Chapitre III - Des anneaux et des corps

1. Anneaux et corps (généralités)
2. Idéal et anneau quotient
3. Corps des fractions d'un anneau
4. Polynômes
5. Arithmétique dans un anneau

1. Anneaux et corps (généralités)

1. Définitions et règles de calcul
2. Morphismes, A-algèbre, caractéristique
3. Sous-anneau, sous-anneau engendré

1. Définitions et règles de calcul

Définitions (anneau et corps)

$(A, +, 0, *, e)$ est un anneau (unitaire) si :

(i) $(A, +, 0)$ est un groupe abélien ;

(ii) $(A, *, e)$ est un monoïde ;

(iii) $*$ est distributive par rapport à $+$:

$$(\forall a, b, c \in A) \qquad a * (b + c) = a * b + a * c \quad \text{et} \quad (a + b) * c = a * c + b * c$$

Si de plus,
(iv) $(A \setminus \{0\}, *, e)$ est un groupe (*i.e.* tout élément distinct de 0 admet un symétrique pour $*$),
on dit que $(A, +, 0, *, e)$ est un corps.

Dans ce cours, on supposera toujours que $e \neq 0$, ainsi un anneau contient toujours au moins 2 éléments.

Exemples et règles de calcul

Exemples :
$(\mathbb{Z}, +, 0, \cdot, 1)$ est un anneau qui n'est pas un corps.
$\mathbb{Z}/2\mathbb{Z} = \{0; 1\}$ est un corps.
$(\mathbb{Z}/n\mathbb{Z}, +, 0, \cdot, 1)$ sont des anneaux qui sont des corps si et seulement si n est un nombre premier.

Proposition (règles de calcul dans un anneau $(A, +, 0, *, e)$)

(i) $(\forall x \in A) \qquad x * 0 = 0 * x = 0.$

(ii) $(\forall x, y \in A) \qquad x * (-y) = -(x * y) = (-x) * y.$

Démonstration :

(i) $x * 0 = x * (0 + 0) = \cdots$ (exercice).

(ii) $x * (-y) + x * y = \cdots$ (exercice).

□

Autres définitions

Définitions (anneau commutatif, anneau intègre)

On dit que l'anneau $(A, +, 0, *, e)$ est :

- commutatif si $*$ est commutative ;
- intègre si

$$(\forall x, y \in A) \qquad x * y = 0 \implies (x = 0 \text{ ou } y = 0)$$

Exemple : $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre $(2 \cdot 3 = 0)$.

Remarque : Tous les anneaux concrets rencontrés dans ce cours sont commutatifs.

le groupe des inversibles A^*

Soit un anneau $(A, +, 0, *, e)$.

Définition-proposition (groupe des éléments inversibles)

On dit que l'élément $x \in A$ est inversible s'il admet un symétrique pour la loi $*$, i.e. s'il existe $x' \in A$ tel que

$$x * x' = x' * x = e$$

S'il existe, un tel x' est unique ; on l'appelle l'inverse de x et on le note x^{-1}.
L'ensemble des éléments inversibles de A se note A^*.
$(A^*, *, e)$ est un groupe.

Exercices :

1. $(x * x' = e \text{ et } x'' * x = e) \Longrightarrow x' = x''$
2. $A^* = A \setminus \{0\} \iff A$ est un corps.
3. $\mathbb{Z}^* = \{-1; 1\}$
4. $(\mathbb{Z}/6\mathbb{Z})^* = \{1; 5\}$

Notation

Soit un anneau $(A, +, 0, *, e)$.
$(\forall x \in A)(\forall n \in \mathbb{Z})$

$$nx \overset{\text{notation}}{=} \begin{cases} 0 & \text{si} \quad n = 0 \\ \underbrace{x + \cdots + x}_{n \text{ fois}} & \text{si} \quad n > 0 \qquad (\text{récurrence}) \\ -\underbrace{(x + \cdots + x)}_{|n| \text{ fois}} & \text{si} \quad n < 0 \quad (\text{récurrence sur } |n|) \end{cases}$$

$$x^n \overset{\text{notation}}{=} \begin{cases} e & \text{si} \quad n = 0 \\ \underbrace{x * \cdots * x}_{n \text{ fois}} & \text{si} \quad n > 0 \\ \underbrace{(x^{-1} * \cdots * x^{-1})}_{|n| \text{ fois}} & \text{si} \quad n < 0 \quad \text{et SEULEMENT si } x \in A^* \end{cases}$$

binôme de Newton

formule du binôme de Newton dans un anneau commutatif

$$(\forall x, y \in A)(\forall n \in \mathbb{N}) \qquad \boxed{(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k * y^{n-k}}$$

$$\text{où : } \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Démonstration : par récurrence sur n (exercice). □

2. Morphismes, A-algèbre, caractéristique

Soient 2 anneaux $(A, +, 0, *, e)$ et $(A', +', 0', *', e')$.

Définition (morphisme d'anneau)

Une application $f : A \to A'$ est un morphisme d'anneau si

(i) $(\forall x_1, x_2 \in A) \qquad f(x_1 + x_2) = f(x_1) +' f(x_2)$

(ii) $f(e) = e'$

(iii) $(\forall x_1, x_2 \in A) \qquad f(x_1 * x_2) = f(x_1) *' f(x_2)$

Remarque :
La condition (ii) ne se déduit pas des deux autres ; considérer par exemple

$$\begin{array}{rcl} f : \mathbb{Z} & \longrightarrow & \mathbb{Z} \times \mathbb{Z} \\ x & \longmapsto & (x, 0) \end{array}$$

Dans ce cours, on se limite au morphisme d'anneau unitaire.

A-algèbre, extension d'anneau, extension de corps

Soit un anneau $(A, +, 0, *, e)$.

Définitions (A-algèbre, extensions)

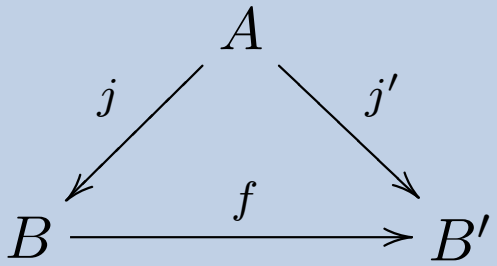
1. Une A-algèbre est un couple (B, j) où B est un anneau et $j : A \to B$ est un morphisme d'anneau.
2. Si de plus j est injective, on dit que (B, j) est une extension d'anneau, et on note :
$$A \overset{j}{\hookrightarrow} B$$
3. Si de plus A et B sont des corps, on parle d'extension de corps.

Morphisme de A-algèbre

Soit un anneau $(A, +, 0, *, e)$.

Définition (morphisme de A-algèbre)

Soient (B, j) et (B', j') deux A-algèbres. Un morphisme de A-algèbre est un morphisme d'anneau $f : B \to B'$ qui rend commutatif ce diagramme :



Caractéristique d'un anneau

Lemme

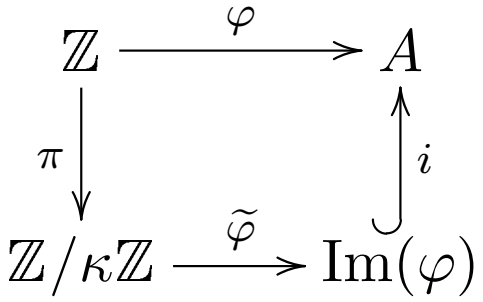
Tout anneau $(A, +, 0, *, e)$ est, de façon unique, une $\mathbb{Z}$-algèbre (A, φ). Tout morphisme d'anneau est un morphisme de $\mathbb{Z}$-algèbre.

Démonstration : c'est la propriété universelle de $\mathbb{Z}$, on doit avoir :
$(\forall n \in \mathbb{Z}) \qquad \varphi(n) = ne.$ □

Définition (caractéristique)

Soit un anneau $(A, +, 0, *, e)$, vu comme $\mathbb{Z}$-algèbre (A, φ). La caractéristique de A, qu'on note $\mathrm{car}(A)$ est l'unique entier $\kappa \in \mathbb{N}$ tel que $\mathrm{Ker}(\varphi) = \kappa\mathbb{Z}$.

$\mathrm{car}(A) = \kappa \iff A$ contient un sous-anneau isomorphe à $\mathbb{Z}/\kappa\mathbb{Z}$



3. Sous-anneau, sous-anneau engendré

Soit un anneau $(A, +, 0, *, e)$.

Définition (sous-anneau)

On dit que $H \subset A$ est un sous-anneau de A si $(H, +, 0, *, e)$, où $+$ et $*$ désignent les restrictions à H des opérations de A, est lui-même un anneau.

Remarque : L'inclusion est alors un morphisme d'anneau $H \overset{i}{\hookrightarrow} A$.

Proposition (caractérisation des sous-anneaux)

$$H \text{ sous-anneau de } A \iff \begin{cases} (i) & (H, +, 0) \text{ sous-groupe de } (A, +, 0) \\ (ii) & e \in H \\ (iii) & (\forall h, h' \in H) \qquad h * h' \in H \end{cases}$$

Démonstration : exercice. □

Sous-anneau, sous-anneau engendré

Exercices :

1. Les anneaux $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ n'ont pas d'autre sous-anneau qu'eux-mêmes.
2. $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$.
3. Soit un anneau $(A, +, 0, *, e)$. Toute intersection de sous-anneaux de A est un sous-anneau de A.

Définition (sous-anneau engendré)

Soit un anneau $(A, +, 0, *, e)$. On appelle sous-anneau de A engendré par une partie $S \subset A$ le plus petit sous-anneau de A contenant S.

C'est l'intersection de tous les sous-anneaux de A qui contiennent S.

Exercices : Soit $f : A \to A'$ un morphisme d'anneau.

1. $H \hookrightarrow A \quad \Longrightarrow \quad f(H) \hookrightarrow A'$
   En particulier, $\mathrm{Im}(f)$ est un sous-anneau de A'.
2. En général, $\mathrm{Ker}(f)$ n'est pas un sous-anneau de A.