Université de Rennes 1 - 2011-2012 - Master 1 de mathématiques - Module ALGB - Examen du 16/12/2011 - Durée : 2 heures

Documents, calculatrices et téléphones interdits. Barème indicatif.
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.
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.

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.
2- Combien y a-t-il de ($\mathbb{Q}$-)plongements de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$?
3- Soit σ un plongement de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$. Quelles sont les valeurs possibles pour $\sigma(\sqrt{2})$, $\sigma(j)$ et $\sigma(\alpha)$?
4- En déduire que $\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(\mathbb{Q}(\alpha), \mathbb{C}) = \mathrm{Aut}_{\mathbb{Q}\text{-alg}}(\mathbb{Q}(\alpha))$.
5- L'extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ est-elle 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 $\mathbb{Z}$)

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

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 ».
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.
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]`.