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;

(ii) *il existe* u *et* v *dans* $\mathbb{Z}$ *tels que* $uk + vn = 1$*;*

(iii) $k \wedge n = 1$.

Éléments de preuve. Immédiat par traduction des congruences, et par le théorème de Bézout. □

Remarque 3.2. *Le point (ii) nous dit comment trouver un inverse de* k *modulo* n *: il suffit de déterminer une relation de Bézout, et de la réduire modulo* n*.*

Corollaire 3.3 (Le corps $\mathbb{F}_p$)**.** *En particulier, pour* $p \in \mathbb{N}^*$*,* $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ *est un corps si et seulement si* p *est premier. Ce corps est noté* $\mathbb{F}_p$*.*

Éléments de preuve. Si $p \in \mathbb{P}$, tout élément de $[1, p-1]$ est premier avec p. Réciproquement, si $p \notin \mathbb{P}$, un diviseur strict de p n'est pas premier avec p et sa classe n'est pas inversible dans $\mathbb{Z}/p\mathbb{Z}$. □

Exemple 3.4. *Le corps* $\mathbb{F}_2$ *a seulement deux éléments. Le corps* $\mathbb{F}_3$ *en a 3. Décrire leurs lois.*

3.2 Théorème chinois, et systèmes de congruences

Théorème 3.5 (Théorème chinois)**.** *Soit* m *et* n *dans* $\mathbb{N}^*$*, tels que* $m \wedge n = 1$*. Pour* $k \in \mathbb{Z}$*, on note :*

- $\hat{k}$ *la classe de* k *dans* $\mathbb{Z}/mn\mathbb{Z}$*;*
- $\check{k}$ *la classe de* k *dans* $\mathbb{Z}/m\mathbb{Z}$*;*
- $\tilde{k}$ *la classe de* k *dans* $\mathbb{Z}/n\mathbb{Z}$*;*

L'application $\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *définie par*

$$\varphi(\hat{k}) = (\check{k}, \tilde{k})$$

est bien définie, et est un isomorphisme d'anneaux. Ceci s'étend sans difficulté au cas d'un plus grand nombre d'entiers 2 à 2 premiers entre eux.

Éléments de preuve. Pour montrer que c'est un isomorphisme, étudier le noyau en se ramenant à des propriétés arithmétiques. □

Corollaire 3.6 (Unicité modulo $a_1 \cdots a_n$ de la solution d'un système)**.** *Soit* $a_1, \ldots, a_n$ *des entiers deux à deux premiers entre eux, et* $b_1, \ldots, b_n$ *des entiers. Alors le système*

$$\begin{cases} x \equiv b_1 [a_1] \\ \vdots \\ x \equiv b_n [a_n] \end{cases}$$

admet une solution, unique modulo $a_1 \cdots a_n$*.*

Corollaire 3.7 (Cas d'un second membre commun)**.** *En particulier, si* $b_1 = \cdots = b_n = b$*, la seule solution modulo* $a_1 \cdots a_n$ *est* b*.*