

1 Introduction à la théorie des Anneaux

1.1 Introduction et Définitions

Dans le chapitre précédent, on a considéré des ensembles avec une structure définissant des groupes. Mais, on remarque que dans la plus part de ces ensembles, il y a deux structures différentes. Comme l'on a dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_n(\mathbb{R})$ et $\mathbb{R}[x]$, l'ensemble des polynômes à une variable. Ils ont en commun les faits suivants :

- L'addition (+) définit une structure de groupe abélien ;
- La multiplication (\times) définit un monoïde ;
- Distributivité : Pour tout a, b et c , on a : $(a+b) \times c = a \times c + b \times c$ et $c \times (a+b) = c \times a + c \times b$.

La formalisation de cette nouvelle structure est le but de ce chapitre. Par abus de notation, s'il n'y a pas de confusion, la loi binaire qui définit une structure de groupe abélien sur un ensemble quelconque sera notée par +. Tandis que, si la loi binaire définit un monoïde, elle sera notée par \times . L'élément neutre par rapport à l'addition sera noté par 0 et l'identité par rapport à la multiplication sera noté par 1.

1.1.1 Définition

Soit $(A, +, \times)$ une structure algébrique telle que $(A, +)$ est un groupe abélien et (A, \times) est un monoïde. On dit que $(A, +, \times)$ est un anneau si on a la distributivité de deux loi binaires. Si (A, \times) est un monoïde commutatif, on dit que $(A, +, \times)$ est un anneau commutatif. Un élément de A est dit inversible s'il est inversible par rapport à la loi multiplication. L'ensemble des éléments inversibles d'un anneau A est noté par A^\times . Si de plus, on a $A^\times = A \setminus \{0\}$, on dit que $(A, +, \times)$ est un corps.

1.1.2 Exemples

1. Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_n(\mathbb{R})$ et $\mathbb{R}[x]$ sont des anneaux ;
2. $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ et $\mathbb{R}[x]$ sont des anneaux commutatifs ;
3. \mathbb{Z} et $M_n(\mathbb{R})$ ne sont pas des corps ;
4. \mathbb{Q}, \mathbb{R} et \mathbb{C} sont des corps ;
5. $M_n(\mathbb{R})$ n'est pas un anneau commutatif ;
6. $\mathbb{Z}[i] := \{a + ib \in \mathbb{C} : a, b \in \mathbb{Z}\}$ où $i = \sqrt{-1}$ est un anneau commutatif. On a $(\mathbb{Z}[i])^\times = \{-1, 1, i, -i\}$.

1.1.3 Proposition

Soient A_1 et A_2 deux anneaux. Alors, le produit scalaire $A = A_1 \times A_2$ définit une structure d'anneau avec les opérations induites naturellement de celles de A_1 et A_2 .

1.2 Idéaux et Anneaux quotients

Considérons l'anneau des entiers $(\mathbb{Z}, +, \times)$. On sait que les sous groupes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z}$ où n est un entier naturel. Comme $(\mathbb{Z}, +)$ est un groupe abélien, l'ensemble quotient $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien. De plus, la multiplication dans \mathbb{Z} induit une structure monoïde sur $\mathbb{Z}/n\mathbb{Z}$ d'identité $\dot{1}$. De plus, pour tout \dot{a}, \dot{b} et \dot{c} dans $\mathbb{Z}/n\mathbb{Z}$, on a :

$$\dot{c}(\dot{a} + \dot{b}) = \dot{c}\dot{a} + \dot{c}\dot{b} = (\dot{a} + \dot{b})\dot{c}$$

. Ainsi, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau et l'on a :

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\dot{a} : \text{pgcd}(a, n) = 1\}.$$

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier. La généralisation de cet exemple est l'objet de cette section.