Université Paris Diderot
Licence de Mathématiques

Algèbre
Année 2013-14
F. Liret, L. Merel

EXAMEN du 14 janvier 2014

Durée : 3 h

L'usage des calculatrices et téléphones est interdit.
Document autorisé : une feuille de notes personnelles.

I

1. Considérons le polynôme $X^2+1 \in \mathbf{F}_3[X]$. Montrer qu'il est irréductible.
2. En déduire que l'anneau $\mathbf{F}_3[X]/(X^2+1)$ est un corps à 9 élément, que nous noterons $\mathbf{F}_9$. Combien le polynôme X^2+1 a-t-il de racines dans $\mathbf{F}_9$? Fixons l'une de ces racines et notons-la i.
3. Le corps $\mathbf{F}_9$ est-il contenu dans un corps à 27 éléments ? Est-il contenu dans un corps à 81 éléments ?
4. Montrer que tout élément x de $\mathbf{F}_9$ s'écrit de façon unique sous la forme $x = a + ib$ avec a, $b \in \mathbf{F}_3$. On pose alors $\bar{x} = a - ib$.
5. Démontrer qu'on a $x^3 = \bar{x}$ et que $x\bar{x} \in \mathbf{F}_3$ ($x \in \mathbf{F}_9$). En déduire que $x \mapsto \bar{x}$ est un automorphisme de $\mathbf{F}_9$.
6. Combien y a-t-il d'élément $x \in \mathbf{F}_9$ tels que $x\bar{x} = 0$, $x\bar{x} = 1$, $x\bar{x} = -1$?
7. Considérons $A = \{\begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} / x, y \in \mathbf{F}_9\}$. Montrer que c'est un sous-anneau de $M_2(\mathbf{F}_9)$.
8. L'anneau A est-il commutatif ? Est-il intègre ? Est-ce un corps à 81 éléments ?
9. Démontrer que l'application $A^* \to \mathbf{F}_3^*$ qui à $\begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix}$ associe $x\bar{x} + y\bar{y}$ est un homomorphisme de groupes. Montrer que c'est une surjection.
10. Démontrer que $T = \{\begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \in A / x\bar{x} + y\bar{y} = 1\}$ est un sous-groupe distingué de A^*. Combien T a-t-il d'éléments ? Combien A^* a-t-il d'éléments ?

11. Quel est l'ordre de $\mathbf{F}_9^*$? Quel est l'ordre du sous-groupe de $\mathbf{F}_9^*$ engendré par i ?
12. Démontrer que le polynôme $X^4 + 1 \in \mathbf{F}_3[X]$ est réductible. Montrer que $1 + i$ est un générateur du groupe $\mathbf{F}_9^*$.
13. Soit $\mathbf{F}_{81}$ un corps à 81 éléments contenant $\mathbf{F}_9$. Posons $\mathcal{H} = \mathbf{F}_{81} - \mathbf{F}_9$. Montrer qu'on a une action du groupe $\mathrm{GL}_2(\mathbf{F}_9)$ sur l'ensemble $\mathcal{H}$ donnée par

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} .\tau = \frac{x\tau + y}{z\tau + t}.$$

14. Démontrer qu'il existe $\alpha \in \mathbf{F}_{81}$ tel que $\alpha^2 = 1 + i$ et que $\alpha \notin \mathbf{F}_9$. Démontrer que l'orbite de α sous $\mathrm{GL}_2(\mathbf{F}_9)$ est $\mathcal{H}$.

II

Soit p un nombre premier. Soit $P = X^p - X - 1 \in \mathbf{F}_p[X]$. Soit a une racine de P dans un corps de décomposition K.
1. Montrer que $a + u$ est racine de P, lorsque $u \in \mathbf{F}_p$.
2. En déduire que les racines de P dans K sont $\{a, a + 1, ..., a + p - 1\}$.
3. Soient Q, $R \in \mathbf{F}_p[X]$ des polynômes unitaires tels que $P = QR$. Notons d le degré de Q. Montrer que si $d > 0$, le coefficient de X^{d-1} dans Q est de la forme $-da + k$, où $k \in \mathbf{F}_p$.
4. En déduire que $d = 0$ ou $d = p$, puis que P est irréductible dans $\mathbf{F}_p[X]$.
5. Le même raisonnement s'applique-t-il au polynôme $P_b = Y^p - Y - b \in \mathbf{F}_p[Y]$, où $b \in \mathbf{F}_p^*$?
6. Le polynôme $X^{17} - X - 1$ est-il irréductible sur $\mathbf{Q}$?