L3 Algèbre effective — examen — 9 janvier 2020

Durée : 2H. Tout document et appareil électronique interdit

Les exercices sont indépendants entre eux. Justifier raisonnablement chaque réponse

Ex.1 On suppose donnée une fonction Sagemath `f` prenant comme argument un polynôme $P \in K[X]$ et rendant P si P est un unité de K ou est irréductible, un facteur non trivial de P (pas forcément irréductible) sinon.

Ecrire une fonction `factor()` prenant comme argument un polynôme P et rendant une liste de polynômes irréductibles dont P est le produit :

```
def factor(P):
    ...
    return(l)
```

Ex.2 a. Quel est le cardinal du groupe des éléments inversibles pour la multiplication de l'anneau $\mathbb{Z}/15\mathbb{Z}$?

b. Montrer que pour tout entier a vérifiant $a = 1 \bmod 8$ et pour tout entier y on a

$y^a = y \bmod 15$

c. Quels sont les entiers y vérifiants $y^{13} = 3 \bmod 15$? On pourra commencer par chercher un inverse de 13 pour la multiplication modulo 8.

Ex.3 a. Montrer que le polynôme $X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$. L'est il dans $\mathbb{F}_3[X]$? Dans $\mathbb{Z}[X]$?

b. Quel est le cardinal de l'anneau quotient $\mathbb{F}_2[X]/(X^3 + X + 1)$?

Quel est le cardinal du groupe des éléments inversibles pour la multiplication de l'anneau $\mathbb{F}_2[X]/(X^3 + X + 1)$?

c. On note K l'anneau quotient $\mathbb{F}_2[X]/(X^5 + X^4 + 1)$

Montrer que $X^3 + X + 1$ divise $X^5 + X^4 + 1$ dans $\mathbb{F}_2[X]$.

En déduire un isomorphisme d'anneaux à expliciter

$$K \longrightarrow \mathbb{F}_2[X]/(X^3 + X + 1) \times \mathbb{F}_2[X]/(Q)$$

avec Q à déterminer, puis un isomorphisme de groupes

$$\big(K\big)^\times \longrightarrow \big(\mathbb{F}_2[X]/(X^3 + X + 1)\big)^\times \times \big(\mathbb{F}_2[X]/(Q)\big)^\times$$

où $\big(K\big)^\times$ désigne le groupe des éléments inversibles pour la multiplication de K.

d. On note d le cardinal du groupe $\big(K\big)^\times$. Que vaut d ?

Expliciter un élément non nul de K qui ne soit pas inversible pour la multiplication.

e. Montrer que le groupe $\big(K\big)^\times$ est cyclique et expliciter un générateur.

f. On note F l'application Frobenius $K \to K,\ x \mapsto x^2$.

Quelle est la dimension du $\mathbb{F}_2$-espace vectoriel $\mathrm{Ker}(F - \mathrm{id})$?

★ Pouvez vous donner une base de ce noyau ? Pouvez vous expliciter un polynôme $P \in \mathbb{F}_2[X]$ tel que $P \bmod X^5 + X^4 + 1$ soit dans ce noyau et tel que le pgcd de $X^5 + X^4 + 1$ avec P soit un facteur non trivial de $X^5 + X^4 + 1$?

Ex.4 On considère la matrice

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \in \mathrm{M}_4(\mathbb{Z})$$

a. Donner une base et un système d'équations de l'image de D vue comme sous-$\mathbb{Q}$-espace vectoriel de $\mathbb{Q}^4$ (c'est à dire lorsque D est vue comme la matrice d'une application linéaire $\mathbb{Q}^4 \to \mathbb{Q}^4$).

Donner de même une base et un système d'équations de l'image de D vue comme sous-module de $\mathbb{Z}^4$.

b. On a transformé "à la main" par opérations sur les lignes et les colonnes une matrice $A \in \mathrm{M}_4(\mathbb{Z})$ et obtenu les matrices suivantes :

$$\texttt{P} = \begin{pmatrix} -5 & -6 & -3 & -7 \\ -10 & -14 & -6 & -15 \\ 7 & 9 & 4 & 10 \\ -21 & -26 & -12 & -30 \end{pmatrix} \quad \texttt{Q} = \begin{pmatrix} -1 & 0 & -1 & 1 \\ 4 & 2 & 5 & 0 \\ -1 & -1 & -2 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\texttt{P\^{}(-1)} = \begin{pmatrix} 0 & 2 & 6 & 1 \\ 0 & 0 & 3 & 1 \\ -5 & -1 & -2 & 1 \\ 2 & -1 & -6 & -2 \end{pmatrix} \quad \texttt{Q\^{}(-1)} = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 3 & 1 & 1 & -2 \\ -2 & -1 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\texttt{P*A*Q} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

Donner une base et un système d'équations de l'image de A d'abord vue comme sous-espace vectoriel de $\mathbb{Q}^4$ puis vue comme sous-module de $\mathbb{Z}^4$.

Ex.5 On considère la matrice

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \in \mathrm{M}_4(\mathbb{Z})$$

Donner les entiers $d_1, \ldots, d_4$ et la liste des opérations sur les lignes et les colonnes transformant D en sa forme normale de Smith

$$\begin{pmatrix} d_1 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 \\ 0 & 0 & d_3 & 0 \\ 0 & 0 & 0 & d_4 \end{pmatrix} \text{ avec } d_1 \mid d_2 \mid d_3 \mid d_4 \quad (d_1 \text{ divise } d_2,\ d_2 \text{ divise } d_3, \ldots)$$

En déduire les matrices P, Q inversibles dans $\mathrm{M}_4(\mathbb{Z})$ telles que

$$PDQ = \begin{pmatrix} d_1 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 \\ 0 & 0 & d_3 & 0 \\ 0 & 0 & 0 & d_4 \end{pmatrix}$$