Chapitre

Anneaux, corps, algèbres

2.1 Structures d'anneau, de corps

2.1.1 Définition d'un anneau et exemples fondamentaux (rappel de MPSI)

Définition 2.1.1 : structure d'anneau
Soit A un ensemble muni de deux LCI notées $+$ et $\times$. On dit que $(A,+,\times)$ est un anneau lorsque :

1. $(A,+)$ est un groupe abélien ; son neutre est noté 0_A.
2. La loi $\times$ est associative.
3. La loi $\times$ est distributive par rapport à la loi $+$.
4. La loi $\times$ admet un élément neutre, noté 1_A et appelé élément unité de A.

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

Remarque 2.1.2 :
Dans un anneau $(A,+,\times)$ on note $-x$ le symétrique de x pour $+$.
Attention : *a priori* un élément n'a pas de symétrique pour $\times$, donc la notation x^{-1} n'a pas de sens en général.

Exemple 2.1.3 :

1. $(\mathbb{Z},+,\times)$ est un anneau commutatif unitaire.
2. $(\mathbb{R}^{\mathbb{R}},+,\times)$ est un anneau commutatif unitaire, d'unité la fonction constante de valeur 1.
3. $\mathcal{M}_n(\mathbb{R})$ est un anneau unitaire, non commutatif si $n>1$.
4. $(2\mathbb{Z},+,\times)$ est un anneau commutatif non unitaire.
5. $\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} ; (a,b)\in\mathbb{Z}^2\right\}$ est un anneau non unitaire et non commutatif.

2.1.2 Règles de calcul dans un anneau (rappel de MPSI), éléments inversibles

Proposition 2.1.4 : règles de calcul dans un anneau (rappel de MPSI)
Soit $(A,+,\times)$ un anneau.

1. 0_A est un élément absorbant : $\forall a\in A,\ a\times 0_A = 0_A\times a = 0_A$.
2. $\forall a\in A,\ (-1_A)\times a = a\times(-1_A) = -a$.
3. $\forall (a,b)\in A^2,\ (-a)\times b = a\times(-b) = -ab$.
4. $\forall (a,b,c)\in A^3,\ (a-b)\times c = ac-bc \ \wedge\ c(a-b)=ca-cb$.

Notations : dans un anneau $(A,+,\times)$ on note pour $a\in A$ et $n\in\mathbb{N}$:

1. $na=\begin{cases}\underbrace{a+a+\cdots+a}_{n \text{ fois}} & \text{si } n\neq 0\\ 0_A & \text{si } n=0\end{cases}$.
2. $(-n)a=n(-a)=\underbrace{(-a)+\cdots+(-a)}_{n \text{ fois}}$ si $n\neq 0$.
3. $a^n=\begin{cases}\underbrace{a\times a\times\cdots\times a}_{n \text{ fois}} & \text{si } n\neq 0\\ 1_A & \text{si } n=0\end{cases}$.

Attention ! a^{-n} n'a pas de sens si a n'est pas inversible pour $\times$.

Théorème 2.1.5 : binôme de Newton (rappel de MPSI)
Dans un anneau $(A,+,\times)$, lorsque deux éléments a et b commutent on a la formule suivante :

$$\forall n\in\mathbb{N},\quad (a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}.$$

Théorème 2.1.6 : formules de factorisation (rappel de MPSI)
Soit $(A,+,\times)$ un anneau.

1. $\forall a\in A,\ \forall n\in\mathbb{N}$,
$$1-a^n=(1-a)\left(\sum_{k=0}^{n-1}a^k\right)=\left(\sum_{k=0}^{n-1}a^k\right)(1-a).$$
2. $\forall a\in A,\ \forall p\in\mathbb{N}$,
$$1+a^{2p+1}=(1+a)\left(\sum_{k=0}^{2p}(-a)^k\right)=\left(\sum_{k=0}^{2p}(-a)^k\right)(1+a).$$
3. $\forall a\in A,\ \forall n\in\mathbb{N}^*,\ \forall(b_1,\dots,b_n)\in A^n$,
$$\sum_{i=1}^{n}ab_i=a\left(\sum_{i=1}^{n}b_i\right)\quad\wedge\quad\sum_{i=1}^{n}b_ia=\left(\sum_{i=1}^{n}b_i\right)a.$$
4. $\forall(n,p)\in(\mathbb{N}^*)^2,\ \forall(a_1,\dots,a_n)\in A^n,\ \forall(b_1,\dots,b_p)\in A^p$,
$$\sum_{i=1}^{n}\left(\sum_{j=1}^{p}a_ib_j\right)=\sum_{j=1}^{p}\left(\sum_{i=1}^{n}a_ib_j\right)=\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{n}b_j\right).$$
5. Formule de Bernoulli. Si $ab=ba$ alors :
$$\forall n\in\mathbb{N}^*,\quad a^n-b^n=(a-b)\left(a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1}\right)=(a-b)\left(\sum_{k=0}^{n-1}a^kb^{n-k-1}\right).$$

Proposition 2.1.7 : éléments inversibles d'un anneau
L'ensemble des éléments inversibles d'un anneau est un groupe pour le produit.

En d'autres termes : si A est un anneau alors, en notant $\mathcal{U}(A)$ l'ensemble de ses éléments inversibles, le couple $(\mathcal{U}(A),\times)$ est un groupe.

Définition 2.1.8 : éléments associés
Deux éléments d'un anneau sont associés lorsqu'ils sont égaux à multiplication près par un inversible.

Exemple 2.1.9 :

- Les inversibles de $\mathbb{Z}$ étant 1 et -1, on en déduit que tout entier est associé à un entier naturel et un seul.
- Les inversibles de $\mathbb{Z}[i]$ étant 1, -1, i et $-i$, on en déduit que $1+2i$ et $i-2$ sont associés.
- Les inversibles de $\mathbb{K}[X]$ étant les éléments non-nuls de $\mathbb{K}$, on en déduit que tout polynôme est associé à un polynôme unitaire et un seul.

2.1.3 Sous-anneau

Définition 2.1.10 : sous-anneau

On considère un anneau $(A,+,\times)$ et une sous-partie A' de A. On dit que la partie A' est un sous-anneau de A lorsque :

1. $(A',+)$ est un sous-groupe de $(A,+)$.
2. La partie A' est stable pour la loi $\times$: $\forall (a,b)\in A'^2,\ ab\in A'$.
3. L'élément unité de A est dans A' : $1_A\in A'$.

Théorème 2.1.11 : caractérisation d'un sous-anneau

Soit $(A,+,\times,1_A)$ un anneau unitaire. Une partie A' de A est un sous-anneau de A si et seulement si :

(i) $1_A\in A'$.

(ii) $\forall (a,b)\in A'^2,\ a-b\in A'$.

(iii) $\forall (a,b)\in A'^2,\ a\times b\in A'$.

Exemple 2.1.12 :

1. L'ensemble $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.
2. L'ensemble $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$, appelé anneau des entiers de Gauss.
3. L'ensemble des application continues de $\mathbb{R}$ dans $\mathbb{R}$ est un sous-anneau de l'anneau des applications de $\mathbb{R}$ dans $\mathbb{R}$.
4. L'ensemble des suites bornées, l'ensemble des suites périodiques, sont des sous-anneaux de $\mathbb{R}^{\mathbb{N}}$.

2.1.4 Produit d'anneaux

Théorème 2.1.13 : produit de deux anneaux

Soit $(A,+_A,\times_A,1_A)$ et $(B,+_B,\times_B,1_B)$ deux anneaux unitaires. On définit deux lois de composition interne $+$ et $\times$ sur $A\times B$ en posant :

$$\forall (a_1,a_2)\in A^2,\ \forall (b_1,b_2)\in B^2,\quad (a_1,b_1)+(a_2,b_2)=(a_1+_A a_2,b_1+_B b_2),\quad (a_1,b_1)\times(a_2,b_2)=(a_1\times_A a_2,b_1\times_B b_2).$$

Alors $(A\times B,+,\times,(1_A,1_B))$ est un annueau unitaire. appelé anneau produit.

On effectue de même le produit d'un nombre fini d'anneaux.

2.1.5 Morphisme d'anneaux

Définition 2.1.14 : morphisme d'anneaux

Soit $(A,+,\times)$ et $(B,+,\times)$ deux anneaux.

1. Un morphisme d'anneaux est une application $f:A\to B$ respectant les structures d'anneaux, c'est-à-dire vérifiant :
$$\forall (a,b)\in A^2,\quad f(a+b)=f(a)+f(b)\ \wedge\ f(a\times b)=f(a)\times f(b).$$
Lorsque $A=B$, on parle d'endomorphisme de l'anneau A.

2. Un morphisme d'anneaux bijectif est appelé isomorphisme d'anneaux.
   Lorsque $A = B$, on parle d'automorphisme de l'anneau A.

Exemple 2.1.15 :
Si a est un élément inversible de l'anneau A, alors l'application $\varphi_a : x \mapsto axa^{-1}$ est un automorphisme d'anneau de A, appelé automorphisme intérieur. Sa bijection réciproque est $\varphi_{a^{-1}}$.

Proposition 2.1.16 : image directe et image réciproque de sous-anneaux par un morphisme
L'image directe et l'image réciproque de sous-anneaux par un morphisme d'anneaux sont des sous-sous-anneaux.
Plus précisément soit $f : A \to B$ un morphisme d'anneaux, et A' et B' des sous-anneaux de A et B respectivement. Alors $f(A')$ est un sous-anneau de B et $f^{-1}(B')$ est un sous-anneau de A.

Définition 2.1.17 : noyau et image d'un morphisme d'anneaux
Soit $f : A \to B$ un morphisme d'anneaux.

1. On appelle noyau de f, noté $\mathrm{Ker}\,(f)$, l'ensemble des antécédents par f de 0_B dans A :
$$\mathrm{Ker}\,(f) = f^{-1}(\{0_B\}) = \{x \in A\,;\, f(x) = 0_B\}.$$
   C'est d'après la proposition précédente un sous-anneau de A.
2. On appelle image de f, noté $\mathrm{Im}\,(f)$, l'ensemble des images par f des éléments de A :
$$\mathrm{Im}\,(f) = f(A) = \{y \in B\,;\, \exists x \in A,\, y = f(x)\}.$$
   C'est d'après la proposition précédente un sous-anneau de B.

Attention : un noyau n'est jamais vide ! En effet il contient toujours au moins 0_A.

Théorème 2.1.18 : caractérisation des morphismes injectifs/surjectifs
Soit $f : A \to B$ un morphisme d'anneaux.

1. f est injective si et seulement si $\mathrm{Ker}\,(f) = \{0_A\}$.
2. f est surjective si et seulement si $\mathrm{Im}\,(f) = B$.

Théorème 2.1.19 : réciproque d'un isomorphisme d'anneaux
La bijection réciproque d'un isomorphisme d'anneaux est elle-même un isomorphisme d'anneaux.

2.1.6 Intégrité, corps (rappel de MPSI)

Définition 2.1.20 : diviseurs de zéro, anneau intègre
Soit $(A, +, \times)$ un anneau.

1. Lorsqu'il existe des éléments a et b de A non-nuls tels que $ab = 0_A$, on dit que a et b sont des diviseurs de zéro.
2. L'anneau A est intègre lorsque :
   (a) $A \neq \{0_A\}$.
   (b) $\times$ est commutative.
   (c) Il n'y a pas de diviseur de zéro : $\forall (a, b) \in A^2,\ ab = 0 \Longrightarrow (a = 0) \vee (b = 0)$.
   Ceci équivaut à : si $a \neq 0$ et $b \neq 0$ alors $ab \neq 0$.

Exemple 2.1.21 :

1. $(\mathbb{Z}, +, \times)$ est un anneau intègre.
2. Dans l'anneau $(\mathbb{R}^{\mathbb{R}}, +, \times)$ il y a des diviseurs de zéro. En effet les fonctions $f = 1_{[-2,-1]}$ et $g = 1_{[1,2]}$, indicatrices de $[-2, -1]$ et $[1, 2]$ respectivement, sont non-nulles mais de produit nul.

3. $\mathcal{M}_2(\mathbb{R})$ admet des diviseurs de zéro : $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. On généralise sans problème à $\mathcal{M}_n(\mathbb{R})$.

Définition 2.1.22 : structure de corps
Un ensemble K muni de deux LCI $+$ et $\times$ est un corps lorsque :

1. $(K, +, \times)$ est un anneau.
2. $0_K \neq 1_K$.
3. Tout élément de $K \setminus \{0\}$ admet un inverse pour $\times$ dans K.

Si de plus la loi $\times$ est commutative alors le corps $(K, +, \times)$ est commutatif.

Théorème 2.1.23 : caractérisation d'un corps
L'ensemble K muni de deux LCI $+$ et $\times$ est un corps si et seulement si :

(i) Le couple $(K, +)$ est un groupe abélien.
(ii) Le couple $(K \setminus \{0_K\}, \times)$ est un groupe abélien.
(iii) La loi $\times$ est distributive par rapport à la loi $+$.

Exemple 2.1.24 :

- Les ensembles $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ pour les lois $+$ et $\times$ usuelles sont des corps commutatifs.
- $\mathbb{Z}$ est un anneau commutatif unitaire intègre, mais ce n'est pas un corps car par exemple 2 n'a pas de symétrique pour $\times$ (*i.e.* n'admet pas d'inverse).
- $\mathbb{K}[X]$ n'est pas un corps car un polynôme non constant n'a pas d'inverse dans $\mathbb{K}[X]$.

Remarque 2.1.25 :

1. Dans la suite, tous les corps qui interviendront seront commutatifs.
2. Tout corps commutatif est un anneau intègre. La réciproque est fausse : $(\mathbb{Z}, +, \times)$ est intègre mais pas un corps.

Définition 2.1.26 : sous-corps
Soit $(K, +, \times)$ un corps et L une partie de K. On dit que L est un sous-corps de K lorsque :

1. L est un sous-anneau de K.
2. $\forall x \in L \setminus \{0_K\}$, $x^{-1} \in L$.

Ou encore :

(i) $\forall (x, y) \in L^2$, $x - y \in L$.
(ii) $\forall (x, y) \in L^2$, $xy \in L$.
(iii) $1_K \in L$.
(iv) $\forall x \in L \setminus \{0_K\}$, $x^{-1} \in L$.

Exemple 2.1.27 :

- $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, qui est un sous-corps de $\mathbb{C}$ (pour les lois $+$ et $\times$ usuelles).
- L'ensemble $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}\,;\, (a, b) \in \mathbb{Q}^2\}$ est un sous-corps de $\mathbb{R}$.

Remarque 2.1.28 :

1. Tout sous-corps L d'un corps K est un corps pour les lois induites. Les neutres de L pour $+$ et $\times$ sont ceux de K.