

Soit $(A_i, +_i, \cdot_i)$ des anneaux

i. Alors $A = \prod_{i=1}^n A_i = A_1 \times A_2 \times \dots \times A_n$
 est un anneau muni des lois

$$\forall X = (x_1, \dots, x_n) \in A, \quad Y = (y_1, \dots, y_m) \in A, \quad (x_i \in A_i)$$

$$x+y = (x_1+y_1, \dots, x_n+y_n)$$

$$O_A = (O_{A1}, O_{A2}, \dots, O_{An})$$

$$O_A = (O_{A_1}, O_{A_2}, \dots, O_{A_n})$$

$$A = (a_1, \dots, a_n)$$

$X = (x_1, \dots, x_n)$ est univers. dans A

$\Rightarrow (x_n)_{n \in \mathbb{N}}$ est convergente. $\forall n \in \mathbb{N}$

$$X^{-1} = (x_1^{-1}, \dots, x_n^{-1})$$

Diocesi

Definição

$$L(A) = \prod_{i=1}^n L(A_i)$$

Def. $f(1_A) = 1_B$
 $\forall x, y \in A$
 $f(x+y) = f(x) + f(y)$
 $f(x \cdot y) = f(x) \cdot f(y)$

f est un morphisme de groupes de $(A, +) \rightarrow (B, +)$
 $\ker f$ est un idéal de A avec A commutatif
 n'est pas pour anneaux de A . Car $1_A \notin \ker f$.

$f: (A, +_A, \cdot_A) \rightarrow (B, +_B, \cdot_B)$
 est un morphisme d'anneaux

$\text{Im } f$ est un sous-anneau de B

$\forall x \in A$
 $f(nx) = nf(x), n \in \mathbb{Z}$
 $f(x^n) = (f(x))^n, n \in \mathbb{N}$
 Si x est inversible $\Rightarrow f(x)$ inversible
 $f(x^{-1}) = (f(x))^{-1}$
 $\Rightarrow f(x^n) = (f(x))^n, n \in \mathbb{Z}$

Si f morphisme de corps
 f injectif $\Leftrightarrow \ker f = \{0_A\}$
 f surj $\Leftrightarrow \text{Im } f = B$
 f bijectif $\Leftrightarrow f$ isom.

Alors f injective ou $f=0$.
 Car $\ker f$ idéal de $A = \text{corps}$
 $\Rightarrow \ker f = \{0_A\}$ ou $\ker f = A$.

$f: (U(A), +) \rightarrow (U(B), +)$
 est un morphisme de groupes

$f(U(A)) \subset U(B)$

Si f est bijective, alors
 $f(U(A)) = U(B)$
 $\Rightarrow U(B) \subset f(U(A)) \subset U(A)$

Exercice 3.

4) ii) p : premier, $\forall x \in (\mathbb{Z}/p\mathbb{Z})^*$.

on a $(\bar{x})^{p-1} = \bar{1}$

on a $(\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z})^*, x)$
c'est un groupe.

et $\text{Card}(\mathbb{Z}/p\mathbb{Z})^* = p-1$
 $\Rightarrow \forall \bar{x} \in (\mathbb{Z}/p\mathbb{Z})^* \Rightarrow (\bar{x})^{p-1} = \bar{1}$

$\Leftrightarrow \bar{x} \equiv 1(p)$.

5/a) $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre en général
Donc $\mathbb{Z}/n\mathbb{Z}$

$\frac{0}{0} \neq \frac{1}{1} = \bar{1} = \bar{0}$.

Exercice 5.

Partie I.

I idéal non nul de $(K[X]) \Leftrightarrow \exists !$ polynôme P unitaire de degré minimal tq $I = P \cdot (K[X])$

Eneffet

" $\Leftarrow$ " si $I = P \cdot (K[X]) \Rightarrow I$ idéal de $(K[X])$

" $\Rightarrow$ " $A = \{ \deg P \mid P \in I, P \neq 0 \}$

on a $I \neq \{0\} \Rightarrow \exists P_0 \in I, P_0 \neq 0 \Rightarrow \deg P_0 \in A$

$\Rightarrow A \neq \emptyset$

et $A \subset \mathbb{N} \Rightarrow \min A$ existe, soit $k = \min A$.

$\exists \bar{\varphi} \in I, \bar{\varphi} \neq 0$ tq $\deg \bar{\varphi} = k$

$\Rightarrow \forall \varphi = \frac{\bar{\varphi}}{\bar{\varphi}}$

$\deg \varphi = k$ $\Rightarrow \varphi \in I$ (Idéal)

$$\text{ex. } I = \Phi(K[x]).$$

$$\text{ma. } \Phi \in I \Rightarrow \Phi(K[x]) \subset I$$

$$\text{"J" soit } \Phi \in I \Rightarrow \text{divi. } P = \Phi \cdot H + R \text{ avec } 0 \leq \deg R < k$$

$$\text{supp. } R \neq 0.$$

$$\Rightarrow R = \underbrace{P}_{\in I} - \underbrace{\Phi \cdot H}_{\in I} \in I \text{ (Ideal)}$$

$$\Rightarrow \deg R \in \mathbb{A}$$

$$\Rightarrow R = 0 \Rightarrow \deg R \geq k \text{ also.}$$

$$\text{Dici } I = \Phi(K[x]) \Rightarrow I \subset \Phi(K[x])$$

univ.:
 supp $\exists H \in K[x]$ unitaire s.t.

$$I = H \cdot K[x]$$

$$\Phi(K[x])$$

$$\Rightarrow \varphi/H \text{ et } H/\varphi$$

$$\Rightarrow \varphi = \alpha H$$

$$\text{or } \varphi \text{ et } H \text{ sont unitaires} \left\{ \Rightarrow \alpha = 1 \right.$$

$$\Rightarrow \varphi = H$$

$$\text{II)} \text{ donn } E \hookrightarrow \dots; u \in \mathcal{L}(E) \\ x \neq 0_E.$$

$$I_x = \{ P \in K[X] \mid P(u)(x) = 0_E \}$$

$$1) \cdot I_x \subset K[X]$$

$$\text{on } X_u(u) = \vec{0} \Rightarrow X_u(u)(x) = 0_E.$$

$$\text{et } \deg X_u = n \Rightarrow X_u \neq \vec{0}.$$

$$\Rightarrow I_x \neq \{0\}.$$

soit

$$P, \varphi \in I_x$$

$$(P - \varphi)(u)(x) = P(u)(x) - \varphi(u)(x) \\ = 0$$

$$\Rightarrow P, \varphi \in I_x.$$

$$\text{soit } P \in I_x \text{ et } H \in K[X]$$

$$(P \cdot H)(u)(x) = H(u)(P(u)(x)) = 0_E$$

$$\Rightarrow P \cdot H \in I_x.$$

Ainsi, I_x est un idéal de $K[X]$.

2) I_x idéal non nul de $K[X]$
d'après 1) $\exists$! polynôme unitaire de degré minimal P tel que $I_x = \pi_{x,u} K[X]$.

$$\text{et } \pi_{x,u} \in I_x \Rightarrow \pi_{x,u}(u)(x) = 0_E.$$

$$\text{si } P \in I_x \Rightarrow \pi_{x,u} / P$$

$$P(u)(x) = 0_E.$$

$$\text{on not } \overline{P} = \pi_{x,u}$$

ona. $\pi_U(u) = 0 \Rightarrow \pi_U(u)(x) = 0_E$.

$\Rightarrow \pi_U \in I_x \Rightarrow \pi_x / \pi_U$

$\{\pi_x; x \in E \setminus \{0\}\} \subset \left\{ \begin{array}{l} \text{diviseurs. de } \pi_U \\ \text{unitaires.} \end{array} \right\}$

4) $(x, y) \in E \setminus \{0\} \wedge \pi_x \wedge \pi_y = 1$ " fini

Pq. $x+y \neq 0_E$ et q.u. $\pi_{x+y} = \pi_x \cdot \pi_y$.

Supp. $x+y = 0_E \Rightarrow x = -y$.

ona. $\pi_x(u)(x) = 0_E \Rightarrow \pi_x(u)(-y) = 0$

$\Rightarrow \pi_x(u)(y) = 0 \Rightarrow \pi_x \in I_y \Rightarrow \pi_y / \pi_x$.

Supp. $\pi_y = 1 \Rightarrow \pi_y(u) = 1_E \Rightarrow \pi_y(u)(y) = y$ " fini

$\Rightarrow \pi_y / \pi_x$ et $\pi_y \neq 1$

absur.

absur.

Alors $x+y \notin \mathcal{O}_E$.

129. $\pi_{x+y} = \pi_x \cdot \pi_y$.

ora. $(\pi_x \cdot \pi_y | \omega)(x+y) =$

$$(\pi_x \cdot \pi_y | \omega)(x) + (\pi_x \cdot \pi_y | \omega)(y)$$

$$= 0 \in \mathcal{O}_E.$$

" $\mathcal{O}_E$."

$$\Rightarrow (\pi_x \cdot \pi_y | \omega)(x+y) = 0 \in \mathcal{O}_E.$$

$$\Rightarrow \pi_x \cdot \pi_y \in \mathcal{I}_{x+y} \Rightarrow \pi_{x+y} | \pi_x \cdot \pi_y. \textcircled{1}$$

D'autre part ora.

$$\pi_{x+y}(\omega)(x+y) = 0 \in \mathcal{O}_E \Leftrightarrow \pi_{x+y}(\omega)(x) = -\pi_{x+y}(\omega)(y)$$

$$\Rightarrow \pi_x(\omega) \left(\pi_{x+y}(\omega)(x) \right) = -\pi_x(\omega) \left(\pi_{x+y}(\omega)(y) \right)$$

" $\mathcal{O}_E$."

$$\Rightarrow \pi_x \cdot \pi_{x+y}(\omega)(y) = 0$$

$$\Rightarrow \pi_y | \pi_x \cdot \pi_{x+y}$$

Gauss

$$\pi_y \wedge \pi_x = 1 \Rightarrow \pi_y | \pi_{x+y}$$

x et y jouent les rôles inverses.

$$\Rightarrow \pi_x | \pi_{x+y}$$

$$\pi_x \wedge \pi_y = 1 \Rightarrow \pi_x \cdot \pi_y | \pi_{x+y} \textcircled{2}$$

1292

$$\Rightarrow \pi_{x+y} = \pi_x \cdot \pi_y.$$

Exercice 8, $n \in \mathbb{N}^*$.

$$\varphi(n) = \text{Card.} \{ 1 \leq k \leq n : k \wedge n = 1 \}$$

$$= \text{Card.} \{ k \in \mathbb{Z}/n\mathbb{Z} \}$$

1) p : premier.

$$\varphi(p) = \text{card}(\mathbb{Z}/p\mathbb{Z}) = p-1$$

$$\varphi(p^\alpha) = \text{Card.} \{ 1 \leq k \leq p^\alpha : p^\alpha \wedge k = 1 \}$$

$$= p^\alpha - \text{Card.} \{ 1 \leq k \leq p^\alpha : p^\alpha \wedge k \neq 1 \}$$

$$\text{or } p^\alpha \wedge k \neq 1 \Rightarrow p/k \Rightarrow k = p \cdot \alpha \text{ avec } \alpha \in \mathbb{Z}/p\mathbb{Z} \setminus \{1\}$$

$$\Rightarrow \text{Card.} \{ 1 \leq k \leq p^\alpha : p^\alpha \wedge k \neq 1 \} = p^\alpha - p^{\alpha-1}$$

$$\Rightarrow \varphi(p) = p - p^0 = p - 1$$

$d) m \wedge n = 1$
 $f: (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \rightarrow (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$
 $x \mapsto f(x) = (\tilde{x}, \tilde{x})$

a) πq f est bien défini.

• Soit $\tilde{x}, \tilde{y} \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ tq $\tilde{x} = \tilde{y}$.

$\Rightarrow x \equiv y (n.m) \Leftrightarrow n.m | x - y$
 $\Rightarrow n | x - y$ et $m | x - y$.

$\Rightarrow \tilde{x} = \tilde{y}$ et $\tilde{x} = \tilde{y} \Rightarrow f(\tilde{x}) = f(\tilde{y})$.

• $\forall \tilde{x} \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $f(\tilde{x}) = (\tilde{x}, \tilde{x}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$
 $\Rightarrow f$ est bien défini.

$b) f(\tilde{x}) = (\tilde{x}, \tilde{x}) = \tilde{x} \cdot \tilde{x} \pmod{n.m}$
 $f(\tilde{x} + \tilde{y}) = f(\tilde{x} + \tilde{y})$

$= (\tilde{x} + \tilde{y}, \tilde{x} + \tilde{y})$
 $= (\tilde{x} + \tilde{y}, \tilde{x} + \tilde{y})$
 $= (\tilde{x}, \tilde{x}) + (\tilde{y}, \tilde{y})$
 $= f(\tilde{x}) + f(\tilde{y})$

$\star f(\tilde{x} \cdot \tilde{y}) = f(\tilde{x}) + f(\tilde{y})$
 $\Rightarrow f$ multiplicative.

• Soit $\tilde{x} \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ tq $f(\tilde{x}) = (\tilde{0}, \tilde{0})$

$\Leftrightarrow \begin{cases} \tilde{x} = \tilde{0} \\ \text{et } \tilde{x} = \tilde{0} \end{cases} \Leftrightarrow \begin{cases} n | x \\ \text{et } m | x \end{cases}$
 $\Leftrightarrow n \wedge m = 1 \Rightarrow n.m | x$
 $\Rightarrow \tilde{x} = \tilde{0}$

$\Rightarrow \ker f = \{0\} \Rightarrow f$ injective.

$$\text{etona card}(\mathbb{Z}/nm\mathbb{Z}) = n \cdot m \\ = \text{card}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$$

$\Rightarrow f$ is bijective.

c) isomorphism, also.

$$f(\cup(\mathbb{Z}/nm\mathbb{Z})) = \cup(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$$

$$\begin{aligned} \Rightarrow \text{card}(f(\cup(\mathbb{Z}/nm\mathbb{Z}))) &= \text{card}(\cup(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})) \\ &\stackrel{f \text{ bi}}{=} \text{card}(\cup(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})) \\ &= \text{card}(\mathbb{Z}/n\mathbb{Z}) \times \text{card}(\mathbb{Z}/m\mathbb{Z}) \\ &\Rightarrow \varphi(n \cdot m) = \varphi(n) \cdot \varphi(m). \end{aligned}$$

$$g.) \quad n = \prod_{i=1}^N p_i^{d_i}$$

$$\Rightarrow \varphi(n) = \prod_{i=1}^N \varphi(p_i^{d_i})$$

$$= \prod_{i=1}^N (p_i^{d_i} - p_i^{d_i-1}) = \prod_{i=1}^N p_i^{d_i-1} (p_i - 1)$$

Def

$+, \times$ z.l.c. i
l.e.e.

$(A, +, \times)$ anneau.

$(A, +, \cdot)$ est un k.e.u.

$\forall d \in K; d \cdot (x \cdot y) = (d \cdot x) \cdot y = x \cdot (d \cdot y)$

Exemples

$(R, +, \times, \cdot)$ est un R-algèbre.

$(\mathbb{C}, +, \times, \cdot)$ est un $\mathbb{C}$ -algèbre

$(K[X], +, \times, \cdot)$ est un K -algèbre

$(M_n(K), +, \times, \cdot)$ " " "

$(\mathcal{A}(E), +, \cdot, 0, 1)$ " " "

B sous algèbre de A .

$B \subset A$.

$(B, +, \times)$ sous anneau

$(B, +, \cdot) \text{ s.e.u.}$

$(A, +, \times, \cdot)$ est une

K -algèbre.

Exp. Soit $U \in \mathcal{X}(E)$

$K[U] = \{ P(U); P \in K[X] \}$ s. algèbre commutative de $\mathcal{A}(E)$

$A \in M_n(K)$

$K[A] = \{ P(A); P \in K[X] \}$ s. algèbre commutative de $M_n(K)$

$D_n(K) = \{ \text{matrices diagonales} \}$

$T_n(K) = \{ \text{matrices triangulaires sup} \}$

$\varphi: (A, +, \times, \cdot) \rightarrow (B, +, \times, \cdot)$ morphisme d'algèbre

$\varphi(1_A) = 1_B$
 $\varphi(d \cdot x \cdot y) = d \cdot \varphi(x) \cdot \varphi(y)$
 $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$

$B \subset A$.

$1_A \in B$

$\forall x, y \in B, \forall d \in K$

$d \cdot x \cdot y \in B$

$x \cdot y \in B$

Exemples: $\mathbb{R}$ -algèbre.

1) $f: (\mathbb{C}, +, \cdot) \rightarrow (\mathbb{C}, +, \cdot)$
 $z \mapsto \bar{z}$

2) $u \in \pi(E)$ morphisme d'algèbre

$g: K[X] \rightarrow (\mathcal{L}(E), +, \circ, \cdot)$
 $P \mapsto g(P) = P(u)$

est un morphisme d'algèbre ...

$g(1) = \text{id}_E$

$g(P \times Q)(u) = P(u) \circ Q(u)$

$g(dP \times Q)(u) = dP(u) + Q(u)$

$\ker g = \{ P \in K[X] \mid P(u) = 0 \}$
 $= \text{Idéal } P \text{ de } K[X]$

3) Soit $E < \infty$, $B = \text{base de } E$
L'app. $\varphi: (\mathcal{L}(E), +, \circ, \cdot) \rightarrow (\pi_n(K), +, \cdot)$
 $u \mapsto \varphi(u) = \text{Mat}(u, B)$
est un morphisme d'algèbre.