Examen de 2ème session – lundi 26 juin 2023

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

Exercice 1. (sur 8 pts) *Calculs*

1. **i.** Calculer la liste des inversibles de $\mathbb{Z}/22\mathbb{Z}$.
   ii. Calculer l'*orbite* de $[19]_{22}$, c'est-à-dire l'ensemble des $\{[19]_{22}^k : k \geq 0\}$ et en déduire que $[19]_{22}$ est générateur de $\mathbb{Z}/22\mathbb{Z}^\times$. *Indication. On pourra utiliser le fait que* $[19]_{22} = [-3]_{22}$.
   iii. Exprimer chaque élément de $\mathbb{Z}/22\mathbb{Z}^\times$ sous la forme $[19]_{22}^k$ avec $0 \leq k < 10$, et en déduire *sans calcul* l'inverse de chaque élément.
2. Soit $A = \begin{pmatrix} 3 & 9 & 2 \\ 4 & 7 & \frac{1}{3} \\ 6 & 8 & 1 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$.
   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. Déterminer si la matrice $B = \begin{pmatrix} [6]_{13} & [1]_{13} & [1]_{13} \\ [12]_{13} & [10]_{13} & [9]_{13} \\ [6]_{13} & [4]_{13} & [2]_{13} \end{pmatrix} \in \mathbb{Z}/13\mathbb{Z}^{3\times 3}$ est inversible *sans calculer son déterminant*.
4. Soit $A \in \mathbb{K}^{n\times n}$ et $B \in \mathbb{K}^{n\times n}$ deux matrices inversibles.
   i. La matrice $A \times B$ est-elle inversible ?
   ii. La matrice $A + B$ est-elle inversible ?

Exercice 2. (sur 3 pts) *Anneaux*

Soit $z_1, z_2 \in \mathbb{C}$. On définit l'opération $z_1 \otimes z_2 = z_1 z_2 + \Im(z_1)\Im(z_2)$ où $\Im(z)$ désigne la partie imaginaire de z.

1. Montrer que $(\mathbb{C}, +, \otimes)$ est un anneau (préciser les neutres des deux opérations).
2. Montrer que les éléments inversibles (pour $\otimes$) de $(\mathbb{C}, +, \otimes)$ sont les éléments de partie réelle non nulle, et exprimer l'inverse d'un élément $z = a + ib$ où a, $b \in \mathbb{R}$ et $i^2 = -1$.

Exercice 3. (sur 9 pts) *Racines carrées modulo p*

Soit p un nombre premier. Un élément $\alpha \in \mathbb{Z}/p\mathbb{Z}$ est un *carré* [1] s'il existe $\tau \in \mathbb{Z}/p\mathbb{Z}$ (une *racine carrée de* α) tel que $\tau^2 = \alpha$. L'objectif de cet exercice est de décrire un algorithme, dû à René Peralta, qui étant donné $\alpha \in \mathbb{Z}/p\mathbb{Z}$ calcule une racine de α si α est un carré.

Dans la suite, on s'intéresse uniquement au cas $\alpha \in \mathbb{Z}/p\mathbb{Z}^\times$, c'est-à-dire à $\alpha \neq [0]_p$. De plus, on suppose que $p > 2$ (donc p est impair en particulier).

1. On souhaite montrer que $\alpha \in \mathbb{Z}/p\mathbb{Z}^\times$ est un carré si et seulement si $\alpha^{\frac{p-1}{2}} = [1]_p$. Soit γ un générateur de $\mathbb{Z}/p\mathbb{Z}^\times$: pour tout $\alpha \in \mathbb{Z}/p\mathbb{Z}^\times$, il existe un unique $k \in \{0, \dots, p-2\}$ tel que $\alpha = \gamma^k$.

- **i.** Quel résultat du cours permet d'affirmer que pour tout $\alpha \in \mathbb{Z}/p\mathbb{Z}^\times$, $\alpha^{p-1} = [1]_p$?
- **ii.** Montrer que α est un carré si et seulement si k est pair.
- **iii.** En déduire que α est un carré si et seulement si $\alpha^{\frac{p-1}{2}} = [1]_p$.
- **iv.** Déduire de **ii.** qu'exactement la moitié des éléments de $\mathbb{Z}/p\mathbb{Z}^\times$ sont des carrés.

2. Soit $\beta \in \mathbb{Z}/p\mathbb{Z}$ tel que $\beta^2 \neq \alpha$, et $B = A + \beta I$ où $A = \begin{pmatrix} [0]_p & [1]_p \\ \alpha & [0]_p \end{pmatrix}$ et $I \in \mathbb{Z}/p\mathbb{Z}^{2\times 2}$ est la matrice identité.

- **i.** Montrer que pour tout k, $A^{2k+1} = \alpha^{k-1}A$. *Indication. Calculer* A^2 *et utiliser une récurrence sur* k.
- **ii.** Montrer que $B^{p-1} = I$. *Indication. Pour* X, $Y \in \mathbb{Z}/p\mathbb{Z}^{2\times 2}$, $(X+Y)^p = X^p + Y^p$.
- **iii.** Montrer que pour tout $n > 0$, il existe λ, $\mu \in \mathbb{Z}/p\mathbb{Z}$ tels que $B^n = \lambda A + \mu I$.
- **iv.** Déduire des questions précédentes que si $B^{\frac{p-1}{2}} = \lambda A + \mu I$, alors $\lambda = [0]_p$ ou $\mu = [0]_p$.

3. On suppose maintenant que $\beta^2 - \alpha$ n'est pas un carré (ce qui implique entre autre que $\beta^2 \neq \alpha$). On veut montrer qu'on a forcément $\lambda \neq [0]_p$.

- **i.** Montrer que $\det(B^{\frac{p-1}{2}}) = [-1]_p$. *Indication. Utiliser que* $\det(M^k) = \det(M)^k$.
- **ii.** Montrer que si $\lambda = [0]_p$, alors $\det(B^{\frac{p-1}{2}}) = [1]_p$ et en déduire une contradiction. *Indication. Calculer* $\det(B^{p-1})$ *et montrer que* $\mu^2 = [1]_p$.

4. Déduire des questions précédentes que si $\beta^2 - \alpha$ n'est pas un carré, alors $B^{\frac{p-1}{2}} = \lambda A$ avec $\lambda^2 = \alpha^{-1}$.

L'algorithme de Peralta consiste à tirer un β *aléatoirement et à calculer* $B^{\frac{p-1}{2}}$. *On obtient alors une matrice de la forme* $\begin{pmatrix} 0 & \lambda \\ \lambda\alpha & 0 \end{pmatrix}$, *d'où on tire une racine carré* $\tau = \lambda^{-1}$ *de* α. *Pour montrer son efficacité, il suffit de montrer que si* β *est tiré aléatoirement, alors* $\beta^2 - \alpha$ *n'est pas un carré avec bonne probabilité.*

1. Le vrai nom est *résidu quadratique* mais on utilisera *carré* par simplicité.