2.3 Idéaux de $\mathbb{Z}$ et arithmétique

Théorème 2.26 (Les idéaux de $\mathbb{Z}$)**.** *$\mathbb{Z}$ est un anneau principal, dont les idéaux sont exactement les $a\mathbb{Z}$, $a \in \mathbb{N}$.*

Éléments de preuve. Les idéaux de $\mathbb{Z}$ sont en particulier des sous-groupes, dont on connaît la description ! □

Définition 2.27 ((Re)définition du pgcd d'un nombre fini d'entiers)**.** *Soit $n \geq 2$ et $a_1, \ldots, a_n$ des entiers naturels, non tous nuls, et m un entier naturel. Le pgcd $m = a_1 \wedge a_2 \wedge \cdots \wedge a_n$ de $a_1, \ldots, a_n$ est l'unique entier positif engendrant l'idéal $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}$. Ainsi, il est caractérisé par l'égalité*

$$m\mathbb{Z} = a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}.$$

Proposition 2.28 (Interprétation du pgcd par divisibilité)**.** *Le pgcd m de $a_1, \ldots, a_n$ est le plus grand entier (au sens de la divisibilité) tel que m divise chaque a_k. Ainsi, si d est un autre entier divisant chaque a_k, alors $d \mid m$.*

Remarque 2.29 (Lien avec Bézout)**.** *La définition 7.2.24 correspond en fait au théorème de Bézout. Il affirme en effet que si m désigne le pgcd de $a_1, \ldots, a_n$:*

- *il existe $u_1, \ldots, u_n$ des entiers relatifs tels que*

$$m = a_1u_1 + \cdots + a_nu_n;$$

- *réciproquement, si c vérifie*

$$c = a_1u_1 + \cdots + a_nu_n,$$

alors m divise c.

Remarque 2.30 (Définition du PGCD et du PPCM dans un anneau principal)**.** *On peut définir de la même façon un pgcd (mais non nécessairement unique) dans un anneau principal, ainsi qu'un ppcm, en remplaçant la somme par l'intersection. Par exemple, pour 2 éléments a et b :*

- *$aA + bA$ est un idéal principal de A, donc de la forme mA. Un élément m vérifiant cela est appelé pgcd de a et b.*
- *$aA \cap bA$ est un idéal principal de A, donc de la forme MA. Un élément M vérifiant cela est appelé ppcm de a et b.*

On retrouvera cette situation dans $\mathbb{K}[X]$.

3. Anneau $\mathbb{Z}/n\mathbb{Z}$

3.1 Propriétés d'inversibilité

Proposition 3.1 (Inversibles de $\mathbb{Z}/n\mathbb{Z}$)**.** *Soit $n \in \mathbb{N}^*$ et $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$. Les propositions suivantes sont équivalentes:*

(i) $\overline{k}$ est inversible;