Examen partiel du 21 mars 2024

1. (4 points) Soit k un corps. Déterminer en fonction de $\alpha, \beta \in k$ les invariants de similitude de la matrice
$$\begin{pmatrix} 0 & 1 & \alpha \\ 0 & 0 & \beta \\ 0 & 0 & 0 \end{pmatrix}.$$

2. (6 points) Soit k un corps. On considère l'anneau $k[T]$ des polynômes en la variable T et à coefficients dans k ainsi que l'application
$$f : k[T] \to k[T] \times k[T] \qquad P \mapsto (P', TP),$$
où P' désigne le polynôme dérivé de P.
   (a) Est-ce que f est une application k-linéaire ?
   (b) Est-ce que f est une application $k[T]$-linéaire ?
   (c) Est-ce que f est injective ?
   (d) Déterminer le conoyau de f.

3. (7 points) Soit $z = u + iv \in \mathbb{Z}[i]$ avec $\mathrm{PGCD}(u, v) = 1$. On pose $n = u^2 + v^2$.
   (a) Montrer qu'il existe un entier $c \in \{0, \ldots, n-1\}$ vérifiant $u + cv \equiv 0 \quad [n]$.
   (b) Montrer que l'entier c vérifie la congruence $c^2 + 1 \equiv 0 \quad [n]$.
   (c) Montrer que l'application
$$f : \mathbb{Z}[i] \to \mathbb{Z}/n\mathbb{Z}, \qquad a + ib \mapsto a + cb \bmod n$$
   est un homomorphisme d'anneaux qui induit un isomorphisme
$$\overline{f} : \mathbb{Z}[i]/(u + iv) \to \mathbb{Z}/n\mathbb{Z}.$$

4. (3 points) On considère l'anneau de Gauss $\mathbb{Z}[i]$.
   (a) Calculer $\mathrm{PGCD}(8, 3 + i)$ dans $\mathbb{Z}[i]$.
   (b) Donner la relation de Bézout associée à 8 et $3 + i$.

Corrigé de l'examen partiel du 21 mars 2024

1. Les invariants de similitude d'une matrice $A \in \mathcal{M}_3(k)$ sont les facteurs invariants de la matrice $A - XI_3 \in \mathcal{M}_3(k[X])$. On les calcule en effectuant des opérations sur les lignes et les colonnes.

$$A - XI_3 = \begin{pmatrix} -X & 1 & \alpha \\ 0 & -X & \beta \\ 0 & 0 & -X \end{pmatrix}$$

$$C_1 \leftrightarrow C_2 \qquad \begin{pmatrix} 1 & -X & \alpha \\ -X & 0 & \beta \\ 0 & 0 & -X \end{pmatrix}$$

$$C_2 \leftarrow C_2 + XC_1 \qquad \begin{pmatrix} 1 & 0 & \alpha \\ -X & -X^2 & \beta \\ 0 & 0 & -X \end{pmatrix}$$

$$C_3 \leftarrow C_3 - \alpha C_1 \qquad \begin{pmatrix} 1 & 0 & 0 \\ -X & -X^2 & \beta + \alpha X \\ 0 & 0 & -X \end{pmatrix}$$

$$L_2 \leftarrow L_2 + XL_1 \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -X^2 & \beta + \alpha X \\ 0 & 0 & -X \end{pmatrix}$$

$L_2 \leftarrow L_2 + \alpha L_3$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -X^2 & \beta \\ 0 & 0 & -X \end{pmatrix}$

si $\beta = 0$, alors les invariants de similitude sont.
$(1, X, X^2)$ [(-1) est inversible dans k]

si $\beta \neq 0$, il faut faire des opérations supplémentaire

$C_2 \leftrightarrow C_3$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \beta & -X^2 \\ 0 & -X & 0 \end{pmatrix}$

$C_3 \leftarrow C_3 + \beta^{-1} X C_2$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \beta & 0 \\ 0 & -X & -\beta^{-1}X \end{pmatrix}$

$L_3 \leftarrow L_3 + \beta^{-1} X L_2$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & -\beta^{-1}X^3 \end{pmatrix}$

si $\beta \neq 0$, les invariants de similitude sont
$(1, 1, X^3)$ [$\beta, -\beta^{-1}$ sont inversibles dans k].

2. (a) oui, f est k-linéaire.

(b) non, f n'est pas $k[T]$-linéaire

car $f(\lambda P) \neq \lambda . f(P)$ avec $\lambda \in k[T]$.

avec la structure de $k[T]$-module.

naturelle sur $k[T] \times k[T]$.

car $f(\lambda P) = ((\lambda P)', T\lambda P)$

$\lambda . f(P) = \lambda . (P', TP) = (\lambda P', \lambda TP)$

or $(\lambda P)' \neq \lambda P'$

(c) oui, f est injective.

car si $(P', TP) = (0,0)$, alors $P = 0$

(d) soit $(Q,R) \in k[T] \times k[T]$.

si $(Q,R) \in \operatorname{im}(f)$, alors il existe $P \in k[T]$ tel que

$Q = P'$ et $R = TP$

en dérivant la deuxième égalité on obtient

$$R' = TP' + P$$

$$R' = TQ + \frac{R}{T}$$

en multipliant avec T on obtient.

$$TR' = T^2Q + R$$

Inversément soit $(Q,R) \in k[T] \times k[T]$ vérifiant la relation $TR' = T^2Q + R$

alors $T^2Q = TR' - R$

en posant $T=0$, on obtient $R(0) = 0$.

donc R est de la forme $R = TP$.

de plus $TR' - R = T(TP' + P) - TP$

$$= T^2P' + TP - TP$$

$$= T^2P'$$

donc $T^2Q = T^2P' \Rightarrow Q = P'$

Ainsi si l'on définit $g : k[T] \times k[T] \longrightarrow k[T]$.

$$(Q, R) \longmapsto T^2Q - TR' + R$$

on observe que $\mathrm{im}(f) = \ker(g)$.

<u>Attention</u> : g n'est pas surjectif. On voit que

$$\mathrm{im}(g) = \{A \in k[T] \mid A'(0) = 0\} \subset k[T].$$

$\Leftrightarrow A$ n'a pas de terme de degré 1

donc $\mathrm{coker}(f) = \mathrm{im}(g) = \{A \in k[T] \mid A'(0) = 0\}$.

3. (a) Si $v \neq 0$, $PGCD(v, n) = PGCD(v, u^2 + v^2) = PGCD(v, u^2)$

$$= PGCD(v, u) = 1.$$

Donc v est inversible mod n, notons v^{-1} cet inverse. On peut prendre $c = -u \cdot v^{-1}$

Si $v = 0$, alors $u = \pm 1$ et $n = 1$, car $PGCD(u, v) = 1$

on peut alors prendre $c = 0$

(b) si $c = -uv^{-1}$, alors $c^2 \equiv u^2(v^{-1})^2 \equiv -v^2(v^{-1})^2 \equiv -1 \mod n$

car $u^2 \equiv -v^2 \mod n$

(c) Vérifions que f est un homomorphisme d'anneaux

$$f((a+ib))\, f(a'+ib') = (a+cb)(a'+cb') = (aa'+c^2bb') + c(ab'+ba')$$

$$f((aa'-bb')+i(ab'+ba')) = (aa'-bb') + c(ab'+ba')$$

On veut que les deux expressions sont les mêmes modulo n, car $c^2 \equiv -1 \mod n$.

donc f est un homomorphisme d'anneaux.

Pour montrer que f est un isomorphisme, il faut montrer que $\ker(f) = (u+iv)\mathbb{Z}[i]$

- Comme f est un homomorphisme d'anneaux, $\ker(f)$ est un idéal. Comme $f(u+iv) = u+cv \equiv 0\ [n]$ (voir (a)), on obtient que $(u+iv)\mathbb{Z}[i] \subset \ker(f)$
- Inversément, si $a+ib \in \ker(f)$, on fait la division euclidienne de $a+ib$ par $u+iv$:

$$a+ib = (u+iv)\,q + r$$

avec $r = \alpha + i\beta$ et $\alpha^2+\beta^2 < n$ et $\alpha, \beta \in \mathbb{Z}$.

de plus comme $u+iv \in \ker(f)$, on obtient que $r \in \ker(f)$, donc $\alpha + c\beta \equiv 0\ [n]$. Ce ci implique que $\alpha^2 \equiv c^2\beta^2 \equiv -\beta^2\ [n]$, donc $\alpha^2+\beta^2 \equiv 0\ [n]$.

Or $0 \leq \alpha^2+\beta^2 < n$, donc $\alpha^2+\beta^2 = 0 \Rightarrow \alpha = \beta = 0 \Rightarrow r = 0$

donc $a+ib \in (u+iv)\mathbb{Z}[i]$.

4.(a) On fait la division euclidienne de 8 par $3+i$

$$8 = (3+i)(2-i) + (1+i)$$

ensuite la divison euclidienne de $(3+i)$ par $(1+i)$

$$3+i = (1+i)(2-i) + 0.$$

donc $PGCD(8, 3+i) = 1+i$

(b) Relation de Bézout

$$(1+i) = 8 - (3+i)(2-i)$$