Examen – mardi 6 décembre 2022

L'épreuve dure 2 heures. Les réponses doivent être justifiées et rédigées correctement. Toute question non résolue peut être admise dans la suite. Les quatre exercices sont indépendants. Le barême fourni est indicatif et susceptible de modification.

Exercice 1. (sur 8 pts) *Calculs*

1. **i.** Calculer la liste des inversibles de $\mathbb{Z}/14\mathbb{Z}$.
ii. Calculer l'*orbite* de $[3]_{14}$, c'est-à-dire l'ensemble des $\{[3]_{14}^k : k \geq 0\}$ et en déduire que $[3]_{14}$ est générateur de $\mathbb{Z}/14\mathbb{Z}^\times$.
iii. Utiliser la question précédente pour calculer l'inverse de chaque élément de $\mathbb{Z}/14\mathbb{Z}^\times$.

2. Soit $A = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 5 & 4 \\ 1 & 2 & 3 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$.
i. Calculer une forme échelonnée E de A, ainsi que la matrice inversible M telle que $E = M \cdot A$.
ii. En déduire une décomposition de A sous la forme $P \cdot L \cdot E$ où P est une matrice de permutation et L est triangulaire inférieure avec des 1 sur la diagonale.
iii. Déterminer la forme échelonnée réduite de A *sans effectuer de calcul*.

3. Calculer le rang de $B = \begin{pmatrix} [4]_{11} & [4]_{11} & [6]_{11} & [2]_{11} \\ [5]_{11} & [9]_{11} & [8]_{11} & [3]_{11} \\ [7]_{11} & [4]_{11} & [6]_{11} & [10]_{11} \end{pmatrix} \in \mathbb{Z}/11\mathbb{Z}^{3\times 4}$.

4. Soit $A \in \mathbb{K}^{n\times n}$, $C \in \mathbb{K}^{n\times(n-1)}$ et $R \in \mathbb{K}^{(n-1)\times n}$ telles que $A = C \cdot R$. Montrer que A n'est pas inversible.

Exercice 2. (sur 3 pts) *Anneaux*

Soit $\mathscr{A} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$.

1. **i.** Montrer que $(\mathscr{A}, +, \times)$ est un anneau, où $+$ et $\times$ sont l'addition et la multiplication de matrices.
ii. Est-ce un corps ?

2. **i.** Vérifier que $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = -\mathbb{1}$ où $\mathbb{1} \in \mathscr{A}$ est le neutre pour $\times$.
ii. En déduire un isomorphisme ρ entre les anneaux $(\mathbb{C}, +, \times)$ et $(\mathscr{A}, +, \times)$. *Expliciter l'isomorphisme (que vaut $\rho(z)$ pour $z \in \mathbb{C}$?) et démontrer que c'est un isomorphisme.*

Exercice 3. (sur 5 pts) *Permutations RSA*

Soit p et q deux nombres premiers, et $N = p \times q$. On note $\varphi(N)$ l'indicatrice d'Euler de N. Pour tout $d \geq 0$, on définit $\sigma_d : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ par $\sigma_d(\alpha) = \alpha^d$. Soit k un entier inversible modulo $\varphi(N)$, et ℓ son inverse modulo $\varphi(N)$. On cherche à montrer que σ_k est une permutation de $\mathbb{Z}/N\mathbb{Z}$, de réciproque σ_ℓ.

1. On étend la définition de σ_d à $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire qu'on pose $\sigma_d(\alpha_p) = \alpha_p^d$ pour tout $\alpha_p \in \mathbb{Z}/p\mathbb{Z}$.

- **i.** Montrer que k est inversible modulo $p-1$. *Indication. Que vaut $\varphi(N)$?*
- **ii.** En déduire que pour tout $\alpha_p \in \mathbb{Z}/p\mathbb{Z}$, $\sigma_\ell \circ \sigma_k(\alpha_p) = \alpha_p$.

2. Soit $\rho : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ la fonction définie par $\rho([a]_N) = ([a]_p, [a]_q)$.

- **i.** Citer le théorème, *avec ses hypothèses exactes de validité*, qui affirme que ρ est un isomorphisme d'anneaux.
- **ii.** Montrer que pour tout $d \geq 0$ et $\alpha \in \mathbb{Z}/N\mathbb{Z}$, $\rho(\sigma_d(\alpha)) = (\sigma_d(\alpha_p), \sigma_d(\alpha_q))$ où $(\alpha_p, \alpha_q) = \rho(\alpha)$.
- **iii.** En déduire que pour tout $\alpha \in \mathbb{Z}/N\mathbb{Z}$, $\sigma_\ell \circ \sigma_k(\alpha) = \alpha$.

Exercice 4. (sur 4 pts) *Noyau et image*

Soit $A \in \mathbb{K}^{n \times n}$. On note $\mathrm{im}(A) = \{A \cdot x : x \in \mathbb{K}^n\}$ son espace colonne, et $\ker(A)$ son noyau.

1. Montrer que $\ker(A) \subset \ker(A^2)$ où $A^2 = A \cdot A$.
2. Montrer que $\mathrm{im}(A^2) \subset \mathrm{im}(A)$.
3. Montrer que $\ker(A) \cap \mathrm{im}(A) = A \cdot \ker(A^2)$ où $A \cdot \ker(A^2) = \{A \cdot x : x \in \ker(A^2)\}$.
4. En déduire que $\ker(A) \cap \mathrm{im}(A) = \{0\}$ si et seulement si $\ker(A) = \ker(A^2)$.