Chapitre 3 : Anneaux

I Généralités

A) Définition

Soit A un ensemble muni de deux lois notées $+$ et $\times$. On dit que $(A, +, \times)$ est un anneaux lorsque :

- $(A, +)$ est un groupe commutatif.
- $\times$ est associative et distributive sur $+$.
- Il y a dans A un élément neutre pour $\times$.

Si de plus $\times$ est commutative, on dit que $(A, +, \times)$ est un anneau commutatif.

Remarque, notation :
D'après les résultats généraux sur les lois de composition interne, si $(A, +, \times)$ est un anneau, il ne possède qu'un seul élément neutre pour $+$, il est noté 0_A et est appelé le zéro de A, et il ne possède qu'un seul élément neutre pour $\times$, il est noté 1_A et est appelé l'élément unité de A.

À moins que l'anneau A ne soit réduit au singleton $\{0_A\}$, on a $0_A \neq 1_A$. En effet, si on a $0_A = 1_A$ alors, pour tout $x \in A$, on a :

$$x = x \times 1_A = x \times 0_A = x \times (0_A + 0_A) = x \times (1_A + 1_A) = x \times 1_A + x \times 1_A = x + x \tag{3.1}$$

De $x = x + x$ on tire, selon la règle de régularité des éléments du groupe $(A, +)$, que $x = 0_A$.

B) Règles de calcul

Soit $(A, +, \times)$ un anneau, et a, b, c, d des éléments quelconques de A. On a :

- $a \times 0_A = 0_A \times a = 0_A$ (on dit que 0_A est absorbant).
  En effet, $a \times 0_A = a \times (0_A + 0_A) = a \times 0_A + a \times 0_A$, d'où, par régularité des éléments dans le groupe $(A, +)$, $a \times 0_A = 0_A$, et on fait de même de l'autre côté.
- $a \times (-b) = -(a \times b) = (-a) \times b$
  En effet, $ab + a(-b) = a(b + (-b)) = a \times 0_A = 0_A$, d'où $a(-b) = -(ab)$. De même pour l'autre égalité.
- Développement des produits de sommes : $(a + b)(c + d) = ac + ad + bc + bd$, attention à l'ordre dans les produits !
  (Immédiat en appliquant deux fois la distributivité)
- Pour $n \in \mathbb{N}$, on définit a^n par $a^0 = 1_A$ et $\forall n \in \mathbb{N}, a^{n+1} = a^n a$. Alors $\forall (n, p) \in \mathbb{N}^2, a^{n+p} = a^n a^p$ (immédiat par associativité de $\times$).
  Et $\forall (n, p) \in \mathbb{N}^2, (a^n)^p = a^{np}$ (mais attention : $(ab)^n = ab \times ab \dots ab$, $\times$ n'est pas nécessairement commutative).

- Dans le groupe $(A, +)$, on a toujours la définition et les propriétés pour $n.a$ ($n \in \mathbb{Z}$), et de plus : $(n.a) \times b = n.(ab) = a \times (n.b)$ (qu'on peu noter $n.ab$).

  En effet, pour $n \in \mathbb{N}$, on le montre aisément par récurrence, en utilisant la distributivité de $\times$ sur $+$, puis pour $n = -p$ avec $p \in \mathbb{N}$, on a $(p(-a)) \times b = (p(-a) \times b) = p(-ab) = p(a(-b)) = a \times (p(-b))$ d'après les règles précédentes, d'où $(n.a) \times b = n.(ab) = a \times (n.b)$ selon la règle $(-p)x = p(-x)$.

C) Deux identités remarquables

Proposition :

Dans tout anneau $(A, +, \times)$, a et b étant deux éléments de A qui commutent, on a, pour tout $n \in \mathbb{N}$:

$$(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^p b^{n-p} \quad \text{(formule du binôme)} \tag{3.2}$$

$$a^n - b^b = (a-b) \sum_{p=0}^{n-1} a^p b^{n-p-1} \quad \text{(avec } n \geqslant 1\text{)} \tag{3.3}$$

Démonstration :

- Pour la formule du binôme, on peut reprendre la démonstration faite dans l'anneau $(\mathbb{R}, +, \times)$, étant donné qu'elle n'utilise que les règles de calculs dans un anneau et le fait que a et b commutent.
- Pour la seconde :

$$\begin{aligned}
(a-b) \sum_{p=0}^{n-1} a^p b^{n-p-1} &= a \sum_{p=0}^{n-1} a^p b^{n-p-1} - b \sum_{p=0}^{n-1} a^p b^{n-p-1} \quad \text{(distributivité)} \\
&= \sum_{p=0}^{n-1} a^{p+1} b^{n-p-1} - \sum_{p=0}^{n-1} b a^p b^{n-p-1} \quad \text{(distributivité)} \\
&= \sum_{p=0}^{n-1} a^{p+1} b^{n-p-1} - \sum_{p=0}^{n-1} a^p b^{n-p} \quad (a \text{ et } b \text{ commutent}) \\
&= \sum_{p=1}^{n} a^p b^{n-p} - \sum_{p=0}^{n-1} a^p b^{n-p} \quad \text{(changement de variable)} \\
&= a^n - b^n
\end{aligned} \tag{3.4}$$

D) Exemples d'anneaux

$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ pour les lois usuelles sont des anneaux.

E étant un ensemble, et $(A, +, \times)$ un anneau, en définissant les lois $+$ et $\times$ sur $\mathscr{F}(E, A)$ par : pour $f, g \in \mathscr{F}(E, A)$, $f+g \colon x \mapsto f(x)+g(x)$, $fg \colon x \mapsto f(x)g(x)$, on vérifie immédiatement que $(\mathscr{F}(E, A), +, \times)$ est un anneau, commutatif si A l'est.

En particulier :

- En prenant pour $(A, +, \times)$ l'anneau $(\mathbb{R}, +, \times)$, et en prenant toujours E un ensemble quelconque : $\mathscr{F}(E, \mathbb{R})$, muni des lois « naturelles » $+$ et $\times$ d'addition et de multiplication de fonctions est un anneau commutatif.

  Et si on prend $E = \mathbb{N}$, on obtient $\mathscr{F}(\mathbb{N}, \mathbb{R})$, c'est-à-dire l'ensemble des suites réelles indexées par $\mathbb{N}$

(noté aussi $\mathbb{R}^{\mathbb{N}}$) ; muni des lois naturelles d'addition et de multiplication de suites, c'est un anneau commutatif.

- Et de même en prenant pour $(A,+,\times)$ l'anneau $(\mathbb{C},+,\times)$, $(\mathscr{F}(E,\mathbb{C}),+,\times)$ est un anneau commutatif, et en particulier $(\mathbb{C}^{\mathbb{N}},+,\times)$ est un anneau commutatif.

II Sous anneaux

Définition :
Soit $(A,+,\times)$ un anneau, et soit B une partie de A. On dit que B est un sous anneau de A lorsque :

- B est stable par $+$ et $\times$.
- $1_A \in B$
- $\forall x \in B, (-x) \in B$

Proposition :
Soit $(A,+,\times)$ un anneau, et soit B une partie de A. Si B est un sous anneau de $(A,+,\times)$, alors $+$ et $\times$ constituent des lois de composition internes sur B, et $(B,+,\times)$ est un anneau, commutatif si A l'est.

Exemple :

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sont des sous anneaux de $(\mathbb{C},+,\times)$.
- L'ensemble des suites réelles convergentes (et indexées par $\mathbb{N}$) constitue un sous anneau de $(\mathbb{R}^{\mathbb{N}},+,\times)$.

III Morphismes d'anneaux

Définition :
Soient $(A,+,\times)$ et $(B,+,\times)$ deux anneaux. Un morphisme d'anneaux de A vers B est une application $\varphi\colon A \to B$ telle que :

- $\forall (x,y) \in A^2, \varphi(x+y) = \varphi(x) + \varphi(y)$,
- $\forall (x,y) \in A^2, \varphi(x\times y) = \varphi(x) \times \varphi(y)$
- $\varphi(1_A) = 1_B$

Remarque :
Un morphisme d'anneau φ de $(A,+,\times)$ vers $(B,+,\times)$ est en particulier un morphisme de groupes de $(A,+)$ vers $(B,+)$, on a donc nécessairement $\varphi(0_A) = 0_B$. En revanche, la dernière condition ne doit pas être oubliée car elle ne résulte pas des deux premières.

Exemple :
L'application $u \to \lim u$ constitue un morphisme de l'anneau des suites réelles convergentes indexées par $\mathbb{N}$, muni des lois naturelles $+$ et $\times$ vers l'anneau $(\mathbb{R},+,\times)$.

Définition :
De même que dans les groupes, on définit pour un morphisme φ de $(A, +, \times)$ vers $(B, +, \times)$ l'image de φ par $\operatorname{Im}\varphi = \{\varphi(x), x \in A\} = \varphi(A)$ et le noyau de φ par $\ker\varphi = \{x \in A, \varphi(x) = 0_B\}$ (c'est le noyau du morphisme de groupes correspondant).
Ici encore, $\operatorname{Im}\varphi$ et $\ker\varphi$ sont des sous anneaux respectivement de $(B, +, \times)$ et $(A, +, \times)$ (la démonstration est quasiment la même que pour les groupes)

Proposition :
Si φ est un morphisme d'anneaux de $(A, +, \times)$ vers $(B, +, \times)$, et si A' est un sous anneau de A, alors $\varphi(A')$ est un sous anneau de B.

Démonstration :
Évident en considérant $\operatorname{Im}\varphi_{|A'}$.

Proposition, définition :
Si φ est un morphisme d'anneaux de $(A, +, \times)$ vers $(B, +, \times)$, et si φ est bijectif, alors φ^{-1} est un morphisme d'anneaux bijectif de $(B, +, \times)$ vers $(A, +, \times)$. On dit alors que φ est un isomorphisme d'anneaux.

Démonstration :
Se baser toujours sur les morphismes de groupes.

IV Compléments

A) Éléments inversibles

Définition :
Soit A un anneau non réduit à $\{0\}$. Un élément x de A est inversible lorsqu'il existe $x' \in A$ tel que $xx' = x'x = 1_A$.

Proposition, définition :
Si x est inversible, alors il existe un unique $x' \in A$ tel que $xx' = x'x = 1_A$. On l'appelle l'inverse de x, et on le note x^{-1}.

Proposition :
L'ensemble A^* des éléments inversibles de A forme un groupe pour $\times$.

Démonstration :

- Pour tous $x, y \in A^*$, $xy \in A^*$. En effet, $xyy^{-1}x^{-1} = y^{-1}x^{-1}xy = 1_A$, donc $xy \in A^*$ et $(xy)^{-1} = y^{-1}x^{-1}$
- $\times$ est associative.
- $1_A \in A^*$ et est neutre pour $\times$
- Si $x \in A^*$, alors évidemment $x^{-1} \in A^*$ et est symétrique de x pour $\times$.

B) Anneau intègre

Soit $(A, +, \times)$ un anneau quelconque. Il est faux en général que, pour $a, b \in A, ab = 0_A \implies a = 0_A$ ou $b = 0_A$.

Un élément a tel qu'il existe $b \neq 0_A$ de sorte que $ab = 0_A$ s'appelle un diviseur de 0_A (0_A est donc un diviseur de 0_A, puisque on a même pour tout $b \neq 0_A$, $0_A b = 0_A$).

Définition :

Soit $(A, +, \times)$ un anneau. On dit que A est intègre lorsque :

- A n'est pas réduit à $\{0_A\}$.
- A est commutatif.
- A n'admet pas de diviseur de 0_A autre que 0_A, c'est-à-dire :

$$\forall x, y \in A, xy = 0_A \implies x = 0_A \text{ ou } y = 0_A. \tag{3.5}$$

Exemple :

$\mathbb{Z}$ est intègre. $\mathscr{F}(\mathbb{R}, \mathbb{R})$ ne l'est pas.

Attention : dans un anneau où il y a des diviseurs de 0_A autres que 0_A (c'est-à-dire non intègre), les éléments non nuls de A ne sont pas toujours réguliers pour $\times$. En effet,

$$ab = ac \implies ab - ac = 0_A \implies a(b - c) = 0_A, \tag{3.6}$$

ce qui peut arriver même si $a \neq 0_A$ et $b - c \neq 0_A$.