2.2 Idéaux

Définition 2.15 (Idéal d'un anneau commutatif)**.** *Soit A un anneau commutatif. Un idéal de A est une partie $I \subset A$ telle que :*

(i) *I est un sous-groupe de $(A, +)$,*

(ii) *I est fortement stable par produit : $A \cdot I \subset I$, c'est-à-dire :*

$$\forall a \in A, \quad \forall x \in I, \quad ax \in I.$$

Proposition 2.16 (Noyau d'un homomorphisme)**.** *Soit A et B deux anneaux, et $f : A \to B$ un morphisme d'anneaux. On suppose A commutatif. Alors Ker(f) est un idéal de A.*

Proposition 2.17 (Idéal engendré par x)**.** *Soit A un anneau commutatif, et $x \in A$.*

(i) *$xA = \{xa, a \in A\}$ est un idéal.*

(ii) *C'est le plus petit idéal de A contenant x.*

xA est appelé idéal engendré par x.

Définition 2.18 (Idéal principal)**.** *Soit A un anneau commutatif et I un idéal de A. On dit que I est un idéal principal, s'il existe x tel que $I = xA$.*

Définition 2.19 (Anneau principal)**.** *Un anneau principal est un anneau intègre dont tous les idéaux sont principaux.*

Exercise 2.20. *Soit A un anneau principal et (I_n) une suite croissante d'idéaux. Montrer que (I_n) est stationnaire.*

Définition 2.21 (Divisibilité dans un anneau commutatif intègre)**.** *Soit A un anneau commutatif intègre, et a et b deux éléments de A. On dit que a divise b s'il existe $c \in A$ tel que $ac = b$.*

Proposition 2.22 (Caractérisation de la divisibilité par les idéaux)**.** *Soit A un anneau commutatif intègre, et a et b deux éléments de A. Les propositions suivantes sont équivalentes :*

(i) *a divise b,*

(ii) *$bA \subseteq aA$.*

Proposition 2.23 (Somme d'idéaux)**.** *Soit I et J deux idéaux d'un anneau commutatif A. Alors :*

(i) *$I \cap J$ est un idéal de A,*

(ii) *$I + J = \{x + y \mid x \in I, y \in J\}$ est un idéal de A,*

(iii) *C'est le plus petit idéal K tel que $I \subseteq K$ et $J \subseteq K$.*

Cela s'étend par récurrence immédiate à un nombre fini quelconque d'idéaux.

Exercise 2.24. *Soit A un anneau commutatif non réduit à $\{0\}$. Montrer que A est un corps si et seulement si les seuls idéaux de A sont $\{0\}$ et A.*

Exercise 2.25. *Soit K un corps et $A = K \times K$.*

1. *Définir la structure d'anneau canonique sur A.*
2. *L'anneau A est-il un corps?*
3. *Déterminer les idéaux de A.*

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;