Université Claude Bernard Lyon 1 — Algèbre et Géométrie
Semestre d'automne 2022-23 — L3 MGA

Examen 1 – Durée 180 min – le mercredi 25 mai 2022

La notation tiendra compte du soin apporté à la rédaction des réponses.
Les **réponses mal justifiées** ne permettront pas d'obtenir tous les points.
L'énoncé comporte 5 exercices.

Exercice 1. Une forme quadratique.

Soit $A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix}$.

1. Déterminer la signature de la forme quadratique associée à la matrice A.
2. Déterminer une matrice inversible P et une matrice diagonale D avec des coefficients ± 1 telles que :

$$^tPAP = D.$$

Exercice 2. Géométrie Affine. Soit $\mathbb{K}$ un corps de caractéristique différente de 2. Soit $\mathcal{E}$ un espace affine de direction le $\mathbb{K}$-espace vectoriel E. Une application affine $s : \mathcal{E} \to \mathcal{E}$ est appelée symétrie si $s \circ s = \mathrm{Id}_{\mathcal{E}}$. Elle est dite centrale de centre I si I est son unique point fixe.

(I) Soit Γ l'ensemble des applications affines $f : \mathcal{E} \to \mathcal{E}$ telles que $\overrightarrow{f} \in \{\mathrm{Id}_E, \ -\mathrm{Id}_E\}$.

1. Montrer que Γ est un sous-groupe du groupe affine de $\mathcal{E}$ et que Γ est la réunion des translations et des symétries centrales de $\mathcal{E}$.

   On vérifie immédiatement que $\{\mathrm{Id}_E, \ -\mathrm{Id}_E\}$ est stable par composition et inversion : c'est un sous-groupe de $GL(E)$.

   Si f et g sont deux applications affines de $\mathcal{E}$ dans lui-même, on a vu en cours que $\overrightarrow{f \circ g} = \overrightarrow{f} \circ \overrightarrow{g}$. On en déduit immédiatement que Γ est stable par composition.

   De même, si f est bijective, on a vu en cours que $\overrightarrow{f^{-1}} = (\overrightarrow{f})^{-1}$. Donc Γ est stable par inverse. Finalement, Γ est un sous-groupe.

   Soit f dans Γ tel que $\overrightarrow{f} = \mathrm{Id}_E$. D'après le cours f est une translation.

   Soit f dans Γ tel que $\overrightarrow{f} = -\mathrm{Id}_E$. Par la règle rappelée ci-dessus, on a $\overrightarrow{f \circ f} = \mathrm{Id}_E$. Donc $f \circ f$ est une translation.

   Montrons que f admet au moins un point fixe. Soit $A \in \mathcal{E}$ et $B = f(A)$. On a

$$f(A + \frac{\overrightarrow{AB}}{2}) = B - \frac{\overrightarrow{AB}}{2} = A + \frac{\overrightarrow{AB}}{2}.$$

   Donc f a un point fixe.

   Donc $f \circ f$ a un point fixe et est une translation. Donc $f \circ f$ est l'identité. C'est une symétrie par définition.

2. Soient f, g deux symétries centrales de centres respectifs A et B. Montrer que $g \circ f$ est une translation et donner le vecteur de cette translation en fonction de A et B.

   Comme $\overrightarrow{g \circ f} = \mathrm{Id}_E$, $g \circ f$ est une translation. Or $g \circ f(A) = g(A)$. Donc le vecteur de $g \circ f$ est $\overrightarrow{Ag(A)} = 2\overrightarrow{AB}$.

3. Soit s une symétrie centrale de centre A et t une translation de vecteur u. Justifier que $s \circ t$ et $t \circ s$ sont des symétries centrales et donner leur centre en fonction de A et u.

   $s \circ t$ et $t \circ s$ sont des éléments de Γ dont l'application linéaire associée est -$Id_E E$. Ceux sont deux symétries.

   Par ailleurs, $s(M) = M + 2\overrightarrow{MA}$ et $t(M) = M + u$, pour tout point M.

Donc, M est un point fixe de $s \circ t$ ssi $s \circ t(M) = M$ ssi $M = s(M+u) = s(M) - u = M + 2\overrightarrow{MA} - u$ ssi $2\overrightarrow{MA} = u$ ssi $M = A - \frac{u}{2}$. Donc $s \circ t$ a un unique point fixe et est une symétrie centrale.

De même, M est un point fixe de $t \circ s$ ssi $t \circ s(M) = M$ ssi $M = M + 2\overrightarrow{MA} + u$ ssi $2\overrightarrow{MA} = -u$ ssi $M = A + \frac{u}{2}$. Donc $t \circ s$ a un unique point fixe et est une symétrie centrale.

Donner une condition nécessaire et suffisante pour que s et t commutent.

$s \circ t$ et $t \circ s$ sont deux symétries centrales. Elles coïncident ssi leurs centres sont égaux ssi $A + \frac{u}{2} = A - \frac{u}{2}$ ssi $u = 0$ ssi t est l'identité.

(II) Soient $P_1, \ldots, P_n$, n points de l'espace affine $\mathcal{E}$. On se pose le problème suivant :
Peut-on trouver n points $M_1, \ldots, M_n$ de $\mathcal{E}$ tels que pour tout $i \leq n-1$, P_i soit le milieu du segment $[M_i, M_{i+1}]$ et P_n le milieu du segment $[M_n, M_1]$?
Voici une manière de répondre. Soit s_i la symétrie de centre P_i.

1. En supposant le problème résolu, montrer que pour tout $i \geq 2$, $M_i = s_{i-1} \circ s_{i-2} \circ \cdots \circ s_1(M_1)$.
   L'hypothèse donne $s_i(M_{i-1}) = M_i$ pour tout $i \geq 2$. L'égalité demandée en découle par une récurence immédiate.
2. En déduire que le problème admet une solution si et seulement si $s_n \circ s_{n-1} \circ \cdots \circ s_1$ admet un point fixe.
   Si le probléme a une solution, on a $s_n \circ s_{n-1} \circ \cdots \circ s_1(M_1) = s_n(M_n) = M_1$. D'où une direction.
   Réciproquement, si $s_n \circ s_{n-1} \circ \cdots \circ s_1$ admet un point fixe noté M_1. On obtient une solution en posant $M_i = s_{i-1} \circ s_{i-2} \circ \cdots \circ s_1(M_1)$.
3. Montrer que si n est impair alors il y a une solution unique au problème.
   Si n est impair, l'application linéaire associée à $s_n \circ s_{n-1} \circ \cdots \circ s_1$ est -Id_E. Il s'agit donc d'une symétrie qui a au moins un point fixe. D'après la question précédente, le problème a une solution.
4. Si n est pair, donner une condition nécessaire et suffisante pour qu'il existe au moins une solution. Est-elle unique ?
5. Illustration sur $E = \mathbb{R}^2$: Faire la construction explicite pour $P_1 = (-1, 1), P_2 = (0, 1/2), P_3 = (1, 1), P_4 = (1, -1), P_5 = (-1, -1)$.
6. Montrer que pour que quatre points soient les milieux des côtés d'un quadrilatère il faut et il suffit qu'ils soient les sommets d'un parallélogramme.

Exercice 3. Polynômes irréductibles.
Soit $P(X) = X^3 - 3X + 1$.

1. Montrer que P est irréductible sur $\mathbb{Q}$.
   D'après le théorème de Gauss sur le contenu, il suffit de montrer que P est irréductible dans $\mathbb{Z}[X]$. Or $aX + b \in \mathbb{Z}[X]$ divise P implique $a = \pm 1$ (d'après le coefficient dominant). Mais alors, $\pm b$ est une racine de P. Il suffit donc de montrer que P n'a pas de racine dans $\mathbb{Z}$.
   Supposons par l'absurde que $P(b) = 0$ avec $b \in \mathbb{Z}$. Bien sûr $b \neq 0$. Or $|b^3| = |3b-1| \leq 3|b|+1 \leq 4|b|$. Donc $|b| \leq 2$ et $b \in \{\pm 2, \pm 1\}$. On vérifie immédiatement qu'aucune de ces 4 valeurs conviennent. Contradiction.
2. Montrer que $\theta := 2\cos\frac{2\pi}{9}$ est racine de P. *Indication.* $\forall x \in \mathbb{R}$, $\cos 3x = 4\cos^3 x - 3\cos x$.
   La formule donnée pour $x = \frac{2\pi}{9}$ donne
   $$-\frac{1}{2} = \cos\frac{2\pi}{3} = 4(\cos\frac{2\pi}{9})^3 - 3(\cos\frac{2\pi}{9}),$$
   puis $P(\theta) = 0$.
3. Quel est la dimension du corps $\mathbb{Q}\left(\cos\frac{2\pi}{9}\right)$ comme $\mathbb{Q}-$espace vectoriel sur $\mathbb{Q}$? En donner une base.
   D'après les 2 questions précédentes P est le polynôme minimal de θ. Donc la dimension de $\mathbb{Q}(\theta) = \mathbb{Q}\left(\cos\frac{2\pi}{9}\right)$ comme $\mathbb{Q}$-ev est 3.
   Une base est $(1, \theta, \theta^2)$.

Exercice 4. Idéaux maximaux de $\mathbb{C}[X_1, \dots, X_n]$.

1. Soit $\mathbb{C}(X)$ le corps des fractions rationnelles.

   Montrer que la famille $\left(\frac{1}{X-z}\right)_{z\in\mathbb{C}}$ est libre.

   Soit $\sum \lambda_i \frac{1}{X-z_i} = 0$ une combinaison linéaire nulle. Ici les z_i sont en nombre fini et 2 à 2 distincts et les λ_i sont des réels. En multipliant cette identité par $X - z_j$, puis en évaluant en $X = z_j$, on obtient $\lambda_j = 0$. Donc tous les λ_j sont nuls. CQFD

2. Soit $\mathbb{C}[X_1, \dots, X_n]$ l'anneau des polynômes en n variables avec $n \in \mathbb{N}$ non nul.

   Soit $a_1, \dots, a_n$ n nombre complexes. Montrer que $\mathcal{I} = (X - a_1, \dots, X - a_n)$ est un idéal maximal de $\mathbb{C}[X_1, \dots, X_n]$.

   Considérons le morphisme $\varphi : \mathbb{C}[X_1, \dots, X_n] \longrightarrow \mathbb{C}, P \longmapsto P(a_1, \dots, a_n)$. Alors φ est surjectif et Kerφ contient $\mathcal{I}$. Donc Ker$\varphi/\mathcal{I}$ est un sous-anneau de $\mathbb{C}$. C'est donc un corps. Donc $\mathcal{I}$ est maximal.

   On se propose de montrer que tout idéal maximal est de ce type.

3. Ecrire $\mathbb{C}[X_1, \dots, X_n]$ comme une réunion dénombrable d'espaces vectoriels de dimension finie.

   Soit $\mathbb{C}[X_1, \dots, X_n]_d$ l'ensemble des polynômes de degré total inférieur ou égal à d. La dimension de $\mathbb{C}[X_1, \dots, X_n]_d$ est finie et leur réunion est $\mathbb{C}[X_1, \dots, X_n]$.

4. Soit $\mathcal{I}$ un idéal de $\mathbb{C}[X_1, \dots, X_n]$. Montrer que $\mathbb{C}[X_1, \dots, X_n]/\mathcal{I}$ est une réunion dénombrable d'espaces vectoriels de dimension finie.

   $\mathbb{C}[X_1, \dots, X_n]/\mathcal{I}$ est la réunion des images des $\mathbb{C}[X_1, \dots, X_n]_d$ qui sont des sous-espaces vectoriels de dimension finie.

5. Soit $\mathcal{M}$ un idéal maximal de $\mathbb{C}[X_1, \dots, X_n]$ et

   $$\begin{array}{rccc} \phi_i : & \mathbb{C}[X_i] & \longrightarrow & \mathbb{C}[X_1, \dots, X_n]/\mathcal{M} \\ & P & \longmapsto & P + \mathcal{M} \end{array}$$

   On suppose que ϕ_i est injectif.

6. Montrer que ϕ_i s'étend alors en un morphisme injectif de $\mathbb{C}(X_i)$ dans $\mathbb{C}[X_1, \dots, X_n]/\mathcal{M}$.

   Puisque $\mathbb{C}[X_1, \dots, X_n]/\mathcal{M}$ est un corps, $\phi_i(Q)$ est inversible pour Q non nul (ϕ_i étant injectif). Donc la formule $\phi_i(\frac{P}{Q}) = \phi_i(P)\phi_i(Q)^{-1}$ prolonge ϕ_i.

7. En utilisant les questions 1 et 3 aboutir à une contradiction.

   Soit F_d des sous-espaces de dimension finie dont la réunion est $\mathbb{C}[X_1, \dots, X_n]/\mathcal{M}$. L'image de la famille de la question est libre. Donc elle vérifie

   (a) son intersection avec chaque F_d est finie ;

   (b) est égale à la réunion de ses intersections avec les F_d ;

   (c) est non dénombrable (comme $\mathbb{C}$).

   Ces propriétés sont contradictoires !

   On suppose désormais que $\mathrm{Ker}(\phi_i) = (P_i)$ avec P_i polynôme unitaire.

8. Montrer que le degré de P_i vaut 1.

   $\mathbb{C}[X]/(P_i)$ est un sous-anneau d'un corps. Il est donc intègre. Donc $\deg(P_i) = 1$.

   On écrit $P_i = X - z_i$ avec $z_i \in \mathbb{C}$.

9. Montrer que $\mathcal{M} = (X - z_1, \dots, X - z_n)$.

   D'après la question précédente, P_i appartient à $\mathcal{M}$. Comme l'idéal $(X-z_1, \dots, X-z_n)$ est maximal, on en déduit que $\mathcal{M} = (X - z_1, \dots, X - z_n)$.

Exercice 5. Un Anneau
Soit $A = \mathbb{Z} + \mathbb{Z}\sqrt{2}$.

1. Montrer que A est un sous-anneau de $\mathbb{R}$.
   Immédiat car $(\sqrt{2})^2 = 2 \in \mathbb{Z}$.
2. L'élément $1+\sqrt{2}$ est-il inversible dans A.
   Dans $\mathbb{R}$*, on a* $(1+\sqrt{2})^{-1} = \frac{1-\sqrt{2}}{(1+\sqrt{2})(1-\sqrt{2})} = \sqrt{2}-1 \in A$. *Donc* $1+\sqrt{2}$ *est inversible dans* A.
3. Montrer que l'application
   $$N : A \to \mathbb{Z},\ a+b\sqrt{2} \longmapsto a^2-2b^2$$
   (si $a, b \in \mathbb{Z}$) est multiplicative.
   Calcul direct sans difficulté.
   En déduire que si $a, b \in \mathbb{Z}$, alors :
   $$a+b\sqrt{2} \in A^\times \quad \text{ssi} \quad a^2-2b^2 = \pm 1.$$
   Posons $x = a+b\sqrt{2}$. *Si* $x \in A^\times$*, il existe* $x' \in A$ *tel que* $xx' = 1$. *La question précédente montre que* $N(x)N(x') = 1$. *Donc* $N(x)$ *est inversible dans* $\mathbb{Z}$*, c'est-à-dire* $N(x) = \pm 1$.

   Réciproquement, supposons que $N(x) = \pm 1$. *Alors* $N(x) = x.(a-b\sqrt{2}) = \pm 1$. *Donc* $\pm(a-b\sqrt{2})$ *est un inverse de* x *dans* A.
4. Soient $a, b \in \mathbb{F}_3$. Montrer que
   $$a^2-2b^2 = 0 \quad \Leftrightarrow \quad a = b = 0.$$
   $\mathbb{F}_3 = \{\pm 1, 0\}$. *Donc les carrés de* $\mathbb{F}_3$ *sont* 0 *et* 1. *On en déduit l'équivalence demandée en énumérant les cas.*
   En déduire que le quotient
   $$K = A/(3)$$
   est un corps.
   Soit $x = a+b\sqrt{2} \in A$ *dont la classe dans* K *est non nulle. Montrons que la classe* $\bar{x}$ *de* x *est inversible dans* K. *La classe de* $N(x)$ *dans* $\mathbb{F}_3$ *est non nulle. En effet, sinon , d'après la question précédente 3 divise* a *et* b *et* $\bar{x} = 0$.
   Donc la classe de $N(x)$ *dans* $\mathbb{F}_3$ *vaut* ± 1. *Comme à la question 3, on en déduit que* $\bar{x}$ *est inversible.*
   Quel est son cardinal ?
   Son cardinal est 9 (3 choix pour a *et* b*).*
5. Montrer que l'élément $1+\sqrt{2} \mod 3$ engendre le groupe des inversibles $K^\times$.
   Le groupe $K^\times$ *est de cardinal 8. Notons* x *la classe de* $1+\sqrt{2}$ *dans* K. *On a* $x^2 = -\sqrt{2}$*, puis* $x^4 = 2 = -1$. *Donc l'ordre de* x *divise* 8 *et vaut ni* 1*, ni* 2 *ni* 4. *Il vaut donc* 8 *!*
6. Montrer que l'idéal $(3, X^2-2)$ de $\mathbb{Z}[X]$ est maximal.
   $(3, X^2-2)$ *est le noyau du morphisme* $P \longmapsto P(\sqrt{2}) mod 3$ *de* $\mathbb{Z}[X]$ *dans* K. *Comme* K *est un corps, il est maximal.*
   Est-il principal ?
   Non. Un polynôme P *qui engendrerait cet idéal diviserait* 3 *donc serait* 1 *ou* 3. *Aucun de ces deux polynômes ne convient.*
7. Déterminer les polynômes unitaires irréductibles de degré 2 sur le corps $\mathbb{F}_3$.
   Ceux sont les polynômes qui n'ont pas de racine. Le résultat découle alors d'une discussion au cas par cas.
   En déduire la factorisation de $X^9 - X$ en produit d'irréductibles sur $\mathbb{F}_3$.
   On a $X^8 - X = (X^6+X^5+X^4+X^3+X^2+1)(X-1)X$. *Le polynôme* $(X^6+X^5+X^4+X^3+X^2+1)$ *est le produit des trois polynômes irréductibles de degré 2 (calcul direct).*
8. Montrer que pour chacun de ces polynômes P, $\mathbb{F}_3[X]/(P) \simeq K$.
   Par unicité des corps finis, $\mathbb{F}_3[X]/(P)$ *ne dépend que du degré de* P *qui vaut 2.*