Université Paris 7-Denis Diderot
Licence de mathématiques et informatique

Algèbre et Géométrie
Année 2002-03
M. Fouquet, L. Merel

EXAMEN du 16 décembre 2002

Durée : 3 h

L'usage des calculatrices, téléphones et de tout document est interdit.

Soit p un nombre premier impair. Considérons les corps à p et p^2 élements notés $\mathbf{F}_p$ et $\mathbf{F}_{p^2}$. On considère $\mathbf{F}_p$ comme un sous-corps de $\mathbf{F}_{p^2}$. On dit que $\lambda \in \mathbf{F}_{p^2}$ est *imaginaire pur* si on a $\lambda \in \mathbf{F}_{p^2} - \mathbf{F}_p^*$ et $\lambda^2 \in \mathbf{F}_p$. Un imaginaire pur non nul sera fixé à partir de la question **II**.4. On pose $H_p = \mathbf{F}_{p^2} - \mathbf{F}_p$.

On rappelle que, lorsque K est un corps, $\mathrm{M}_2(K)$ muni de l'addition et de la multiplication des matrices est un anneau dont le groupe des éléments inversibles est $\mathrm{GL}_2(K)$.

I

1. Rappeler quels sont les ordres des groupes multiplicatifs $\mathbf{F}_p^*$ et $\mathbf{F}_{p^2}^*$.
2. Quel est le plus grand ordre d'un élément de $\mathbf{F}_p^*$? Même question pour $\mathbf{F}_{p^2}^*$.
3. Combien le polynôme $X^{p-1} - 1$ a-t-il de racines dans $\mathbf{F}_p$ et dans $\mathbf{F}_{p^2}$? En déduire que $\mathbf{F}_p^* = \{z \in \mathbf{F}_{p^2} / z^{p-1} = 1\}$.
4. Démontrer qu'il y a un élément λ_0 de $\mathbf{F}_{p^2}^*$ d'ordre $2(p-1)$. Quel est l'ordre de λ_0^2 ? En déduire que λ_0 est imaginaire pur non nul.

Fixons désormais un imaginaire pur non nul λ.

5. Démontrer qu'on a $\lambda^{2(p-1)} = 1$. Que vaut alors λ^{p-1} ?
6. Démontrer que tout imaginaire pur est de la forme $x\lambda$ avec $x \in \mathbf{F}_p$. En déduire le nombre d'imaginaires purs.
7. Démontrer que tout élément de $\mathbf{F}_{p^2}$ s'écrit de façon unique sous la forme $x + y\lambda$ avec $x, y \in \mathbf{F}_p$.

II

1. Rappeler quel est l'ordre de $\mathrm{GL}_2(\mathbf{F}_p)$.
2. Quel est l'ordre du sous-groupe de $\mathrm{GL}_2(\mathbf{F}_p)$ engendré par la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$?
3. Quel est l'ordre du sous-groupe de $\mathrm{GL}_2(\mathbf{F}_p)$ engendré par la matrice $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$, où x est un générateur de $\mathbf{F}_p^*$?
4. Démontrer que l'application $\phi : \mathbf{F}_{p^2} \to \mathrm{M}_2(\mathbf{F}_p)$ qui à $x + y\lambda$ associe la matrice $\begin{pmatrix} x & y\lambda^2 \\ y & x \end{pmatrix}$ est un homomorphisme injectif d'anneaux.
5. En déduire qu'on a un homomorphisme injectif de groupes $\mathbf{F}_{p^2}^* \to \mathrm{GL}_2(\mathbf{F}_p)$, puis que $O_\lambda = \{\begin{pmatrix} x & y\lambda^2 \\ y & x \end{pmatrix} \in M_2(\mathbf{F}_p) / (x, y) \neq (0,0)\}$ est un sous-groupe de $\mathrm{GL}_2(\mathbf{F}_p)$. Quel est l'ordre de O_λ ?

III

1. Considérons l'application $\mathrm{GL}_2(\mathbf{F}_p) \times H_p \to H_p$ qui à $(g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, z)$ associe $g.z = (az + b)/(cz + d)$. Démontrer que cette application est bien définie et bien à valeurs dans H_p. Démontrer qu'il s'agit d'une action du groupe $\mathrm{GL}_2(\mathbf{F}_p)$ sur l'ensemble H_p.
2. Démontrer que cette action est transitive. (On pourra montrer que tout élément est dans l'orbite de λ.)
3. Démontrer que O_λ est le stabilisateur de λ dans $\mathrm{GL}_2(\mathbf{F}_p)$.
4. Le sous-groupe O_λ de $\mathrm{GL}_2(\mathbf{F}_p)$ est-il distingué ?