Examen terminal

18 décembre 2012

Seuls les résultats du cours pourront être admis. Documents et calculatrices ne sont pas autorisés. Le barème envisagé, indiqué entre parenthèses, est donné à titre indicatif.

Justifiez toutes vos réponses !

Exercice 1 (6 points)

1. (1 point) Soit A un anneau, M un A-module et N un sous-A-module de M. Énoncez le théorème d'existence et de propriété universelle du A-module quotient M/N.

   On considère l'anneau $A = \mathbb{Z}$ et le module libre $M = \mathbb{Z}^3$. Soit $u : M \to M$ l'endomorphisme donné par sa matrice U dans la base canonique :

$$U = \begin{pmatrix} 6 & 3 & 9 \\ 3 & 9 & 0 \\ 5 & 6 & 4 \end{pmatrix}.$$

2. (2 points) Calculez les facteurs invariants et le déterminant de U.
3. (1 point) Montrez que u est injectif.
4. (1 point) Soit N l'image de u. Quel est le cardinal de M/N ? Le groupe M/N est-il cyclique ?
5. (1 point) Donnez la liste de tous les groupes abéliens de cardinal $|M/N|$ à isomorphisme près.

Exercice 2 (4 points) Soient k un corps commutatif et A la k-algèbre des matrices triangulaires

$$M = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \quad \text{avec } a, b, c \in k,$$

aussi notées $M = aE_{11} + bE_{12} + cE_{22}$, où E_{ij}, $1 \leqslant i, j \leqslant 2$ sont les matrices élémentaires.

1. (1 point) L'anneau A est-il commutatif ? Possède-t-il des éléments nilpotents non nuls ?
2. (1 point) Montrez que tout idéal (à gauche ou à droite) de A est un sous-k-espace vectoriel.
3. (1,5 point) Soit I un idéal à gauche de A. Pour tout couple $(a, b) \neq (0, 0)$ dans k^2, on note $V_{(a,b)}$ la k-droite vectorielle engendrée par la matrice $aE_{11} + bE_{12}$.
   (a) Pour $M = aE_{11} + bE_{12} + cE_{22}$, calculez $E_{11}M$, $E_{12}M$ et $E_{22}M$.
   (b) Montrez que si $\dim_k(I) = 1$, alors $I = V_{(a,b)}$ pour un certain $(a, b) \neq (0, 0)$.
   (c) Montrez que si $\dim_k(I) = 2$, alors $I = kE_{11} \oplus kE_{12}$ ou $I = kE_{12} \oplus kE_{22}$.
4. (0,5 point) Donnez un idéal bilatère I distinct de $\{0\}$ et de A, et décrivez l'anneau quotient A/I.

Exercice 3 (4 points) La première question est indépendante des suivantes.

1. (1 point) Déterminer le nombre de polynômes irréductibles unitaires distincts de degré 4 dans $\mathbb{F}_3[X]$ (on ne demande pas de trouver ces polynômes).

2. (1 point) Montrer que :

   (a) $K_1 = \mathbb{F}_3[X]/(X^2 + X + 2)$ et $K_2 = \mathbb{F}_3[Y]/(Y^2 + 1)$ sont des corps,

   (b) $Z^2 + 1 \in \mathbb{F}_3[Z]$ est le polynôme minimal sur $\mathbb{F}_3$ des éléments d'ordre 4 de K_1^*,

   (c) $\overline{X}$ est un générateur de K_1^*.

3. (1 point) En déduire (justifier !) un isomorphisme entre les deux corps K_1 et K_2.

4. (1 point) Déterminer le polynôme minimal sur $\mathbb{F}_3$ de chaque générateur de K_1^*.

Exercice 4 (6 points) Posons $f = X^4 - 3 \in \mathbb{Q}[X]$ et $i \in \mathbb{C}$ avec $i^2 = -1$. On note K le corps de décomposition de f sur $\mathbb{Q}(i)$.

1. (2 points) Déterminer $[K : \mathbb{Q}(i)]$ et en déduire que f est irréductible sur $\mathbb{Q}(i)$.

2. (2 points) Montrer que l'extension $K/\mathbb{Q}(i)$ est galoisienne, déterminer le groupe de Galois de l'extension $K/\mathbb{Q}(i)$ et montrer que c'est un groupe cyclique.

3. (2 points) Déterminer toutes les extensions intermédiaires $\mathbb{Q}(i) \subsetneq L \subsetneq K$ en précisant lesquelles sont galoisiennes et donner la factorisation de f dans chaque extension intermédiaire L ainsi construite.

Corrigé de l'exercice 1.

1. Les objets A, M, N étant comme dans l'énoncé, il existe un module M/N et un morphisme de A-modules $\pi : M \to M/N$ tels que : pour tout A-module P et tout morphisme $f : M \to P$ tel que $N \subset \ker(f)$, il existe un unique morphisme $f' : M/N \to P$ tel que $f = f' \circ \pi$.

2. Par opérations élémentaires sur les lignes et les colonnes, la matrice U est équivalente aux matrices suivantes :

$$\begin{pmatrix} 6 & 3 & 9 \\ 3 & 9 & 0 \\ 5 & 6 & 4 \end{pmatrix} \overset{L_1 \to L_1 - L_3}{\sim} \begin{pmatrix} 1 & -3 & 5 \\ 3 & 9 & 0 \\ 5 & 6 & 4 \end{pmatrix} \overset{\substack{C_2 \to C_2 + 3C_1 \\ C_3 \to C_3 - 5C_1}}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 3 & 18 & -15 \\ 5 & 21 & -21 \end{pmatrix}$$

$$\overset{\substack{L_2 \to L_2 - 3L_1 \\ L_3 \to L_3 - 5L_1}}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 18 & -15 \\ 0 & 21 & -21 \end{pmatrix} \overset{c_2 \to C_2 + C_3}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & -15 \\ 0 & 0 & -21 \end{pmatrix} \overset{C_3 \to C_3 + 5C_2}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -21 \end{pmatrix}.$$

Les facteurs invariants de U sont donc $1, 3, 21$. Le calcul montre de plus que $PUQ = D$ où D est la matrice diagonale de coefficients diagonaux $1, 3, -21$ et P (resp. Q) est la matrice produit des matrices correspondant aux opérations élémentaires effectuées sur les lignes (resp. sur les colonnes). Comme on n'a fait aucun échange de lignes ou de colonnes, seules apparaissent des matrices élémentaires $E_{ij}(a)$, qui sont de déterminant 1. Ainsi $\det(P) = \det(Q) = 1$ et

$$\det(U) = \det(PUQ) = \det(D) = -63.$$

(Bien sûr, on peut aussi calculer le déterminant directement.)

3. Dans les bases $\{e_1, e_2, e_3\}$ et $\{f_1, f_2, f_3\}$ données par les matrices P et Q, l'endomorphisme u est déterminé par $u(e_1) = f_1$, $u(e_2) = 3e_2$ et $u(e_3) = -21f_3$. Soit $x \in \mathbb{Z}^3$ tel que $u(x) = 0$. Sur la base des e_i, on peut écrire $x = a_1e_1 + a_2e_2 + a_3e_3$ avec $a_i \in \mathbb{Z}$. On a alors $0 = u(x) = a_1f_1 + 3a_2e_2 - 21a_3f_3$. Comme les f_i forment une base, on en déduit que $a_1 = 3a_2 = -21a_3 = 0$. Comme 3 et 21 sont non diviseurs de zéro dans $\mathbb{Z}$, on en déduit $a_1 = a_2 = a_3 = 0$ donc $x = 0$. Ceci montre que u est injectif. On pouvait aussi raisonner, soit en montrant directement que $\ker(u) = \{0\}$ en résolvant un système, soit en utilisant un résulat du cours qui dit que u est injectif lorsque $\det(u)$ est non diviseur de 0.

4. Comme on vient de le voir, on a :

$$N = \mathbb{Z}f_1 \oplus \mathbb{Z}.3f_2 \oplus \mathbb{Z}.21f_3 \subset \mathbb{Z}f_1 \oplus \mathbb{Z}.f_2 \oplus \mathbb{Z}.f_3 = M.$$

Il en découle que :

$$\begin{aligned} M/N &\simeq \big(\mathbb{Z}f_1 \oplus \mathbb{Z}.f_2 \oplus \mathbb{Z}.f_3\big)/\big(\mathbb{Z}f_1 \oplus \mathbb{Z}.3f_2 \oplus \mathbb{Z}.21f_3\big) \\ &\simeq (\mathbb{Z}f_1/\mathbb{Z}f_1) \oplus (\mathbb{Z}.f_2/\mathbb{Z}.3f_2) \oplus (\mathbb{Z}.f_3/\mathbb{Z}.21f_3) \\ &\simeq (\mathbb{Z}/\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/21\mathbb{Z}) \\ &\simeq (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/21\mathbb{Z}). \end{aligned}$$

Ce groupe est de cardinal 63. Il est visible pour tout $x \in M/N$ on a $21x = 0$; en particulier M/N ne possède pas d'élément d'ordre 63 et n'est donc pas cyclique.

5. D'après le théorème de structure des $\mathbb{Z}$-modules finis, les classes d'isomorphisme de groupes abéliens de cardinal 63 sont en bijection avec les listes de facteurs invariants, c'est-à-dire les listes d'entiers $d_1, \ldots, d_r$ strictement plus grands que 1, qui se divisent successivement et dont le produit vaut 63. Comme $63 = 3^2 \times 7$, les seules listes possibles sont $\{3, 21\}$ et $\{63\}$. À isomorphisme près, il y a donc deux groupes abéliens de cardinal 63 qui sont $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z}$ et $\mathbb{Z}/63\mathbb{Z}$.

Corrigé de l'exercice 2.

1. L'anneau A n'est pas commutatif car $E_{11}E_{12} = E_{12} \neq 0 = E_{12}E_{11}$. N.B. trop nombreux sont ceux qui se contentent de dire que

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix} \; ; \; \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a'a & a'b + b'c \\ 0 & c'c \end{pmatrix},$$

   et d'en déduire que A n'est pas commutatif puisque $ab' + bc' \neq a'b + b'c$. Mais il n'est pas clair qu'on puisse trouver des valeurs des paramètres $a, b, \ldots$ tels que $ab' + bc' \neq a'b + b'c$ et la seule manière convaincante de le faire est de donner des valeurs précises aux paramètres, c'est-à-dire de donner un vrai contre-exemple comme ci-dessus.

   L'anneau A possde des nilpotents non nuls, par exemple $E_{12} \neq 0$ vérifie $(E_{12})^2 = 0$.

2. Un idéal (à gauche ou à droite) de A est un sous-groupe de $(A, +)$ qui est stable par multiplication (à gauche ou à droite, respectivement) par les éléments de A. En particulier c'est un sous-groupe additif qui est stable par multiplication par tous les éléments de k (c'est-à-dire les matrices d'homothétie), à droite ou à gauche indifféremment puisque ceux-ci sont dans le centre de A. C'est donc bien un sous-k-espace vectoriel.

3. (a) $E_{11}M = aE_{11} + bE_{12}$; $E_{12}M = cE_{12}$; $E_{22}M = cE_{22}$.

   (b) Si $\dim_k(I) = 1$, il existe $M \neq 0$ dans I. Comme I est un idéal à gauche, les trois matrices $E_{11}M, E_{12}M, E_{22}M$ sont dans I. En particulier, si on écrit $M = aE_{11} + bE_{12} + cE_{22}$ comme dans la question précédente, on trouve que cE_{12} et cE_{22} sont dans I ; si $c \neq 0$ ceci implique $E_{12}, E_{22} \in I$ ce qui contredit $\dim_k(I) = 1$. Donc $c = 0$ et $M = aE_{11} + bE_{12}$. Il s'ensuit que $V_{(a,b)} \subset I$ et pour des raisons de dimension, on a égalité.

   Remarque. Bien que ce ne soit pas demandé, notons que les formules de (i) montrent immédiatement que $V_{(a,b)}$ est un idéal à gauche.

   (c) Supposons que $\dim_k(I) = 2$. S'il existe une matrice $M = aE_{11} + bE_{12} + cE_{22}$ dans I telle que $c \neq 0$, alors cE_{12} et cE_{22} sont dans I, donc E_{12} et E_{22} sont dans I, donc $kE_{12} \oplus kE_{22} \subset I$. Pour des raisons de dimension, il y a égalité. Si au contraire toutes les matrices $M = aE_{11} + bE_{12} + cE_{22}$ de I vérifient $c = 0$, alors $I \subset kE_{11} \oplus kE_{12}$. Pour des raisons de dimension, il y a égalité.

   Remarque. Bien que ce ne soit pas demandé, notons que les formules de (i) montrent immédiatement que $kE_{12} \oplus kE_{22}$ et $kE_{11} \oplus kE_{12}$ sont des idéaux à gauche.

4. Il est facile de voir que $I = kE_{12}$ est un idéal bilatère distinct de $\{0\}$ et de A. De plus, l'application $f : A \to k \times k$ qui envoie $aE_{11} + bE_{12} + cE_{22}$ sur le couple (a, c) est un morphisme d'anneaux surjectif de noyau I, qui induit un isomorphisme $A/I \simeq k \times k$.

Remarque. Soit J un idéal à droite de A. Pour tout couple $(b,c) \neq (0,0)$, on note $W_{(b,c)}$ la k-droite vectorielle engendrée par la matrice $bE_{12}+cE_{22}$. En procédant de la même manière avec les idéaux à droite que ce qu'on a fait avec les idéaux à gauche, on peut montrer facilement que :

(a) Si $\dim_k(J)=1$, alors $J=W_{(b,c)}$ pour un certain $(b,c)\neq(0,0)$.

(b) Si $\dim_k(J)=2$, alors $J=kE_{11}\oplus kE_{12}$ ou $I=kE_{12}\oplus kE_{22}$.

Utilisant cela, on montre ensuite que A possède exactement cinq idéaux bilatères, qui sont $\{0\}$, kE_{12}, $kE_{11}\oplus kE_{12}$, $kE_{12}\oplus kE_{22}$ et A.

Corrigé de l'exercice 3.

1. $X^{3^2}-X$ resp. $X^{3^4}-X$, est le produit des irréductibles unitaires dont le degré divise 2 resp. 4. Il existe donc $(3^2-3)/2=3$, resp. $(3^4-3^2)/4=18$ irréductibles unitaires de degré 2 resp. 4 dans $\mathbb{F}_3[X]$.

2. (a) Comme les polynômes sont de degré deux, il suffit de vérifier qu'il n'ont pas de facteur de degré 1, càd que $\overline{0},\overline{1}$ et $\overline{2}=\overline{-1}$ ne sont pas zéros de ces polynômes.

   (b) Les éléments d'ordre 4 sont zéros de $X^4-1=(X+1)(X-1)(X^2+1)\in\mathbb{F}_3[X]$ et donc de $X^2+1\in\mathbb{F}_3[X]$ qui est irréductible d'après ce qui précède

   (c) Le groupe K_1^* est d'ordre $3^2-1=8$ et l'ordre de ses éléments divisent 8. Comme $\overline{X}\notin\mathbb{F}_3$ n'est pas zéro de $X^2-1\in\mathbb{F}_3[X]$ son ordre ne divise pas 4 et est donc 8.
   Alternativement on peut calculer $\overline{X}^2=2\overline{X}+1$, $\overline{X}^3=2\overline{X}+2$ et $\overline{X}^4=2\neq 1$.

3. Les corps K_1 et K_2 sont tous les deux des corps de rupture du polynôme irréductible X^2+1. D'après le cours il existe un $\mathbb{F}_3$-isomorphisme entre ces corps qui envoie la racine $\overline{Y}\in K_2$ de $Z^2+1\in\mathbb{F}_3[Z]$ sur la racine $\overline{X}^2\in K_1$ de $Z^2+1\in\mathbb{F}_3[Z]$.

4. Les générateurs de K_1^* sont les éléments d'ordre 8, c'est-à-dire $\overline{X},\overline{X}^3,\overline{X}^5$ et $\overline{X}^7$. Nous avons que $\overline{X}$ est zéro de X^2+X+2 et en appliquant le morphisme de Frobenius à $\overline{X}^2+\overline{X}+2=0$ nous obtenons que $\overline{X}$ et $\overline{X}^3$ sont zéros de X^2+X+2. Pour déterminer le polynôme minimal de $\overline{X}^5$ et $\overline{X}^{5\cdot 3}=\overline{X}^7$ qui est d'ordre $2=[K_1:\mathbb{F}_3]$ on pose $X^2+a_1X+a_0$ et on l'évalue en X^5 pour obtenir:

$$\overline{X}^{10}+a_1\overline{X}^5+a_0=\overline{X}^8\overline{X}^2+a_1\overline{X}^4\overline{X}+a_0=\overline{X}^2+2a_1\overline{X}+a_0=2\overline{X}+1+2a_1\overline{X}+a_0$$

   D'où il résulte que $a_0=a_1=2$.

Corrigé de l'exercice 4.

1. Nous avons $[K:\mathbb{Q}]=[K:\mathbb{Q}(i)][\mathbb{Q}(i):\mathbb{Q}]=[K:\mathbb{Q}(\sqrt[4]{3})][\mathbb{Q}(\sqrt[4]{3}):\mathbb{Q}]$. Comme $i\notin\mathbb{R}$ le polynôme X^2+1 qui annule i n'a pas de racine dans $\mathbb{Q}(\sqrt[4]{3})$ et, comme il est de degré 2, il est donc irréductible dans $\mathbb{Q}(\sqrt[4]{3})[X]$. Comme $X^4-3\in\mathbb{Q}[X]$ est irréductible (Eisenstein dans $\mathbb{Z}[X]$ avec le premier $3\in\mathbb{Z}$) nous obtenons $[K:\mathbb{Q}]=2\cdot 4=8$. Comme $i\notin\mathbb{Q}$ le polynôme $X^2+1\in\mathbb{Q}[X]$ est irréductible et $[\mathbb{Q}(i):\mathbb{Q}]=2$. Il en résulte que le corps de rupture $\mathbb{Q}(i)(\sqrt[4]{3})/\mathbb{Q}(i)$ de $X^4-3\in\mathbb{Q}(i)[X]$ est de degré $[\mathbb{Q}(i)(\sqrt[4]{3}):\mathbb{Q}(i)]=[K:\mathbb{Q}(i)]=4$ égal au degré du polynôme annulateur X^4-3 de $\sqrt[4]{3}$. Ce polynôme est donc irréductible.

2. Le corps $\mathbb{Q}(i)$ est de caractéristique nulle et donc parfait. Comme les quatre racines distinctes $\sqrt[4]{3}, -\sqrt[4]{3}, i\sqrt[4]{3}, -i\sqrt[4]{3}$ de $X^4 - 3 \in \mathbb{Q}(i)$ appartiennent au corps de rupture $\mathbb{Q}(i)(\sqrt[4]{3})$ de $X^4 - 3 \in \mathbb{Q}(i)[X]$, l'extension $\mathbb{Q}(i)(\sqrt[4]{3})/\mathbb{Q}(i)$ est un corps de décomposition du polynôme séparable $X^4 - 3 \in \mathbb{Q}(i)[X]$. D'après le cours l'ordre de $G = G(K/\mathbb{Q}(i))$ est $[K : \mathbb{Q}(i)] = 4$. Un $\mathbb{Q}(i)$-automorphisme de G est entièrement déterminé par l'image de $\sqrt[4]{3}$. Comme les coefficients de $X^4 - 3$ sont fixé par G l'image de $\sqrt[4]{3}$ par un élément de G est une des quatre racines de de $X^4 - 3$ et comme $|G| = 4$ ces quatre possibilités correspondent toutes à des automorphismes de G. L'élément $\sigma \in G$ déterminé par $\sigma(\sqrt[4]{3}) = i\sqrt[4]{3}$ est d'ordre 4 et engendre donc G qui est un groupe cyclique d'ordre 4.

3. Il existe un unique sous-groupe $H =< \sigma^2 >$ non trivial d'ordre 2 dans G qui est distingué (car le groupe est abélien) et donc un unique corps intermédiaire K^H qui est galoisien. Comme $\sigma^2(\sqrt[4]{3}) = -\sqrt[4]{3}$ nous obtenons dans la $\mathbb{Q}(i)$-base $(1, \sqrt[4]{3}, \sqrt[4]{3}^2, \sqrt[4]{3}^3)$ de K

$$\sigma^2(a_0 + a_1\sqrt[4]{3} + a_2\sqrt[4]{3}^2 + a_3\sqrt[4]{3}^3) = a_0 - a_1\sqrt[4]{3} + a_2\sqrt[4]{3}^2 - a_3\sqrt[4]{3}^3 \quad (a_i \in \mathbb{Q}(i))$$

et donc $K^H = \mathbb{Q}(i)(\sqrt[4]{3}^2) = \mathbb{Q}(i)(\sqrt{3})$. Nous obtenons la factorisation $X^4 - 3 = (X^2 + i\sqrt{3})(X^2 - i\sqrt{3})$. Les quatre racines de ces deux facteurs étant $\sqrt[4]{3}, -\sqrt[4]{3}, i\sqrt[4]{3}, -i\sqrt[4]{3}$, elle ne peuvent pas appartenir à $\mathbb{Q}(i)(\sqrt{3})$, ce qui entrainerait $\mathbb{Q}(i)(\sqrt{3}) = \mathbb{Q}(i, \sqrt[4]{3})$, car $[\mathbb{Q}(i)(\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(i)(\sqrt{3}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}]$ est de degré au plus 4 alors que $[\mathbb{Q}(i, \sqrt[4]{3}) : \mathbb{Q}] = 8$ d'après la première question.