Algèbre et Arithmétique — Mathématiques L3
Université de Nice Sophia-Antipolis — Année 2007-2008

FEUILLE DE TRAVAUX DIRIGÉS 6

ARITHMÉTIQUE DES ANNEAUX

On rappelle les deux théorèmes de transfert suivants.

Théorème. Soit A un anneau commutatif unitaire.

- Si A est noetherien, alors $A[X]$ est noetherien [Hilbert].
- Si A est factoriel, alors $A[X]$ est factoriel [Gauss].

Exercice 1 (Division euclidienne dans $A[X]$)**.**

Soit A un anneau commutatif unitaire intégre et soit $P \in A[X]$, $P \neq 0$, de coefficient dominant inversible.

(1) Soit $F \in A[X]$, montrer qu'il existe $Q,R \in A[X]$, tels que l'on ait :

$$F = PQ + R \quad \text{et} \quad \deg(R) < \deg(P) \text{ ou } R = 0.$$

Exercice 2 (L'anneau des polynômes à deux variables)**.**

On considère l'anneau des polynômes à deux variables $A = \mathbb{K}[X,Y]$ sur un corps $\mathbb{K}$.

(1) Montrer que le polynôme X est irréductible dans A.
(2) Montrer que X et Y sont premiers entre eux.
(3) Montrer que $\mathbb{K}[X,Y]$ est factoriel mais pas principal.

Exercice 3 (L'anneau $\mathbb{Z}[i\sqrt{5}]$)**.**

On considère l'anneau $A = \mathbb{Z}[i\sqrt{5}] := \{a + ib\sqrt{5}; a, b \in \mathbb{Z}\}$. On définit la *norme* d'un élément $z = a + ib\sqrt{5}$ par $N(z) := z.\bar{z} = a^2 + 5b^2$.

(1) Montrer que la norme est multiplicative : $N(z.z') = N(z).N(z')$.
(2) Montrer que $N(z) = 1$ si et seulement si z est une unité de A.
(3) Montrer que A n'est pas factoriel. On pourra considérer $(1 + i\sqrt{5})(1 - i\sqrt{5}) = 6 = 2.3$. Donner un autre contre-exemple de ce type.
(4) Montrer que le quotient d'un anneau noetherien est noetherien.
(5) Montrer que l'anneau A est isomorphe à $\mathbb{Z}[X]/(X^2+5)$. En conclure que A est noetherien.

Exercice 4 (Un autre théorème de Fermat)**.**

Montrer que les solutions de l'équation diophantienne $y^2 + 4 = z^3$ sont $(\pm 11, 5)$ et $(\pm 2, 2)$.

Indication : Travailler dans l'anneau euclidien $\mathbb{Z}[i]$.

Exercice 5 (Courbe Algébrique). On considère l'anneau $A = \mathbb{C}[X,Y]/(X^2 - Y)$. On note par x et y les images de X et de Y par la projection canonique $\pi : \mathbb{C}[X,Y] \twoheadrightarrow A$.

(1) Montrer que A est intégre.

(2) Montrer qu'il existe un morphisme injectif $\varphi : A \to \mathbb{C}[T]$ tel que $\varphi(x) = T$ et $\varphi(y) = T^2$.
Indication : On pourra considérer le reste de la division euclidienne d'un polynôme P par $X^2 - Y$ dans l'anneau $\mathbb{C}[Y][X]$.

(3) Montrer que A est isomorphe à $\mathbb{C}[T]$. En déduire que A est principal.

Exercice 6 (Racines d'un polynôme).

Soit A un anneau commutatif unitaire. On dit que $\xi \in A$ est une *racine* d'un polynôme $P \in A[X]$ si $P(\xi) = 0$.

(1) Si A est intégre, montrer que ξ est une racine de P si et seulement si $X - \xi$ divise P dans $A[X]$.

(2) En déduire que, si A est intégre, le nombre de racines d'un polynôme P est inférieur ou égal à son degré.

(3) Donner un contre-exemple lorsque A n'est pas intégre.

(4) Déterminer les polynômes irréductibles de degré 3 de $\mathbb{Z}/2\mathbb{Z}[X]$ et ceux de degré 2 de $\mathbb{Z}/3\mathbb{Z}[X]$.

Exercice 7 (Racine d'un polynôme dans $Frac(A)$).

Soit A un anneau factoriel et $P(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ un polynôme de degré n. Soit $r = \frac{p}{q}$ une racine de P dans le corps des fractions de A (cf. Exercice 3 de la Feuille 4), où p et q sont premiers entre eux dans A.

(1) Montrer que p divise a_0 et que q divise a_n.

(2) Déterminer si le polynôme $P(X) = 3X^3 + 2X^2 + X + 4$ est irréductible sur $\mathbb{Q}$.

Exercice 8 (Irréductibilité des polynômes modulo p).

Soit p un nombre premier. On considère l'application $\pi : ,\mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]$, définie pour $P = a_n X^n + \cdots + a_1 X + a_0$ par

$$\pi(a_n X^n + \cdots + a_1 X + a_0) := \overline{P} = \overline{a_n} X^n + \cdots + \overline{a_1} X + \overline{a_0}.$$

(1) Montrer que π est un morphisme d'anneaux surjectif.

(2) soit $P \in \mathbb{Z}[X]$ un polynôme unitaire. Montrer que $\overline{P}$ irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ implique P irrédictible dans $\mathbb{Z}[X]$.

(3) Le polynôme $P = X^4 + 2X^3 + X + 1$ est-il irrédictible dans $\mathbb{Z}[X]$?