ALGÈBRE COMMUTATIVE ET THÉORIE DE GALOIS

Partiel du 9 novembre 2005. Durée 3 heures. Documents autorisés : le texte du cours.

L'exercice 1 est utilisé dans la question *(ix)* de l'exercice 2. Ceci mis à part, les quatres exercices sont indépendants.

Exercice 1. — *Soit A un anneau qui n'est pas un corps, euclidien pour une application $\varphi : A \setminus \{0\} \to \mathbb{N}$. L'ensemble des $\varphi(a)$ pour a non inversible et non nul a un plus petit élément $\varphi(x)$ avec x non inversible et non nul dans A.*

(i) Montrer que l'application $A^\times \cup \{0\} \to A/(x)$ est surjective (ici $A^\times$ est l'ensemble des éléments inversibles de A).

(ii) Montrer que l'idéal (x) est maximal.

Exercice 2. — *Soit A l'anneau $\mathbb{R}[X,Y]/(X^2+Y^2+1)$ et notons x et y les images de X et Y dans A.*

(i) Montrer que tout élément a de A s'écrit $a = P(x)y + Q(x)$ où P et Q sont des éléments de $\mathbb{R}[X]$. Montrer que $a = 0$ équivaut à $P(X) = Q(X) = 0$ dans $\mathbb{R}[X]$.

(ii) Montrer que la donnée d'un morphisme de $\mathbb{R}$-algèbre de A dans $\mathbb{C}$ équivaut à la donnée d'un couple $(u,v) \in \mathbb{C}^2$ tel que $u^2+v^2+1=0$.

(iii) Soit $P(x)y+Q(x)$ un élément inversible de A et $R(x)y+S(x)$ son inverse. Montrer que dans $\mathbb{R}[X]$ on a

$$P(X)S(X) + Q(X)R(X) = 0 \quad \text{et} \quad -(1+X^2)P(X)R(X) + Q(X)S(X) = 1.$$

(iv) Montrer que P est alors un multiple de R. On posera $P = RU$.
Supposons que R est non nul.

(v) Montrer que U est inversible dans $\mathbb{R}[X]$ puis qu'il existe $\lambda \in \mathbb{R}^*$ tel que $U(X) = \lambda$.

(vi) Montrer que l'on doit avoir

$$(1+X^2)R(X)^2 = -\frac{1}{\lambda} - S(X)^2$$

et en déduire que pour tout $x \in \mathbb{R}$, on a

$$|S(x)| \leq \sqrt{-\frac{1}{\lambda}}.$$

(vii) En déduire que S est une constante puis une contradiction. Conclure que $R = 0$.

(viii) Montrer que $Q(X)$ et $S(X)$ sont des réels non nuls, puis que les inversibles de A sont les éléments de $\mathbb{R}^*$.

(ix) Supposons l'anneau A euclidien. D'après l'exercice 1, il existe $a \in A$ non inversible tel que l'application $A^\times \cup \{0\} \to A/(a)$ est surjective et $A/(a)$ est un corps. Montrer que l'on a $A/(a) = \mathbb{R}$.

(x) En utilisant la question (ii) aboutir à une contradiction.

Exercice 3. — *Soit A un anneau intègre et noethérien. On suppose que tout idéal maximal de A est principal.*

($\imath$) Montrer que tout élément a de A admet une décomposition en produit d'irréductibles.

Soit p un élément de A.

($\imath\imath$) Montrer que si (p) est un idéal premier alors p est irréductible.

($\imath\imath\imath$) Montrer que si p est irréductible, alors (p) est maximal (et donc premier). En déduire que A est factoriel.

($\imath v$) Montrer que tout idéal $I = (a, b)$ est égal à l'idéal (c) avec $c = \mathrm{pgcd}(a, b)$ (on pourra se ramener au cas où a et b sont premiers entre eux).

(v) Conclure que A est principal.

Cet exercice et une étude des idéaux maximaux de $A = \mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$ permettrait de montrer que A est principal (c'est donc d'après l'exercice 2 un anneau principal non euclidien).

Exercice 4. — *Soit M le sous-ensemble de $\mathbb{Z}^3$ formé des triplets (x, y, z) tels que la somme $x + y + z$ est paire.*

($\imath$) Montrer que M est le noyau d'un morphisme de $\mathbb{Z}$-modules (i.e. de groupes abéliens) $\pi : \mathbb{Z}^3 \to \mathbb{Z}/2\mathbb{Z}$. Déterminer le quotient $\mathbb{Z}^3/M$.

($\imath\imath$) Montrer que M est libre en donnant une base (formée de trois éléments) de M.