2.2 Idéal et homomorphismes d'anneaux

2.2.1 Définition d'idéal

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

1. On appelle idéal à gauche de R, un sous-groupe additif I_g de R tel que
$$(\forall x \in R)\,(\forall a \in I_g)\,(xa \in I_g)$$
2. On appelle idéal à droite de R, un sous-groupe additif I_d de R tel que
$$(\forall x \in R)\,(\forall a \in I_d)\,(ax \in I_d)$$
3. On appelle idéal bilatère un sous-groupe additif I qui est à la fois un idéal à gauche et un idéal à droite

Remarque 6 :

1. Naturellement, dans un anneau commutatif $(R, +, \times)$, les notions d'idéal à gauche, d'idéal à droite ou d'idéal bilatère se confondent. On parle alors seulement **d'idéal** de R
2. Evidemment, un idéal de R est un sous-anneau de R

Exemple 3 :

1. L'exemple le plus simple *(et le plus parlant)* se situe dans $(\mathbb{Z}, +, \times)$: les ensembles $n\mathbb{Z}$ sont des idéaux bilatères de $\mathbb{Z}$.

   En effet, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$
   De plus, si $u \in n\mathbb{Z}$, alors, pour tout $a \in \mathbb{Z}$, $au \in n\mathbb{Z}$. En effet, il existe $k \in \mathbb{Z}$ tel que $u = nk$, et donc $au = ank = akn$; ainsi $au \in n\mathbb{Z}$
2. L'intersection de 2 idéaux *(à gauche ou à droite)* de R est encore un idéal de R
3. Soient I_1 et I_2 2 idéaux de R *(à gauche ou à droite)*. Nous définissons l'ensemble
$$I_1 + I_2 = \{i_1 + i_2 \text{ où } i_1 \in I_1 \text{ et } i_2 \in I_2\}$$
   Alors, $I_1 + I_2$ est aussi un idéal contenant I_1 et I_2
4. Si $(R, +, \times)$ est un anneau, alors $\{0\}$ et R sont aussi des idéaux ; nous les appelons les **idéaux triviaux**

2.2.2 Définition d'idéal et d'anneau principal

Soit $(R, +, \times)$ un anneau commutatif
Soit $a \in R$ et $aR = \{y \in R \text{ tel qu'il existe } r \in R \text{ tel que } y = ar\}$

1. aR est l'ensemble des multiples de a et c'est un idéal de R. Tout idéal de ce type est appelé idéal principal
2. On appelle anneau principal un anneau $(R, +, \times)$ commutatif dans lequel tout idéal est principal

Remarque 7 :

Il est facile de démontrer que aR est un idéal de R

1. On démontre que $(aR, +)$ est un sous-groupe de $(R, +)$
   - ⋆ Tout d'abord $aR \neq \emptyset$ puisque $0 \in aR$; en effet, $0 = a \times 0 = 0 \times 0$
   - ⋆ Ensuite, soient $x \in aR$ et $y \in aR$; alors $x = ar_1$ et $y = ar_2$ avec $r_1 \in R$ et $r_2 \in R$. Et donc :
$$x - y = ar_1 - ar_2 = a\,(r_1 - r_2)$$
     De $r_1 - r_2 \in R$, nous avons $a\,(r_1 - r_2) \in aR$, c'est à dire $x - y \in aR$

De là, nous déduisons que $(aR,+)$ est un sous-groupe de $(R,+)$

2. D'autre part, soit $x \in R$ et $z \in aR$. Alors :

$$xz = x\,(ar) = (xa)\,r = a\,(xr)$$

Comme $xr \in R$ nous avons $a\,(xr) \in aR$, c'est à dire $xz \in aR$

En conclusion aR est un idéal de R

Exemple 4 :

1. Un exemple d'idéal principal est l'idéal $n\mathbb{Z}$ avec $n \in \mathbb{N}^*$. Ce sont d'ailleurs les seuls types d'idéal de l'anneau $(\mathbb{Z},+,\times)$ des entiers relatifs
2. $(\mathbb{Z},+,\times)$ est donc un anneau principal.

2.2.3 Définition

Soit $(R,+,\times)$ un anneau
Une relation d'équivalence $\mathcal{R}$ définie sur un anneau R est dite compatible avec la structure d'anneau de R si et seulement si

1. Pour tout $x \in R$ nous avons l'implication $a\mathcal{R}b \Longrightarrow (a+x)\,\mathcal{R}\,(b+x)$
2. Pour tout $x \in R$ nous avons les implications $a\mathcal{R}b \Longrightarrow (a\times x)\,\mathcal{R}\,(b\times x)$ et $a\mathcal{R}b \Longrightarrow (x\times a)\,\mathcal{R}\,(x\times b)$

2.2.4 Proposition

Soit $(R,+,\times)$ un anneau et $\mathcal{R}$ une relation d'équivalence définie sur R compatible avec la structure d'anneau de R
Alors, $\dot{0}$ est un idéal bilatère de R

Démonstration

1. Il faut d'abord démontrer que $(\dot{0},+)$ est un sous-groupe du groupe $(R,+)$
   - ⋆ Tout d'abord $\dot{0} \neq \emptyset$ puisque $0 \in \dot{0}$
   - ⋆ Ensuite, soient $x \in \dot{0}$ et $y \in \dot{0}$. Alors $x\mathcal{R}0$ et $y\mathcal{R}0$ et donc $x\mathcal{R}y$.
     Comme $\mathcal{R}$ est compatible avec la structure d'anneau de R, nous avons $(x-y)\,\mathcal{R}\,(y-y) \Longleftrightarrow (x-y)\,\mathcal{R}0$, c'est à dire $x-y \in \dot{0}$

   Donc, $(\dot{0},+)$ est un sous-groupe du groupe $(R,+)$
2. Soit $x \in R$, avons nous pour tout $a \in \dot{0}$, $ax \in \dot{0}$ et $xa \in \dot{0}$?

   Soit $a \in \dot{0}$ alors $a\mathcal{R}0$ et donc par compatibilité de la relation $\mathcal{R}$ avec la structure d'anneau, nous avons $xa\mathcal{R}0$ et $ax\mathcal{R}0$, c'est à dire $xa \in \dot{0}$ et $ax \in \dot{0}$

$\dot{0}$ est donc un idéal bilatère de R

2.2.5 Corollaire

Soit $(R,+,\times)$ un anneau
$\mathcal{R}$ est une relation d'équivalence définie sur R compatible avec la structure d'anneau de R si et seulement si $\mathcal{R}$ est de la forme $x\mathcal{R}y \Longleftrightarrow x-y \in I$ où I est un idéal bilatère de R

Démonstration

La démonstration est simple et laissée au lecteur. Nous remarquerons que $I = \dot{0}$

2.2.6 Proposition

Soit $(R, +, \times)$ un anneau et $I \subset R$, un idéal bilatère de R.
Soit $\mathcal{R}$, la relation d'équivalence liée à I, c'est à dire celle définie par :

$$(\forall x \in R)\,(\forall y \in R)\,((x\mathcal{R}y) \iff (x - y \in I))$$

L'ensemble quotient de cette relation d'équivalence est noté R/I et nous définissons sur cet ensemble quotient les opétations suivants :

$$\dot{x} + \dot{y} = \overset{\bullet}{\widehat{x+y}} \text{ et } \dot{x} \times \dot{y} = \overset{\bullet}{\widehat{x \times y}}$$

Muni de ces 2 opérations, A/I est un anneau ; c'est l'anneau quotient de R par I

Démonstration

→ Il est connu, et démontré que $\mathcal{R}$ est une relation d'équivalence.
→ En considérant $(R, +)$ comme un groupe commutatif et $(I, +)$ comme un sous-groupe de $(R, +)$, nous avons vu, dans la théorie des groupes, que $(R/I, +)$ est un groupe.
→ Il faut, maintenant, montrer l'associativité de la multiplication, et la distributivité de la multiplication par rapport à l'addition
- ⋆ Associativité de la multiplication
  Soient $\dot{x} \in R/I$, $\dot{y} \in R/I$ et $\dot{z} \in R/I$ 3 éléments de R/I. Alors :

$$\dot{x}\,(\dot{y}\dot{z}) = \dot{x}\left(\overset{\bullet}{\widehat{y \times z}}\right) = \overset{\bullet}{\widehat{x \times y \times z}} = \left(\overset{\bullet}{\widehat{x \times y}}\right)\dot{z} = (\dot{x}\dot{y})\,\dot{z}$$

- ⋆ Distributivité de la multiplication par rapport à l'addition
  Soient $\dot{x} \in R/I$, $\dot{y} \in R/I$ et $\dot{z} \in R/I$ 3 éléments de R/I. Alors :

$$\dot{x}\,(\dot{y} + \dot{z}) = \dot{x}\left(\overset{\bullet}{\widehat{y+z}}\right) = \overset{\bullet}{\widehat{x\,(y+z)}} = \overset{\bullet}{\widehat{x \times y + x \times z}} = \overset{\bullet}{\widehat{x \times y}} + \overset{\bullet}{\widehat{x \times z}} = \dot{x}\dot{y} + \dot{x}\dot{z}$$

2.2.7 Définition d'homomorphisme d'anneaux

Soient $(R, +, \times)$ et $(R_1, +_1, \times_1)$ 2 anneaux
$f : R \longrightarrow R_1$ est un homomorphisme d'anneaux si et seulement si

$$(\forall x \in R)\,(\forall y \in R)\,((f(x+y) = f(x) +_1 f(y)) \text{ et } f(x \times y) = f(x) \times_1 f(y))$$

1. Si $f : R \longrightarrow R_1$ est un homomorphisme d'anneaux bijectif, alors f est appelé isomorphisme
2. Un homomorphisme $f : R \longrightarrow R$ de R dans lui même est un endomorphisme
3. Un homomorphisme $f : R \longrightarrow R$ de R dans lui même bijectif est un automorphisme

Exemple 5 :

Un premier exemple d'homomorphisme d'anneau est la projection canonique sur un anneau-quotient :

$$\left\{\begin{array}{rcl} p : R & \longrightarrow & R/I \\ x & \longmapsto & p(x) = \dot{x} \end{array}\right.$$

Remarque 8 :

1. $f : R \longrightarrow R_1$, homomorphisme d'anneaux est aussi un homomorphisme du groupe $(R, +)$ vers le groupe $(R_1, +_1)$. f hérite donc de toutes les propriétés d'homomorphisme de groupe additif. Ainsi $f(0_R) = 0_{R_1}$ et $f(-x) = -f(x)$
2. Il est facile à démontrer que la composée de 2 homomorphismes d'anneaux est un homomorphisme d'anneaux

2.2.8 Théorème

Soit $f : R \longrightarrow R_1$ est un homomorphisme d'anneaux. Alors

1. $f(0_R) = 0_{R_1}$ et $f(-x) = -f(x)$
2. $f(R)$ est un sous-anneau de R_1
3. $\ker f = f^{-1}(\{0_{R_1}\})$ est un idéal bilatère de R ; c'est donc le noyau de f

Démonstration

Nous ne démontrons pas tout. nous allons réutiliser les résultats liés aux homomorphismes de groupe.

1. **Montrons que $f(R)$ est un sous-anneau de R_1**

   $\rightarrow$ D'après les résultats sur les homomorphismes de groupe, $(f(R), +_1)$ est un sous-groupe de $(R_1, +_1)$

   $\rightarrow$ Il faut maintenant montrer que si $a \in f(R)$ et si $b \in f(R)$ alors $ab \in f(R)$.
   Soient donc $a \in f(R)$ et $b \in f(R)$; il existe alors $x \in R$ tel que $a = f(x)$ et $y \in R$ tel que $b = f(y)$. Alors :
   $$ab = f(x) \times f(y) = f(xy)$$
   Et donc $ab \in f(R)$ puisqu'il existe $z = xy \in R$ tel que $ab = f(xy)$

   $f(R)$ est donc bien un sous-anneau de R_1

2. **$\ker f = f^{-1}(\{0_{R_1}\})$ est un idéal bilatère de R**

   $\rightarrow$ D'après la théorie des groupes, nous savons que $(\ker f, +)$ est un sous-groupe de $(R, +)$

   $\rightarrow$ Soient $y \in \ker f$ et $x \in R$; il faut montrer que $xy \in \ker f$ et $yx \in \ker f$; alors
   $$f(xy) = f(x) \times f(y) = f(x) \times 0_{R_1} = 0_{R_1}$$
   Et donc $xy \in \ker f$. Nous démontrerions de même que $yx \in \ker f$

   $\ker f = f^{-1}(\{0_{R_1}\})$ est donc un idéal bilatère de R

2.2.9 Corollaire

Soit $f : R \longrightarrow R_1$ est un homomorphisme d'anneaux. Alors f est injective si et seulement si $\ker f = \{0_R\}$

Exercice 16 :

Soient $(R, +, \times)$ et $(R_1, +_1, \times_1)$ 2 anneaux et $f : R \longrightarrow R_1$ un homomorphisme d'anneaux.

1. Démontrer que si $(R, +, \times)$ est un anneau commutatif, alors $f(R)$ l'est aussi
2. Démontrer que si $(R, +, \times)$ est un anneau unitaire d'unité 1_R, alors $f(1_R)$ est l'unité de $f(R)$
3. Démontrer que si $x \in R$ est un élément inversible, alors $f(x)$ est aussi inversible dans $f(R)$ et $f(x^{-1}) = (f(x))^{-1}$

2.2.10 Théorème

Soit $f : R \longrightarrow R_1$ est un isomorphisme d'anneaux. Alors $f^{-1} : R_1 \longrightarrow R$ est aussi un isomorphisme d'anneaux. On dit que les anneaux R et R_1 sont isomorphes

Démonstration

Soit $f : R \longrightarrow R_1$ est un isomorphisme d'anneaux.

$\Rightarrow$ Tout d'abord, $f : (R, +) \longrightarrow (R_1, +_1)$ est aussi un isomorphisme de groupe, et donc, d'après la théorie des groupes, $f^{-1} : (R_1, +_1) \longrightarrow (R, +)$ est aussi un isomorphisme de groupe

⇒ Il faut maintenant montrer que c'est un isomorphisme d'anneaux, c'est à dire que, pour tout $x \in R_1$ et tout $y \in R_1$, $f^{-1}(xy) = f^{-1}(x) \times f^{-1}(y)$
Soient donc $x \in R_1$ et $y \in R_1$. de l'isomorphisme qu'est f, on peut déduire qu'il existe $u \in R$ et $v \in R$ tels que $f(u) = x$ et $f(v) = y$, ou, ce qui est équivalent, $f^{-1}(x) = u$ et $f^{-1}(y) = v$. Alors :

$$f^{-1}(xy) = f^{-1}(f(u)f(v)) = f^{-1}(f(uv)) = f^{-1} \circ f(uv) = uv = f^{-1}(x) \times f^{-1}(y)$$

Nous avons donc $f^{-1}(xy) = f^{-1}(x) \times f^{-1}(y)$

Ce qui termine de montrer que f^{-1} est un isomorphisme d'anneaux.

Remarque 9 :

Comme dans la théorie des groupes, nous pouvons décomposer canoniquement un homomorphisme d'anneaux.
Si $f : R \longrightarrow R_1$ est un homomorphisme d'anneaux, $\ker f$ est un idéal bilatère, et la relation $\mathcal{S}$ définie par :

$$x\mathcal{S}y \Longleftrightarrow f(x) = f(y) \Longleftrightarrow f(x-y) = 0_{R_1} \Longleftrightarrow x - y \in \ker f$$

est une relation d'équivalence. D'où la proposition qui suit, en tout point semblable à la proposition 1.3.4

2.2.11 Décomposition canonique d'un morphisme $f : G \longrightarrow G'$

Soient $(R, +, \times)$ et $(R_1, +_1, \times_1)$ deux anneaux. Soit $f : R \longrightarrow R_1$ un homomorphisme d'anneaux.
Alors, $f : R \longrightarrow R_1$ se décompose de manière canonique en $f = i \circ \overline{f} \circ \varphi$ où :

- → φ est la projection canonique $\varphi : R \longrightarrow R/\ker f$
- → $\overline{f}$ est l'isomorphisme $\overline{f} : R/\ker f \longrightarrow f(R)$
- → Et $i : f(R) \longrightarrow R_1$ est l'application d'insertion (ou injection canonique

Nous obtenons alors le diagramme suivant :

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\varphi"'] & R_1 \\ R/\ker f \arrow[r, "\overline{f}"'] & f(R) \arrow[u, "i"'] \end{tikzcd}$$

Exercice 17 :

On considère $(R, +, \times)$ un anneau unitaire et $a \in R$, un élément inversible. Démontrer que l'application $f : R \longrightarrow R$ définie par :

$$\begin{cases} f : R & \longrightarrow & R \\ \quad x & \longmapsto & f(x) = axa^{-1} \end{cases}$$

est un automorphisme d'anneau.

2.2.12 Théorème et définition

Soit $(R, +, \times)$ un anneau unitaire d'unité e. Soit $f : \mathbb{Z} \longrightarrow R$ une application définie par :

$$\begin{cases} f : \mathbb{Z} & \longrightarrow & R \\ \quad n & \longmapsto & f(n) = ne = \underbrace{e + e + \cdots + e + e}_{n \text{ fois}} \end{cases}$$

Alors

1. f est un homomorphisme d'anneaux
2. Si f est injective, c'est à dire si $\ker f = \{0\}$, alors le seul entier $p \in \mathbb{Z}$ tel que $f(p) = 0$ est $p = 0$ et $f(\mathbb{Z})$ est isomorphe à $\mathbb{Z}$. On dit alors que <u>R est de caractéristique nulle</u>
3. Si l'application f n'est pas injective, alors, il existe un plus petit entier $p > 0$ tel que $f(p) = pe = 0_R$ et $f(\mathbb{Z})$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On dit alors que <u>R est de caractéristique p</u>

Démonstration

1. f est un homomorphisme d'anneaux
   R est anneau unitaire d'unité e. Considérons le sous-groupe additif A' monogène engendré par e et l'application $f : \mathbb{Z} \longrightarrow A'$ définie par, pour $n \in \mathbb{Z}$, par $f(n) = ne$. Les règles de calculs dans un groupe additif montrent que pour tout $m \in \mathbb{Z}$ et tout $n \in \mathbb{Z}$:
   $$f(m+n) = (m+n)e = me + ne = f(m) + f(n)$$
   Et
   $$f(mn) = (mn)e = m(ne) = (me)(ne) = f(m) f(n)$$
   f est donc un homomorphisme d'anneau. $f : \mathbb{Z} \longrightarrow A'$ est surjective
2. En utilisant le schéma
   $$\begin{tikzcd} \mathbb{Z} \arrow[r, "f"] \arrow[d, "\varphi"'] & R \\ \mathbb{Z}/\ker f \arrow[r, "\overline{f}"'] & f(\mathbb{Z}) = A' \arrow[u, "i"'] \end{tikzcd}$$
   Nous voyons que :
   ⋆ Si f est injective, alors $A' = f(\mathbb{Z})$ est un anneau isomorphe à $\mathbb{Z}$
   ⋆ Si f n'est pas injective, alors $\ker f$ est du type $p\mathbb{Z}$ où $p > 0$, et donc $A' = f(\mathbb{Z})$ est un anneau isomorphe à $\mathbb{Z}/p\mathbb{Z}$

Remarque 10 :

Remarquons que si $(R, +, \times)$ un anneau unitaire d'unité e et de caractéristique $p > 0$, alors, pour tout $a \in R$, nous avons $pa = 0$

En effet, $pa = p(ea) = (pe)a = 0 \times a = 0$

2.2.13 Exercices

Exercice 18 :

Soit $f : \mathbb{C} \longrightarrow \mathbb{C}$ un morphisme d'anneaux tel que pour tout $x \in \mathbb{R}$, $f(x) = x$. Montrer que f est l'identité ou la conjugaison complexe.

Exercice 19 :

Soit $a \in \mathbb{R}$ un réel et on appelle $\mathcal{F}(\mathbb{R}, \mathbb{R})$ l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$. Nous appelons Ev_a l'application suivante :
$$\left\{ \begin{array}{rcl} Ev_a : \mathcal{F}(\mathbb{R}, \mathbb{R}) & \longrightarrow & \mathbb{R} \\ f & \longmapsto & Ev_a(f) = f(a) \end{array} \right.$$
Montrer l'application Ev_a est un morphisme d'anneaux.

Exercice 20 :

On note $\mathbb{D} = \left\{ \dfrac{m}{10^n} \text{ avec } m \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$ l'ensemble des nombres décimaux

1. Montrer que $\mathbb{D}$ est un sous-anneau de $(\mathbb{Q}, + \times)$
2. Montrer que les idéaux de $\mathbb{D}$ sont principaux *(c'est-à-dire de la forme $a \times \mathbb{D}$ avec $a \in \mathbb{D}$)*

Exercice 21 :

Nilradical d'un anneau
On appelle nilradical d'un anneau commutatif $(R, +, \times)$, l'ensemble N formé des éléments nilpotents de R, c'est à dire des $x \in R$ tels qu'il existe $n \in \mathbb{N}$ vérifiant $x^n = 0_R$. Montrer que N est un idéal de R

Exercice 22 :

Soient $(R, +, \times)$ un anneau commutatif et $a \in R$ un élément idempotent de R, c'est à dire tel que $a^2 = a$.

1. Montrer que $J = \{x \in R \text{ tel que } ax = 0\}$ est un idéal de R.
2. On note $I = aR$ l'idéal principal de R engendré par a. Déterminer $I + J$ et $I \cap J$.
3. Établir que pour tout idéal K de R : $(K \cap I) + (K \cap J) = K$.