Contrôle final

Calculatrice et documents sont interdits.
Tous les résultats doivent être correctement rédigés et rigoureusement justifiés.
Le barème est donné à titre indicatif.
La qualité de la rédaction sera fortement prise en compte dans la notation.

Exercice 1 : réciprocité quadratique (suite) (8 points)

- Soit p un nombre premier impair. Nous notons $\mathbf{F}_p = (\mathbf{Z}/p\mathbf{Z})^*$ et nous nous placerons dans tout l'exercice dans le groupe $(\mathbf{F}_p, \times)$.
- Pour $\overline{a} \in \mathbf{F}_p$, on dit que $\overline{a}$ est un **carré** s'il existe $\overline{b} \in \mathbf{F}_p$ tel que $\overline{a} = \overline{b}^2$.
- Nous notons $\mathcal{C}$ l'ensemble des carrés de $\mathbf{F}_p$.
- Nous définissons sur $\mathbf{F}_p$ l'application $f : \overline{a} \mapsto \overline{a}^{\frac{p-1}{2}}$.

1. Montrer que $\mathcal{C}$ est un sous-groupe de $(\mathbf{F}_p, \times)$.

   — Soient $\overline{a}$ et $\overline{a}'$ dans $\mathcal{C}$. Donc $\overline{a}$ et $\overline{a}'$ sont des carrés : il existe $\overline{b}$ et $\overline{b}'$ dans $\mathbf{F}_p$ tels que $\overline{a} = \overline{b}^2$ et $\overline{a}' = \overline{b}'^2$. Alors $\overline{aa}' = \overline{b}^2\overline{b}'^2 = \overline{bb}'^2$. Donc $\overline{aa}'$ est un carré, c'est encore un élément de $\mathcal{C}$.
   — L'élément neutre de $\mathbf{F}_p$ est $\overline{1}$. Or $\overline{1} = \overline{1}^2$, donc $\overline{1} \in \mathcal{C}$.
   — Soit $\overline{a} \in \mathcal{C}$. Alors il existe $\overline{b}$ tel que $\overline{a} = \overline{b}^2$. Passons à l'inverse : $\overline{a}^{-1} = \left(\overline{b}^2\right)^{-1} = \left(\overline{b}^{-1}\right)^2$. Donc $\overline{a}^{-1}$ est un carré : $\overline{a}^{-1} \in \mathcal{C}$.

   Ainsi $\mathcal{C}$ est un sous-groupe de $(\mathbf{F}_p, \times)$.

   Remarque : une preuve plus simple est possible. On peut démontrer (comme dans la question 4) que l'application $\varphi : \overline{a} \mapsto \overline{a}^2$ est un endomorphisme de $\mathbf{F}_p$. L'ensemble $\mathcal{C}$ est égal à $f(\mathbf{F}_p$. Or l'image d'un morphisme est un sous-groupe du groupe d'arrivée, donc $\mathcal{C}$ est un sous-groupe de $(\mathbf{F}_p, \times)$.

2. Montrer que dans $\mathbf{F}_p$, $\overline{a}^2 = \overline{b}^2$ si et seulement si $\overline{a} = \overline{b}$ ou $\overline{a} = -\overline{b}$.
   On en déduit en particulier que $\overline{a}^2 = \overline{1}$ si et seulement si $\overline{a} = \overline{1}$ ou $\overline{a} = -\overline{1}$.

   Raisonnons par équivalence :
   $\overline{a}^2 = \overline{b}^2$ si et seulement si $\overline{a}^2 - \overline{b}^2 = \overline{0}$ ssi $(\overline{a} - \overline{b})(\overline{a} + \overline{b}) = \overline{0}$. Or, comme p est premier, la multiplication dans $\mathbf{Z}/p\mathbf{Z}$ est intègre. Notre égalité est donc équivalente à : $\overline{a} - \overline{b} = \overline{0}$ ou $\overline{a} + \overline{b} = \overline{0}$.
   Ainsi $\overline{a}^2 = \overline{b}^2$ si et seulement si $\overline{a} = \overline{b}$ ou $\overline{a} = -\overline{b}$.

3. En déduire que $\mathcal{C}$ contient $\frac{p-1}{2}$ éléments.

   Il y a $p-1$ éléments $\overline{a}$ dans $\mathbf{F}_p$. Il y a donc au plus $p-1$ carrés $\overline{a}^2$ différents dans $\mathbf{F}_p$. La proposition précédente affirme que $\overline{a}$ et $-\overline{a}$ ont le même carré (ce qui est évident) mais elle affirme surtout qua $-\overline{a}$ est le seul élément à avoir le même carré que $\overline{a}$. Comme p est un nombre impair, il est impossible que $\overline{a} = -\overline{a}$ dans $\mathbf{F}_p$ (sinon $\overline{2}\overline{a} = \overline{0}$, ce qui implique $\overline{a} = \overline{0}$ qui n'appartient pas à $\mathbf{F}_p$. Conclusion : tout carré de $\mathbf{F}_p$ est le carré d'exactement

2 éléments différents de $\mathbf{F}_p$. Comme il y a $p-1$ éléments dans $\mathbf{F}_p$, il y a exactement $\frac{p-1}{2}$ carrés différents dans $\mathbf{F}_p$. Donc $\mathcal{C}$ est de cardinal $\frac{p-1}{2}$.

4. Montrer que f est un endomorphisme de $(\mathbf{F}_p, \times)$.

   Soient $\overline{a}$ et $\overline{a}'$ dans $\mathcal{C}$. Alors

   $$f(\overline{a} \times \overline{a}') = f(\overline{aa'}) = (\overline{aa'})^{\frac{p-1}{2}} = \overline{a}^{\frac{p-1}{2}} \overline{a'}^{\frac{p-1}{2}} = f(\overline{a}) \times f(\overline{a}'),$$

   par commutativité de la multiplication dans $\mathbf{F}_p$. Donc f est bien un endomorphisme de $\mathbf{F}_p$.

5. Soit $\overline{a} \in \mathbf{F}_p$. Que vaut $f(\overline{a})^2$? En déduire que $f(\overline{a}) = \overline{1}$ ou $-\overline{1}$.

   Nous avons : $f(\overline{a})^2 = \left(\overline{a}^{\frac{p-1}{2}}\right)^2 = \overline{a}^{p-1} = \overline{1}$ d'après le petit théorème de Fermat. D'après la remarque de la question 2, nous déduisons que $f(\overline{a}) = \overline{1}$ ou $-\overline{1}$.

6. Rappeler la définition de $\mathrm{Ker}(f)$ et montrer que $\mathcal{C} \subset \mathrm{Ker}(f)$.

   L'élément neutre de $\mathbf{F}_p$ est $\overline{1}$, donc le noyau de f est défini par : $\mathrm{Ker}(f) = \{\overline{a} \in \mathbf{F}_p \mid f(\overline{a}) = \overline{1}\}$.

   Soit $\overline{a} \in \mathcal{C}$ et soit donc $\overline{b}$ tel que $\overline{a} = \overline{b}^2$. Alors $f(\overline{a}) = \overline{a}^{\frac{p-1}{2}} = \left(\overline{b}^2\right)^{\frac{p-1}{2}} = \overline{b}^{p-1} = \overline{1}$, toujours d'après le petit théorème de Fermat. Donc $f(\overline{a}) = \overline{1}$ et $\overline{a} \in \mathrm{Ker}(f)$. Ainsi : $\mathcal{C} \subset \mathrm{Ker}(f)$.

7. D'après une propriété du cours, il existe un élément $\overline{c}$ de $\mathbf{F}_p$ d'ordre $p-1$ dans le groupe. Que vaut alors $f(\overline{c})$?

   Nous savons d'après la question 2 que $f(\overline{c}) = \overline{1}$ ou $-\overline{1}$. Si $f(\overline{c}) = \overline{1}$, alors $\overline{c}^{\frac{p-1}{2}} = \overline{1}$. Or l'ordre de $\overline{c}$ est la plus petite puissance d telle que $\overline{c}^d = \overline{1}$. Nous en déduisons donc que $\overline{c}$ est d'ordre inférieur à $\frac{p-1}{2}$. Or nous savons que $\overline{c}$ est d'ordre $p-1$, donc c'est contradictoire. Donc $f(\overline{c}) \neq \overline{1}$ et nous concluons : $f(\overline{c}) = -\overline{1}$.

8. Déduire du théorème de Lagrange que $\mathcal{C} = \mathrm{Ker}(f)$.

   Le noyau $\mathrm{Ker}(f)$ est un sous-groupe de $\mathbf{F}_p$. Nous savons qu'il contient $\mathcal{C}$ et d'après la question précédente, il ne contient pas tous les éléments de $\mathbf{F}_p$. Son cardinal est donc supérieur ou égal à $\frac{p-1}{2}$ et inférieur strictement à $p-1$. Or d'après le théorème de Lagrange, ce cardinal divise $p-1$. La seule possibilité est qu'il soit égal à $\frac{p-1}{2}$. Ses éléments sont donc les $\frac{p-1}{2}$ éléments de $\mathcal{C}$. Donc $\mathcal{C} = \mathrm{Ker}(f)$.

   Conclusion : $\overline{a}$ est un carré si et seulement si $f(\overline{a}) = \overline{1}$, et $\overline{a}$ n'est pas un carré si et seulement si $f(\overline{a}) = -\overline{1}$. La fonction f permet de définir le **symbole de Legendre**.

9. En déduire que si $\overline{a}$ et $\overline{b}$ ne sont pas des carrés, alors $\overline{ab}$ est un carré.

   Supposons que $\overline{a}$ et $\overline{b}$ ne sont pas des carrés. Alors $f(\overline{a}) = -\overline{1}$ et $f(\overline{b}) = -\overline{1}$. Donc, comme f est un morphisme :

   $$f(\overline{ab}) = f(\overline{a})f(\overline{b}) = (-\overline{1}) \times (-\overline{1}) = \overline{1}.$$

   Donc $\overline{ab}$ est un carré.

Exercice 2 : racines carrées de matrices

Nous nous plaçons dans l'ensemble $\mathcal{M}_n(\mathbf{C})$ des matrices carrées de taille n à coefficients complexes.

Comme dans l'exercice précédent, nous disons qu'une matrice $A \in \mathcal{M}_n(\mathbf{C})$ est un **carré** s'il existe une matrice $B \in \mathcal{M}_n(\mathbf{C})$ telle que $A = B^2$. On dit alors que B est une **racine carrée** de A.

1. **Exemples** **(3,5 points)**

   (a) Soit $A = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}$. Trouver une matrice $B \in \mathcal{M}_3(\mathbf{C})$ telle que $B^2 = A$.

   La matrice diagonale $B = \begin{bmatrix} \sqrt{2} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \mathrm{i} \end{bmatrix}$ convient immédiatement.

   (b) Soit $R_\theta = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$ la matrice de la rotation d'angle θ. Est-elle un carré ?

   La matrice de rotation $\frac{\theta}{2}$ convient. En effet, le produit matriciel $R_{\frac{\theta}{2}} \times R_{\frac{\theta}{2}}$ revient à composer la rotation d'angle $\frac{\theta}{2}$ avec elle-même. Comme $r_{\frac{\theta}{2}} \circ r_{\frac{\theta}{2}} = r_\theta$, $R_{\frac{\theta}{2}} \times R_{\frac{\theta}{2}} = R_\theta$. Donc R_θ est un carré.

   (c) Donner une racine carrée dans $\mathbf{C}$ du nombre complexe i.

   Sa forme polaire est : $\mathrm{i} = \mathrm{e}^{\mathrm{i}\frac{\pi}{2}}$. Donc une racine carrée de i est : $\omega = \mathrm{e}^{\mathrm{i}\frac{\pi}{4}}$.

   (d) Soit $B = \begin{bmatrix} \mathrm{i} & 1 \\ 0 & \mathrm{i} \end{bmatrix}$. Calculer B^2, B^3 et B^4, puis démontrer que pour tout entier n : $B^n = \begin{bmatrix} \mathrm{i}^n & n\mathrm{i}^{n-1} \\ 0 & \mathrm{i}^n \end{bmatrix}$.

   $B^2 = \begin{bmatrix} -1 & 2\mathrm{i} \\ 0 & -1 \end{bmatrix}$, $B^3 = \begin{bmatrix} -\mathrm{i} & -3 \\ 0 & -\mathrm{i} \end{bmatrix}$ et $B^4 = \begin{bmatrix} 1 & -4\mathrm{i} \\ 0 & 1 \end{bmatrix}$.
   Montrons le résultat proposé par récurrence sur n : d'après ce qui précède, le résultat est vérifié aux rangs 1, 2, 3 et 4.
   Supposons qu'au rang n, $B^n = \begin{bmatrix} \mathrm{i}^n & n\mathrm{i}^{n-1} \\ 0 & \mathrm{i}^n \end{bmatrix}$. Alors

   $$B^{n+1} = BB^n = \begin{bmatrix} \mathrm{i} & 1 \\ 0 & \mathrm{i} \end{bmatrix} \begin{bmatrix} \mathrm{i}^n & n\mathrm{i}^{n-1} \\ 0 & \mathrm{i}^n \end{bmatrix} = \begin{bmatrix} \mathrm{i}^{n+1} & n\mathrm{i}^n + \mathrm{i}^n \\ 0 & \mathrm{i}^{n+1} \end{bmatrix} = \begin{bmatrix} \mathrm{i}^{n+1} & (n+1)\mathrm{i}^n \\ 0 & \mathrm{i}^{n+1} \end{bmatrix}.$$

   C'est bien l'expression voulue au rang $n+1$. Le résultat est ainsi démontré pour tout n.

   (e) Trouver une racine carrée de B. *Indication : essayer* $n = \frac{1}{2}$.

   Pour $n = \frac{1}{2}$, nous obtenons formellement : $B^{\frac{1}{2}} = \begin{bmatrix} \mathrm{i}^{\frac{1}{2}} & \frac{1}{2}\mathrm{i}^{-\frac{1}{2}} \\ 0 & \mathrm{i}^{\frac{1}{2}} \end{bmatrix}$. La notation $B^{\frac{1}{2}}$ n'est pas admise dans le monde des matrices et $\mathrm{i}^{\frac{1}{2}}$ n'est pas rigoureux dans $\mathbf{C}$, mais cela nous incite à utiliser une racine carrée de i.

Posons $C = \begin{bmatrix} \omega & \frac{1}{2\omega} \\ 0 & \omega \end{bmatrix}$. Alors

$$C^2 = \begin{bmatrix} \omega^2 & \frac{1}{2} + \frac{1}{2} \\ 0 & \omega^2 \end{bmatrix} = \begin{bmatrix} \mathrm{i} & 1 \\ 0 & \mathrm{i} \end{bmatrix} = B$$

Donc C est une racine carrée de B.

2. **Matrices diagonalisables** **(2 points)**

Soit $M \in \mathcal{M}_n(\mathbf{C})$. On suppose qu'elle est diagonalisable : il existe une matrice inversible P et une matrice diagonale D telles que $PMP^{-1} = D$.

(a) Justifier que D est un carré dans $\mathcal{M}_n(\mathbf{C})$.

Notons $d_1, \ldots, d_n$ les valeurs diagonales de D. Ce sont des nombres complexes. Or tout nombre complexe admet une racine carrée dans $\mathbf{C}$. Posons alors $\omega_1, \ldots, \omega_n$ des racines carrées des nombres $d_1, \ldots, d_n$, et posons W la matrice diagonale de coefficients diagonaux $\omega_1, \ldots, \omega_n$. Alors, par multiplication de matrices diagonales, nous obtenons : $W^2 = D$. Donc D est bien un carré dans $\mathcal{M}_n(\mathbf{C})$.

(b) En déduire que M est également un carré dans $\mathcal{M}_n(\mathbf{C})$.

Reprenons la matrice W précédente et posons $Z = P^{-1}WP$. Alors $Z^2 = P^{-1}WPP^{-1}WP = P^{-1}W^2P = P^{-1}DP$. Or, comme $PMP^{-1} = D$, nous déduisons $M = P^{-1}DP$, donc $M = Z^2$. Toute matrice diagonalisable dans $\mathcal{M}_n(\mathbf{C})$ est donc un carré.

3. **Un contre-exemple** **(3 points)**

Soit $N = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

Nous supposons par l'absurde que N admet une racine carrée $C \in \mathcal{M}_2(\mathbf{C})$.

(a) Montrer que $C^4 = 0$. En déduire que C n'est pas inversible.

Remarquons tout d'abord que N^2 est égale à la matrice nulle. Par définition de C, $N = C^2$. Donc $C^4 = N^2 = 0$.
Si C était inversible, alors C^4 serait également inversible (car un produit de matrices inversibles est inversible). Or la matrice nulle n'est pas inversible donc C n'est pas inversible.

(b) D'après un résultat (vu en TD) propre aux matrices de taille 2, il existe α et β dans $\mathbf{C}$ tels que : $C^2 + \alpha C + \beta I_2 = 0$.
Justifier que $\beta = 0$ puis montrer que $C^2 = 0$.

Si $\beta \neq 0$, nous pouvons déduire de l'égalité : $C(-\frac{1}{\beta}C - \frac{\alpha}{\beta}I_2) = I_2$. Donc C est inversible de matrice inverse $-\frac{1}{\beta}C - \frac{\alpha}{\beta}I_2$. Or nous avons vu que C n'était pas inversible, donc β est nécessairement nul.
Donc $C^2 + \alpha C = 0$, donc $C^2 = -\alpha C$. Alors $C^4 = (-\alpha C)^2 = \alpha^2 C^2$. Comme $C^4 = 0$, nous déduisons $\alpha = 0$ ou $C^2 = 0$. Si $\alpha = 0$, notre égalité devient $C^2 = 0$. Donc dans tous les cas, nous concluons que $C^2 = 0$.

(c) Conclure.

Or $N = C^2$ par hypothèse. Nous concluons donc de ce qui précède que $N = 0$ ce qui est visiblement faux. Notre hypothèse initiale est donc absurde : N n'admet pas de racine carrée dans $\mathcal{M}_2(\mathbf{C})$.

4. **Propriétés algébriques** **(2 points)**

(a) Si on se restreint aux matrices inversibles, l'application $\varphi : M \mapsto M^2$ définit-elle un morphisme de groupe pour le produit matriciel ?

Soient M et M' deux matrices inversibles. Alors $\varphi(MM') = (MM')^2 = MM'MM'$. Si les matrices M et M' ne commutent pas, nous ne pouvons pas déduire que $\varphi(MM') = M^2M'^2 = \varphi(M)\varphi(M')$.
Hormis le cas des matrices de taille 1, il est facile d'exhiber des contre-exemples. Par exemple, avec $M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ et $M' = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, nous obtenons :

$$\varphi(MM') = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad \neq \quad \varphi(M)\varphi(M') = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

(b) L'ensemble des matrices qui admettent une racine carrée est-il stable par addition ou par multiplication ?
On pourra par exemple considérer les matrices suivantes qui sont des carrés (d'après les résultats des parties précédentes) :

$$\begin{bmatrix} -\mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{bmatrix} \qquad \begin{bmatrix} \mathrm{i} & 1 \\ 0 & \mathrm{i} \end{bmatrix} \qquad R_{\frac{\pi}{2}} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 \\ 0 & -1 \end{bmatrix}$$

Les deux premières matrices sont des carrés (d'après les questions 2 et 1-e) mais leur somme $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ n'est pas un carré d'après la question 3. Être un carré n'est donc pas une propriété stable par addition.
Les deux dernières matrices sont des carrés (d'après les questions 1-b et 2) mais leur produit $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ n'est pas un carré. Être un carré n'est donc pas une propriété stable par multiplication.

5. **Un dernier exemple** **(3,5 points)**

$$\text{Soient} \qquad M = \begin{bmatrix} 2 & 3 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 2-\mathrm{i} & 2 & \mathrm{i} & 1 \\ 0 & -1-\mathrm{i} & 0 & \mathrm{i} \end{bmatrix} \quad \text{et} \quad P = \begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

(a) Montrer que P est inversible et calculer sa matrice inverse.

Avec l'algorithme du pivot de Gauss, nous obtenons que P est inversible et $P^{-1} = \begin{bmatrix} 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & -1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$.

(b) Calculer PMP^{-1}.

Nous obtenons :

$$PMP^{-1} = \begin{bmatrix} \mathrm{i} & 1 & 0 & 0 \\ 0 & \mathrm{i} & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

(c) En déduire que M est un carré.

Reprenons la racine carrée ω de i dans $\mathbf{C}$. Posons alors $S = \begin{bmatrix} \omega & \frac{1}{2\omega} & 0 & 0 \\ 0 & \omega & 0 & 0 \\ 0 & 0 & \sqrt{2} & 0 \\ 0 & 0 & 0 & \mathrm{i} \end{bmatrix}$ et $T = P^{-1}SP$. En reprenant les résultats de la partie 1, nous obtenons que $S^2 = PMP^{-1}$ et nous en déduisons, comme dans la partie 2, que $T^2 = M$. Donc M est bien un carré.