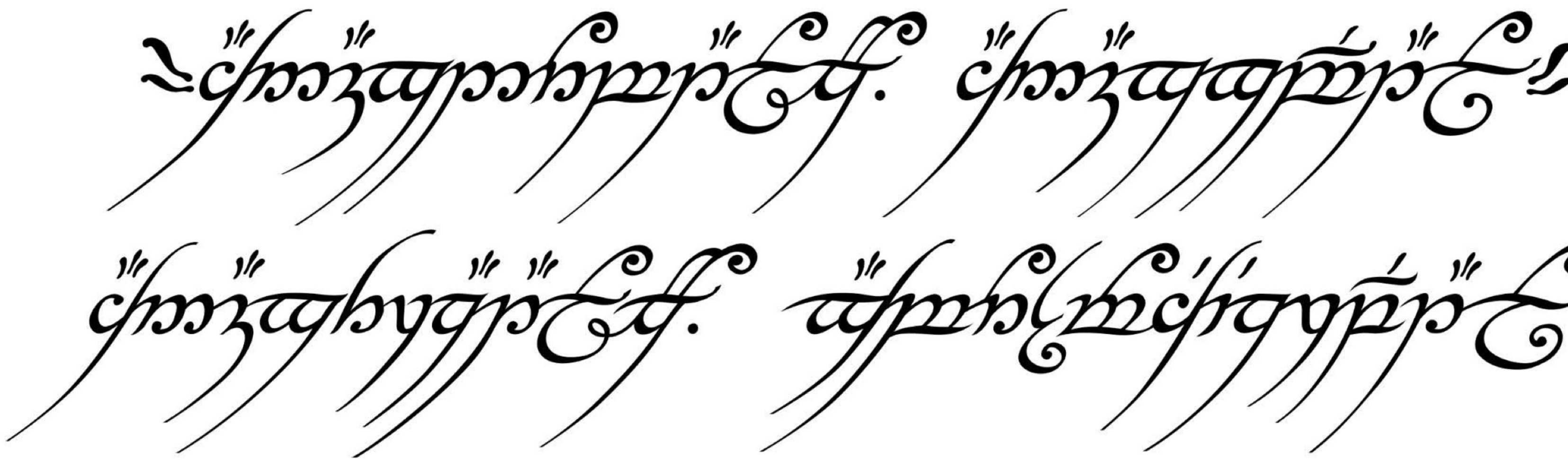

”Un Anneau pour les gouverner tous,
Un Anneau pour les trouver,
Un Anneau pour les amener tous,
Et dans les ténèbres les lier”

"Trois anneaux pour les rois Elfes sous le ciel,

$\mathrm{B}_{\mathrm{crys}}, \; \mathrm{B}_{\mathrm{st}}, \; \mathrm{B}_{\mathrm{dR}},$

Sept pour les Seigneurs Nains dans leurs demeures de pierre,

$E_{\mathbb{Q}_p}, \; A_{\mathbb{Q}_p}, \; B_{\mathbb{Q}_p}, \; E, \; A, \; B, \; \tilde{A}$

Neuf pour les Hommes Mortels destinés au trépas,

$\mathbb{Q}_p, \; \mathbb{Z}_p, \; \mathbb{F}_p, \; \overline{\mathbb{Q}_p}, \; \overline{\mathbb{F}_p}, \; \mathbb{C}_p, \; \mathcal{O}_{\mathbb{C}_p}, \; \mathbb{Q}_p^{nr}, \; \mathrm{B}_{\mathrm{HT}}$

Un pour le Seigneur Ténébreux sur son sombre trône

$\mathrm{A}_{\mathrm{inf}}$"

Anneaux et Modules

DÉFINITION 3.1. *Un anneau* $(A,+,.,1_A)$ *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:

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

Exemples

Anneau Nul : $\{0\}$ $\quad 0+0=0 \quad 0.0=0 \quad 1_{\{0\}}=0$

$$\{0\} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \hookrightarrow \mathbb{C}[X]$$

commutatifs.

Anneau de congruences

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

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

$$a \pmod q + b \pmod q := a + b \pmod q$$

$$a \pmod q \,.\, b \pmod q := a . b \pmod q$$

$$0_{\mathbb{Z}/q\mathbb{Z}} = 0 \pmod{q}$$

$$1_{\mathbb{Z}/q\mathbb{Z}} = 1 \pmod{q}$$

Anneau commutatif des congruences (de Gauss) modulo q.

Anneaux de fonctions

X ensemble

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

$$f+g : x \in X \to f(x)+g(x)$$

$$f \cdot g : x \in X \to f(x) \cdot g(x)$$

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

A anneau commutatif

$\mathcal{F}(X,A)$ a une structure d'anneau héritée de A

$$0_{\mathcal{F}(X,A)} = \underline{0}_A \qquad 1_{\mathcal{F}(X,A)} = \underline{1}_A$$

Anneaux de Polynômes

$$\mathbb{R}[x] = \left\{ \begin{array}{l} P : \mathbb{R} \to \mathbb{R} \\ \quad x \in \mathbb{R} \mapsto a_d x^d + a_{d-1} x^{d-1} + \dots + a_0 \\ \quad a_0, a_1, \dots, a_d \in \mathbb{R} \end{array} \right\}$$

$$\cap$$

$$\mathcal{F}(\mathbb{R}, \mathbb{R})$$

= anneau des fcts polynomiales.

Plus generalement pour A anneau commutatif on definit l'anneau des polynomes a coefs dans A

$$A[X] = \left\{ P(X) = a_d X^d + \dots + a_1 X^1 + a_0 X^0 \;\middle|\; \begin{array}{l} a_d, \dots, a_0 \in A \\ d \geq 0 \end{array} \right\}$$

Anneaux d'Endomorphismes

$(M,+)$ Groupe commutatif

$$\left(\mathrm{End}_{Gr}(M)\,,\,+\,,\,\circ\,,\,\underline{0}_M\,,\,1_{\mathrm{End}} = \mathrm{Id}_M\right)$$

anneau non-commutatif.

Anneau de Matrices

A = anneau commutatif

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

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

$$\shortparallel$$

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

$$\rightsquigarrow (M_2(A), +) = \text{gpe commutatif} \quad 0_{M_2(A)} = \begin{pmatrix} 0_A & 0_A \\ 0_A & 0_A \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \left(\begin{array}{c|c} aa'+bc' & ab'+bd' \\ \hline ca'+dc' & cb'+dd' \end{array}\right)$$

$(M_2(A), +, \cdot)$ forme un anneau non-commutatif d'unité

$$1_{M_2(A)} = \underbrace{Id_2} = \begin{pmatrix} 1_A & 0_A \\ 0_A & 1_A \end{pmatrix}$$

= anneau des matrices 2×2 à coefs dans A.

L'anneau des Endomorphismes d'un gpe commutatif

$(M, +)$ un gpe commutatif.

$$\mathrm{End}_{Gr}(M) = \mathrm{Hom}_{Gr}(M, M)$$

$$= \left\{ \varphi : M \to M \quad \varphi = \text{morphisme de gpe} \right\}$$

- $\mathrm{End}(M)$ est muni de la loi de composition

$$\circ : \varphi, \psi \in \mathrm{End}(M) \longrightarrow \varphi \circ \psi \quad \rightsquigarrow \text{multiplication}$$

$$1_{\mathrm{End}(M)} = \mathrm{Id}_M.$$

$+ : \quad \varphi, \psi \in \mathrm{End}(M)$

$$\varphi + \psi : \quad m \in M \longrightarrow \varphi(m) +_M \psi(m)$$

$$0_{\mathrm{End}(M)} = \underline{0}_M : \quad m \longrightarrow 0_M$$

$$\left(\mathrm{End}(M), +, \underline{0}_M, \circ, \mathrm{Id}_M \right)$$

forme un anneau non commutatif
(en general)

End(M) n'est pas commutatif

$$\exists\, \varphi, \psi \text{ tq } \varphi \circ \psi \neq \psi \circ \varphi$$

(si M est assez gros)

$M = (\mathbb{Z}^2, +)$ le gpe commutatif

$$(m,n) + (m',n') \longrightarrow (m+m', n+n')$$

End$(\mathbb{Z}^2)$ s'identifie avec $M_2(\mathbb{Z})$.

$(\mathrm{End}(M), +, \circ)$ est un anneau.

- $(\mathrm{End}, +)$ est un gpe commutatif

$\varphi \in \mathrm{End}(M)$ on défini son opposé

$$-\varphi : m \longrightarrow -\varphi(m)$$

opposé ds $(M, +)$

on doit voir que $-\varphi$ est un morphisme de gpes

$\forall m, m' \in M$

$$-\varphi(m+m') \overset{?}{=} -\varphi(m) + -\varphi(m')$$

$$= -\left(\varphi(m) + \varphi(m')\right) \overset{?}{=} -\varphi(m) + \left(-\varphi(m')\right)$$

vrai car M est commutatif : on calcule

$$\left(\varphi(m) + \varphi(m')\right) + \left(-\varphi(m) + \left(-\varphi(m')\right)\right) \overset{?}{=} 0_M$$

commutativité

$$= \varphi(m) + \left(-\varphi(m)\right) + \varphi(m') + \left(-\varphi(m')\right)$$

$$\varphi(m) + (-\varphi(m)) + \varphi(m') + (-\varphi(m'))$$

$$= 0_M + 0_M = 0_M$$

$$= \varphi(-m) = -\varphi(m) \text{ ?}$$ oui car φ = morphisme

$(\mathrm{End}(M), +)$ est un gpe commutatif

$$\varphi + \psi = \psi + \varphi$$

$\circ$ est associative

Id_M est un morphisme de gpe et
est neutre pour $\circ$

- $\circ$ est distributive / $+$

$\varphi, \varphi', \psi \in End(M)$

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

$\forall m \in M$ $(\varphi + \varphi') \circ \psi\,(m) = (\varphi + \varphi')(\psi(m))$

def de $\varphi + \varphi'$ $\Longrightarrow$ $= \varphi(\psi(m)) + \varphi'(\psi(m))$

$= \varphi \circ \psi\,(m) + \varphi' \circ \psi\,(m)$

def de $\varphi \circ \psi + \varphi' \circ \psi$ $= (\varphi \circ \psi + \varphi' \circ \psi)(m)$

$\square$

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 : $1_A \cdot a = a$

$$1_A = 1_A + 0_A$$

$$a = 1_A \cdot a = (1_A + 0_A) \cdot a = 1_A \cdot a + 0_A \cdot a$$

$$a = a + 0_A \cdot a$$

$$0_A = 0_A \cdot a \quad \ldots\ldots\ldots$$

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: $(\mathbb{Z}, +, \times)$ 1 est inversible -1 inversible

2 n'est pas inversible.

$(\mathbb{R}, +, \times)$ 2 est inversible (on prend $b = 1/2$)

0 n'est pas inversible

$A = \{0\}$ 0 est inversible ds A car

$0 . 0 = 0$ $0 = 1_{\{0\}}$.

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

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

et b' tq $b'.a = 1_A$ $b = b'$?

$$b.a - b'.a = 1_A - 1_A = 0_A$$

$(b-b').a = 0_A$ on multiplie par b à dte

$$(b-b')\cdot a\cdot b = 0_A\cdot b = 0_A$$

$$(b-b')\cdot 1_A = 0_A$$

$$b-b' = 0_A$$

$$b = b' \quad \ldots\ldots$$

$$\square$$

<u>Notation</u>: si a est inversible on note $b = a^{-1}$ c'est l'inverse de a (ds A)

- si a est inversible $\Rightarrow$ a^{-1} est inversible $a.a^{-1} = a^{-1}.a = 1_A$ et son inverse est $(a^{-1})^{-1} = a$.

On note $A^\times = \{a \in A \quad a \text{ inversible}\}$
$=$ les unités de A.

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.

<u>Exemples</u>

$$\mathbb{Z}^\times = \{\pm 1\}$$

$$\mathbb{Q}^\times = \mathbb{Q} - \{0\}$$

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

$$\mathcal{F}(X,A)^\times = \mathcal{F}(X,A^\times)$$

$$\mathrm{End}(M)^\times = \mathrm{Aut}_{Gr}(M)$$

$M_2(A)^\times$ $\qquad$ $\bigcup$

Bezout.

$$\left(\mathbb{Z}/q\mathbb{Z}\right)^\times = \{\, a \pmod q \ \text{ tq } \ (a,q)=1 \,\}$$

$$\text{pgcd}(a,q)$$

Définition 3.3. *Soit $(A, +, .)$ un anneau commutatif et $a, c \in A$, on dit que a divise c et on le note*

$$a|c$$

si il existe $b \in A$ tel que

$$c = a.b.$$

On dit egalement que a est un diviseur de c.

la relation $\cdot|\cdot$ est reflexive et transitive (mais pas forcement antisymetrique)

Si $a|c$ et $c|a$ alors $c = a.b$ avec $b \in A^{\times}$ et $a = b^{-1}.c$

Sous-Anneaux

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:*

$$\times\, 0_A \qquad \forall b, b' \in B,\ b.b' \in B.$$

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*

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

<u>Preuve</u>: Si $B = \{0_A\}$ on a fini.

Si $1_A \in B$ (et $1_A \neq 0_A$) on a que $(B,+)$ est un ssgpe car $\forall\, b, b'' \in B$

$$b - b'' = b.1_A - b'' \in B \Rightarrow$$

On utilise l'hypothese avec $b, b' \in B$ et $b'' = 0_A$ (car $(B,+)$ est un ssgpe de A donc contient 0_A)

$$b.b' - 0_A \in B$$

$$\shortparallel$$

$$b.b' \in B.$$

$\square$

Exemples

- $\{0_A\} \subset A$

- $\cap$: Si $B, B' \subset A$ sont des ssanneaux alors $B \cap B'$ est un ssanneaux.

- $\{0\} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

- $\mathbb{Z}[X] \subset \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$

Sous-Anneaux de $\mathbb{Z}$, de $\mathbb{Z}/_{q}\mathbb{Z}$?

$\{0\}$, $\mathbb{Z} \subset \mathbb{Z}$. Y-en a t-il d'autres ?

Non car si $B \neq \{0\}$ alors $1 \in B$

et le ssgpe engendré par 1 $\mathbb{Z}.1 \subset B$

$$\overset{\shortparallel}{\mathbb{Z}} \subset B$$

Idem pour $\mathbb{Z}/_{q}\mathbb{Z}$.

- Endomorphismes Scalaires

$(M, +)$ gpe commutatif

$$A = \mathrm{End}_{Gr}(M)$$

$$n \in \mathbb{Z} : \quad n.\bullet : m \in M \longrightarrow n.m \in M$$

$$n.m = \begin{cases} m + m + \cdots + m \quad n\text{-fois} & \text{si } n > 0 \\ 0_M & \text{si } n = 0 \\ \cdots\cdots\cdots \quad |n|\text{-fois} & \text{si } n < 0 \end{cases}$$

l'application

$n.\bullet$ est un morphisme $(M,+)$

on la note $n.Id_M$ $\quad (-1).Id : m \mapsto -m$

et l'ensemble de $\{ n.Id_M \quad n \in \mathbb{Z} \}$

forme un sous-anneau de $End(M)$.

(endomorphisme scalaires)

Matrices Scalaires   A commutatif

$$M_2(A) \supset \left\{ a.I_2 = \begin{pmatrix} a & 0_A \\ 0_A & a \end{pmatrix} \quad a \in A \right\}$$

$$\|$$

$A.I_2$ = l'anneau des matrices scalaires 2×2.

Morphismes d'Anneaux

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

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

$$\forall a, a' \in A,\ \varphi(a.a') = \varphi(a).\varphi(a').$$

<u>Rmq</u>: Si $\varphi(1_A) = 0_B$ alors $\varphi = 0_B$

Si $a \in A$ $\varphi(a) = \varphi(a.1_A) = \varphi(a).\varphi(1_A)$

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

Exemple: le morphisme canonique

Soit A un anneau quelconque

$$\text{Soit } \mathrm{Can}_A : \mathbb{Z} \longrightarrow A \qquad \boxed{n \underline{\cdot} 1_A = n_A \cdot 1_A}$$

$$n \longmapsto n \underline{\cdot} 1_A = n_A$$

$:= 1_A + 1_A + \dots + 1_A$ n fois si $n>0$

$:= 0_A$ si $n = 0_{\mathbb{Z}}$

$:= -_A(|n| \underline{\cdot} 1_A)$ si $n < 0$

Exo: C'est un morphisme d'anneau

$$\bullet\ I_2 : A \longrightarrow M_2(A)$$
$$a \longrightarrow aI_2 = \begin{pmatrix} a & 0_A \\ 0_A & a \end{pmatrix}$$

est un <u>morphisme d'anneaux</u>

$$- \quad \mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z}$$
$$m \longrightarrow m + q\mathbb{Z}$$

est un morphisme d'anneaux qui coïncide avec $Can_{\mathbb{Z}/q\mathbb{Z}}$

$$n \,\underline{\cdot}\, m = n \times m$$

Noyau - Image

Proposition 3.4. *(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*:*

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

Rmq : si B' = ssanneau contenant 1_B alors $\varphi^{(-1)}(B')$ = ssanneau de A.

Par contre $\varphi^{(-1)}(\{0_B\}) = \ker\varphi$ n'est pas en général un ssanneau de A

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

<u>Preuve</u> : Comme φ est un morphisme de gpe $(+)$

$\varphi(A) \subset B$ est un ssgpe de B.

si $\varphi(A) = \{0_B\}$ on a fini. $\varphi = \underline{0}_B$

- si $\varphi(A) \neq \{0_B\}$ alors $\varphi(1_A) \neq 0_B$

(sinon $\forall a \in A \quad \varphi(a) = \varphi(a \cdot 1_A) = \varphi(a)\varphi(1_A) = 0_B$)

alors $\varphi(1_A) = 1_B \in \varphi(A)$

$\varphi(A)$ est un ssgpe pour $+$

$\varphi(A) \ni 1_B$

$\varphi(A)$ est stable par $\cdot_B$

soient $b, b' \in \varphi(A)$ $\quad b = \varphi(a)$

$b \cdot b' = \varphi(a) \cdot \varphi(a') = \varphi(a \cdot a') \in \varphi(A)$ $\quad b' = \varphi(a')$

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

= c'est le noyau d'un morphisme de gpes $(+)$

$\Rightarrow$ s'est un ss gpe de $(A, +)$

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

$a.k \, , \, k.a \in \ker \varphi$

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

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

$\square$

Rmq: $\ker(\varphi)$ n'est pas un ss-anneau

PROPOSITION 3.5. *Un morphisme d'anneaux* $\varphi \in \mathrm{Hom}_{Ann}(A, B)$ *est injectif ssi* $\ker(\varphi) = \{0_A\}$.

PROPOSITION 3.6. *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 : Exercice.

Notation 3.3. *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, endomorphismes, isomorphismes et automorphismes d'anneaux.

<u>Rmq</u> $\quad \mathrm{End}_{Ann}(A) \subset \mathrm{End}_{Gr}(A)$

$$\mathrm{Aut}_{Ann}(A) \subset \mathrm{Aut}_{Gr}(A)$$

Modules sur un Anneau

Définition 3.6. *Soit $(A,+,.)$ un anneau, un A-module (a gauche) est un groupe commutatif $(M,+)$ muni d'une loi de multiplication externe*

$$\bullet * \bullet : \begin{array}{ccc} A \times M & \mapsto & M \\ (a,m) & \mapsto & a * m \end{array}$$

(appellee multiplication par les scalaires) ayant les proprietes suivantes:

(1) *Associativite:* $\forall a, a' \in A,\ m \in M$,

$$(a.a') * m = a * (a' * m).$$

(2) *Distributivite:* $\forall a, a' \in A,\ m, m' \in M$,

$$(a + a') * m = a * m + a' * m,\ a * (m + m') = a * m + a * m'.$$

(3) *Neutralite de* 1_A: $\forall m \in M$,

$$1_A * m = m.$$

$a * \bullet : m \to a * m$ est un morphisme de gpe $(M,+)$

Rem: Module a droite:

$m * (a.a') = (m * a) * a'$

Exemples : $(A, +, \cdot)$

A est un A-module sur lui-même

$$A \times A \longrightarrow A$$
$$(a, a') \longrightarrow a * a' = a \cdot a'$$

$$A^d = \{(a_1, a_2, \dots, a_d) \quad a_i \in A \quad i = 1, \dots, d\}$$

A^d est un A module en posant

$$a * (a_1, a_2, \dots, a_d) = (a \cdot a_1, a \cdot a_2, \dots, a \cdot a_d) \in A^d$$

$(M,+)$ Groupe commutatif

a une structure canonique de $\mathbb{Z}$-module

$$(n \in \mathbb{Z}, m \in M) \longrightarrow n \underline{\cdot} m$$

$$= m + m + \dots + m \text{ (n fois) si } n > 0$$

$$= 0_M \quad \text{si } n = 0$$

$$= -(|n| \underline{\cdot} m) \quad \text{si } n < 0$$

opposé dans $(M,+)$

$\underline{\varphi : A \longrightarrow B}$ morphisme d'anneaux

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

$\ker \varphi \subset A$ c'est un A-module

- gpe commutatif
- $a * k = a . k \in \ker \varphi$

produit ds A

$\varphi : A \to B$ un morphisme d'anneau fait de B un A module.

$$A \times B \longrightarrow B$$
$$\varphi \ (a, b) \longrightarrow a \cdot_{\varphi} b = \varphi(a) \cdot_B b$$

En particulier la structure de $\mathbb{Z}$-module sur $(B,+)$ c'est la structure de $\mathbb{Z}$-module induite par $\mathrm{Can}_B : \mathbb{Z} \to B$.

$\mathcal{F}(X,A) = \{ f : X \to A \}$ est un gpe commutatif avec l'addition des fcts (et même un anneau) et de A module en posant $a * f : x \to a.f(x)$ $a \in A$

$\underline{a} \cdot f$

· $A[X]$ $a \in A$ $P(X) = a_0.X^0 + a_1 X^1 + \dots + a_d X^d$

A commut.

$a * P(X) = a.a_0 X^0 + a.a_1 X^1 + \dots + a.a_d X^d$

« $a.X^0 . P(X)$

$A[X]_{\leq d}$

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

$$\lambda \in A \qquad M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\lambda * M = \begin{pmatrix} \lambda . a & \lambda b \\ \lambda c & \lambda d \end{pmatrix} = \lambda I_2 \cdot M$$

$$\lambda I_2 = \begin{pmatrix} \lambda & 0_A \\ 0_A & \lambda \end{pmatrix}.$$

<u>Exo</u> : $(M,+)$ = A-module
= $\mathbb{Z}$-module (en $(M,+)$ est un gpe com)

Mq $\forall n \in \mathbb{Z} \quad \forall m \in M$

$$n_A * m = n \cdot m$$

$$n_A = \mathrm{Can}_A(n) = 1_A + \cdots + 1_A \text{ n fois}$$

En particulier $(-1_A) * m = -m$

Sous-module

DÉFINITION 3.8. *Soit M un A-module. Un sous-module $N \subset M$ d'un A-module M est un sous-groupe de $(M, +)$ qui est stable pour la multiplication par les scalaires:*

$$\forall a \in A,\ n \in N,\ a * n \in N.$$

On a donc $\forall n, n' \in N,\ a, a' \in A$

$$a * n + a' * n' \in N$$

combinaison linéaire de n et n'

On a le critere suivant

PROPOSITION 3.7. *(Critere de sous-module) Soit $N \subset M$ un sous-ensemble d'un A-module M alors N est un sous-module de M ssi*

non-vide

$$\forall a \in A,\ n, n' \in N,\ a * n + n' \in N. \tag{3.2.1}$$

Preuve : $\Longrightarrow$ évident

$\Longleftarrow$ on prend $a = -1_A$ on sait que

$\forall n, n' \in N \quad (-1)_A * n + n' \in N$

$= -n + n' = n' - n \in N$

$\Longrightarrow$ $(N,+)$ est un ssgpe

et $0_M \in N$ on applique l'hypothese

à $a \in A$ $n \in N$ $n' = 0_M \in N$

$a * n + 0_M \in N$

$a * n \in N$

$\square$

<u>Exemple</u> : M = A-mod

$\{0_M\}$, $A*m$, $A*m + A*m'$

$$A*m = \{ a*m \quad a \in A \} \subset M$$ est un ss module de M

$m, m' \in M$

$$A*m + A*m' = \{ a*m + a'*m' \quad a, a' \in A \} \subset M$$

est un ss module de M.

Ideal d'un Anneau

DÉFINITION 3.9. *Un ideal (a gauche) de A est un sous-ensemble $I \subset A$ de A qui est un sous-module du A-module A (pour la multiplication a gauche dans A). De maniere equivalente, un ideal de A est un sous-groupe additif $(I, +) \subset (A, +)$ qui est stable par multiplication (a gauche) par les elements de A:*

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

- *On defini de maniere analogue la notion d'ideal "a droite".*
- *Un sous-ensemble qui est un ideal a gauche et a droite est appele un ideal "bilatere".*

Ex: $\ker(\varphi : A \longrightarrow B) \subset A$ $\quad \varphi$ morphisme d'anneaux

$\ker \varphi$ est un ssgpe de $(A,+)$

$\forall k \in \ker\varphi \quad a \in A \qquad a.k \in \ker\varphi \qquad k.a \in \ker\varphi$

Question : quels sont les idéaux de $(\mathbb{Z}, +, \cdot)$?

- les $\mathbb{Z}.q = \{ n.q \quad n \in \mathbb{Z} \}$ $\quad q \in \mathbb{Z}$

  $q \in \mathbb{N}$

Module Engendré

Proposition 3.8. *Soit* $(M, +, *)$ *un* A*-module et* M_1, M_2 *des sous-modules* de M *alors*

$$M_1 \cap M_2 \subset M$$

est un sous-module et plus generalement soit $(M_i)_{i\in I}$ *une collection de sous-modules alors*

$$\bigcap_{i\in I} M_i \subset M$$

est un sous-module.

Définition 3.10. *Soit* $X \subset M$ *un sous-ensemble d'un* A*-module, le* A-*module engendre par* X *est le plus petit sous-module de* M *contenant* X *(l'intersection de tous les sous-modules contenant* X*):*

$$\langle X \rangle_A := \bigcap_{X\subset N\subset M} N.$$

N ssmodule de M

<u>Rmq</u> : $A = \mathbb{Z}$

les $\mathbb{Z}$-modules sont les gpes commutatifs

et $\langle X \rangle_A$ le $\mathbb{Z}$-module engendre par X

= le ssgpe engendre par X.

PROPOSITION 3.9. *Soit $X \subset M$ un ensemble alors $\langle X \rangle_A$ est soit le module nul $\{0_M\}$ si X est vide, soit l'ensemble des combinaisons lineaires d'elements de X a coefficients dans A:*

$$\langle X \rangle_A = \mathrm{CL}_A(X) := \{\sum_{i=1}^{n} a_i * x_i,\ n \geqslant 1,\ a_1, \cdots, a_n \in A,\ x_1, \cdots, x_n \in X\}.$$

"

$$a_1 * x_1 + a_2 * x_2 + \cdots + a_n * x_n$$

__Preuve__ : $\langle X \rangle_A = CL_A(X)$

Soit $N \subset M$ un sous module contenant X

comme est stable par $+$ et par $*$

Soient $x_1, \ldots, x_n \in X \subset N$ et $a_1, \ldots, a_n \in A$

par stabilité on a

$$a_1 * x_1 + a_2 * x_2 + \dots + a_n * x_n \in N$$

toute CL d'elements de X est dans N

$$CL_A(X) \subset N$$

$$\Rightarrow CL_A(X) \subset \langle X \rangle_A$$

pour mq $\langle X \rangle_A \subset CL_A(X)$

il suffit de mq $CL_A(X)$ est un sous-module contenant X.

$CL_A(X) \supset X$

$\forall x \in X \quad x = 1_A * x \in CL_A(X)$

On applique le critere de ss module

Soit $a \in A$ $\quad m, m' \in CL_A(X)$

$$m = a_1 * x_1 + \dots + a_n * x_n \qquad n, n' \geq 1$$

$$m' = a'_1 * x'_1 + \dots + a'_{n'} * x_{n'}$$

$$a * m + m' = a * (a_1 * x_1 + \dots + a_n * x_n)$$

$$+ a'_1 * x'_1 + \dots + a'_{n'} * x_{n'}$$

$$= (a \cdot a_1) \cdot x_1 + \dots + (a \cdot a_n) \cdot x_n$$

$$+ a_1' \cdot x_1' + \dots + a_{n'}' \cdot x_{n'}'$$

$=$ CL d'élts de X à coefs ds A

$\in CL_A(X) = A$-module contenant X

$$CL_A(X) \supset \langle X \rangle_A$$

$\square$

du A-module

DÉFINITION 3.11. *Si $\langle X\rangle_A = M$, on dit que X est une famille generatrice de M.*

DÉFINITION 3.12. *Un A-module M est de type fini si il possede une famille generatrice qui est finie.*

Exemples

A^d est engendre par $\{\vec{e}_1, \dots, \vec{e}_d\}$ = base canonique de A^d

$\vec{e}_1 = (1_A, 0_A, \dots, 0_A)$ $\vec{e}_2 = (0_A, 1_A, 0_A \dots)$

$\dots\dots \vec{e}_d = (0_A, 0_A, \dots, 1_A)$

position d.

$d=2$

$\forall\ (a,a') \in A^2$

$$(a,a') = a*(1_A, 0_A) + a'*(0_A, 1_A)$$
$$= a*\vec{e_1} + a'*\vec{e_2}.$$

$A[X]_{\leq d}$ est engendré par

$$\{X^0, X^1, X^2, \dots, X^d\}$$

$A[X]$ est engendré par

$$\left\{X^0, X^1, X^2, \dots\dots, X^d, X^{d+1}, \dots X^n, \dots\right\}_{n \geq 1}$$

n'est pas de type fini comme A-module.

- $A[X]$ est un anneau. donc $A[X]$ est un $A[X]$-module.

Comme $A[X]$-module

$A[X]$ est engendré par $X^0 = 1_A$

$= 1_{A[X]}$

si $P(X) \in A[X]$

$P(X) = P(X) . X^0$

$\langle \{X^0\} \rangle_{A[X]} = A[X]$

- $M = \mathbb{Z}^2$ si $ad - bc = \pm 1$ alors

$$\langle \{(a,b),(c,d)\} \rangle = \mathbb{Z}^2$$

$\mathbb{Z}^2$ est engendré par $\{(1,0),(0,1)\}$

si $(a,b),(c,d) \in \mathbb{Z}^2$ et tq $\underbrace{ad - bc = \pm 1}_{\in \mathbb{Z}^\times}$

alors $\{(a,b),(c,d)\}$ engendre $\mathbb{Z}^2$

Morphisme de Modules

Définition 3.13. *Soit A un anneau et M, N des A-modules, un morphisme de A-modules entre M et N est un morphisme de groupes*

$$\varphi : M \mapsto N$$

qui est compatible avec les lois de multiplications externes $*_M$ et $*_N$:

$$\forall a \in A,\ m \in M,\ \varphi(a *_M m) = a *_N \varphi(m).$$

Rmq: $\varphi(a *_M m + a' *_M m') =$

$= \varphi(a *_M m) + \varphi(a' *_M m')$

$= a *_N \varphi(m) + a' *_N \varphi(m')$

On dit que φ est A-lineaire.

LEMME 3.2. *(Critere d'application lineaire) Soit $\varphi : M \mapsto N$ une application entre deux A-modules alors φ est un morphisme (ie. est A-lineaire) si et seulement si*

$$\forall a \in A,\ m, m' \in M,\ \varphi(a *_M m + m') = a *_N \varphi(m) + \varphi(m'). \tag{3.2.2}$$

Preuve : si $a = 1_A$ $\varphi(1_A * m + m') = 1_A * \varphi(m) + \varphi(m')$

$$\varphi(m + m') = \varphi(m) + \varphi(m')$$

$\Longrightarrow$ φ est morphisme de gpes $+$

$\Longrightarrow$ $\varphi(0_M) = 0_N$ $\quad \varphi(a * m + 0_M) = a * \varphi(m)$

$$\varphi(a*m) = a * \varphi(m) + \cancel{\varphi(0_M)} \qquad \square$$

Noyau - Image

Proposition 3.10. *Soit $\varphi : M \mapsto N$ un morphisme de A-modules et $M' \subset M$ et $N' \subset N$ des sous-modules alors*

$$\varphi(M') \subset N \text{ et } \varphi^{(-1)}(N') \subset M$$

sont des sous-modules de M et N respectivement. En particulier

$$\ker(\varphi) = \varphi^{(-1)}(\{0_N\}) \subset M \text{ et } \mathrm{Im}(\varphi) = \varphi(M) \subset N$$

sont des sous A-modules.

A faire.

Corollaire 3.1. *L'application A-lineaire $\varphi : M \mapsto M'$ est injective ssi $\ker(\varphi) = \{0_M\}$.*

fait

Proposition 3.11. *Soient $\varphi : L \mapsto M$ et $\psi : M \mapsto N$ des morphismes de A-modules alors*

- $\psi \circ \varphi : L \mapsto N$ *est un morphisme de A-modules.*
- *Si $\varphi : L \mapsto M$ est bijectif alors $\varphi^{-1} : M \mapsto L$ est un morphisme de A-modules.*

Exercice

Notation 3.4. *On note*

$$\mathrm{Hom}_{A-mod}(M,N),\ \mathrm{Isom}_{A-mod}(M,N),$$
$$\mathrm{End}_{A-mod}(M) = \mathrm{Hom}_{A-mod}(M,M),$$
$$\mathrm{Aut}_{A-mod}(M) = \mathrm{GL}_{A-mod}(M) = \mathrm{Isom}_{A-mod}(M,M)$$

les ensembles de morphismes, morphismes bijectifs (ou isomorphismes), d'endomorphismes et d'automorphismes des A-modules M et N.

Corollaire 3.2. *L'ensemble* $\mathrm{Aut}_{A-mod}(M) \subset \mathrm{Bij}(M)$ *est un sous-groupe de* $\mathrm{Bij}(M)$. *Plus precisement* $\mathrm{Aut}_{A-mod}(M)$ *est un sous-groupe de* $Aut_{Gr}(M)$.

Proposition 3.12. *Soient M et N des A-modules alors $\mathrm{Hom}_{A-mod}(M, N)$ a une structure naturelle de groupe commutatif. Si de plus A est commutatif alors $\mathrm{Hom}_{A-mod}(M, N)$ a une structure naturelle de A-module.*

<u>Preuve</u> : $\varphi, \psi : M \to N$

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

Si φ et ψ sont A linéaires $\Rightarrow$ $\varphi + \psi$ est A-linéaire

$$(\varphi + \psi)(a * m + m') = \varphi(a * m + m') + \psi(a * m + m')$$

$$= a * \varphi(m) + \varphi(m') + a * \psi(m) + \psi(m')$$

$$= a * \left(\varphi(m) + \psi(m)\right) + \varphi(m') + \psi(m')$$

$$= a * (\varphi+\psi)(m) + (\varphi+\psi)(m')$$

$\varphi+\psi$ est A-linéaire.

Si A est commutatif.

$\mathrm{Hom}_A(M,N)$ est un A-module

la multiplication externe est la suivante

$$(a*\varphi) : m \longrightarrow a *_N \varphi(m)$$

$a*\varphi$ est linéaire.

$$a*\varphi(\alpha * m + m') =$$

$$a *_N (\varphi(\alpha * m + m')) = a *_N (\alpha *_N \varphi(m) + \varphi(m'))$$

$$= a * \alpha * \varphi(m) + a * \varphi(m')$$

$$= (a \cdot \alpha) * \varphi(m) + a * \varphi(m')$$

$$= (\alpha \cdot a) * \varphi(m) + a * \varphi(m')$$

$$= \alpha * (a * \varphi)(m) + (a * \varphi)(m')$$

$$\cdots\cdots\cdots\cdots \qquad \square$$