Anneaux

Ring

Ring

”Un Anneau pour les gouverner tous,
Un Anneau pour les trouver,
Un Anneau pour les amener tous,
Et dans les ténèbres les lier”

Three rings for the Elven-kings under the sky,
$\mathbf{B}_{\mathrm{cris}}$, $\mathbf{B}_{\mathrm{st}}$, $\mathbf{B}_{\mathrm{dR}}$,
Seven for the Dwarf-lords in their halls of stone,
$\mathbf{E}_{\mathbf{Q}_p}$, $\mathbf{A}_{\mathbf{Q}_p}$, $\mathbf{B}_{\mathbf{Q}_p}$, $\mathbf{E}$, $\mathbf{A}$, $\mathbf{B}$, $\widetilde{\mathbf{A}}$,
Nine for mortal Men doomed to die,
$\mathbf{Q}_p$, $\mathbf{Z}_p$, $\mathbf{F}_p$, $\overline{\mathbf{Q}}_p$, $\overline{\mathbf{F}}_p$, $\mathbf{C}_p$, $\mathscr{O}_{\mathbf{C}_p}$, $\mathbf{Q}_p^{\mathrm{nr}}$, $\mathbf{B}_{\mathrm{HT}}$,
One ring to rule them all,
$\mathbf{A}_{\mathrm{inf}}$.

Pierre Colmez

DÉFINITION 3.1. *Un anneau $(A, +, ., 0_A, 1_A)$ est la donnee, d'un groupe commutatif $(A, +)$ (note additivement) d'element neutre note 0_A, d'une loi de composition interne (dite de multiplication)*

$$\bullet.\bullet : \begin{array}{ccc} A \times A & \mapsto & A \\ (a, b) & \mapsto & a.b \end{array}$$

et d'un element unite $1_A \in A$ ayant les proprietes suivantes

(1) Associativite de la multiplication:

$$\forall a, b, c \in A,\ (a.b).c = a.(b.c) = a.b.c.$$

(exemple $a.b \neq b.a$)

(2) distributivite:

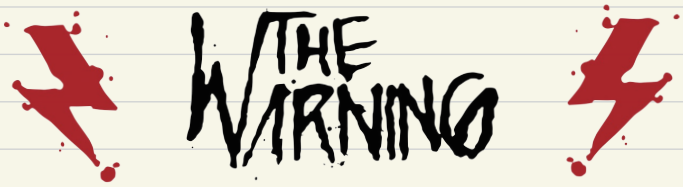
$$\forall a, b, c \in A,\ (a + b).c = a.c + b.c,\ c.(a + b) = c.a + c.b.$$

(3) Neutralite de l'unite:

$$\forall a \in A,\ a.1_A = 1_A.a = a.$$

Un anneau est dit commutatif si de plus la multiplication est commutative:

$$\forall a, b \in A,\ a.b = b.a.$$



$(A, \cdot, 1_A)$ n'est pas un gp en general.

Exemples : $(\mathbb{Z}, +, \cdot, 0, 1)$

$(\mathbb{Q}, +, \cdot, 0, 1)$ $\quad \mathbb{Q} \supset \mathbb{Z}$

$(\mathbb{R}, +, \cdot, 0, 1)$ $\quad \mathbb{R} \supset \mathbb{Q} \supset \mathbb{Z}$

$(\mathbb{C}, +, \cdot, 0, 1)$ $\quad \mathbb{C} \supset \mathbb{R} \supset \mathbb{Q} \supset \mathbb{Z}$

Anneau nul :

$$(\{0\}, +, \cdot, 0, 1=0)$$

$$0.0=0 \qquad 0+0=0$$

Rmq : Si dans un anneau A on a $1_A = 0_A$ alors $A = \{0_A\}$.

$$\mathbb{Z}/q\mathbb{Z} = \{ a(q) = a + \mathbb{Z}q \quad a \in \mathbb{Z} \} \subset \mathcal{P}(\mathbb{Z})$$

$$a(q) + b(q) = a+b(q)$$

$$a(q) \cdot b(q) := ab(q)$$

Bien defini car si $a'(q) = a(q)$

$$a' + q\mathbb{Z} = a + q\mathbb{Z}$$

et $b'(q) = b(q)$

alors $a'.b'(q) = a.b(q)$

$0_{\mathbb{Z}/q\mathbb{Z}} = q\mathbb{Z} = 0(q)$ $\quad 1_{\mathbb{Z}/q\mathbb{Z}} = 1(q) = 1 + q\mathbb{Z}$

Anneau Produit si A et B sont des anneau alors

$A \times B = \{(a,b) \quad a \in A, b \in B\}$ a une structure d'anneau

$$(a,b) +_{A\times B} (a',b') := (a +_A a', b +_B b')$$

$$(a,b) \cdot_{A\times B} (a',b') := (a \cdot_A a', b \cdot_B b')$$

$$0_{A\times B} = (0_A, 0_B) \qquad 1_{A\times B} = (1_A, 1_B)$$

Si on a une collection d'anneaux $(A_i)_{i\in I}$ on peut munir le produit

$$\prod_{i\in I} A_i$$

d'une structure d'anneau produit.

Anneau de fcts : $X = \text{ens}$

$$\mathcal{F}(X;\mathbb{R}) = \{f : X \to \mathbb{R}\} = \mathbb{R}^X$$

$f, g \in \mathcal{F}(X;\mathbb{R})$

$$f+g : x \in X \to f(x)+g(x) \in \mathbb{R}$$

$$f \cdot g : x \in X \to f(x) \cdot g(x) \in \mathbb{R}$$

$$0_{\mathcal{F}(X;\mathbb{R})} = \underline{0} \qquad 1_{\mathcal{F}(X;\mathbb{R})} = \underline{1}$$

De même si A = anneau X ensemble

$$\mathcal{F}(X;A) = \{f : X \to A\} = A^X$$

a une structure d'anneau hertée de celle de A

$$f+g : x \to f(x) +_A g(x) \in A$$
$$f \cdot g : x \to f(x) \cdot_A g(x) \in A$$

- Anneau de Polynômes

$\mathbb{R}[X]$ = ensemble des fcts $\mathbb{R} \to \mathbb{R}$
de la forme $x \to P(x)$

$$P(X) = a_d X^d + a_{d-1} X^{d-1} + \dots + a_0$$

$a_0, a_1, \dots, a_d \in \mathbb{R}$

$\mathbb{R}[X] \subset \mathcal{F}(\mathbb{R}, \mathbb{R})$

$\mathbb{R}[X]_g = \mathbb{R}[Y]$

A = anneau commutatif

l'anneau de fct polynomiales de $A \to A$

$$A[X]_f = \{ P : x \in A \to P(x) \in A$$
$$P(X) = a_d X^d + \dots + a_2 X^2 + a_1 X + a_0 \}$$
$$a_0, a_1, \dots, a_d \in A$$
$$\subset \mathcal{F}(A, A)$$

: A doit etre commutat. f
pour que $A[X]_f$ soit un anneau

Il existe des anneau
(eg $\mathbb{Z}/p\mathbb{Z}$ p premier)
tq il existe des polynomes differents
$P_1(X)$ $P_2(X)$ qui definissent

la même fct polynomiale :

$A = \mathbb{Z}/p\mathbb{Z}$

$P_1(X) = 0$

$P_2(X) = X^p - X$

les 2 fct poly sont égales (sur $\mathbb{Z}/p\mathbb{Z}$)

$\forall a \in \mathbb{Z}$

$$a^p - a \equiv 0 (p)$$

Anneaux d'endomorphismes

$(M,+)$ = gpe commutatif.

$End(M) = End_{Gr}(M) = Hom_{Gr}(M,M)$

a une structure d'anneau.

$\varphi, \psi \in End(M)$ $\varphi+\psi : m \to \varphi(m)+\psi(m)$

$(End(M), +, \underline{0}_M)$ est un gpe commutatif

$$\varphi \circ \psi : m \to \varphi \circ \psi(m) = \varphi(\psi(m))$$

$(End(M), +, \circ, 0_M, Id_M)$ forme un anneau

Distributivité : $\varphi, \psi, \xi \in End(M)$

$$\varphi \circ (\psi + \xi) \overset{?}{=} \varphi \circ \psi + \varphi \circ \xi$$

$$\varphi \circ (\psi + \xi)(m) = \varphi((\psi + \xi)(m))$$
$$= \varphi(\psi(m) + \xi(m))$$
$$= \varphi(\psi(m)) + \varphi(\xi(m))$$
$$= \varphi \circ \psi(m) + \varphi \circ \xi(m)$$
$$= (\varphi \circ \psi + \varphi \circ \xi)(m)$$

Anneau de matrices 2x2

$M = \mathbb{Z}^2 = \{(x,y) \quad x,y \in \mathbb{Z}\}$ $0_{\mathbb{Z}^2} = (0,0)$

$(End(\mathbb{Z}^2), +, \circ, 0_{\mathbb{Z}^2}, Id_{\mathbb{Z}^2}) = \text{Anneau}$

$\forall (x,y) \in \mathbb{Z}^2 \quad (x,y) = x(1,0) + y(0,1)$

$\mathbb{Z}^2 = \langle (1,0), (0,1) \rangle$

Soit $\varphi \in End(\mathbb{Z}^2)$

$$\varphi(x,y) = \varphi(x(1,0) + y(0,1))$$
$$= x \cdot \varphi(1,0) + y \cdot \varphi(0,1)$$

$\Longrightarrow$ φ est complètement déterminé par $\varphi(1,0)$ et $\varphi(0,1)$

$$\varphi(1,0) = (a,c) \quad \varphi(0,1) = (b,d)$$
$$a,b,c,d \in \mathbb{Z}$$

$\varphi, \psi \in \mathrm{End}(\mathbb{Z})$

$\varphi(1,0) = (a,c) \quad \varphi(0,1) = (b,d)$

$\psi(1,0) = (a',c') \quad \psi(0,1) = (b',d')$

$(\varphi+\psi)(1,0) = (a+a', c+c')$ $\Rightarrow$ permet de calculer

$(\varphi+\psi)(0,1) = (b+b', d+d')$ $(\varphi+\psi)(x,y)$

$$\varphi\circ\psi(1,0) = \varphi(\psi(1,0))$$

$$= \varphi(a', c')$$

$$= a'\varphi(1,0) + c'\varphi(0,1)$$

$$= a'(a,c) + c'(b,d)$$

$$= (aa' + bc', ca' + dc')$$

$$\varphi\circ\psi(0,1) = (ab' + bd', cb' + dd')$$

Tout $\varphi \in \mathrm{End}(M)$ st caractérise par (a,c) et (b,d)

On met cette information ds un tableau pour forme la matrice associée a φ

$$m(\varphi) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

l'ensemble de ces matrices est note $M_2(\mathbb{Z})$

$$M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \; a,b,c,d \in \mathbb{Z} \right\}$$

$m(\cdot) : \varphi \in End \longrightarrow m(\varphi) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

est une bij entre $End(M)$ et $M_2(\mathbb{Z})$

on peut transposer la structure d'anneau de $End(M)$ à l'ensemble $M_2(\mathbb{Z})$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} := \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$$

et $$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} := \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

$$m(0_{\mathbb{Z}^2}) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_2 \qquad m(Id_{\mathbb{Z}^2}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id_2$$

$(M_2(\mathbb{Z}), +, \times, O_2, Id_2)$ forme un anneau (non commutatif)

Anneau de Matrices a coef dsun anneau :

A commatatif

$$M_2(A) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad a,b,c,d \in A \right\}$$

$$0_{A2} = \begin{pmatrix} 0_A & 0_A \\ 0_A & 0_A \end{pmatrix} \qquad Id_2 = \begin{pmatrix} 1_A & 0_A \\ 0_A & 1_A \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} := \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} := \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

$\left(M_2(A), +, \times, O_{A,2}, Id_{A,2}\right)$ est un anneau.

$M_2(A)$ code l'anneau $\mathrm{End}_{A\text{-mod}}(A^2)$

$A^2 = A \times A$ muni d'une structure de A-module.

Proprietes de Base

Définition 3.1. *Un anneau $(A, +, ., 0_A, 1_A)$ est la donnee, d'un groupe commutatif $(A, +)$ (note additivement) d'element neutre note 0_A, d'une loi de composition interne (dite de multiplication)*

$$\bullet.\bullet : \begin{array}{ccc} A \times A & \mapsto & A \\ (a, b) & \mapsto & a.b \end{array}$$

et d'un element unite $1_A \in A$ ayant les proprietes suivantes

(1) Associativite de la multiplication:

$$\forall a, b, c \in A,\ (a.b).c = a.(b.c) = a.b.c.$$

(2) distributivite:

$$\forall a, b, c \in A,\ (a + b).c = a.c + b.c,\ c.(a + b) = c.a + c.b.$$

(3) Neutralite de l'unite:

$$\forall a \in A,\ a.1_A = 1_A.a = a.$$

Un anneau est dit commutatif si de plus la multiplication est commutative:

$$\forall a, b \in A,\ a.b = b.a.$$

LEMME 3.1. *Pour tout* $a, b \in A$, *on a*

$$0_A.a = a.0_A = 0_A,$$

(on dit que l'element neutre de l'addition 0_A *est* absorbant*). Pour l'oppose, on a*

$$(-a).b = -(a.b) = a.(-b).$$

Preuve : on a $a = 1_A.a$

$$= (1_A + 0_A).a$$

$$= 1_A.a + 0_A.a$$

$$= a + 0_A.a$$

$$\Rightarrow 0_A = 0_A.a.$$

le reste en exo.

Exo : Mq 1_A est unique.

Si il existe $1'_A$ t.q $\forall a \in A \; 1'_A \cdot a = a \cdot 1'_A = a$

$\Rightarrow 1'_A = 1_A$.

Exo : Mq $0_A = 1_A \Rightarrow A = \{0_A\}$

Elements Inversibles

Unités

Définition 3.2. *Soit A un anneau. Un element $a \in A$ est inversible si il existe $b \in A$ tel que*

$$a.b = b.a = 1_A.$$

On dit alors que b est un inverse (a gauche et a droite) de a (pour la multiplication).

Ex: 0_A n'est presque jamais inversible :
sauf si $0_A = 1_A \Rightarrow A = \{0_A\}$.

PROPOSITION 3.1. *(Unicite de l'inverse) Soit A un anneau et $a \in A$ un element inversible et soit b tel que $a.b = b.a = 1_A$.*

Soit b' verifiant

$$a.b' = 1_A$$

alors $b' = b$; de meme si b' verifie

$$b'.a = 1_A$$

alors $b' = b$

Preuve : soit a inversible et b tq $ab = ba = 1_A$ et soit b' tq

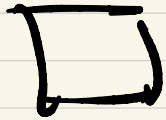
$$a.b' = 1_A$$

$$a.b' = 1_A \Longrightarrow b.a.b' = b.1_A = b$$

$$\| \quad \|$$

$$b' = 1_A \cdot b' = b$$

.....



NOTATION 3.1. *Par la Proposition precedente si un element $a \in A$ est inversible son inverse est unique. On notera cet inverse*

$$a^{-1}.$$

Notons que a^{-1} est egalement inversible et on a

$$(a^{-1})^{-1} = a.$$

On deduit de cette discussion que

PROPOSITION 3.2. *Soit $A^\times$ l'ensemble des elements inversibles d'un anneau A, alors*

$$(A^\times, ., 1_A, \bullet^{-1})$$

forme un groupe: le groupe des elements inversibles de A.

$A^\times$ est aussi appelle ensemble des unités de A

Exemples $(\mathbb{Z}, +, \cdot, 0, 1)$

$$\mathbb{Z}^\times = \{\pm 1\} \subsetneq \mathbb{Z}^* = \mathbb{Z} - \{0\}$$

$(\mathbb{Q}, +, \cdot, 0, 1)$

- $\mathbb{Q}^\times = \mathbb{Q}^* = \mathbb{Q} - \{0\} \rightsquigarrow$ $\mathbb{Q}$ est un corps.
- $\mathbb{R}^\times = \mathbb{R}^* = \mathbb{R} - \{0\} \rightsquigarrow \mathbb{R}$ un corps
- $\mathbb{C}^\times = \mathbb{C}^* = \mathbb{C} - \{0$

$$\left(\mathbb{Z}/q\mathbb{Z}\right)^{\times} = \left\{ a(q) = a + q\mathbb{Z} \;\; \text{pgcd}(a,q) = 1 \right\}$$

Preuve : $\subset$: Soit $a(q) \in \left(\mathbb{Z}/q\mathbb{Z}\right)^{\times}$

il existe $b(q)$ t$_q$

$$a(q) \cdot b(q) = 1(q) = ab(q)$$

$\Leftrightarrow$ $ab - 1$ est divisible par q

$\exists c$ tq $ab = 1 + qc$

$\Rightarrow ab - qc = 1$ Relation de Bezout

$a \wedge q = 1$

Soit a premier a q : par Bezout

il existe b et c tq

$$ab + qc = 1$$

$$ab - 1 = -qc \qquad ab \equiv 1 \ (q)$$

$$\Rightarrow a(q) \cdot b(q) = 1 \ (q)$$

$$a(q) \in (\mathbb{Z}/q)^{\times}$$

□

$$|(\mathbb{Z}/q)^\times| = |\{1 \le a \le q \text{ t.q. } a \wedge q = 1\}|$$

$$= \varphi(q) = \text{fct d'Euler.}$$

A commutativ

$$M_2(A) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad a,b,c,d \in A \right\}$$

$$M_2(A)^\times = \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ tq } \det M = ad-bc \in A^\times \right\}$$

Prouve que $M_2(A)^\times \subset \{ M \text{ tq } ad-bc \in A^\times \}$

On a la relation de multicativite

suivant $M, N \in M_2(A)$

$$\det(M.N) = \det M . \det N$$

$$\det \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix} = (ad-bc)(a'd'-b'c')$$

si $M \in M_2(A)^\times$, $\exists N \in M_2(A)$ tq

$$M.N = Id_2 = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$$

$$\det(M.N) = \det M \cdot \det N = \det \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} = 1$$

$$\det M \in A^\times$$

$\subset$

EXERCICE 3.2. Soit A un anneau commutatif et $M_2(A)$ l'anneau des matrices a coefficients dans A. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(A)$, la transposee de la matrice des *cofacteurs* de M est la matrice definie par

$$\mathrm{tcof}(M) := \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

(1) Montrer que

$$M.\mathrm{tcof}(M) = \mathrm{tcof}(M).M = \det(M).\mathrm{Id}_2 = \begin{pmatrix} \det(M) & 0 \\ 0 & \det(M) \end{pmatrix}$$

ou $\det(M)$ (le determinant de M) est defini par

$$\det(M) := ad - bc \in A.$$

(2) En deduire que

$$M_2(A)^\times =: \mathrm{GL}_2(A) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a, b, c, d \in A,\ \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \in A^\times \}.$$

$(M,+)$

$$End_{Gr}(M)^{\times} = \left\{ \varphi \in End_{Gr}(M) \text{ tq } \exists \right.$$
$$\left. \psi \in End_{Gr}(M) \text{ avec } \varphi \circ \psi = \psi \circ \varphi = Id_M \right\}$$

$\Rightarrow \varphi$ est bijective et $\psi = \varphi^{-1}$

$$End_{Gr}(M)^{\times} = Aut_{Gr}(M)$$

A non-commutatif

$P(X) = a_d X^d + \dots + a_0 \quad a_i, b_j \in A$

$Q(X) = b_d X^d + \dots + b_0$

est ce que $P.Q \overset{?}{=} c_{2d} X^{2d} + c_{2d-1} X^{2d-1} + \dots + c_0$

$P(X) = a_d X^d \quad Q(X) = b_d X^d$

$$P(X).Q(X) = a_d X^d . b_d X^d \doteq a_d b_d X^d . X^d$$

en pensant que X est une variable à valeurs dans A

$x \in A$

$$a_d . x^d . b_d x^d =$$

Sous - Anneau

Définition 3.4. *Soit $(A, +, .)$ un anneau. Un sous-anneau $B \subset A$ est un sous-groupe de $(A, +)$ qui est*

- *soit le sous-groupe trivial $\{0_A\}$,*
- *soit qui contient l'unite 1_A et qui est stable par multiplication:*

$$\forall b, b' \in B,\ b.b' \in B.$$

Ainsi $(B, +, ., 0_A, 1_A)$ est un anneau.

Proposition 3.3. *(Critere de sous-anneau) Soit $(A, +, .)$ un anneau et $B \subset A$ un sous-ensemble non-vide; alors B est un sous-anneau ssi $B = \{0_A\}$, ou bien $1_A \in B$ et*

$$\forall b, b', b'' \in B,\ b.b' - b'' \in B \tag{3.1.1}$$

Preuve: Exercice. □

Exemples $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Sous-Anneaux de $\mathbb{Z}$: $\{0\}$; si $B \subset \mathbb{Z}$ et un ssanneau

alors $1 \in B$ $\forall k \in \mathbb{Z}$ $k.1 \in B$ $\{0\}^+$ $\mathbb{Z} = B$

Sous-anneaux de $\mathbb{Z}/q\mathbb{Z}$: $\{0\}$ si $B \subset \mathbb{Z}/q\mathbb{Z}$

contient $1(q)$ alors $\forall k \in \mathbb{Z}$

B contient $k.1(q) = k(q)$ $B = \mathbb{Z}/q\mathbb{Z}$

- A commutatif $M_2(A)$

Matrices Scalaires:

$$A\,Id_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} a \in A \right\}$$

Matrices Diagonales

$$D_2(A) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} a, d \in A \right\}$$

- Matrices triangulaires supérieures

$$B_2^+(A) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \; a,b,d \in A \right\}$$

- Matrices triangulaires inf/s

$$B_2^-(A) = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \; a,c,d \in A \right\}$$

Anneau engendré : A = Anneau

Si I = ens et $(A_i)_{i \in I}$ une famille de sous-anneaux indexés par I

alors $\bigcap_{i \in I} A_i = \{ a \in A \text{ tq } \forall i \ a \in A_i \}$

est un ss anneau de A

Preuve : si un des $A_i = \{0_A\}$ alors

$\bigcap_{i=1} A_i = \{0_A\}$ et on a l'anneau nul

Si $\forall i \; A_i \neq \{0_A\} \Rightarrow \forall i \; 1_A \in A_i$

et $1_A \in \bigcap_{i \in I} A_i$ il reste à voir que

si $b, b', b'' \in \bigcap_{i \in I} A_i$ alors $b.b' - b'' \in \bigcap_i A_i$

mais $b.b' - b'' \in A_i$ car $b, b', b'' \in A_i$

et donc $b.b' - b'' \in \bigcap_i A_i$ □

Si $X \subset A$ est un ensemble

$\bigcap_{X \subset A' \subset A} A'$ = l'intersection des sous-anneaux de A contenant X

A' = sous-anneau

est un ss anneau de A qui contient X
et c'est le + petit ss anneau de A contenant X

on l'appelle le ss anneau engendré par X

= l'ensemble des sommes et différences
de produit d'élément de X
et de $-X$

$P(x) \quad Q(x)$

$P(x) \quad Q(x)$

$x \longmapsto P(x) \cdot Q(x) = R(x)$?

Morphismes

Définition 3.5. *Soient* $(A, +_A, .A)$, $(B, +_B, .B)$ *des anneaux. Un morphisme d'anneaux* $\varphi : A \mapsto B$ *est un morphisme de groupes commutatif* $\varphi : (A, +_A) \mapsto (B, +_B)$ *tel que*

$$\varphi(1_A) = 1_B \text{ ou bien } \varphi(1_A) = 0_B,$$

$$\forall a, a' \in A,\ \varphi(a._A a') = \varphi(a).{}_B\varphi(a').$$

Rmq: $\varphi(1_A) = 0_B$ $\forall a \in A$

$a = a.1_A$ $\varphi(a) = \varphi(a)\varphi(1_A)$

$= \varphi(a)0_B = 0_B$

$\varphi = 0_B$

Exemple : Le morphisme canonique.

A anneau.

$$Can_A : \mathbb{Z} \longrightarrow A$$

$$n \longrightarrow n_A = 1_A + \dots + 1_A \ (n_A \text{ fois}) = n.1_A$$

(si $n<0$ $n_A = -|n|.1_A$)

$n \to n_A$ est un morphisme d'anneaux

le morphisme Canonique existe pour tout anneau.

Exemple :

$$\mathrm{Can}_{\mathbb{Z}/q\mathbb{Z}} : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/q\mathbb{Z} \\ a & \longrightarrow & a \pmod q = a + q\mathbb{Z} \end{array}$$

est le morphisme canonique

Caractéristique :

Can_A est un morphisme de groupes additifs

$$\ker(Can_A) = \{ n \in \mathbb{Z} \text{ tq } n_A = 0_A \}$$

$$= q_A \mathbb{Z} \quad q_A \in \mathbb{N}$$

q_A = Caractéristique de A.

Ex: $a \in \mathbb{Z} \to a(q) \in \mathbb{Z}/q\mathbb{Z}$

$$\ker\left(\mathrm{Can}_{\mathbb{Z}/q\mathbb{Z}}\right) = q\mathbb{Z}$$

$$\mathrm{Car}\left(\mathbb{Z}/q\mathbb{Z}\right) = q.$$

Noyau - Image

PROPOSITION 3.5. *(Stabilite par morphismes) Soient $\varphi \in \mathrm{Hom}_{Ann}(A, B)$ un morphisme alors $\varphi(A) \subset B$ est un sous-anneau. Par ailleurs le sous-groupe $\ker(\varphi)$ est un sous-groupe de $(A, +)$ qui est de plus stable par multiplication (a gauche et a droite) par A:*

$$\forall a \in A, k \in \ker(\varphi),\ a.k,\ k.a \in \ker(\varphi).$$

Preuve: Soit $\varphi : A \to B$ un morphisme alors $\varphi(A)$ est un anneau.

- $\varphi(1_A) = 0_B \rightsquigarrow \varphi = 0_B$

$\varphi(A) = \{0_B\}$

$\varphi(1_A) = 1_B \rightsquigarrow \varphi(A) \ni 1_B$

- $\varphi(A)$ est un sous-groupe de $(B, +)$
- $\forall a, a' \in A \quad \varphi(a) \cdot \varphi(a') = \varphi(aa') \in \varphi(A)$

$\varphi(A) \quad \varphi(A)$

$$\ker\varphi = \varphi^{(-1)}(\{0_B\}) = \{k \in A \text{ tq } \varphi(k) = 0_B\}$$

$\ker\varphi$ est un ssgpe.

$\forall a \in A \ \forall k \in \ker\varphi$ on veut mq $k.a$ et $a.k$ $\in \ker\varphi$.

$$\varphi(a.k) = \varphi(a).\varphi(k) = \varphi(a).0_B$$
$$= 0_B$$

□

PROPOSITION 3.6. *Un morphisme d'anneaux $\varphi \in \mathrm{Hom}_{Ann}(A, B)$ est injectif ssi $\ker(\varphi) = \{0_A\}$.*

En general

$\ker\varphi$ n'est pas un sous-anneau

sauf si $\ker\varphi = \{0_A\}$

sinon $\ker\varphi \ni 1_A$ en general.

Si $1_A \in \ker\varphi$ $\forall a \in A$

$$\varphi(a) = \varphi(a \cdot 1_A) = \varphi(a)\varphi(1_A)$$
$$= \varphi(a) 0_B = 0_B$$

Si $1_A \in \ker\varphi \Rightarrow \varphi = 0_B$

et $1_A \in \ker\varphi \Rightarrow \ker\varphi = A$

Rmq (Anneau quotient)

Si $\varphi : A \to B$ morphisme d'anneau

alors $\ker \varphi$ = Idéal Bilatère

- Est ce que tout idéal bilatère $I \subset A$ est le $\ker \varphi$ pour $\varphi : A \to B$

Oui : Utilise la construction d'anneau quotient

$$A/I = \{ a+I = a(I) \quad a \in A \} \subset \mathcal{P}(A)$$

A/I admet une structure d'anneau

$$a(I) + b(I) := a+b(I)$$
$$a(I) \cdot b(I) := a.b(I)$$

Et $A \to A/I$ est un morphisme

$a \to a(I) = a + I$ de noyau I.

Définition 3.6. *Soit A un anneau pas forcement commutatif.*

- *Un ideal (a gauche) de A est un sous-groupe additif $(I,+) \subset (A,+)$ qui est stable par multiplication (a gauche) par les elements de A:*

$$\forall a \in A,\ b \in I,\ a.b \in I.$$

- *Un ideal (a droite) de A est un sous-groupe additif $(I,+) \subset (A,+)$ qui est stable par multiplication (a droite) par les elements de A:*

$$\forall a \in A,\ b \in I,\ b.a \in I.$$

- *Un ideal bilatere de A est un sous-groupe additif $(I,+) \subset (A,+)$ qui est un ideal a gauche et a droite:*

$$\forall a \in A,\ b \in I,\ a.b,\ b.a \in I.$$

En particulier si A est commutatif les notion d'ideal a gauche, a droite ou bilatere sont toutes les memes.

ker φ est un ideal bilatere.

Stabilité par composition

PROPOSITION 3.7. *Soient $\varphi : A \mapsto B$ et $\psi : B \mapsto C$ des morphismes d'anneaux alors*

- *$\psi \circ \varphi : A \mapsto C$ est un morphisme d'anneaux.*
- *Soit $\varphi \in \mathrm{Hom}_{Ann}(A, B)$ un morphisme d'anneaux bijectif, l'application reciproque $\varphi^{-1} : B \mapsto A$ est un morphisme d'anneaux. On dit que φ est un isomorphisme d'anneaux et on dit que A et B sont des anneaux isomorphes.*

Preuve: on sait que $\psi \circ \varphi$ = morphisme de gpes et que $\psi \circ \varphi(1_A) = \psi(\varphi(1_A)) = \begin{cases} 0_C \\ 1_C \end{cases}$

$\forall a, a' \in A \quad \psi \circ \varphi(a.a') = \psi(\varphi(aa'))$

$$\psi(\varphi(a) \cdot_B \varphi(a')) = \psi\circ\varphi(a) \cdot_C \psi\circ\varphi(a')$$

- si $\varphi \in \mathrm{Hom}_{\mathrm{Ann}}(A,B)$ et Bijectif

φ^{-1} est un morphisme de gpes

$\varphi^{-1}(1_B) = 1_A$ sauf si $A = B = \{0\}$

$$\varphi^{-1}(b \cdot_B b') \overset{?}{=} \varphi^{-1}(b) \cdot_A \varphi^{-1}(b')$$

on calcule $\varphi(\varphi^{-1}(b \cdot b')) = b \cdot_B b'$

$$\varphi(\varphi^{-1}(b) \cdot_A \varphi^{-1}(b')) =$$

$$\varphi(\varphi^{-1}(b)) \cdot_B \varphi(\varphi^{-1}(b'))$$

$$= b \cdot_B b'$$

□

NOTATION 3.2. *Soient A, B des anneaux. On note*

$$\mathrm{Hom}_{Ann}(A,B), \mathrm{End}_{Ann}(A) = \mathrm{Hom}_{Ann}(A,A)$$

$$\mathrm{Isom}_{Ann}(A,B),\ \mathrm{Aut}_{Ann}(A) = \mathrm{Isom}_{Ann}(A,A)$$

l'ensemble des morphismes d'anneaux entre A et B, des endomorphismes de l'anneau A, des isomorphismes d'anneaux entre A et B et des automorphismes de l'anneau A.

Rmq : $\mathrm{End}_{Ann}(A)$ est un ssanneau de $(\mathrm{End}_{Gr}(A), +, 0, \underline{0}_A, \mathrm{Id}_A)$

- $\mathrm{Aut}_{Ann}(A) = \mathrm{End}_{Ann}(A)^\times$ = ss gpe de $\mathrm{Aut}_{Gr}(A)$