Algèbre et Arithmétique 3

UNIVERSITÉ DE RENNES 1

Devoir maison
à rendre pour le mardi 12 mars dernier délai

Exercice 1

Soit P et Q des polynômes à coefficients entiers, de degrés respectifs m et n, supposés strictement positifs. On a donc

$$P = \sum_{i=0}^{m} a_i X^i, \quad Q = \sum_{i=0}^{n} b_i X^i, \quad a_i, b_i \in \mathbf{Z}, \quad a_m \neq 0,\, b_n \neq 0.$$

On note

$$P.Q = \sum_{i=0}^{n+m} c_i X^i.$$

Soit p un nombre premier. Soit $\widetilde{P}$ (respectivement $\widetilde{Q}$) l'élément de $\mathbf{F}_p[X]$ dont les coefficients sont les images des coefficients de P (respectivement de Q)dans $\mathbf{F}_p$.

1 Vérifier que les coefficients de $\widetilde{P}.\widetilde{Q}$ sont les images dans $\mathbf{F}_p$ des coefficients de $P.Q$.

2 On suppose que p divise tous les coefficients c_i. Déduire de la question précédente que soit p divise tous les a_i, soit p divise tous les b_i.

3 On suppose $a_m = b_n = 1$. On suppose que p divise tous les coefficients c_i pour $i \in \{0, \ldots, m+n-1\}$. Déduire de la première question que p divise tous les a_i pour $i \in \{0, \ldots, m-1\}$ et tous les b_i pour $i \in \{0, \ldots, n-1\}$.

4 On suppose dans cette question que P et Q sont des polynômes à coefficients *rationnels* et que $P.Q$ est à coefficients entiers et unitaire. Soit μ_1 (respectivement μ_2) le ppcm des dénominateurs des coefficients (écrits sous forme irréductible) de P (respectivement Q). Soit δ_1 (respectivement δ_2) le pgcd des numérateurs des coefficients (écrits sous forme irréductible) de P (respectivement Q). Vérifier que $\frac{\mu_1}{\delta_1}.P$ est à coefficients entiers. En déduire que $\frac{\mu_1\mu_2}{\delta_1\delta_2} \in \mathbf{Z}$. Montrer que les coefficients de $\frac{\mu_1}{\delta_1}.P$ sont premiers entre eux. En appliquant le résultat de la question 2 à $\frac{\mu_1}{\delta_1}.P$ et $\frac{\mu_2}{\delta_2}.Q$, montrer qu'aucun facteur premier ne divise $\frac{\mu_1\mu_2}{\delta_1\delta_2}$. En déduire qu'il existe $\alpha, \beta \in \mathbf{Q}^\times$ tel que $\alpha.P$ et $\beta.Q$ sont des polynômes unitaires à coefficients entiers vérifiant $(\alpha.P)(\beta.Q) = T$.

5 Soit T un polynôme unitaire à coefficients entiers, $T = X^m + \sum_{i=0}^{m-1} a_i X^i$, avec $a_i \in \mathbf{Z}$. On suppose qu'il existe un nombre premier p tel que p divise tous les coefficients a_i et p^2 ne *divise pas* a_0. Montrer que T ne peut pas s'écrire comme le produit de 2 polynômes unitaires à coefficients entiers de degré $\geqslant 1$.

En déduire que T est irréductible dans $\mathbf{Q}[X]$ (critère d'Eisenstein).

6 En déduire que $X^n - 2$ est irréductible dans $\mathbf{Q}[X]$ pour tout entier $n \geqslant 1$.

Exercice 2

Soit A un anneau commutatif.

1 Soit $a \in A$. Redémontrez que $a.A$ est un idéal de A et que tout idéal de A qui contient a contient aussi $a.A$.

2 Soit $\{I_n\}_n$ une suite d'idéaux de A croissante pour l'inclusion (c'est-à-dire pour tout $n \in \mathbf{N}$ on a $I_n \subset I_{n+1}$) ; montrer que $I \overset{\text{déf}}{=} \bigcup_{n \in \mathbf{N}} I_n$ est un idéal de A.

3 On suppose désormais A principal, c'est-à-dire pour mémoire que A est intègre et que tout idéal de A est de la forme $a.A$ pour $a \in A$. On va montrer que tout élément non nul et non inversible de A s'écrit d'une manière essentiellement unique comme produit d'éléments irréductibles de A.

Sous les même hypothèses que la question précédente, montrer qu'il existe N tel que pour tout $n \geqslant N$, on a $I_n = I$ (considérer $a \in A$ tel que $I = a.A$).

4 Soit $a \in A \setminus \{0\}$. On suppose a non inversible. Montrer que a admet un diviseur irréductible (raisonner par l'absurde et montrer que si ça n'est pas le cas, on peut constuire une suite strictement croissante d'idéaux de A, contredisant ainsi le résultat de la question précédente).

5 Dans cette question, et dans cette question seulement, on suppose que A est l'anneau $k[X]$, où k est un corps. Donner une autre démonstration du fait que tout polynôme non nul non inversible admet un diviseur irréductible.

6 Soit a un élément de A non nul, non inversible. Montrer qu'il existe des éléments irréductibles $\pi_1, \ldots, \pi_r$ de A tels que $a = \prod_{i=1}^{r} \pi_i$ (utiliser les questions 3 et 4).

7 Soit $\pi_1, \ldots, \pi_r$ et $\theta_1, \ldots, \theta_s$ des éléments irréductibles de A. On suppose qu'on a

$$\prod_{i=1}^{r} \pi_i = \prod_{j=1}^{s} \theta_j$$

Montrer qu'on a $r = s$ et que quitte à renuméroter les θ_i, on a que, pour tout $i \in \{1, \ldots, r\}$, il existe $\alpha_i \in A^\times$ tel que $\pi_i = \alpha_i.\theta_i$.

Exercice 3

Soit p un nombre premier et $A \subset \mathbf{Q}$ l'ensemble des éléments qui s'écrivent $\frac{a}{b}$ avec $a \in \mathbf{Z}$, $b \in \mathbf{Z} \setminus \{0\}$ et p ne divise pas b.

1 Montrer que A est un sous-anneau de $\mathbf{Q}$ qui contient $\mathbf{Z}$. Vérifier que pour tout idéal I de A, $I \cap \mathbf{Z}$ est un idéal de $\mathbf{Z}$.

2 Déterminer $A^\times$.

3 Montrer que l'ensemble des éléments irréductibles de A est $\{\alpha.p, \quad \alpha \in A^\times\}$.

4 Soit I un idéal de A, supposé différent de $\{0\}$. Montrer qu'il existe $n \in \mathbf{N}$ tel que $p^n \in I$ (on pourra considérer $I \cap \mathbf{Z}$). Montrer qu'il existe $a \in A$ tel que $I = a.A$ (on pourra considérer $\nu = \mathrm{Min}\{n \in \mathbf{N}, \quad p^n \in I\}$).

5 Comment s'écrit le résultat de l'exercice 2 pour cet anneau ?

Exercice 4

Exercice 16 de la feuille de TD 2

Exercice 5

Choisissez P un polynôme irréductible de degré 3 à coefficients dans $\mathbf{F}_3$. Déterminer la table de multiplication de l'anneau quotient $\mathbf{F}_3[X]/P$. Vérifier que $(\mathbf{F}_3[X]/P)^\times$ est cyclique et en donner un générateur. On pourra s'aider d'un logiciel de calcul formel.