

Correction " Anneau-Corps-Algèbre "

Exercice 1

1)  $f: (A, +, \times) \longrightarrow (B, +, \times)$  un morphisme d'anneau

$$\begin{cases} f(1_A) = 1_B \\ f(x+y) = f(x) + f(y), \forall (x, y) \in A^2 \\ f(xy) = f(x) \cdot f(y) \end{cases}$$

i)  $f(0_A + 0_A) = f(0_A) + f(0_A) \Rightarrow f(0_A) = 0_B$

$f(0_A) = 0_B$

ii) soit  $x \in A$ :  $f(-x + x) = f(-x) + f(x) \Rightarrow f(0_A) = 0_B$

$\Rightarrow f(-x) = -f(x)$

iii) on vérifie par récurrence que  $\forall k \in \mathbb{N}$ :  $f(kx) = kx$

Si  $k \in \mathbb{Z}^-$ , alors  $-k \in \mathbb{N}$ , d'où  $f(-kx) = -kx$

or  $f(-kx) = -f(kx)$

d'où  $f(kx) = kx$

iv) par récurrence,  $f(x^k) = (f(x))^k$

v) si  $x$  inversible dans  $A \Leftrightarrow$

$x \cdot x^{-1} = 1_A$

$\Rightarrow f(x \cdot x^{-1}) = f(x) \cdot f(x^{-1})$

$\Rightarrow f(1_A) = 1_B$

$\Rightarrow f(x)$  est inversible avec  $(f(x))^{-1} = f(x^{-1})$

2) a)  $\ker f$  est un idéal de  $A$ .

avec  $A$  un anneau commutatif.

a) on ~~est~~ un morphisme d'anneau, alors  $f$  est un morphisme de groupes

d'où  $\ker f$  est un sous groupe de  $A$

$f(0_A) \in \ker f$  ①

$\Rightarrow \forall x, y \in \ker f \Rightarrow x - y \in \ker f$  ②

• Soient  $a \in A$  et  $x \in \ker f$

$f(ax) = f(a) \cdot f(x) = f(a) \cdot 0_B = 0$   
 $\Rightarrow f(ax) = 0$

$$\Rightarrow a \cdot x = x a \in \ker f. \textcircled{1}$$

1+2+3  $\Rightarrow \ker f$  est un idéal de  $A$ .

b)  $\Pi q \operatorname{Im} f$  est un sous-anneau de  $B$

$$\cdot \operatorname{Im} f \in B \quad \cdot 1_B = f(1_A) \in \operatorname{Im} f$$

$\cdot f$  morphisme de groupe  $\Rightarrow$

$\operatorname{Im} f$  est un  $\Lambda$ -g de  $B$

$\cdot$  Soit  $y_1 \in \operatorname{Im} f, y_2 \in \operatorname{Im} f$

$$\downarrow \quad \downarrow$$

$$\exists x_1 \in A \text{ tq } y_1 = f(x_1) \quad \exists x_2 \in A \text{ tq } y_2 = f(x_2)$$

$$y_1 \cdot y_2 = f(x_1) \cdot f(x_2) = f(x_1 \cdot x_2) \in \operatorname{Im} f$$

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

c) Soient  $I$  et  $J$  deux idéaux de  $A$

$\Pi q I \cap J$  est un idéal de  $A$ .

$\cdot 0_A \in I$  et  $0_A \in J \Rightarrow 0_A \in I \cap J$

$\cdot$  Soient  $x, y \in I \cap J$

$$\Rightarrow x, y \in I \Rightarrow x+y \in I \quad (\text{set } I \text{ idéal})$$

$$x, y \in J \Rightarrow x+y \in J \quad (\text{set } J \text{ idéal})$$

Soit  $x, y \in I \cap J$  et  $a \in A$

$$\Rightarrow \begin{cases} x \in I \\ y \in J \end{cases} \Rightarrow \begin{cases} a \cdot x = x a \in I \\ a \cdot y = y a \in J \end{cases} \quad (\text{set } I, J \text{ idéaux})$$

$$\Rightarrow x a = a x \in I \cap J$$

Ainsi  $I \cap J$  est un idéal de  $A$ .

Exercice 2.

$$x \text{ nilpotent} \Leftrightarrow \exists n \in \mathbb{N}^* \text{ tq } x^n = 0$$

$$y \text{ " " } \Leftrightarrow \exists p \in \mathbb{N}^* \text{ tq } y^p = 0$$

$$\cdot \text{ On a } (xy)^n = x^n \cdot y^n = 0$$

D'où  $xy$  est nilpotent

$$(x+y)^{n+p} = \sum_{k=0}^{n+p} C_{n+p}^k x^k y^{n+p-k}$$

$$= \sum_{k=0}^n C_{n+p}^k x^k y^{n+p-k} + \sum_{k=n+1}^{n+p} C_{n+p}^k x^k y^{n+p-k}$$

$$\text{Si } 0 \leq k \leq n \Rightarrow p \leq n+p-k \leq n+p$$

$$\Rightarrow y^{n+p-k} = 0$$

$$\cdot \text{ Si } n+1 \leq k \leq n+p \Rightarrow x^k = 0$$

On déduit que  $(x+y)^{n+p} = 0$

$\Rightarrow x+y$  est nilpotent.

$$x \text{ nilpotent} \Leftrightarrow \exists n \in \mathbb{N}^* \text{ tq } x^n = 0$$

$\Pi q 1-x$  est inversible.

$$\text{On a } 1 = 1 - x^n = (1-x) \sum_{k=0}^{n-1} x^k$$

$$\Rightarrow (1-x) \cdot \sum_{k=0}^{n-1} x^k = 1$$

Ce qui montre que  $(1-x)$  est inversible

$$\text{et } (1-x)^{-1} = \sum_{k=0}^{n-1} x^k$$

### Exercice 3

1)  $U(A)$  : l'ensemble des éléments inversibles de  $A$ .

Ng  $(U(A), \times)$  est un groupe.

•  $1_A \in U(A)$  : c'est l'élément neutre

• Si  $x \in U(A)$  et  $y \in U(A)$ , alors

$xy$  est inversible avec  $(xy)^{-1} = y^{-1}x^{-1}$

$\Rightarrow$  La loi " $\times$ " est une l.c.c.

• Soient  $x, y, z \in U(A)$

$$(x \times y) \times z = x \times (y \times z) = x \times y \times z$$

$\Rightarrow$  la loi " $\times$ " est associative.

• Si  $x \in U(A)$ , alors  $x$  admet un élément symétrique qui est  $x^{-1} \in U(A)$

Ainsi  $(U(A), \times)$  est un groupe.

2)  $(\mathbb{Z}, +, \times)$  est un anneau.

Les éléments inversibles de  $\mathbb{Z}$  sont les entiers  $n \in \mathbb{Z}$  tq  $\exists n' \in \mathbb{Z}$  avec  $nn' = 1$

$$\Rightarrow n = \pm 1$$

$$\text{D'où } U(\mathbb{Z}) = \{-1, 1\}$$

3) a)  $n \in \mathbb{N}$  tq  $n \geq 1$  et  $a \in \mathbb{Z}$   
 $\bar{a}$  inversible dans  $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow a \wedge n = 1$   
 $\Leftarrow$  " on a.  $a \wedge n = 1$ , d'après Bézout  
 $\Leftrightarrow \exists u, v \in \mathbb{Z}$  tq  $ua + nv = 1$

$$\Rightarrow \bar{u} \cdot \bar{a} = \bar{1}$$

$\Rightarrow \bar{u}$  est inversible dans  $\mathbb{Z}/n\mathbb{Z}$

" $\Rightarrow$  Si  $\bar{a}$  est inversible dans  $\mathbb{Z}/n\mathbb{Z}$

$$\Rightarrow \exists \bar{v} \in \mathbb{Z}/n\mathbb{Z} \text{ tq } \bar{a}\bar{v} = \bar{1}$$

$$\Rightarrow au = 1 \in n\mathbb{Z}$$

$$\Rightarrow \exists v \in \mathbb{Z} \text{ tq } au - 1 = nv$$

$$\Leftrightarrow 1 = nv - au$$

$$n \wedge a = 1$$

Bézout

$$U(\mathbb{Z}/n\mathbb{Z}) = \{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} \text{ tq } a \wedge n = 1 \}$$

3) b) on a.  $(\mathbb{Z}/p\mathbb{Z}, +, \times)$  est un anneau  
 D'après 3. b)

$$U(\mathbb{Z}/p\mathbb{Z}) = \{ \bar{a} \in \mathbb{Z}/p\mathbb{Z} \text{ tq } p \wedge a = 1 \}$$

d'où  $\mathbb{Z}/p\mathbb{Z}$  est un corps ssi

$$U(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \stackrel{\text{ssi}}{=} \mathbb{Z}/p\mathbb{Z}$$

$$\forall \bar{a} \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}, p \wedge a = 1$$

ssi  $p$  est un nombre premier

i) Si  $p$  est un nombre premier

On a :  $U(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^*$  est un groupe de cardinal  $(p-1)$ , alors  $\forall \bar{x} \in (\mathbb{Z}/p\mathbb{Z})^* ; \bar{x}^{p-1} = \bar{1}$

5)  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  en général n'est pas un anneau intègre.

par exemple dans  $\mathbb{Z}/4\mathbb{Z}$  il existe  $\bar{x} = \bar{2} \neq \bar{0}$  et  $\bar{y} = \bar{2} \neq \bar{0}$  avec  $\bar{x} \cdot \bar{y} = \bar{4} = \bar{0}$ .

b) On a  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un corps si  $n$  est premier.

D'où si  $n$  est premier alors  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un corps et par suite c'est un anneau intègre.

" $\Rightarrow$ " Il n'y a si  $(\mathbb{Z}/p\mathbb{Z}, +, \times)$  est un anneau intègre, alors  $p$  est premier.

Supposons que  $p$  n'est pas premier alors il existe  $2 \leq a \leq p-1$  tq  $ab = p$   $2 \leq b \leq p-1$

$\Rightarrow \bar{a} \cdot \bar{b} = \bar{0}$   
Puisque  $a, b \in \{2, \dots, p-1\}$ , alors  $\bar{a} \neq \bar{0}$  et  $\bar{b} \neq \bar{0}$

$\Rightarrow \mathbb{Z}/p\mathbb{Z}$  n'est pas intègre.

Ainsi,  $\mathbb{Z}/p\mathbb{Z}$  intègre  $\Leftrightarrow p$  premier

### Exercice 4

$\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$

Soit  $z_1 \in \mathbb{Z}[i]$  et  $z_2 \in \mathbb{Z}[i] \Leftrightarrow \exists a, b, a', b' \in \mathbb{Z}$  tq  $z_1 = a + ib$  et  $z_2 = a' + ib'$

$$z_1 + z_2 = \underbrace{(a + a')}_{\in \mathbb{Z}} + i \underbrace{(b + b')}_{\in \mathbb{Z}} \in \mathbb{Z}[i]$$

$\Rightarrow$  "+" Lci dans  $\mathbb{Z}[i]$ .

$$\begin{aligned} z_1 \times z_2 &= (a + ib)(a' + ib') \\ &= \underbrace{aa' - bb'}_{\in \mathbb{Z}} + i \underbrace{(ba' + b'a)}_{\in \mathbb{Z}} \end{aligned}$$

$$\Rightarrow z_1 \times z_2 \in \mathbb{Z}[i]$$

$\Rightarrow$  Lci "x" est une Lci dans  $\mathbb{Z}[i]$

2) Il n'y a si  $(\mathbb{Z}[i], +, \times)$  est un anneau commutatif. On a  $\mathbb{Z}[i] \subset \mathbb{C}$  ( $\mathbb{C}, +, \times$ ) est un anneau commutatif

$$1 = 1 + 0i \in \mathbb{Z}[i]$$

$$\forall z_1, z_2 \in \mathbb{Z}[i] \Rightarrow z_1 - z_2 = (a - a') + i(b - b') \in \mathbb{Z}[i]$$

(4)

$$z_1 z_2 = (a a' - b b') + i(a b' + b a') \in \mathbb{Z}[i]$$

D'où  $(\mathbb{Z}[i], +, \times)$  est un anneau.  
De plus la loi " $\times$ " est commutatif dans  $\mathbb{C}$ , alors elle est commutatif dans  $\mathbb{Z}[i]$ . Ainsi  $(\mathbb{Z}[i], +, \times)$  est un anneau commutatif.

•  $\text{Int}(\mathbb{Z}[i], +, \times)$  est intègre :

Soit  $z_1 = a + ib \in \mathbb{Z}[i]$   
et  $z_2 = (a' + ib') \in \mathbb{Z}[i]$  tq

$z_1 z_2 = 0 \Rightarrow z_1 = 0$  ou  $z_2 = 0$   
car  $(\mathbb{C}, +, \times)$  est intègre

3)  $(\mathbb{Z}[i], +, \times)$  n'est pas un corps

car  $z = 3 + i \Rightarrow \frac{1}{z} = \frac{3-i}{9+1} = \frac{3-i}{10} \notin \mathbb{Z}[i]$

4) soit  $z \in U(\mathbb{Z}[i]) \Leftrightarrow z$  est inversible dans  $\mathbb{Z}[i] \Leftrightarrow \exists z' \in \mathbb{Z}[i]$  tq.

$$z z' = 1 \Rightarrow N(z z') = 1$$

$$\Rightarrow |z|^2 \cdot |z'|^2 = 1 \quad (*)$$

comme  $|z|^2 = a^2 + b^2 \in \mathbb{N}$

alors (\*) est vérifiéessi

$$|z|^2 = 1 \text{ et } |z'|^2 = 1 \Rightarrow a^2 + b^2 = 1 \Leftrightarrow \begin{cases} a^2 = 1 \\ \text{et } b^2 = 0 \end{cases} \text{ ou } \begin{cases} a^2 = 0 \\ \text{et } b^2 = 1 \end{cases}$$

$$\Leftrightarrow \begin{cases} a = \pm 1 \\ \text{et } b = 0 \end{cases} \text{ ou } \begin{cases} a = 0 \\ \text{et } b = \pm 1 \end{cases}$$

Ainsi  $z = 1$  ou  $z = -1$  ou  $z = i$  ou  $z = -i$

$$\Rightarrow U(\mathbb{Z}[i]) = \{-1, 1, -i, i\}.$$

1)  $K[U] \subset \mathcal{A}(E)$ .

- $\text{Id}_E = U^0 \in K[U]$
- Soient  $f, g \in K[U] \Leftrightarrow \exists P, Q \in K[X]$

$\hookrightarrow f = P(U)$  et  $g = Q(U)$

$$\Rightarrow \forall \lambda \in K; \lambda f + g = \lambda P(U) + Q(U) = (\lambda P + Q)(U) \in K[U]$$

$$\Rightarrow \lambda f + g \in K[U]$$

- $f \circ g = P(U) \circ Q(U) = (P \circ Q)(U) \in K[U]$

Alors  $(K[U], +, \cdot, \circ)$  est une sous-algèbre de  $\mathcal{A}(E)$

e) a)  $\varphi_U: \mathcal{A}(E) \rightarrow \mathcal{A}(E)$   
 $v \mapsto \varphi_U(v) = Uv - vU$

- $\varphi_U$  est linéaire de  $\mathcal{A}(E)$  dans  $\mathcal{A}(E)$

$\Rightarrow \varphi_U$  est un endomorphisme de  $\mathcal{A}(E)$ .

Donc  $\varphi_U(\text{Id}_E) = 0 \Rightarrow \ker \varphi_U \neq \{0\}$

$\Rightarrow \varphi_U$  n'est pas bijective.

b)  $\ker \varphi_U$  est un s.v. de  $\mathcal{A}(E)$ .

Soient  $v, w \in \ker \varphi_U$

$\Leftrightarrow uv = vu$  et  $uw = wu$

$\forall v, w \in \ker \varphi_U$

$$uvw = vuw \Leftrightarrow \varphi_U(vw) = 0$$

$\Rightarrow vw \in \ker \varphi_U$   
 $\Rightarrow \ker \varphi_U$  s. algèbre de  $(\mathcal{A}(E), +, \cdot, \circ)$

### Exercice 7

$f: (K) \rightarrow (L, +, \cdot)$  morphisme de corps

$$\Leftrightarrow \begin{cases} f(1_K) = 1_L \\ f(x+y) = f(x) + f(y) \\ f(x \cdot y) = f(x) \cdot f(y) \end{cases}$$

1)  $K$  est un corps, alors  $\forall x \in K^*$ ,  $x$  est inversible  $\Leftrightarrow x x^{-1} = 1_K$

$\Rightarrow f(x \cdot x^{-1}) = f(1_K) = 1_L$

$\Rightarrow f(x) \cdot f(x^{-1}) = 1_L \Rightarrow f(x)$  est inversible avec  $(f(x))^{-1} = f(x^{-1})$

e)  $\forall f$  si  $f$  est un morphisme de corps alors  $f$  est injective.

Supposons qu'il existe  $x \neq 0_K$  tq  $x \in \ker f$

$\Rightarrow f(x) = 0_L$

or  $f(x)$  est inversible d'après 1) ce qui est absurde.

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

# Exercice 8

$$\begin{aligned}\varphi(n) &= \text{card}(\mathcal{U}(\mathbb{Z}/n\mathbb{Z})) \\ &= \text{card}\{1 \leq k \leq n \text{ tq } k \wedge n = 1\}\end{aligned}$$

1) Si  $p$  est premier, alors  $\forall k \leq p-1$   
 $k \wedge p = 1$ , d'où  $\varphi(p) = p-1$

$$\begin{aligned}\varphi(p^\alpha) &= \text{card}\{1 \leq k \leq p^\alpha \text{ tq } k \wedge p^\alpha = 1\} \\ \text{or no } k \in \mathbb{Z}[1, p^\alpha] \text{ tq } k \wedge p^\alpha \neq 1\end{aligned}$$

Comme  $p$  est premier, alors les diviseurs  
 de  $p^\alpha$  sont  $1, p, p^2, \dots, p^\alpha$ , alors

$$\begin{aligned}p \nmid \gcd(k \wedge p^\alpha) &\in \{1, p, p^2, \dots, p^\alpha\} \\ \Rightarrow p \nmid \gcd(k \wedge p^\alpha) &\Leftrightarrow p \nmid k \\ \Leftrightarrow k &= ap \text{ avec } 1 \leq a \leq p^{\alpha-1}\end{aligned}$$

$$\begin{aligned}\text{Ainsi: } \text{card}\{1 \leq k \leq p^\alpha \text{ tq } k \wedge p^\alpha \neq 1\} &= p^{\alpha-1} \\ \varphi(p^\alpha) &= \text{card}(\mathbb{Z}[1, p^\alpha]) - \text{card}\{k \in \mathbb{Z}[1, p^\alpha] \text{ tq } k \wedge p^\alpha \neq 1\}\end{aligned}$$

$$\begin{aligned}\varphi(p^\alpha) &= p^\alpha - p^{\alpha-1} \\ \text{2) } m, n \in \mathbb{Z} \text{ tq } m \wedge n &= 1 \\ f: \mathbb{Z}/n.m\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ \bar{x} &\longmapsto f(\bar{x}) = (\hat{x}, \tilde{x})\end{aligned}$$

a) Montrons que  $f$  est bien définie.  
 Soient  $\bar{x}, \bar{y} \in \mathbb{Z}/n.m\mathbb{Z}$  tq  
 $\bar{x} = \bar{y} \Leftrightarrow x - y \equiv 0 \pmod{n.m}$   
 $\Rightarrow n \mid x - y \Rightarrow \hat{x} = \hat{y}$   
 et  $m \mid x - y \Rightarrow \tilde{x} = \tilde{y}$ .  
 $\Rightarrow f(\bar{x}) = f(\bar{y}) \Rightarrow f$  est bien définie

b) Mg.  $f$  est un morphisme d'anneau.

$$f(1) = (\hat{1}, \tilde{1})$$

Soient  $\bar{x}, \bar{y} \in \mathbb{Z}/n.m\mathbb{Z}$

$$\begin{aligned}f(\bar{x} + \bar{y}) &= (\hat{x+y}, \tilde{x+y}) \\ &= (\hat{x} + \hat{y}, \tilde{x} + \tilde{y}) \\ &= (\hat{x}, \tilde{x}) + (\hat{y}, \tilde{y}) \\ &= f(\bar{x}) + f(\bar{y})\end{aligned}$$

$$\begin{aligned}f(\bar{x} \cdot \bar{y}) &= f(\overline{xy}) = (\hat{xy}, \tilde{xy}) \\ &= (\hat{x} \cdot \hat{y}, \tilde{x} \cdot \tilde{y}) \\ &= (\hat{x}, \tilde{x}) \cdot (\hat{y}, \tilde{y}) \\ &= f(\bar{x}) \cdot f(\bar{y})\end{aligned}$$

$\Rightarrow f$  morphisme d'anneaux.

\*Injectivité

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

$$\begin{cases} \hat{x} = 0 \\ \text{et } \hat{y} = 0 \end{cases} \Leftrightarrow \begin{cases} x \in n\mathbb{Z} \\ \text{et } x \in m\mathbb{Z} \end{cases} \\ \Leftrightarrow \begin{matrix} n \mid x \\ \text{et } m \mid x \end{matrix} \xRightarrow{n \wedge m = 1} n \cdot m \mid x \Leftrightarrow$$

$$x \in nm\mathbb{Z} \Leftrightarrow \bar{x} = 0$$

$\Rightarrow f$  injective

De plus  $\text{Card}(\mathbb{Z}/n \cdot m\mathbb{Z}) = n \cdot m$   
 $= \text{Card}(\mathbb{Z}/n\mathbb{Z}) \cdot \text{Card}(\mathbb{Z}/m\mathbb{Z})$  et  $x, y = (a+b\alpha)(a'+b'\alpha)$   
 $= \text{Card}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$

$\Rightarrow f$  bijjective

Ainsi  $f$  est un isomorphisme d'anneaux.

3.) Puisque  $f$  est bijective, alors

$$\text{Card}(\mathcal{U}(\mathbb{Z}/n \cdot m\mathbb{Z})) = \text{Card}(\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/m\mathbb{Z})) \\ \parallel = \text{Card}(\mathcal{U}(\mathbb{Z}/n\mathbb{Z})) \times \text{Card}(\mathcal{U}(\mathbb{Z}/m\mathbb{Z}))$$

$$\varphi(n \cdot m) = \varphi(n) \times \varphi(m)$$

$$\begin{aligned} 4) \quad n \cdot n &= \prod_{i=1}^N p_i^{\alpha_i} \\ \Rightarrow \varphi(n) &= \prod_{i=1}^N \varphi(p_i^{\alpha_i}) \quad \text{d'après 3)} \\ &= \prod_{i=1}^N p_i^{\alpha_i} - p_i^{\alpha_i-1} \end{aligned}$$

## Exercice 6

$\alpha$  racine complexe de l'équation  
 $x^2 + x + 2 = 0 \Rightarrow \alpha^2 + \alpha + 2 = 0$

$$\mathbb{Z}[\alpha] = \{a + b\alpha; (a, b) \in \mathbb{Z}^2\}$$

Soient  $x = a + b\alpha \in \mathbb{Z}[\alpha]$

$$y = a' + b'\alpha \in \mathbb{Z}[\alpha]$$

$$\Rightarrow x + y = \underbrace{(a+a')}_{\in \mathbb{Z}} + \underbrace{(b+b')}_{\in \mathbb{Z}} \alpha$$

$$\Rightarrow x + y \in \mathbb{Z}[\alpha] \Rightarrow "+" \text{ L.C.C. dans } \mathbb{Z}[\alpha]$$

$$\Rightarrow x \cdot y = (a + b\alpha)(a' + b'\alpha)$$

$$= aa' + bb'\alpha^2 + (ab' + b'a)\alpha$$

$$= aa' + bb'(-\alpha - 2) + (ab' + b'a)\alpha$$

$$= \underbrace{aa' - 2bb'}_{\in \mathbb{Z}} + \underbrace{(ab' + b'a - bb')\alpha}_{\in \mathbb{Z}}$$

$$\Rightarrow \exists c \cdot y \in \mathbb{Z}[\alpha]$$

$$\Rightarrow "x" \text{ L.C.C. dans } \mathbb{Z}[\alpha]$$

$$\Rightarrow \exists na \quad 0 \in \mathbb{Z}[\alpha]$$

$$1 \in \mathbb{Z}[\alpha]$$

$$x - y = (a - a') + (b - b')\alpha \in \mathbb{Z}[\alpha]$$

$$x, y \in \mathbb{Z}[\alpha]$$

$$\Rightarrow (\mathbb{Z}[\alpha], +, \times) \text{ est un sous-anneau}$$

soit  $z = a + b\alpha \in \mathbb{Z}[\alpha]$

$$\Rightarrow \bar{z} = a + b\bar{\alpha}$$

Comme  $\alpha$  racine de  $x^2 + x + 2 = 0$

$$\Rightarrow \alpha + \bar{\alpha} = -1 \Rightarrow \bar{\alpha} = -1 - \alpha$$

$$\begin{aligned} \Rightarrow \bar{z} &= a + b(-1 - \alpha) \\ &= a - b - \alpha b \\ &= a - b + \alpha(-b) \in \mathbb{Z}[\alpha] \end{aligned}$$

4) Soit  $z \in \mathbb{Z}[\alpha]$

$$\begin{aligned} z &= a + b\alpha \Rightarrow z\bar{z} = (a + b\alpha)(a + b\bar{\alpha}) \\ &= a^2 + ab\bar{\alpha} + ba\alpha + b^2\alpha\bar{\alpha} \\ &= a^2 + ab(\alpha + \bar{\alpha}) + b^2 \cdot 2 \\ &= a^2 + ab(\alpha + \bar{\alpha}) + b^2 \cdot 2 \end{aligned}$$

$$z\bar{z} = a^2 + 2b^2 - ab \in \mathbb{Z}$$

$$\text{Comme } z\bar{z} = |z|^2 \geq 0 \Rightarrow z\bar{z} \in \mathbb{N}$$

5)  $z = a + b\alpha$  est inversible dans  $\mathbb{Z}[\alpha]$

$$\Leftrightarrow \exists z' = a' + b'\alpha \text{ tq } z z' = 1$$

$$\Rightarrow |z z'| = 1 \Rightarrow |z|^2 \cdot |z'|^2 = 1$$

$$\text{Comme } |z|^2 \in \mathbb{N}, \text{ alors } |z|^2 = 1$$

$$\Rightarrow a^2 + 2b^2 - ab = 1$$

reciproquement.

$$\text{Si } a^2 + 2b^2 - ab = 1 \Rightarrow z\bar{z} = 1$$

et puisque  $\bar{z} \in \mathbb{Z}[\alpha]$

$\Rightarrow z$  est inversible et  $z^{-1} = \bar{z}$ .

6) Supposons qu'il existe  $(a, b) \in \mathbb{Z}^2$

tq  $(a, b)$  vérifie l'eq  $ab > 0$

$$\Rightarrow \begin{cases} a^2 + 2b^2 - ab = 1 \\ ab > 0 \end{cases}$$

$$\Rightarrow \begin{cases} a^2 + 2b^2 - ab = 1 \\ ab > 0 \end{cases}$$

$$\Rightarrow \begin{cases} a^2 + 2b^2 - ab = 1 \\ ab > 0 \end{cases}$$

$$\Rightarrow \begin{cases} a^2 + 2b^2 - ab = 1 \\ ab > 0 \end{cases}$$

$$\Rightarrow (a - b)^2 + b^2 ab = 1$$

$$\Rightarrow 0 \leq (a - b)^2 + b^2 = 1 - ab \leq 1$$

$$\Rightarrow 0 \leq \underbrace{(a - b)^2 + b^2}_{\in \mathbb{N}} < 1$$

$$\Rightarrow (a - b)^2 + b^2 = 0 \Leftrightarrow a - b = 0 \Rightarrow a = b$$

imp  $ab > 0$

Supposons qu'il existe  $(a, b) \in \mathbb{Z}^2$

tq  $(a, b)$  vérifie l'eq et  $ab < 0$

$$\Rightarrow \begin{cases} a^2 + 2b^2 - ab = 1 \\ ab < 0 \end{cases}$$

$$\Rightarrow \begin{cases} a^2 + 2b^2 - ab = 1 \\ ab < 0 \end{cases}$$

$$\Rightarrow 0 \leq a^2 + 2b^2 = 1 + ab \leq 1$$

$$\Rightarrow a^2 + 2b^2 = 0 \Rightarrow a = b = 0$$

imp  $(ab < 0)$

7) D'après 5)

10) Si  $a^2 + 2b^2 - ab = 1$   $z = a + b\alpha$  est inversible

car  $ab=0$

• Si  $a=0 \Rightarrow \exists b^2=1$  unip car  $b \in \mathbb{Z}$

• si  $b=0 \Rightarrow a^2=1 \Rightarrow a=\pm 1$

Ainsi l'ensemble des éléments inversibles de  $(\mathbb{Z}[X], \cdot)$  est  $\{-1, 1\}$

Exercice

1)  $yA = \{y \cdot a, a \in A\}$

$y \cdot 0 = 0 \in yA$

• Soit  $x_1 \in yA \Rightarrow \exists a_1 \in A; x_1 = y a_1$

$x_2 \in yA \Rightarrow \exists a_2 \in A; x_2 = y a_2$

$\Rightarrow x_1 - x_2 = y(\underbrace{a_1 - a_2}_{\in A}) \in yA$

• soit  $x \in yA \Rightarrow x = y \cdot a$

et  $b \in A \Rightarrow x b = y \underbrace{ab}_{\in A} \in yA$

Ainsi  $y \cdot A$  est un idéal de  $A$

2) a)  $(\mathbb{Z}, +, \times)$  anneau commutatif

$I \neq \emptyset$

c)  $I$  idéal, alors  $(I, +)$  s-groupe de  $(\mathbb{Z}, +)$

$\Rightarrow \exists n \in \mathbb{N}^* \text{ tq } I = n\mathbb{Z}$

D'après a)  $n\mathbb{Z}$  idéal de  $\mathbb{Z}$

D'où l'équivalence



$$\mathcal{I} \subset \mathcal{P}(K[X]) = \{ P \cdot Q ; Q \in K[X] \}$$

$$\cdot \tilde{0} \in \mathcal{P}(K[X])$$

$$\bullet \text{ Soit } A \in \mathcal{P}(K[X]) ; B \in \mathcal{P}(K[X])$$

$$\Leftrightarrow \exists Q_1 \text{ et } Q_2 \in K[X] \text{ tq.}$$

$$A = P \cdot Q_1 \text{ et } B = P \cdot Q_2$$

$$A - B = P(Q_1 - Q_2) \in \mathcal{P}(K[X])$$

$$\bullet \text{ Soit } A \in \mathcal{P}(K[X]) \Leftrightarrow A = P \cdot Q$$

$$\text{et } H \in K[X], \text{ alors}$$

$$A \cdot H = P \cdot \underbrace{Q \cdot H}_{\in K[X]} \in \mathcal{P}(K[X])$$

Ainsi  $\mathcal{P}(K[X])$  est un idéal de  $K[X]$ .

2)  $\mathcal{I}$  idéal non nul de  $(K[X], +, \cdot)$

$$\mathcal{I} \neq \tilde{0}$$

$$\mathcal{A} = \{ \deg P ; P \in \mathcal{I} \} \cup \{ \tilde{0} \}$$

$$\text{Puisque } \mathcal{I} \neq \tilde{0} \Rightarrow \exists P_0 \neq \tilde{0} \text{ tq } P_0 \in \mathcal{I}$$

$$\Rightarrow \deg P_0 \in \mathcal{A} \Rightarrow \mathcal{A} \neq \emptyset \Rightarrow \text{et } \mathcal{A} \subset \mathbb{N} \Rightarrow$$

$\min \mathcal{A}$  existe : on pose  $k = \min \mathcal{A}$ .

b) On considère  $H \in \mathcal{I}$  tq  $\deg H = k$

$$\text{et } Q = \frac{H}{\text{coeff. dom}(H)} \Rightarrow \deg Q = k$$

$\exists Q$  unitaire et  $Q \in \mathcal{I}$

$$\text{Pq } \mathcal{I} = Q \cdot K[X]$$

On a  $Q \in \mathcal{I}$  et comme  $\mathcal{I}$  est un idéal alors  $Q \cdot K[X] \subset \mathcal{I}$ .

Soit  $P \in \mathcal{I}$ , on effectue la division euclidienne de  $P$  par  $Q$ , alors  $P \in K[X]$  et  $R \in K[X]$  tq

$$P = Q \cdot A + R \text{ avec } \deg R < \deg Q$$

$$\therefore \left. \begin{array}{l} P \in \mathcal{I} \\ Q \in \mathcal{I} \Rightarrow Q \cdot A \in \mathcal{I} \end{array} \right\} \Rightarrow P - Q \cdot A \in \mathcal{I}$$

$$\Rightarrow \left. \begin{array}{l} R \in \mathcal{I} \\ \text{ou } \deg R < \deg Q \end{array} \right\} \Rightarrow R = \tilde{0}$$

$$\Rightarrow P = Q \cdot A \Rightarrow \mathcal{I} = Q \cdot K[X]$$

$\bullet$  Pq  $Q$  est unique

supposons qu'il existe  $\tilde{Q}$  unitaire tq.

$$\mathcal{I} = \tilde{Q} \cdot K[X]$$

$$\text{On a } Q \in \mathcal{I} = \tilde{Q} \cdot K[X] \Rightarrow \tilde{Q} \mid Q$$

$$\tilde{Q} \in \mathcal{I} = Q \cdot K[X] \Rightarrow Q \mid \tilde{Q}$$

Comme  $\deg Q = \deg \tilde{Q}$

$$\Rightarrow \tilde{Q} = \alpha \cdot Q \text{ ou } Q \text{ et } \tilde{Q} \text{ sont unitaires} \Rightarrow \alpha = 1 \Rightarrow Q = \tilde{Q}$$

### 3) Conclusion

$I$  idéal non nul de  $K[X]$   $\Leftrightarrow$   
 $\exists$  un unique polynôme unitaire  $P$ .

$$\text{tg } I = P K[X].$$

II)  $u \in \mathcal{L}(E)$  et  $x \in E \setminus \{0_E\}$

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

On a  $\chi_u$  le polynôme caractéristique.  
 vérifie  $\chi_u \neq \tilde{0}$  et  $\chi_u(u) = \tilde{0} \Rightarrow$   
 $\chi_u(u)(x) = 0_E$

$$\Rightarrow \chi_u \in I_x \Rightarrow I_x \neq \{\tilde{0}\}.$$

$$\bullet I_x \neq \emptyset$$

$$\bullet \forall P_1, P_2 \in I_x$$

$$(P_1 - P_2)(u)(x) = \frac{P_1(u)(x)}{0} - \frac{P_2(u)(x)}{0} = 0_E$$

$$\Rightarrow P_1 - P_2 \in I_x$$

$$\bullet \text{ Soit } P \in I_x \text{ et } Q \in K[X].$$

$$\frac{P(u)(x)}{0} = 0_E.$$

$$(P \cdot Q)(u)(x) = (Q \cdot P)(u)(x) = Q(u) \circ \frac{P(u)(x)}{0} = 0_E$$

$$\Rightarrow P \cdot Q \in I_x$$

Ainsi  $I_x$  est un idéal de  $K[X]$

2) Puisque  $I_x$  est un idéal de  $K[X]$  d'après I/ 3. polynôme de degré minimal

$$\text{tg } I_x = \pi_{x,u} K[X].$$

3) a) On a  $\pi_u$  le polynôme minimal de  $u$   
 vérifie  $\pi_u(u) = \tilde{0} \Rightarrow \pi_u(u)(x) = 0_E$

$$\Rightarrow \pi_u(u) \in I_x = \pi_{x,u} K[X]$$

$$\Rightarrow \pi_{x,u} \text{ divise } \pi_u.$$

b) On a  $\forall x \in E \setminus \{0\}$ ,  $\pi_{x,u}$  divise  $\pi_u$ .  
 or l'ensemble des diviseurs de  $\pi_u$   
 est fini, alors l'ensemble

$\{\pi_{x,u}, x \in E \setminus \{0\}\}$  est fini.

4)  $(x, y) \in (E \setminus \{0\})^2$  tg  $\pi_{x,u} \wedge \pi_{y,u} = 1$   
 $\text{tg } x + y \neq 0_E$

Supposons que  $x + y = 0 \Leftrightarrow y = -x$

$$\Rightarrow \pi_{y,u}(u)(x) = \pi_{y,u}(u)(-y) = -\pi_{y,u}(u)(y) = 0$$

$$\Rightarrow \pi_{y,u}(u)(x) = 0_E \Rightarrow \pi_{y,u} \in I_x = \pi_{x,u} K[X]$$

$$\Rightarrow \pi_{x,u} \text{ divise } \pi_{y,u} \text{ absurde}$$

$$\Rightarrow x + y \neq 0_E$$

$$\star \text{ tg } \pi_{x+y,u} = \pi_{x,u} \cdot \pi_{y,u}$$

$$\begin{aligned} \min_{\alpha} \pi_{x,u} \cdot \pi_{y,u}(u) (x+y) &= \pi_{x,u}(u) \circ \pi_{y,u}(u) (x+y) \\ &= \pi_{x,u}(u) \circ \pi_{y,u}(x) + \pi_{x,u}(u) \circ \pi_{y,u}(y) \\ &= \pi_{y,u}(\underbrace{\pi_{x,u}(x)}_{=0}) + \pi_{x,u}(u) \circ \underbrace{\pi_{y,u}(y)}_{=0} \end{aligned}$$

$$\Rightarrow \pi_{x,u} \cdot \pi_{y,u}(u) (x+y) = 0$$

$$\Rightarrow \pi_{x,u} \cdot \pi_{y,u} \in \Gamma_{x+y,u} = \pi_{x+y,u} K[x]$$

$$\Rightarrow \pi_{x+y,u} \text{ divide } \pi_{x,u} \cdot \pi_{y,u} \quad \textcircled{1}$$

D'autre part on a :

$$\pi_{x+y,u}(u) (x+y) = 0 \in \Rightarrow$$

$$\pi_{x+y,u}(u)(x) = -\pi_{x+y,u}(u)(y)$$

$$\begin{aligned} \Rightarrow \pi_{y,u}(u) \circ \pi_{x+y,u}(x) &= \pi_{y,u}(u) \pi_{x+y,u}(y) \\ &= \pi_{x+y,u}(u) \circ \underbrace{\pi_{y,u}(y)}_{=0} \\ &= 0 \in \end{aligned}$$

$$\Rightarrow \pi_{y,u} \cdot \pi_{x+y,u} \in \Gamma_x \Rightarrow$$

$$\pi_{x,u} / \pi_{y,u} \cdot \pi_{x+y,u}$$

$$\text{Donc } \pi_{y,u} / \pi_{x,u} \cdot \pi_{x+y,u}$$

$$\text{or } \pi_{x,u} \wedge \pi_{y,u} = 1$$

$$\underline{\text{Gauche}} \Rightarrow \pi_{x,u} / \pi_{x+y,u} \in \pi_{y,u} / \pi_{x+y,u} \quad \textcircled{2}$$

$$\Rightarrow \frac{\pi_{x,u} \cdot \pi_{y,u}}{\pi_{x+y,u}} \mid \pi_{x+y,u} \quad \textcircled{2}$$

$$\xrightarrow{\text{K(e)}} \pi_{x,u} \cdot \pi_{y,u} = \pi_{x+y,u} \quad (\text{can ils sent unitaires})$$