Anneaux et corps

Table des matières

---

1 Anneaux : généralités

Définition : un *anneau* est un triplet $(A, +, \times)$ où : $(A, +)$ est un groupe commutatif ; $\times$ est une loi sur A associative, possédant un élément neutre, et *distributive* par rapport à $+$, c'est-à-dire : $x\times(y+z) = (x\times y)+(x\times z)$ et $(x + y) \times z = (x \times z) + (y \times z)$ quels que soient x, y et z.

L'élément neutre de la loi $\times$ est noté $\mathbf{1}_A$ ou $\mathbf{1}$ s'il n'y a aucun risque de confusion. L'anneau est commutatif lorsque la loi $\times$ est l'est.

Nous supposons toujours $1_A \neq \mathbf{0}_A$; les deux lois sont dont distinctes, et A contient au moins deux éléments.

Exemples — $(\mathbb{Z}, +, \times)$, $(\mathbb{Z}[\sqrt{d}], +, \times)$ où $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d},\ a \in \mathbb{Z},\ b \in \mathbb{Z}\}$ sont des anneaux commutatifs. Si A est un anneau, et E un ensemble quelconque, alors l'ensemble $\mathcal{F}(E, A)$ (noté aussi A^E) des fonctions de E dans A est muni d'une structure naturelle d'anneau : si f et g sont dans A^E, alors $f \oplus g$ et $f \otimes g$ par $(f \oplus g)(a) = f(a)+g(a)$ et $(f \otimes g)(a) = f(a) \times g(a)$ pour tout $a \in A$. En pratique, nous noterons $f + g$ et $f \times g$.

Exemple — l'ensemble $\mathcal{M}_2(\mathbb{K})$ des matrices carrées d'ordre 2, à coefficients dans $\mathbb{K}$ (où $\mathbb{K}$ désigne $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$) est un anneau non commutatif.

2 Règles de calcul dans un anneau

Proposition : pour tout $x \in A$, on a $\mathbf{0}_A \times x = x \times \mathbf{0}_A = \mathbf{0}_A$.

Preuve : $x = x \times 1_A = x \times (1_A + \mathbf{0}_A) = (x \times 1_A) + (x \times \mathbf{0}_A) = x + (x \times \mathbf{0}_A)$, d'où le résultat par régularité.

Proposition : pour tous x et y dans A, on a $x \times (-y) = (-x) \times y = -(x \times y)$.

Preuve : $\mathbf{0}_A = x \times \mathbf{0}_A = x \times \big(y + (-y)\big) = \big(x \times y\big) + \big(x \times (-y)\big)$, d'où le résultat.

Proposition : si deux éléments x et y d'un anneau A commutent, alors on peut leur appliquer la formule du binôme :

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Preuve : par récurrence sur n.

3 Sous-anneaux

Définition : une partie B d'un anneau A est un *sous-anneau* de A si elle contient 0_A et $\mathbf{1}_A$ et est stable pour les deux lois de A.

Exemples — l'ensemble des fonctions $\varphi : \mathbb{R} \mapsto \mathbb{R}$ paires est un sous-anneau de l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, muni de sa structure naturelle d'anneau. L'ensemble des rationnels de la forme $\frac{p}{2q+1}$ est un sous-anneau de $\mathbb{Q}$, de même que l'ensemble des rationnels de la forme $\frac{p}{q^k}$ où $q \geqslant 2$ est fixé, $p \in \mathbb{Z}$ et $k \in \mathbb{N}^*$.

Proposition : B est un sous-anneau de A ssi B n'est pas vide et contient $x - y$ et $x \times y$ dès qu'il contient x et y.

Proposition : l'intersection de deux sous-anneaux d'un même anneau A est un sous-anneau de A.

4 Morphismes d'anneaux

Définition : soient A et B deux anneaux (les lois sont notées $+$ et $\times$ dans les deux cas). Un (homo)morphisme d'anneaux de A dans B est, soit le morphisme nul (qui, à tout $x \in A$, associe $\mathbf{0}_B$), soit une fonction $\varphi : A \mapsto B$ vérifiant :

- $\varphi(a + b) = \varphi(a) + \varphi(b)$ quels que soient a et b appartenant à A ;
- $\varphi(a \times b) = \varphi(a) \times \varphi(b)$ quels que soient a et b appartenant à A ;
- $\varphi(\mathbf{1}_A) = \mathbf{1}_B$.

Proposition : soient A, B, C trois anneaux. Si$f : A \mapsto B$ et $g : B \mapsto C$ sont des morphismes d'anneaux, alors $g \circ f$ est un morphisme d'anneaux.

Définition : le noyau d'un morphisme d'anneaux $\varphi : A \mapsto B$ est l'ensemble $\{x \in A : \varphi(x) = \mathbf{0}_B\}$; il est noté $\ker(\varphi)$.

Proposition : un morphisme d'anneaux φ est injectif ssi $\ker(\varphi) = \{\mathbf{0}_A\}$.

Un *isomorphisme* d'anneaux est un homomorphisme bijectif ; un *automorphisme* d'un anneau A est un isomorphisme de A sur A. L'ensemble $\mathbf{Aut}(A)$ des automorphismes d'un anneau A est un groupe pour la composition des fonctions.

Proposition : soit A un anneau ; il existe un et un seul morphisme d'anneau de $\mathbb{Z}$ dans A.

Preuve : ce morphisme φ est défini par $\varphi(0) = \mathbf{0}_A$; $\varphi(n + 1) = \varphi(n) + \mathbf{1}_A$ pour tout naturel n ; et $\varphi(-n) = -\varphi(n)$ pour tout naturel n non nul.

Proposition : si $\varphi : A \mapsto B$ est un morphisme d'anneaux, alors $\varphi(A)$ est un sous-anneau de B, et $\varphi^{-1}(B)$ est un sous-anneau de A.

5 Diviseurs de zéro

Définition : un *diviseur de zéro* d'un anneau A est un élément $x \neq 0$ pour lequel il existe au moins un élément $y \neq 0$ de A tel que $xy = 0$. Un anneau est dit *intègre* s'il ne posède aucun diviseur de zéro.

Exemple — $\mathbb{Z}$ est intègre. L'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, muni des lois $+$ et $\times$ usuelles, n'est pas intègre : considérer $x \mapsto x^+ = \max(x, 0)$ et $x \mapsto x^- = \max(-x, 0)$.

Proposition : un élément régulier d'un anneau A ne peut être diviseur de zéro.

Remarque : soient A et B deux anneaux. L'*anneau produit* de A et B est $(A \times B, \oplus, \otimes)$, les deux lois étant définies par $(a, b) \oplus (c, d) = (a + c, b + d)$ et $(a, b) \otimes (c, d) = (a \times c, b \times d)$. Constatons que, même si A et B sont intègres, l'anneau produit $A \times B$ ne l'est pas car $(\mathbf{1}_A, \mathbf{0}_B) \otimes (\mathbf{0}_A, \mathbf{1}_B) = (\mathbf{0}_A, \mathbf{0}_B)$.

6 Corps

Définition : un *corps* est un anneau $(\mathbb{K}, +, \times)$ commutatif dans lequel tout élément autre que $0_{\mathbb{K}}$ est inversible.

Exemples — avec les lois usuelles, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps ; $\mathbb{Q}[\sqrt{d}]$ est un corps ssi d n'est pas un carré parfait.

Définition : un *sous-corps* d'un corps $\mathbb{K}$ est une partie L non vide de $\mathbb{K}$, qui est stable pour les lois de $\mathbb{K}$, et qui est un corps, pour les lois induites par celles de $\mathbb{K}$.

Exemples — $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, qui est lui-même un sous-corps de $\mathbb{C}$

FIN