2. Anneaux et idéaux

2.1 Rappels

Définition 2.1 (Anneau). $(A, +, \times)$ *(ou plus simplement A) est un anneau si :*

(i) $(A, +)$ *est un groupe abélien ; le neutre est noté* 0_A *ou* 0*;*

(ii) $\times$ *est associative, et admet un neutre* 1_A*;*

(iii) $\times$ *est distributive sur* $+$*.*

On dit que A est un anneau commutatif si de plus $\times$ est commutative.

Définition 2.2 (Corps). $(K, +, \times)$ *est un corps si c'est un anneau commutatif, tel que tout $x \neq 0$ de K admet un inverse pour $\times$.*

Exemple 2.3.
1. *$\mathbb{Z}, \mathbb{R}, \mathbb{Q}$ et $\mathbb{C}$ munis des opérations usuelles sont des anneaux. $\mathbb{R}, \mathbb{Q}$ et $\mathbb{C}$ sont même des corps.*
2. *Pour tout $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif.*
3. *L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans un corps $\mathbb{K}$ est un anneau commutatif.*
4. *L'ensemble $M_n(\mathbb{R})$ des matrices carrées est un anneau non commutatif.*

Exercise 2.4. *Soit $\mathbb{K}$ un corps fini. On admet que tout polynôme non nul à coefficients dans $\mathbb{K}$, de degré $n \geq 0$, admet au plus n racines. Soit $n = |\mathbb{K}| - 1$.*

1. *Montrer que tout élément de $\mathbb{K}^*$ est racine de $X^n - 1$.*
2. *Montrer que s'il n'existe pas un élément de $\mathbb{K}^*$ dont l'ordre est n, il existe $p < n$ tel que tout élément de $\mathbb{K}^*$ soit racine de $X^p - 1$.*
3. *En déduire que $(\mathbb{K}^*, \times)$ est un groupe cyclique.*

Théorème 2.5 (Groupe des inversibles d'un anneau). *Soit A un anneau. Alors l'ensemble des éléments inversibles de A, généralement noté $A^\times$ ou $U(A)$, est stable pour la loi $\times$, et la loi induite munit $A^\times$ d'une structure de groupe multiplicatif.*

Définition 2.6 (Régularité et diviseurs de 0). *Soit A un anneau commutatif. Un élément $a \in A$ est appelé :*

- *élément régulier s'il est simplifiable : $ax = ay$ implique $x = y$;*
- *diviseur de 0 s'il est non nul, et qu'il existe $b \neq 0$ tel que $ab = 0$.*

Proposition 2.7 (Description des éléments réguliers). *Soit A un anneau commutatif et $a \in A\backslash\{0\}$. Les propositions suivantes sont équivalentes:*

(i) a *est régulier.*

(ii) a *n'est pas diviseur de 0.*

Définition 2.8 (Anneau intègre). *Un anneau A est intègre si :*

(i) $A \neq \{0\}$*;*

(ii) A *est commutatif;*

(iii) A *ne possède pas de diviseur de 0.*

La troisième propriété se traduit par : $ab = 0 \Longrightarrow (a = 0)$ *ou* $b = 0$*.*

Exemple 2.9 (Calculs dans un anneau)**.** *Sous certaines conditions de commutativité, certains outils calculatoires connus sur* $\mathbb{C}$ *restent valides dans un anneau :*

1. *la formule du binôme pour le développement de* $(A + B)^n$*, lorsque* $AB = BA$*;*
2. *la factorisation de* $A^n - B^n$ *par* $A - B$ *(factorisation de Bernoulli), lorsque* $AB = BA$*.*

Définition 2.10 (Homomorphisme d'anneaux)**.** *Soit* A *et* B *deux anneaux.*

(i) Un homomorphisme d'anneaux de A *à* B *est une application* $f : A \longrightarrow B$*, soit égale à la fonction nulle, soit vérifiant :*

$$\forall (x, y) \in A^2, f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y) \quad \textit{et} \quad f(1_A) = 1_B.$$

(ii) Un isomorphisme est un homomorphisme bijectif. Sa réciproque est alors aussi un morphisme d'anneau.

Définition 2.11 (Sous-anneau)**.** *Soit* $(A, +, \times)$ *un anneau. Un sous-anneau de* A *est un sous-ensemble* $B \subset A$ *tel que :*

(i) B *soit stable pour les lois* $+$ *et* $\times$*,*

(ii) $1_A \in B$*,*

(iii) les lois induites sur B *définissent sur* B *une structure d'anneau.*

Proposition 2.12 (Caractérisation des sous-anneaux)**.** *Un sous-ensemble* B *d'un anneau* A *est un sous-anneau de* A *si et seulement si :*

(i) $1_A \in B$*,*

(ii) pour tout $(x, y) \in B, x - y \in B$*,*

(iii) pour tout $(x, y) \in B, xy \in B$*.*

Proposition 2.13 (Anneau produit)**.** *Soit* $(A, +, \times)$ *et* $(B, +, \times)$ *deux anneaux. On munit le produit cartésien* $A \times B$ *des deux opérations :*

$$\forall ((a, b), (a', b')) \in (A \times B)^2, (a, b) + (a', b') = (a + a', b + b') \quad \textit{et} \quad (a, b) \times (a', b') = (a \times a', b \times b').$$

Muni de ces deux lois, $A \times B$ *est un anneau, donc les neutres sont* $(0_A, 0_B)$ *et* $(1_A, 1_B)$*. Si de plus,* A *et* B *sont commutatifs, il en est de même de* $A \times B$*.*

Proposition 2.14 (Inversibles d'un anneau produit)**.** *Soit* $(A, +, \times)$ *et* $(B, +, \times)$*. Alors*

$$(A \times B)^\times = A^\times \times B^\times.$$

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.*