17/04/2007

III Anneaux et corps

1 Définitions et exemples

def un anneau est $(A,+,\perp)$ un ensemble muni de deux lois $+$ et $\perp$ t.q.

(1) $(A,+)$ est un groupe abélien, $+$ est dit addition de l'anneau
son neutre noté $0_A = 0$

(2) $\perp$ est associative

(3) $\perp$ a un élément neutre noté 1_A

(4) $\perp$ est distributive par rapport à $+$: $\forall a, b, c \in A$ on a

(i) $(a+b)\perp c = a\perp c + b\perp c$

(ii) $c\perp(a+b) = c\perp a + c\perp b$

$\perp$ est dit multiplication de l'anneau, souvent notée $\perp = \times$ (ou $\cdot$ ou rien)

un anneau est commutatif si sa multiplication est commutative

Exemples a) $(\mathbb{R},+,\times)$; $(\mathbb{Q},+,\times)$; $(\mathbb{Z},+,\times)$, $0 \neq N \in \mathbb{N}$ $(\mathbb{N}/_{\text{mod } N}, \bar{+}, \bar{\times})$
sont des anneaux commutatifs

b) $n \in \mathbb{N}\setminus\{0\}$. $(M_n(\mathbb{R}),+,\circ)$ matrices $n\times n$ avec l'addition des matrices et le produit des matrices est un anneau qui est commutatif si et seulement si $n=1$

Rmq quand les opérations sont claires on dit l'anneau A pour $(A,+,\perp)$

Lemme 1 Soit $(A,+,\times)$ un anneau alors $\forall a, b \in A$ on a

$$(i) \quad 0.a = 0 = a.0$$

$$(ii) \quad (-a).b = -(a.b) = a.(-b)$$

pv (i) $0 = 0.a - 0.a = (0+0).a - 0.a = (0.a + 0.a) - 0.a = 0.a + (0.a - 0.a) = 0.a + 0 = 0.a$

(ii) $0 = 0.b = (a + (-a)).b = a.b + (-a).b$ donc $(-a).b = -(a.b)$

Exercice $a.0 = 0$ et $a.(-b) = -(a.b)$

def un élément $a \in A$ d'un anneau A est $\begin{cases} \text{inversible} \\ \text{une unité de } A \end{cases}$

si il est inversible pour $\perp$: il y a $a' \in A$ tq $a \perp a' = 1_A = a' \perp a$

on note $A^* = \{a \in A ; a \text{ inversible}\}$

Exemples $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$; $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$; $\mathbb{Z}^* = \{-1, 1\}$; $M_2(\mathbb{R})^* = GL_2(\mathbb{R})$

Lemme et def Si A est un anneau A^* est stable par $\perp$ et $(A^*, \perp)$ est un groupe le groupe des unités de l'anneau A.

pv $a, b \in A^*$ a', b' inverses de a et b alors $b' \perp a'$ inverse de $a \perp b$

donc $a \perp b \in A^*$ et A^* stable par $\perp$

comme $\perp$ est associative sur A $\perp_1$ est associative sur A^*

$1 \in A^*$ et si $a \in A^*$ $a' \in A^*$ puisque $(a')' = a$ $\square$

<u>def</u> un <u>corps</u> est un anneau commutatif $(K,+,\times)$ tel que :

(1) $K^{*} = K \setminus \{0\}$ (un élément est inversible ssi il est non nul)

<u>Remarque</u> comme $1_K \in K^{*}$ on a $1_K \in K \setminus \{0_K\}$ donc $1_K \neq 0_K$ □

<u>Exemples</u> a) $\mathbb{R}, \mathbb{Q}, \mathbb{C}$; si $p \in \mathbb{N}$ est premier $\mathbb{N}/_{\text{mod } p} \simeq \mathbb{Z}/_{p\mathbb{Z}}$ sont des corps

b) $\mathbb{Z}$ n'est pas un corps

c) si $n > 1$ $M_n(\mathbb{R})$ n'est pas un corps 2 raisons

(1) $M_n(\mathbb{R})$ non commutatif

(2) $\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & & & \\ 0 & 0 & \cdots & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \end{pmatrix} = 0$ mais $\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & \cdots & & 0 \end{pmatrix} \neq 0 \neq \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \end{pmatrix}$

2 Sous-anneaux et morphismes d'anneaux

<u>def</u> un <u>sous-anneau</u> d'un anneau A est une partie $B \subset A$ contenant 1_A, stable par $+$ et $\times$ et t.q. muni des opérations induites $(B,+,\times)$ est un anneau.

<u>Lemme</u> Si B est un sous-anneau de A alors $1_B = 1_A$

pv $1_A \in B$ donc $1_A \underset{\uparrow}{=} 1_A \times 1_B \underset{\uparrow}{=} 1_B$

1_B unité de B $\quad$ 1_A unité de A

<u>Exercice</u> $C = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a,b \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$ est stable par $+$ et $\circ$

$(C,+,\circ)$ est un anneau mais $1_C = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq 1_A$

<u>Exemple</u> $\left\{\lambda Id_n = \begin{pmatrix}\lambda & 0 & \cdots & 0\\ 0 & \ddots & & \vdots\\ \vdots & & \ddots & 0\\ 0 & \cdots & 0 & \lambda\end{pmatrix} \,\middle|\, \lambda \in \mathbb{R}\right\}$ est un sous-anneau de $M_n(\mathbb{R})$

<u>def</u> un <u>morphisme d'un anneau</u> A <u>vers</u> un anneau B est $f : A \to B$ tq

$\forall x, y \in A$ (1) $f(x+y) = f(x) + f(y)$ (f morphisme de $(A,+)$ vers $(B,+)$)

(2) $f(x \cdot y) = f(x) \cdot f(y)$ (——— $(A,\times)$ — $(B,\times)$)

(3) $f(1_A) = 1_B$

<u>Exemples</u> a) $f : \mathbb{R} \to M_n(\mathbb{R})$, $f(\lambda) = \lambda Id_n = \begin{pmatrix}\lambda & 0 & \cdots & 0\\ 0 & \ddots & & \vdots\\ \vdots & & \ddots & 0\\ 0 & \cdots & 0 & \lambda\end{pmatrix}$

b) Si $A, B \in \mathbb{Z}$ $\mathbb{Z}/_{AB\mathbb{Z}} \to \mathbb{Z}/_{A\mathbb{Z}}$, $m + AB\mathbb{Z} \mapsto m + A\mathbb{Z}$

c) $Id_A : A \to A$ $a \mapsto a$

<u>Lemme</u> Soit $f : A \to B$ et $g : B \to C$ des morphismes d'anneau alors $g \circ f : A \to C$ est un morphisme d'anneau. □

pv c'est un morphisme pour les lois $+$ et $\times$

$$g \circ f(1_A) = g(f(1_A)) = g(1_B) = 1_C \quad \square$$

<u>def</u> un <u>isomorphisme</u> d'un anneau A sur un anneau B est un morphisme d'anneau $f : A \to B$ tel qu'il y a un morphisme d'anneau $g : B \to A$ avec $g \circ f = Id_A$ et $f \circ g = Id_B$

<u>Rmq</u> un isomorphisme d'anneau est bijectif et $g = f^{-1}$

<u>Lemme</u> Soit $f : A \to B$ un morphisme d'anneau bijectif alors $f^{-1} : B \to A$ est un morphisme d'anneau. En particulier f est un isomorphisme

pv : Exercice □

__def__ Soit A et B deux anneaux. L'anneau produit $A\times B$ est l'ensemble $A \times B$ muni de l'addition et de la multiplication composante par composante. Ainsi si C est un anneau et $f : C \to A$, $g : C \to B$ alors $(f,g) : C \to A\times B$ $c \mapsto (f(c), g(c))$ est un morphisme d'anneaux ssi f et g sont des morphismes d'anneaux

__Corollaire__ Soit $M, N \in \mathbb{N}$ alors $\mathbb{Z}/_{MN\mathbb{Z}} \to \mathbb{Z}/_{M\mathbb{Z}} \times \mathbb{Z}/_{N\mathbb{Z}}$ est un isomorphisme d'anneaux ssi M et N sont premiers entre eux. En particulier si M et N sont premiers entre eux $\mathbb{Z}/_{MN\mathbb{Z}} \to \mathbb{Z}/_{M\mathbb{Z}} \times \mathbb{Z}/_{N\mathbb{Z}}$ induit un isomorphisme de groupe $\left(\mathbb{Z}/_{MN\mathbb{Z}}\right)^* \to \left(\mathbb{Z}/_{M\mathbb{Z}}\right)^* \times \left(\mathbb{Z}/_{N\mathbb{Z}}\right)^*$

pv $\mathbb{Z}/_{MN\mathbb{Z}} \to \mathbb{Z}/_{M\mathbb{Z}} \times \mathbb{Z}/_{N\mathbb{Z}}$ est un morphisme d'anneaux bijectif ssi le morphisme de groupe $(\mathbb{Z}/_{MN\mathbb{Z}}, +) \to (\mathbb{Z}/_{M\mathbb{Z}}, +) \times (\mathbb{Z}/_{N\mathbb{Z}}, +)$ est bijectif donc (Théorème chinois) ssi M et N premiers entre eux. $\square$

Comme la multiplication de $(\mathbb{Z}/_{M\mathbb{Z}}) \times (\mathbb{Z}/_{N\mathbb{Z}})$ est composante par composante $\left(\mathbb{Z}/_{M\mathbb{Z}} \times \mathbb{Z}/_{N\mathbb{Z}}\right)^* = \left(\mathbb{Z}/_{M\mathbb{Z}}\right)^* \times \left(\mathbb{Z}/_{N\mathbb{Z}}\right)^*$ d'où le en particulier $\square$

Exemple $\left(\mathbb{Z}/_{12\mathbb{Z}}\right)^*$ isomorphe à $\left(\mathbb{Z}/_{3\mathbb{Z}}\right)^* \times \left(\mathbb{Z}/_{4\mathbb{Z}}\right)^*$

$$= \left(\{1,2\}, \begin{matrix} 1\times 1 = 1 = 2\times 2 \\ 1\times 2 = 2 = 2 \times 1\end{matrix}\right) \times \left(\{1,3\}, \begin{matrix} 1\times 1 = 1 = 3\times 3 \\ 1\times 3 = 3 = 3\times 1\end{matrix}\right)$$

isomorphe à $(\mathbb{Z}/_{2\mathbb{Z}}, +) \times (\mathbb{Z}/_{2\mathbb{Z}}, +)$

__Exercice__ $\left(\mathbb{Z}/_{15\mathbb{Z}}\right)^*$ isomorphe à $\left(\mathbb{Z}/_{3\mathbb{Z}}\right)^* \times \left(\mathbb{Z}/_{5\mathbb{Z}}\right)^*$ isomorphe à $(\mathbb{Z}/_{2\mathbb{Z}}, +) \times (\mathbb{Z}/_{4\mathbb{Z}}, +)$

3 Anneau des matrices $n \times n$ sur un anneau A

def Soit A un anneau et $n \in \mathbb{N} \setminus \{0\}$ un entier positif

$$M_n(A) = \{(a_{ij})_{1 \le i,j \le n} \mid a_{ij} \in A\} \text{ muni de}$$

$$(a_{ij})_{1 \le i,j \le n} + (b_{ij})_{1 \le i,j \le n} = (a_{ij} + b_{ij})_{1 \le i,j \le n}$$

$$(a_{ij})_{1 \le i,j \le n} \cdot (b_{ij})_{1 \le i,j \le n} = \left(\sum_{k=1}^{n} a_{ik} b_{kj}\right)_{1 \le i,j \le n}$$

est un anneau d'unité $1_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \vdots & \ddots & & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix} = (a_{ij})_{1 \le i,j \le n}$ $\quad i \neq j \; a_{ij} = 0$, $a_{ii} = 1$

pr ~~Le~~ calcul fait en M111 ~~dans~~ le cas $A = \mathbb{R}$ n'a utilisé que les propriétés d'anneau de $\mathbb{R}$

Dans la suite on se limite au cas $n = 2$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a+\alpha & b+\beta \\ c+\gamma & d+\delta \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix}$$

Lemme Soit A un anneau commutatif alors $\sim : M_2(A) \to M_2(A)$, $\widetilde{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ est un anti-automorphisme c'est à dire $\forall M, N \in M_2(A)$ on a

(1) $\widetilde{M+N} = \tilde{M} + \tilde{N}$, (2) $\widetilde{MN} = \tilde{N}\tilde{M}$, (3) $\widetilde{Id_2} = Id_2$

pv. (1) et (3) exercice

(2) $\widetilde{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}} = \widetilde{\begin{pmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{pmatrix}} = \begin{pmatrix} c\beta+d\delta & -(a\beta+b\delta) \\ -(c\alpha+d\gamma) & a\alpha+b\gamma \end{pmatrix} = \begin{pmatrix} \delta d+\beta c & -(\delta b+\beta a) \\ -(\gamma d+\alpha c) & \gamma b+\alpha a \end{pmatrix}$

$\widetilde{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}}\widetilde{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} \delta d+(-\beta)(-c) & \delta(-b)+(-\beta)a \\ (-\gamma)d+\alpha(-c) & (-\gamma)(-b)+\alpha a \end{pmatrix} = \begin{pmatrix} \delta d+\beta c & -(\delta b+\beta a) \\ -(\gamma d+\alpha c) & \gamma b+\alpha a \end{pmatrix}$ $\square$

on suppose dorénavant l'anneau A commutatif

4 <u>def</u> $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad-bc$ ainsi $\det\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$

<u>Lemme</u> $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\widetilde{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \widetilde{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = (ad-bc)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

pv $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad+b(-c) & a(-b)+ba \\ cd+d(-c) & c(-b)+da \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & -bc+da \end{pmatrix}$

A commutatif ⇒ ‖

$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} da+(-b)c & db+(-b)d \\ (-c)a+ac & (-c)b+ad \end{pmatrix} = \begin{pmatrix} da-bc & 0 \\ 0 & ad-bc \end{pmatrix} \overset{\downarrow}{=} \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$ $\square$

<u>Corollaire</u> $\det(MN) = \det(M)\det(N)$

pv $\det(MN)I_2 = \widetilde{MN}\,MN = (\tilde{N}\tilde{M})MN = \tilde{N}(\tilde{M}M)N = \tilde{N}\det(M)I_2N = \det(M)\tilde{N}N$

$= \det(M)\det(N)I_2$ d'où $\det(MN) = \det(M)\det(N)$ $\blacksquare$

<u>Cocorollaire</u> $M_2(A)^* = \{M \in M_2(A) \mid \det(M) \in A^*\}$

pv ⊆ : $M \in M_2(A)^*$ et N tq $M.N = I_2$ d'où $1 = \det(M)\det(N) \Rightarrow \det M \in A^*$

car A commutatif

⊇ $M \times (\det(M))^{-1}(\tilde{M}) = \overset{\text{H ‖}}{\det(M)^{-1}} M\times\tilde{M} = \det(M)^{-1}\det M\, I_2 = I_2$

$((\det M)^{-1}\tilde{M})M = (\det(M))^{-1}\tilde{M}\times M = (\det M)^{-1}\det(M)I_2 = I_2$ $\blacksquare$

4 Identités remarquables commutatives

Ce sont des relations entre lettres + et × qui, quand on substitue aux lettres des éléments d'un anneau A commutatif donnent une relation vraie dans A

Formule du binôme Soit n un entier positif $a, b \in A$ alors

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

où $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ et les coefficients du binôme vérifient

$$\binom{0}{0} = 1, \quad \binom{n}{n} = 1 \quad 0<k<n \quad \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k-1}$$

par récurrence sur n $\quad n = 1 \quad (a+b)^1 = a+b$

$$\sum_{k=0}^{1} \binom{1}{k} a^{n-k} b^k = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a+b$$

$$(a+b)^{n+1} = (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1}$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{\ell=1}^{n+1} \binom{n}{\ell-1} a^{n+1-\ell} b^\ell =$$

$\ell = k+1$

$$= \binom{n}{0} a^{n+1-0} b + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1}\right) a^{n+1-k} b^k + \binom{n}{n} a^{n+1-(n+1)} b^{n+1}$$

$$= \binom{n+1}{0} a^{n+1} b^0 + \sum_{k=1}^{n} \binom{n+1}{k} a^{n+1-k} b^k + \binom{n+1}{n+1} a^0 b^{n+1} = \sum_{\ell=0}^{n+1} \binom{n+1}{\ell} a^{n+1-\ell} b^\ell \quad \square$$

Formule de telescopage Soit n un entier positif, $a, b \in A$ alors

$$a^{n+1} - b^{n+1} = (a-b)\sum_{k=0}^{n} a^{n-k} b^{k}$$

pv Exercice

multiplicativité du determinant $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $N = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(A)$

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

$$(a\alpha + b\gamma)(c\beta + d\delta) - (a\beta + b\delta)(c\alpha + d\gamma) = (ad - bc)(\alpha\delta - \beta\gamma) \quad \square$$

def La trace de $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(A)$ est $T_r(M) = a + d$

Théorème Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(A)$ alors

$$M^2 - T_r(M) M + \det(M) I_2 = 0$$

pv $M^2 - T_r(M) I + \det(M) I_2 = M \times M - T_r(M) I_2 \times M + \tilde{M} \times M$

$$= \left(M - T_r(M) I_2 + \tilde{M}\right) \times M = \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix} + \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\right) M$$

$$= 0 \cdot M = 0 \quad \square$$