Feuille d'exercices 5

Théorème des restes chinois

Exercice 1. Soit a et b deux entiers tels que $a, b \leq 1$. Notons $m = \operatorname{ppcm}(a, b)$ et $d = \operatorname{pgcd}(a, b)$. Considérons la fonction

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ x & \longmapsto & (x + a\mathbb{Z}, x + b\mathbb{Z}) \end{array}$$

Montrer que φ est un morphisme d'anneaux dont le noyau est $\ker(\varphi) = m\mathbb{Z}$ et l'image est

$$\operatorname{im}(\varphi) = \{(x + a\mathbb{Z}, y + b\mathbb{Z}) : d \text{ divise } x - y\}.$$

Théorème de correspondance

Exercice 2. Soit $\varphi : A_1 \to A_2$ un morphisme d'anneaux.

a. Soit B_2 un sous-anneau de A_2 et $B_1 = \varphi^{-1}(B_2)$. Montrer que B_1 est un sous-anneau de A_1 contenant $\ker(\varphi)$.

b. Montrer que $\varphi(B_1) = B_2$ si φ est surjectif. En déduire que $B_2 \cong B_1/\ker(\varphi)$.

c. Soit I_2 un idéal à gauche (respectivement, à droite, bilatère) de A_2 et $I_1 = \varphi^{-1}(I_2)$. Montrer que I_1 est un idéal à gauche (resp., à droite, bilatère) de A_1 contenant $\ker(\varphi)$.

d. Soit I_2 un idéal bilatère de A_2 et $I_1 = \varphi^{-1}(I_2)$. Montrer que l'application $\psi : A_1 \to A_2/I_2$ définie par $a \mapsto \varphi(a) + I_2$ est un morphisme d'anneaux qui induit une injection

$$\begin{array}{rcl} \widehat{\psi} : A_1/I_1 & \longrightarrow & A_2/I_2 \\ a + I_1 & \longmapsto & \varphi(a) + I_2 \end{array}$$

et si φ est surjectif, alors $\widehat{\psi}$ est un isomorphisme.

Anneaux de polynômes

Définition. Soit $p(x) = a_0 + a_1 x + \cdots a_d x^d \in A[x]$ un polynôme avec $a_d \neq 0$. Le *degré* de $p(x)$ est d ; le *coefficient dominant* de $p(x)$ est a_d ; et $p(x)$ est dit *unitaire* si son coefficient dominant est 1.

Exercice 3. Soit $f, g \in A[x]$ des polynômes dont les coefficients dominants sont a et b, respectivement.

a. Si $ab \neq 0$, alors le coefficient dominant de fg est ab et $\deg(fg) = \deg(f) + \deg(g)$.

b. Montrer que si f est unitaire, alors f n'est pas un diviseur de zéro.

Exercice 4. Soit K un corps. Montrer que $K[x]/\langle x^2+1\rangle \cong K[x]/\langle x^2+8x+17\rangle$.

Exercice 5. Soit A un anneau commutatif. Si $p(x) = b_0 + b_1x + b_2x^2 + \cdots b_dx^d \in A[x]$, alors la *fonction polynomiale* induite par $p(x)$ est la fonction de A dans A définie par

$$a \quad \longmapsto \quad p(a) = b_0 + b_1a + b_2a^2 + \cdots b_da^d.$$

a. Montrer que $x^4 + x$ et $x^2 + x$ induisent la même fonction polynomiale sur $\mathbb{Z}/3\mathbb{Z}$.

b. Déterminer si $x^8 + 1$ et $x^3 + 1$ induisent la même fonction polynomiale sur $\mathbb{Z}/5\mathbb{Z}$.

c. Montrer que l'application $A \to \mathrm{Fon}(A)$ qui associe à chaque polynôme dans $A[X]$ la fonction polynomiale correspondante est un morphisme d'anneaux. Est-il injectif ?

(Rappel : $\mathrm{Fon}(A)$ *est l'anneau de fonctions de A dans A.)*

Exercice 6. Soit $f, g \in A[x]$ deux polynômes unitaires.

a. Montrer que si f divise g et si g divise f, alors $f = g$.

b. Est-ce vrai si l'on laisse tomber l'hypothèse que f et g sont unitaires ?

Exercice 7. Un polynôme p est un *plus petit commun multiple* (ppcm) de f et g si : f divise p ; g divise p ; et si f divise p' et g divise p', alors p divise p'. Soit K un corps et $f, g \in K[x]$. Montrer qu'il existe un unique polynôme unitaire qui est un ppcm de f et g.

Exercice 8. Soit K un corps.

a. Montrer qu'il existe une infinité de polynômes unitaires et irréductibles sur K.

(Voir la démonstration d'Euclid sur l'existence d'une infinité de nombres premiers.)

b. En déduire que si K est un corps commutatif fini, alors il existe pour tout entier $n \geq 1$ des polynômes irréductibles sur K de degré supérieur à n.