Université de Rennes 1 - 2011-2012 - Master 1 de mathématiques - Module ALGB - Corrigé de l'examen du 16/12/2011 - Durée : 2 heures

Les anneaux et morphismes d'anneaux sont supposés unitaires.

Exercice 1 - (5 points)
1- (question de cours) Donner les définitions : (a) d'un module de type fini ; (b) d'une algèbre (commutative) de type fini.
Remarque : on rappelle que toutes les notations utilisées doivent être définies.

1 (a) Soit k un anneau. Un k-module (à gauche) M est de type fini s'il existe une partie finie de M qui engendre M (comme k-module).

1 (b) Soit k un anneau commutatif. Une k-algèbre commutative A est de type fini s'il existe une partie finie de A qui engendre M (comme k-algèbre).

2- Soit k un anneau commutatif non nul. Montrer que $k[X]$ est une k-algèbre de type fini mais n'est pas un k-module de type fini.

1 Comme k-algèbre, $k[X]$ est engendrée par $\{X\}$, donc est de type fini.

2 Soit S une partie finie de $k[X]$, et soit $d := \sup_{P\in S} \deg P$. Alors toute combinaison k-linéaire d'éléments de S est un polynôme de degré au plus d. En particulier, le k-module engendré par S (qui est l'ensemble de ces combinaisons linéaires) ne contient pas X^{d+1}, donc n'est pas égal à $k[X]$. (L'hypothèse que k n'est pas nul intervient dans le fait que le terme de degré $d+1$ de X^{d+1} est non nul !).

Exercice 2 - (9 points) Soit α le nombre complexe $j+\sqrt{2}$, où $j = e^{2i\pi/3}$. On rappelle que j est racine du polynôme X^2+X+1.

1- Calculer le polynôme minimal (unitaire) de α sur $\mathbb{Q}$. On justifiera soigneusement la méthode utilisée (Il pourra être utile de remarquer en cours de calcul que j et $\sqrt{2}$ appartiennent à $\mathbb{Q}(\alpha)$).
Dans la suite, on note P ce polynôme minimal.

3 La relation $(\alpha-\sqrt{2})^2 = j^2$ donne $\alpha^2 - 2\sqrt{2}\alpha + 2 = -j-1 = \sqrt{2}-\alpha-1$, puis $\alpha^2+\alpha+3 = \sqrt{2}(2\alpha+1)$. En réélevant au carré, on obtient $P(\alpha)=0$, où P est le polynôme $\boxed{X^4+2X^3-X^2-2X+7}$.

[**Commentaires :** quelques erreurs de calcul pour P. D'autre part, quelques-uns l'ont trouvé en calculant $(X-\alpha)(X-j+\sqrt{2})(X-j^2-\sqrt{2})(X-j^2+\sqrt{2})$, ce qui marche aussi très bien. Plusieurs sont partis de la relation $j^3=1$ au lieu de $j^2+j+1=0$, ce qui donne un polynôme de degré 6 réductible, et *beaucoup* d'erreurs de calcul : ceux-là ont eu du mal à s'en sortir par la suite.]

D'autre part, $\sqrt{2} = \frac{\alpha^2+\alpha+3}{2\alpha+1} \in \mathbb{Q}(\alpha)$, donc $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{Q}(\alpha)$. La formule de multiplicativité des degrés donne $[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}\left(\sqrt{2}\right)] \times [\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}] = 2 \times [\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}]$.

Comme $\alpha \notin \mathbb{Q}\left(\sqrt{2}\right)$ (car α est non réel), on a $[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}] \geq 2$, et donc $[\mathbb{Q}(\alpha):\mathbb{Q}] \geq 4$. Comme par ailleurs α admet un polynôme annulateur de degré 4, ce degré est aussi inférieur à 4, donc au final il est égal à 4 (on peut aussi remarquer que $\alpha - j \in \mathbb{Q}(\sqrt{2})$ et donc que $\mathbb{Q}(\alpha) = \mathbb{Q}(j,\sqrt{2})$).

[**Commentaire :** si l'on ne remarque pas d'abord que $\sqrt{2} \in \mathbb{Q}(\alpha)$, le degré $[\mathbb{Q}(\alpha) : \mathbb{Q}\left(\sqrt{2}\right)]$ n'a pas de sens et l'argument s'effondre].

Le polynôme P est ainsi un polynôme annulateur unitaire de degré minimal, c'est donc le polynôme minimal de α.

2- Combien y a-t-il de ($\mathbb{Q}$-)plongements de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$?

1 Comme $\mathbb{Q}$ est de caractéristique 0, l'extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ est séparable, donc il y a exactement $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ plongements de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$. (Ou bien : puisque $\mathbb{Q}(\alpha) \cong \mathbb{Q}[X]/(P)$, il y en a autant que de racines de P dans $\mathbb{C}$, c'est-à-dire 4 puisque P est séparable).

[**Commentaire :** argument de séparabilité souvent escamoté ; d'une manière ou d'une autre il faut montrer que P a bien 4 racines complexes distinctes.]

3- Soit σ un plongement de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$. Quelles sont les valeurs possibles pour $\sigma(\sqrt{2})$, $\sigma(j)$ et $\sigma(\alpha)$?

1,5 Le polynôme $X^2 - 2 \in \mathbb{Q}[X]$ annule $\sqrt{2}$, donc il doit également annuler $\sigma\left(\sqrt{2}\right)$ car σ est un morphisme de $\mathbb{Q}$-algèbres. Les racines de $X^2 - 2$ dans $\mathbb{C}$ étant $\sqrt{2}$ et $-\sqrt{2}$, on en déduit $\sigma(\sqrt{2}) \in \left\{\sqrt{2}, -\sqrt{2}\right\}$. De la même manière, j est annulé par $X^2 + X + 1$ de racines j et j^2, donc $\sigma(j) \in \{j, j^2\}$. Comme $\sigma(\alpha) = \sigma\left(\sqrt{2}\right) + \sigma(j)$, on en déduit $\sigma(\alpha) \in \left\{\sqrt{2} + j, \sqrt{2} + j^2, -\sqrt{2} + j, -\sqrt{2} + j^2\right\}$.

4- En déduire que $\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(\mathbb{Q}(\alpha), \mathbb{C}) = \mathrm{Aut}_{\mathbb{Q}\text{-alg}}(\mathbb{Q}(\alpha))$.

2 Pour tout $\sigma \in \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(\mathbb{Q}(\alpha), \mathbb{C})$, on a vu que $\sigma(\alpha) \in \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, j)$. Comme α engendre $\mathbb{Q}(\alpha)$ en tant que $\mathbb{Q}$-algèbre, on en déduit que $\sigma(\mathbb{Q}(\alpha)) \subset \mathbb{Q}(\alpha)$, et ainsi $\sigma \in \mathrm{Aut}_{\mathbb{Q}\text{-alg}}(\mathbb{Q}(\alpha))$. Comme l'autre inclusion est évidente, on a l'égalité annoncée.

5- L'extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ est-elle galoisienne ?

1,5 Cette extension est séparable (déjà vu question 2) ; la question précédente montre donc que l'extension est galoisienne. (On peut aussi remarquer que $\mathbb{Q}(\alpha)$ est une extension de décomposition du polynôme P, et les racines de P sont simples dans $\mathbb{Q}(\alpha)$, donc l'extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ est galoisienne).

Exercice 3 - (2 points) Trouver une matrice diagonale de Smith équivalente (« G-équivalente », selon la terminologie du cours) à la matrice (à coefficients dans $\mathbb{Z}$)

$$A = \begin{pmatrix} 0 & 2 \\ -12 & -6 \\ 6 & 2 \end{pmatrix}.$$

Soient d_1 et d_2 les coefficients « diagonaux » de la matrice cherchée (de sorte que d_1 divise d_2). On peut les choisir positifs, quitte à multiplier par une matrice diagonale à coefficients ± 1. Le pgcd des mineurs de taille 1 de A vaut 2, d'où l'on déduit $d_1 = 2$. Les mineurs de taille

2 de A sont 24, -12 et 12, leur pgcd vaut 12 et est égal à $d_1 d_2$, donc $d_2 = 6$. On trouve donc la matrice $\begin{pmatrix} 2 & 0 \\ 0 & 6 \\ 0 & 0 \end{pmatrix}$. Les autres solutions s'obtiennent en changeant les signes.

Remarque : on peut aussi procéder par opérations élémentaires.

Exercice 4 - (4 points) Soit p un nombre premier impair, on considère le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\star$.

1- Donner un moyen permettant d'inclure le package « numtheory ».

0,5

```
#1- inclure le package numtheory
with(numtheory):
```

2- Donner une procédure `ordre(x,p)` qui permet de trouver l'ordre multiplicatif d'un élément non nul x de $\mathbb{Z}/p\mathbb{Z}$. Par exemple `ordre(2,7)` doit rendre 3.

2

```
#2- Ordre multiplicatif d'un élément
ordre := proc(x,p)
local i,L;
L := divisors(p-1);
for i from 1 to nops(L) do
  if x&^L[i] mod p = 1 then
    return(L[i]);
  end if;
end do;
end:
```

3- En déduire une procédure `Generateurs(p)` qui permet de trouver la liste des générateurs de $(\mathbb{Z}/p\mathbb{Z})^\star$. Par exemple `Generateurs(5)` doit rendre `[2,3]`.

1,5

```
#3- Les générateurs
Generateurs := proc(p)
local a,L;
L := [];
for a from 1 to p-1 do
  if (ordre(a,p) = p-1) then
    L := [op(L),a];
  end if;
od;
return L;
end:
```