière équivalente que « *a divise b* » ou :

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

DÉFINITION 1.2.0.2. —
Soient $a, b \in \mathbf{Z}$.
On a que $\boldsymbol{a}+\boldsymbol{b}$ est un sous-groupe de $\mathbf{Z}$ de la forme $\boldsymbol{d}$ avec $d \in \mathbf{Z}$. On note $\text{pgcd}(a, b) = d$.
$\boldsymbol{a} \cap \boldsymbol{b}$ est un sous-groupe de $\mathbf{Z}$ de la forme $\boldsymbol{m}$ 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 $x \in \mathbf{Z}$. $x \mid a$ et $x \mid b \iff \boldsymbol{a} \subset \boldsymbol{x}$ et $\boldsymbol{b} \subset \boldsymbol{x} \iff \boldsymbol{a} + \boldsymbol{b} \subset \boldsymbol{x} \iff x \mid \text{pgcd}(a,b)$.
2. Soit $x \in \mathbf{Z}$. $a \mid x$ et $b \mid x \iff \boldsymbol{x} \subset \boldsymbol{a}$ et $\boldsymbol{x} \subset \boldsymbol{b} \iff \boldsymbol{x} \subset \boldsymbol{a} \cap \boldsymbol{b} \iff \text{ppcm}(a,b) \mid x$.

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 $a \in \mathbf{Z}$, $\mathbf{Z}/\boldsymbol{a}$ est le sous-ensemble de $\mathbf{Z}$ obtenu par le quotient de la relation d'équivalence $\cdot \mid \cdot$ de $\mathbf{Z}$ par $\boldsymbol{a}$.
Si $x \in \mathbf{Z}$ alors $\overline{x}$ est la classe d'équivalence de x dans $\mathbf{Z}/\boldsymbol{a}$.

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

$$x = y + ua$$

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

Proposition 2.1.0.2. —
Soit $a \in \mathbf{N}$, $\mathbf{Z}/\boldsymbol{a} = \{\overline{0}, \overline{1}, \ldots, \overline{a-1}\}$.

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

Théorème 2.1.0.3. —
$\mathbf{Z}/\boldsymbol{p}$ est un groupe si, et seulement si, p est premier.

Démonstration 2.1.0.3. —
Soit p premier et $\overline{x} \in \mathbf{Z}/\boldsymbol{p}$. Soit x un représentant de $\overline{x}$ 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