Université Paris 7-Denis Diderot — Algèbre et Géométrie
Licence de mathématiques et informatique — Année 2004-05

Corrigé de l'EXAMEN du 16 décembre 2004

1. Ce polynôme est de degré 2. Comme ni 0, ni 1, ni -1 n'en est racine, il est irréductible. D'après le cours, l'anneau quotient $\mathbf{F}_3[X]/(X^2+1)$ est un corps à $3^2=9$ élément puisque X^2+1 est irréductible et de degré 2. Les deux racines du polynôme sont X et $-X$.
2. Un corps à 3^n éléments s'identifie à un sous-corps d'un corps à 3^m éléments si et seulement si $n|m$. C'est pourquoi $\mathbf{F}_9$ n'est pas contenu dans un corps à $27=3^3$ éléments mais est bien contenu dans un corps à $81=3^4$ éléments.
3. Le corps $\mathbf{F}_9$ est un espace vectoriel de dimension 2 sur $\mathbf{F}_3$. La famille $(1,i)$ est libre sur $\mathbf{F}_3$. C'est donc une base.
4. On a $(a+ib)^3=a^3+3a^2ib-3ab^2-ib^3=a+0-0-ib=a-ib$ (a, $b\in\mathbf{F}_3$). L'application $x\mapsto x^3$ est donc la substitution de Frobenius, qui est un automorphisme de $\mathbf{F}_9$.

On a $(a+ib)(a-ib)=a^2+b^2$. On a $0^2+0^2=0$, $1^2+0^2=(-1)^2+0^2=0^2+1^2=0^2+(-1)^2=1$, $1^2+1^2=1^2+(-1)^2=(-1)^2+1^2=(-1)^2+(-1)^2=-1$.

5. Les matrices nulles et identité sont dans A. Posons $M_{a,b}=\begin{pmatrix} a & b \\ -\bar{b} & \bar{a}\end{pmatrix}$. On a $-M_{a,b}=M_{-a,-b}$ (stabilité par passage à l'opposé). On a $M_{a,b}+M_{a',b'}=M_{a+a',b+b'}$ et $M_{a,b}M_{a',b'}=M_{aa'-\bar{b}'b,ab'+b\bar{a}'}$ (stabilités par addition et multiplication).
6. Les matrices $\begin{pmatrix} i & 0 \\ 0 & -i\end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0\end{pmatrix}$ ne commutent pas. La matrice $\begin{pmatrix} i & 1+i \\ 1-i & -i\end{pmatrix}$ est de déterminant nul et n'est donc pas inversible. L'anneau A n'est pas intègre. Ce n'est donc pas un corps.
7. C'est la restriction de l'application déterminant, qui est un homomorphisme de groupes. Il reste à voir qu'elle est à valeurs dans $\mathbf{F}_3^*$. Cela résulte du fait qu'elle est non nulle sur les éléments inversibles de A et que si a est dans $\mathbf{F}_9$, $a\bar{a}$ est dans $\mathbf{F}_3$ et donc $a\bar{a}+b\bar{b}\in\mathbf{F}_3$ (a, $b\in\mathbf{F}_9$).

L'ensemble T est le noyau de l'homomorphisme. C'est donc un sous-groupe distingué de A^*. À l'aide de la question **4.**, comptons les éléments de T. C'est le nombre de couple $(a,b)\in\mathbf{F}_9$ tels que $a\bar{a}+b\bar{b}=1$. On a donc $(a\bar{a},b\bar{b})\in\{(0,1),(1,0),(-1,-1)\}$. Cela donne $4+4+4^2=24$ possibilités pour (a,b). Revenons à notre homomorphisme. Il a pour image $\mathbf{F}_3^*$ (car la matrice $\begin{pmatrix} 1+i & 0 \\ 0 & 1-i\end{pmatrix}$ a pour déterminant -1). Son noyau est T. On a donc $|A^*|=|T||\mathbf{F}_3^*|=24.2=48$.
8. Le groupe $\mathbf{F}_9^*$ est d'ordre 8. On a $i^2=-1$ et $i^4=1$; c'est pourquoi i est d'ordre 4. Soit x un générateur de $\mathbf{F}_9^*$. On a $x^8=1$ et $x^4\neq 1$. C'est pourquoi on a $x^4=-1$ et x est une racine de X^4+1. On a $(1+i)^2=-i$, qui est d'ordre 4. C'est pourquoi $(1+i)$ est d'ordre 8 et engendre donc $\mathbf{F}_9^*$.
9. Montrons que l'action est bien définie. On a $c\tau+d\neq 0$ (c, $d\in\mathbf{F}_9$, $\tau\in\mathcal{H}$), sauf peut-être si $(c,d)=(0,0)$, ce qui est impossible si $\begin{pmatrix} a & b \\ c & d\end{pmatrix}\in\mathrm{GL}_2(\mathbf{F}_9)$. En effet, sinon on aurait $\tau=-d/c$ (absurde car $\tau\notin\mathbf{F}_9$). Par ailleurs $\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}.\tau=\tau$ et $(\begin{pmatrix} a & b \\ c & d\end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d'\end{pmatrix}).\tau=\begin{pmatrix} a & b \\ c & d\end{pmatrix}.(\begin{pmatrix} a' & b' \\ c' & d'\end{pmatrix}.\tau)$ ($\begin{pmatrix} a & b \\ c & d\end{pmatrix}$, $\begin{pmatrix} a' & b' \\ c' & d'\end{pmatrix}\in\mathrm{GL}_2(\mathbf{F}_9)$, $\tau\in\mathcal{H}$).
10. Le polynôme X^2-i-1 n'a pas de racine dans $\mathbf{F}_9$. Il est donc irréductible. Le corps $\mathbf{F}_9[X]/(X^2-i-1)$ possède donc $9^2=81$ éléments. Comme tous les corps à 81 éléments sont isomorphes, le polynôme X^2-i-1 possède des racines. Notons $\sqrt{1+i}$ l'une d'entre elles dans $\mathbf{F}_{81}$.

La famille $(1,\sqrt{1+i})$ est une base de $\mathbf{F}_{81}$ comme $\mathbf{F}_9$-espace vectoriel. Tout élément de $\mathcal{H}$ s'écrit donc de façon unique sous la forme $u\sqrt{1+i}+v$ avec $u\in\mathbf{F}_9$ et $v\in\mathbf{F}_9$. La condition $u\sqrt{1+i}+v\notin\mathbf{F}_9$ se traduit par $u\neq 0$. Soit $u\sqrt{1+i}+v\in\mathcal{H}$ avec $u\in\mathbf{F}_9$, $u\neq 0$ et $v\in\mathbf{F}_9$. La matrice $\begin{pmatrix} u & v \\ 0 & 1\end{pmatrix}$ appartient à $\mathrm{GL}_2(\mathbf{F}_9)$ et on a $\begin{pmatrix} u & v \\ 0 & 1\end{pmatrix}.\sqrt{1+i}=u\sqrt{1+i}+v$. C'est pourquoi $u\sqrt{1+i}+v$ est dans l'orbite de $\sqrt{1+i}$ sous $\mathrm{GL}_2(\mathbf{F}_9)$.