Examen d'Algèbre, Semestre 2, 2013.

Durée 3 heures. 21 Mai 2013, 14h-17h
Notes de cours autorisées. Sujet de 3 pages.

Exercice 1

Soit q une puissance d'un nombre premier p, et $n \geq 1$. Soit $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ défini par $\sigma(x) = x^q$.

1. Montrer que σ est un automorphisme de $\mathbb{F}_{q^n}$.

2. Montrer que σ induit l'identité sur $\mathbb{F}_q$.

3. Le groupe de Galois $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ est le groupe de tous les automorphismes de $\mathbb{F}_{q^n}$ induisant l'identité sur $\mathbb{F}_q$. Montrer que $|\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)| \leq n$.

4. Montrer que $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ est un groupe cyclique, engendré par σ.

Exercice 2

1. Montrer que l'algèbre de Lie du groupe $SL_n(\mathbb{R})$ dans $\mathcal{M}_n(\mathbb{R})$ est l'espace des matrices de trace nulle.

2. Montrer que l'exponentielle $\exp : \mathcal{M}_n(\mathbb{R}) \to GL_n(\mathbb{R})$ définit un homéomorphisme de l'espace des matrices symétriques sur l'ensemble des matrices symétriques définies positives, que l'on note $\mathcal{S}^{++}$.

3. En déduire que l'ensemble des matrices symétriques définies positives de déterminant 1 est homéomorphe à $\mathbb{R}^{\frac{n(n+1)}{2}-1}$.

4. Montrer que toute matrice dans $GL_n(\mathbb{R})$ s'écrit de manière unique comme produit QS d'une matrice orthogonale Q et d'une matrice S de $\mathcal{S}_n^{++}$.

   (On utilisera une matrice S de $\mathcal{S}_n^{++}$ dont le carré vaut ${}^tMM$, afin de décomposer M comme $(MS^{-1})S$.

5. En utilisant la compacité de $O(n,\mathbb{R})$, montrer que $\mathrm{pol} : O(n,\mathbb{R}) \times \mathcal{S}_n^{++} \to GL_n(\mathbb{R})$ définie par $\mathrm{pol}(Q,S) = QS$ est un homéomorphisme.

6. En déduire que $SL_2(\mathbb{R})$ est homéomorphe à l'interieur d'un "tore solide" (ou "tore plein"), c'est à dire à $S^1 \times D$ où S^1 est le cercle unité, et D le disque unité ouvert de $\mathbb{R}^2$.

Exercice 3

Soit K un corps de caractéristique différente de 2. On note $K^* = K \setminus \{0\}$.

Une *algèbre de quaternions* $\mathcal{A}$ sur K est une K-algèbre de dimension 4 admettant une base $\{1,\, i,\, j,\, k\}$ qui vérifie

$$1 = 1_{\mathcal{A}} = 1_K, \quad ij = -ji = k, \quad i^2 = a \in K^*, \quad j^2 = b \in K^*.$$

On dit dans ce cas que $\mathcal{A}$ munie de cette base est de symbole de Hilbert $\left(\frac{a,b}{K}\right)$. Par exemple, l'algèbre des Quaternions de Hamilton vue en cours est de symbole de Hilbert $\left(\frac{-1,-1}{\mathbb{R}}\right)$.

Le but du problème est de voir que pour $K = \mathbb{C}$ ou $\mathbb{R}$, cette construction ne donne rien de nouveau, mais que cependant, pour $K = \mathbb{Q}$ il se passe des choses nouvelles (que l'on ne fait qu'entrapercevoir ici).

On admet que étant donnés $a, b \in K^*$ une algèbre de quaternions de symbole $\left(\frac{a,b}{K}\right)$ existe et est unique à isomorphisme près.

Rappels et conventions : $K.1$ est une sous-algèbre centrale dans $\mathcal{A}$. Une K-algèbre dont tout élément non nul est inversible est appelée une *algèbre de division*. On pourrait tout aussi bien dire "un corps non necessairement commutatif".

On note $\mathcal{A}_0 = \mathrm{Vect}(i, j, k)$, appelé le sous-espace imaginaire pur de $\mathcal{A}$. Pour tout $x \in \mathcal{A}$, on ecrit $x = \Re(x) + \Im(x)$ avec $\Re(x) \in K.1$ et $\Im(x) \in \mathcal{A}_0$, et on note $x^* = \Re(x) - \Im(x)$.

1. Premiers exemples.

   (a) En considérant $i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, montrer que $\mathcal{M}_2(K)$ est une algèbre de quaternions de symbole $\left(\frac{1,1}{K}\right)$.

   (b) Montrer que pour tout $a, b, x, y \in K^*$, deux algèbres de quaternions de symboles $\left(\frac{a,b}{K}\right)$ et $\left(\frac{ax^2, by^2}{K}\right)$ sont isomorphes.

   (c) Montrer que si K est algébriquement clos, toute algèbre de quaternion est isomorphe à $\mathcal{M}_2(K)$.

   (d) Dans cette question seulement, $K = \mathbb{R}$. Montrer qu'une algèbre de quaternions sur $\mathbb{R}$ est soit isomorphe à $\mathcal{M}_2(\mathbb{R})$, soit isomorphe à l'algèbre des quaternions de Hamilton.

(e) Considérons $\mathcal{A}$ une algèbre de quaternions, et la forme quadratique $(N : x \mapsto xx^*)$. Montrer que soit $\mathcal{A}$ est une algèbre de division, soit la forme N possède un vecteur isotrope (c'est à dire un vecteur $v \neq 0$ tel que $N(v) = 0$).

(f) Montrer que

  i. le centre de $\mathcal{A}$ est $K.1$,

  ii. $\mathcal{A}_0 \setminus \{0\} = \{x \in \mathcal{A},\ x \notin K.1,\ x^2 \in K.1\}$,

(g) Montrer que deux algèbres de quaternions $\mathcal{A}$ et $\mathcal{A}'$ sur un même corps K sont isomorphes si, et seulement si, il existe une application K-linéaire $\phi : \mathcal{A}_0 \to \mathcal{A}'_0$ verifiant $N(\phi(x)) = N(x)$, pour tout x dans $\mathcal{A}_0$.

2. Algèbres de quaternions sur $\mathbb{Q}$.

(a) On considère dans cette question que $K = \mathbb{Q}$. Soient p et q des nombres premiers distincts, avec $p \equiv -1[4]$.
Montrer que si les symboles de Hilbert de $\mathcal{A}$ et $\mathcal{A}'$ sont respectivement $\left(\dfrac{-1,p}{\mathbb{Q}}\right)$ et $\left(\dfrac{-1,q}{\mathbb{Q}}\right)$, et que $\mathcal{A}$ et $\mathcal{A}'$ sont isomorphes, alors il existe $M \in GL_3(\mathbb{Q})$, de determinant $\pm q/p$ telle que

$$
{}^tM \begin{pmatrix} 1 & 0 & 0 \\ 0 & -p & 0 \\ 0 & 0 & -p \end{pmatrix} M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -q & 0 \\ 0 & 0 & -q \end{pmatrix}.
$$

(b) On note $p^\alpha n$ le ppcm des dénominateurs des coefficients de M avec $n \wedge p = 1$, et on note $p^\alpha n \times M = (m_{i,j})$. Justifier que $\alpha \geq 1$. Puis montrer que

$$
m_{1,1} \equiv\ 0\,[mod\, p], \qquad \text{et que} \qquad m_{2,1}^2 + m_{3,1}^2 \equiv 0\,[mod\, p].
$$

(c) En déduire que $m_{2,1}$ et $m_{3,1}$ sont $\equiv 0\,[mod\, p]$, puis aboutir à une contradiction. *(On pourra utiliser le fait que -1 n'est pas un carré de $\mathbb{F}_p$).*

(d) Conclure qu'il existe une infinité d'algèbres de quaternions sur $\mathbb{Q}$ deux à deux non isomorphes.

Fin.