Chapitre 2

Anneaux et corps

2.1 Définitions d'anneau, premières propriétés

2.1.1 Définition

Un anneau R est un ensemble muni de 2 lois notées $+$ et $\times$ telles que :

1. $(R,+)$ est un groupe abélien
2. La multiplication $\times$ est associative
3. La multiplication est distributive par rapport à l'addition, c'est à dire :

$$(\forall a \in R)\,(\forall b \in R)\,(\forall c \in R)\,(a \times (b+c)) = a \times b + a \times c \text{ et } (b+c) \times a = b \times a + c \times a$$

4. L'anneau $(R,+,\times)$ est dit unitaire si la multiplication possède un élément neutre (ou unité)
5. L'anneau $(R,+,\times)$ est dit commutatif si la multiplication est commutative

Remarque 1 :

1. Nous utilisons l'addition $+$ et la multiplication $\times$ plutôt que des lois génériques comme $\star$ ou $\perp$, puisque, la plupart du temps, ce sera ce type d'opérations que nous utiliserons
2. Nous considérerons tous les anneaux comme des anneaux unitaires. Par contre, les anneaux ne sont pas forcément commutatifs.
3. Si aucune confusion n'est à craindre, nous noterons 0 le neutre pour l'addition $+$ et 1 l'élément neutre pour la multiplication $\times$
4. On appelle anneau trivial l'anneau réduit à 0, c'est à dire $R = \{0\}$
5. Nous oublierons souvent l'opérateur $\times$ en écrivant $a \times b = ab$
6. Dans un anneau non forcément commutatif, on dit que 2 éléments particuliers $a \in R$ et $b \in R$ sont permutables ou commutables si et seulement si $ab = ba$

2.1.2 Quelques propriétés immédiates des anneaux

Soit $(R,+,\times)$ un anneau unitaire. Alors

1. Pour tout $a \in R$, nous avons $a \times 0 = 0 \times a = 0$
2. Pour tout $a \in R$ et tout $b \in R$, nous avons $(-a) \times b = -(a \times b) = a \times (-b)$
3. Si l'anneau R n'est pas trivial, alors $0 \neq 1$

Démonstration

1. Soit $a \in R$.
   Nous avons alors $a + 0 = a$; en multipliant par a, nous avons $a(a+0) = a^2 \iff a^2 + a \times 0 = a^2$

MATHIEU ANNES©

De la régularité dans le groupe $(R,+)$, nous avons $a\times 0=0$.
Ce que nous voulions

2. Soient $a\in R$, $b\in R$
   D'après la démonstration précédente, nous avons $0=0b$, et donc
   $$0=(a+(-a))\,b=ab+(-a)\,b$$
   On montre ainsi que $(-a)\,b$ est l'opposé de ab, et nous pouvons écrire $-ab=(-a)\,b$
   Nous démontrerions de même que $a\,(-b)=-ab$
3. Soit R un anneau non trivial, c'est à dire qu'il existe $r\in R$ tel que $r\neq 0$
   Supposons que $0=1$ et soit $a\in R$ quelconque. Alors :
   $$a=a\times 1=a\times 0=0$$
   R est donc l'anneau trivial

2.1.3 Définition

Soit $(R,+,\times)$ un anneau unitaire.

1. Si, pour $r\in R$, il existe un élément $s\in R$ tel que $rs=sr=1$, alors r est dit inversible et son inverse s est noté $s=r^{-1}$
2. S'il existe dans $(R,+,\times)$ des éléments $a\in R$ et $b\in R$ tels que $a\neq 0$, $b\neq 0$ et $ab=0$, on dit que a et b sont de véritables diviseurs de zéro
3. On appelle anneau intègre un anneau unitaire commutatif, non trivial et n'admettant pas de diviseurs de zéro.

Exercice 1 :

1. *Soit $(R,+,\times)$ un anneau unitaire. Montrer qu'un véritable de zéro n'est pas inversible dans R*
   Soit $a\in R$, avec $a\neq 0$, un véritable diviseur de zéro. Il existe donc $b\in R$, avec $b\neq 0$ tel que $ab=0$.
   Supposons que a soit inversible. Il existe alors $a^{-1}\in R$ tel que $a\times a^{-1}=a^{-1}\times a=1$. Nous avons donc :
   $$a^{-1}\,(ab)=0\Longleftrightarrow\left(a^{-1}a\right)b=0\Longleftrightarrow 1\times b=0\Longleftrightarrow b=0$$
   Et donc $b=0$; contradiction.
2. *Démontrer que, dans un anneau $(R,+,\times)$, la multiplication est distributive par rapport à la soustraction, c'est à dire*
   $$a\,(c-b)=ac-ab$$
   On peut écrire $a\,(c-b)+ab\overset{\text{Distributivité}}{=}a\,((c-b)+b)=a\,(c-b+b)=ac$.
   Nous avons donc $a\,(c-b)+ab=ac\Longleftrightarrow a\,(c-b)=ac-ab$

Exemple 1 :

Des exemples d'anneaux

1. $(\mathbb{Z},+,\times)$ est un anneau commutatif unitaire. Les éléments inversibles dans $\mathbb{Z}$ sont $+1$ et -1.
2. $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est aussi un anneau commutatif unitaire.
   $\rightarrow$ Dans l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$, l'élément $(n-1)$ est toujours inversible, puisque :
   $$(n-1)\times(n-1)=n^2-2n+1\equiv 1\,[n]$$
   Donc, $(n-1)$ est son propre inverse ; ce qui n'était pas étonnant, puisque $(n-1)\equiv -1\,[n]$, et que $(n-1)^2\equiv(-1)^2\equiv 1\,[n]$

MATHINFO VANNES©

→ Considérons l'anneau $(\mathbb{Z}/6\mathbb{Z},+,\times)$. cet anneau contient de véritables diviseurs de 0 ; par exemple, comme $2\times 3\equiv 0\,[6]$, 2 et 3 sont de véritables diviseurs de zéro dans $(\mathbb{Z}/6\mathbb{Z},+,\times)$

→ A quelle condition un élé ment $a\in\mathbb{Z}/n\mathbb{Z}$ est-il inversible ?

Si a est premier avec n, alors a est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

En effet, d'après l'identité de Bachet-Bezout, a et n étant premiers entre eux, il existe $u\in\mathbb{Z}$ et $v\in\mathbb{Z}$ tels que $au+vn=1\iff au=1-vn$, c'est à dire que $au\equiv 1\,[n]$ et donc $\dot{u}\in\mathbb{Z}/n\mathbb{Z}$ est l'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$

3. $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont trivialement des anneaux.
4. $\mathbb{K}[X]$, ensemble des polynômes à une indéterminée et à coefficients dans $\mathbb{K}$ est un anneau.
5. $\mathcal{M}_n(\mathbb{K})$ muni de l'addition et de la multiplication des matrices est un anneau.

→ Ce n'est pas un anneau intègre ; en effet, si $A=\begin{pmatrix}1&0\\0&0\end{pmatrix}$ et $B=\begin{pmatrix}0&0\\0&1\end{pmatrix}$, A et B sont deux matrices carrées d'ordre 2, non nulles telles que $AB=BA=\mathcal{O}_2$

→ Tous les éléments de $\mathcal{M}_n(\mathbb{K})$ ne sont pas inversibles.

6. On considère l'ensemble $\mathbb{R}^{\mathbb{R}}=\mathcal{F}(\mathbb{R},\mathbb{R})$ des applications de $\mathbb{R}$ dans $\mathbb{R}$. On muni cet ensemble des lois suivantes :

⇒ **L'addition**

Pour tout $f\in\mathcal{F}(\mathbb{R},\mathbb{R})$ et tout $g\in\mathcal{F}(\mathbb{R},\mathbb{R})$, on définit $f+g$ par $(f+g)(x)=f(x)+g(x)$

⇒ **La multiplication**

Pour tout $f\in\mathcal{F}(\mathbb{R},\mathbb{R})$ et tout $g\in\mathcal{F}(\mathbb{R},\mathbb{R})$, on définit $f\times g$ par $(f\times g)(x)=f(x)\times g(x)$

Muni de ces deux lois, $\mathcal{F}(\mathbb{R},\mathbb{R})$ est un anneau commutatif unitaire

⋆ Le neutre pour l'addition est la fonction nulle $\mathcal{O}$ définie par :

$$\begin{cases}\mathcal{O}:\mathbb{R}&\longrightarrow&\mathbb{R}\\ x&\longmapsto&\mathcal{O}(x)=0\end{cases}$$

⋆ L'élément unité pour la multiplication est la fonction 1 définie par :

$$\begin{cases}1:\mathbb{R}&\longrightarrow&\mathbb{R}\\ x&\longmapsto&1(x)=1\end{cases}$$

7. L'anneau $\mathcal{F}(\mathbb{R},\mathbb{R})$ n'est pas un anneau intègre. Si nous définissons 2 fonctions f et g par :

$$\begin{cases}f:\mathbb{R}&\longrightarrow&\mathbb{R}\\ x&\longmapsto&f(x)=\begin{cases}0\text{ si }x<0\\ x^2\text{ si }x\geqslant 0\end{cases}\end{cases}\quad\text{et}\quad\begin{cases}g:\mathbb{R}&\longrightarrow&\mathbb{R}\\ x&\longmapsto&g(x)=\begin{cases}x\text{ si }x<0\\ 0\text{ si }x\geqslant 0\end{cases}\end{cases}$$

Alors, pour tout $x\in\mathbb{R}$, $f(x)\,g(x)=0$, c'est à dire $f\times g=\mathcal{O}$ alors que ni f, ni g ne sont nulles. $\mathcal{F}(\mathbb{R},\mathbb{R})$ n'est donc pas un anneau intègre.

2.1.4 Définition

Soit $(R,+,\times)$ un anneau unitaire.

1. On dit qu'un élément $a\in R$ est nilpotent s'il existe $n\in\mathbb{N}$ tel que $a^n=0$
2. On dit qu'un élément $a\in R$ est idempotent si $a^2=a$

Remarque 2 :

1. Si $a\in R$ est un élément nilpotent, a est un véritable diviseur de 0
2. Si $A\in\mathcal{M}_3(\mathbb{K})$ où $A=\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}$, alors $A^3=\mathcal{O}_3$. A est donc nilpotente d'ordre 3
3. Soit $(R,+,\times)$ un anneau unitaire ; soit $x\in R$ et $n\in\mathbb{N}^*$. Nous définissons nx par :

$$nx=\begin{cases}x+x+\cdots+x\text{ avec }n\text{ termes, si }n\in\mathbb{N}^*\\ 0\text{ si }n=0\\ -((-n)\,x)\text{ si }n\in\mathbb{Z}^-\end{cases}$$

MATHINFOVANNES©

4. Les règles de calcul classiques dans $\mathbb{Z}$, $\mathbb{Q}$,$\mathbb{R}$ ou $\mathbb{C}$ ne sont pas toujours valides puisqu'à priori, un anneau n'est pas forcément commutatif. Nous avons donc :
   - $(a+b)^2 = (a+b)\times(a+b) = a^2+ab+ba+b^2$
   - $(a+b)\times(a-b) = a^2-ab+ba-b^2$
5. Si **l'anneau est commutatif** ou si les éléments $a \in R$ et $b \in R$ commutent, c'est à dire $ab = ba$, nous avons les formules classiques :
   - $(a+b)^2 = (a+b)\times(a+b) = a^2+2ab+b^2$
   - $(a+b)\times(a-b) = a^2-b^2$
6. Si $(R,+,\times)$ est un anneau unitaire de caractéristique p, alors, pour tout $a \in R$, nous avons $pa = 0$. En effet
$$pa = p\times(ea) = (pe)\times a = 0\times a = 0$$

2.1.5 Théorème : la formule du binôme

Soit $(R,+,\times)$ un anneau unitaire ; soient $x \in R$ et $y \in R$, 2 éléments de R qui commutent, c'est à dire que $xy = yx$. Nous avons alors la formule du binôme :

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

Démonstration

La démonstration est très semblable à celle qui a été faite dans le cours de L_0

Exercice 2 :

Nous avons démontré, en L_0, que, si p est un nombre premier, alors, pour tout $q \in \mathbb{N}$ tel que $1 \leqslant q \leqslant p-1$, $C_p^q = \binom{p}{q}$ est divisible par p, c'est à dire qu'il existe $k_q \in \mathbb{N}$ tel que $C_p^q = \binom{p}{q} = k_q p$

1. Soit $(R,+,\times)$ un anneau commutatif de caractéristique p où p est un nombre premier. Démontrer que $(a+b)^p = a^p + b^p$
2. En déduire que $(a-b)^p = a^p - b^p$
3. Pour $a_1, a_2, \cdots, a_k$ k éléments de l'anneau R. Montrer que
$$(a_1+a_2+\cdots+a_k)^p = (a_1)^p + (a_2)^p + \cdots + (a_k)^p$$
4. p est toujours un nombre premier et $k \in \mathbb{N}$ quelqconque. Démontrer que $k^p \equiv k\,[p]$

Exercice 3 :

Soit $(R,+,\times)$ un anneau unitaire. Soient $a \in R$ et $b \in R$ tels que $ab+ba = 1$ et $a^2b+ba^2 = a$

1. Montrer que $a^2b = ba^2$ et que $2aba = a$
2. Etablir que a est inversible que son inverse est $2b$, c'est à dire $a^{-1} = 2b$

Exercice 4 :

Soit $(R,+,\times)$ un anneau unitaire.
On suppose que, pour tout $x \in R$ et tout $y \in R$, nous avons $(xy)^2 = x^2y^2$

1. Démontrer que, pour tout $x \in R$ et tout $y \in R$, nous avons $xyx = x^2y = yx^2$
2. En déduire que l'anneau R est commutatif

MATHINFOVANNES©

Exercice 5 :

Soit $(R, +, \times)$ un anneau unitaire.
Soit $a \in R$ un élément de R tel qu'il existe $b \in R$ tel que $ab = 1$

1. Démontrer que, si pour tout $x \in R$ et tout $y \in R$ nous avons $ax = ay$, alors $x = y$ *(On dit que a est régulier à gauche)*
2. Démontrer que a est un élément inversible de R et que $b = a^{-1}$

Exercice 6 :

Soit $(R, +, \times)$ un anneau unitaire. Nous appelons $\mathcal{U} \subset R$ l'ensemble des éléments inversibles de R.
Il faut démontrer que $(\mathcal{U}, \times)$ est un groupe.

Exercice 7 :

Montrer qu'un anneau $(R, +, \times)$ n'a pas de diviseurs de zéro si, et seulement si, tous ses éléments non nuls sont réguliers

Exercice 8 :

Soient a et b deux éléments d'un anneau $(R, +, \times)$ tels que ab soit inversible et b non diviseur de 0.
Montrer que a et b sont inversibles.

2.1.6 Définition de sous-anneau

Soit $(R, +, \times)$ un anneau.
On appelle sous-anneau d'un anneau R toute partie non vide $A \subset R$, non vide stable pour les lois $+$ et $\times$ et telle que la structure induite sur A par ces lois $+$ et $\times$ soit une structure d'anneau

Remarque 3 :

1. Ce qui veut donc dire que $(A, +, \times)$ un anneau et que, donc $(A, +)$ est un sous-groupe additif du groupe abélien additif $(R, +)$
2. A est donc aussi une partie stable pour la multiplication
3. La multiplication étant associative et distributive par rapport à l'addition sur R, elle l'est aussi sur A

2.1.7 Théorème

Soit $(R, +, \times)$ un anneau.
Pour qu'une partie non vide $A \subset R$ soit un sous-anneau de R, il faut et il suffit que :

$$(\forall x \in A)\,(\forall y \in A)\,((x - y \in A) \text{ et } (x \times y \in A))$$

Démonstration

La démonstration est simple et laissée au lecteur. La majorité des arguments est dans la remarque précédente.

Remarque 4 :

Si l'anneau R est commutatif et intègre, il en est de même du sous anneau $A \subset R$. Par contre, l'anneau R peut être unitaire sans que A ne le soit.

2.1.8 Théorème

Les seuls sous anneaux de l'anneau $(\mathbb{Z}, +, \times)$ sont les sous-ensembles de type $n\mathbb{Z}$ où $n \in \mathbb{N}^*$

MATHINFOVANNES©

Démonstration

1. Tout d'abord, les seuls sous-groupes additifs de $\mathbb{Z}$ sont du type $n\mathbb{Z}$ avec $n \in \mathbb{N}^*$. Les sous-anneaux sont donc, au mieux, des ensembles du type $n\mathbb{Z}$
2. Ensuite, ces ensembles du type $n\mathbb{Z}$, avec $n \in \mathbb{N}^*$, sont-ils stables pour la multiplication ?

   Soit donc $x \in n\mathbb{Z}$ et $y \in n\mathbb{Z}$.
   Il existe donc $k_1 \in \mathbb{Z}$ et $k_2 \in \mathbb{Z}$ tels que $x = k_1 n$ et $y = k_2 n$.
   Alors, $xy = k_1 k_2 n^2 = (k_1 k_2 n)\, n$, ce qui met en évidence que xy est un multiple de n et que, donc, $xy \in n\mathbb{Z}$

Remarque 5 :

Un sous-anneau n'hérite pas forcément de toutes les propriétés de l'anneau.
Ici, nous avons comme exemple que si $(\mathbb{Z}, +, \times)$ est un anneau unitaire, $(n\mathbb{Z}, +, \times)$ ne l'est pas, puisque jamais $1 \in n\mathbb{Z}$

Exemple 2 :

1. Premier exemple simple de sous-anneau : $(\mathbb{Z}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$
2. Considérons l'anneau unitaire $(\mathbb{Z}/6\mathbb{Z}, +, \times)$. Quel sont ses sous-anneaux ?
   Ce sont d'abord des sous groupes additifs de $(\mathbb{Z}/6\mathbb{Z}, +)$, et, d'après le théorème de Lagrange, l'ordre de ces sous-groupes doit diviser l'ordre du groupe. Les sous-groupes auront donc pour cardinal 1,2 et 3
   - ⋆ Sous-anneau à un seul élément $A_1 = \{\dot{0}\}$
   - ⋆ Sous-anneau à 2 éléments $A_2 = \{\dot{0}, \dot{3}\}$
   - ⋆ Sous-anneau à 3 éléments $A_3 = \{\dot{0}, \dot{2}, \dot{4}\}$

Exercice 9 :

Dans l'anneau $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$ des applications de $\mathbb{R}$ dans $\mathbb{R}$, on considère l'ensemble A_{x_0} des fonctions $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ telles que $f(x_0) = 0$. Il faut démontrer que $(A_{x_0}, +, \times)$ est un sous-anneau de $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$

Exercice 10 :

Soit $(R, +, \times)$ un anneau et nous considérons $Z(R)$, le centre de R, c'est à dire :

$$Z(R) = \{u \in R \text{ tels que, pour tout } x \in R \text{ nous avons } ux = xu\}$$

Il faut démontrer que $(Z(R), +, \times)$ est un sous-anneau de $(R, +, \times)$

Exercice 11 :

Soit $(R, +, \times)$ un anneau et $a \in R$. Nous considérons le sous-ensemble $A(a)$ défini par :

$$A(a) = \{x \in R \text{ tels que nous avons } ax = xa\}$$

Il faut démontrer que $(A(a), +, \times)$ est un sous-anneau de $(R, +, \times)$

Exercice 12 :

Soit $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{Q}$
Nous notons $\mathbb{Z}\left[\sqrt{d}\right] = \left\{x = a + b\sqrt{d} \text{ où } a \in \mathbb{Z} \text{ et } b \in \mathbb{Z}\right\}$.
Il faut montrer que $\mathbb{Z}\left[\sqrt{d}\right]$ est un sous-anneau de $(\mathbb{R}, +, \times)$

MATHINFOVANNES©

Exercice 13 :

On pose $r = \sqrt[3]{2}$ et $A = \left\{x \in \mathbb{R} \text{ où } x = m + nr + pr^2 \text{ avec } m \in \mathbb{Z}, n \in \mathbb{Z}, p \in \mathbb{Z}\right\}$.
Il faut démontrer que $(A, +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$

Exercice 14 :

Soit $A = \left\{\dfrac{m}{2n+1} \text{ avec } m \in \mathbb{Z} \text{ et } n \in \mathbb{N}\right\}$

1. Démontrer que A est un sous-anneau de $(\mathbb{Q}, +, \times)$
2. Quels sont les éléments inversibles de A ?

Exercice 15 :

Soit $A = \left\{\dfrac{m}{2^n} \text{ avec } m \in \mathbb{Z} \text{ et } n \in \mathbb{N}\right\}$

1. Démontrer que A est un sous-anneau de $(\mathbb{Q}, +, \times)$
2. Quels sont les éléments inversibles de A ?

MATHINFOVANNES©