6. ANNEAUX, CORPS ET POLYNÔMES

CONVENTION : *tous les anneaux considérés sont unitaires, c'est-à-dire qu'ils possèdent un élément neutre 1 pour la multiplication, et tout homomorphisme d'anneaux envoie 1 sur 1.*

Exercice 1. On appelle *entier de Gauss* un nombre complexe de la forme $a+ib$ avec $a,b \in \mathbb{Z}$.

1. Vérifier que l'ensemble $\mathscr{E}$ des entiers de Gauss, muni de l'addition et de la multiplication usuelles, est un anneau commutatif intègre.
2. Quel est le corps des fractions de $\mathscr{E}$?
3. Quels sont les éléments inversibles de $\mathscr{E}$?

Exercice 2. (*Idéaux de* $\mathrm{M}_n(k)$) Étant donné un anneau A, on rappelle qu'un *idéal* (bilatère) de A est un sous-groupe additif I de A tel que, pour tout $x \in \mathrm{I}$ et tout $a \in \mathrm{A}$, $ax \in \mathrm{I}$ et $xa \in \mathrm{I}$.

1. Soit A un anneau commutatif non nul. Démontrer que A est un corps si et seulement si les seuls idéaux de A sont $\{0\}$ et A.
2. Soit k un corps commutatif et soit n un nombre entier strictement positif. On considère un idéal non nul I de l'anneau $\mathrm{M}_n(k)$.

(i) Démontrer que I contient une matrice de rang un. (*Indication : considérer une matrice non nulle* $\mathrm{M} \in \mathrm{I}$ *et choisir convenablement* $\mathrm{P} \in \mathrm{M}_n(k)$ *de sorte que la matrice* PM *soit de rang un.*)

(ii) En déduire que I contient la matrice $\mathrm{E}_{11} = \mathrm{diag}(1,0,\ldots,0)$ puis que I contient chacune des matrices élémentaires E_{ii}, $1 \leq i \leq n$.

(iii) Conclure que l'on a $\mathrm{I} = \mathrm{M}_n(k)$.

3. Comparer les résultats des deux questions précédentes.

Exercice 3. Soient p et q deux nombres premiers distincts. Quels sont les diviseurs de zéro dans l'anneau $\mathbb{Z}/p^2\mathbb{Z}$? Dans l'anneau $\mathbb{Z}/p^2q\mathbb{Z}$?

Exercice 4. On considère dans l'anneau $\mathbb{Z}[\mathrm{X}]$ l'idéal I engendré par 2X et X^3, ainsi que l'idéal J engendré par 3X et X^2+1.

1. Vérifier que $\mathrm{X}^3 - 2\mathrm{X}$ appartient à l'idéal $\mathrm{I} \cap \mathrm{J}$.
2. Vérifier que l'on a $\mathrm{I}+\mathrm{J} = \mathbb{Z}[\mathrm{X}]$ et en déduire que $\mathrm{I} \cap \mathrm{J} = \mathrm{IJ}$.
3. Montrer qu'il n'existe pas de polynômes $\mathrm{P} \in \mathrm{I}$ et $\mathrm{Q} \in \mathrm{J}$ tels que $\mathrm{X}^3 - 2\mathrm{X} = \mathrm{PQ}$.

Exercice 5. On considère l'anneau $\mathbb{R}[\mathrm{X}]$.

1. Déterminer le pgcd des polynômes $\mathrm{X}^3+4\mathrm{X}^2+4\mathrm{X}+3$ et $\mathrm{X}^3+5\mathrm{X}^2+8\mathrm{X}+6$ puis en déduire un isomorphisme d'anneaux
$$\mathbb{R}[\mathrm{X}]/\mathrm{I} \to \mathbb{R},$$
où I est l'idéal de $\mathbb{R}[\mathrm{X}]$ engendré par $\mathrm{X}^3+4\mathrm{X}^2+4\mathrm{X}+3$ et $\mathrm{X}^3+5\mathrm{X}^2+8\mathrm{X}+6$.
2. Déterminer un générateur de l'idéal J de $\mathbb{R}[\mathrm{X}]$ engendré par les polynômes $\mathrm{X}^3+3\mathrm{X}^2+4\mathrm{X}+2$ et $\mathrm{X}^4+2\mathrm{X}^3+3\mathrm{X}^2+2\mathrm{X}+2$ puis en déduire un isomorphisme d'anneaux
$$\mathbb{R}[\mathrm{X}]/\mathrm{J} \to \mathbb{C}.$$

Exercice 6. Soit K un corps commutatif et soit $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ un polynôme de degré 2 ou 3. Démontrer que P est irréductible si et seulement si P n'a pas de racine dans K.

Exercice 7. (*Racines rationnelles des polynômes à coefficients entiers*)

1. Soit $\mathrm{P} \in \mathbb{Z}[\mathrm{X}]$ un polynôme *unitaire*. Si un nombre rationnel $r \in \mathbb{Q}$ est une racine de P, montrer que r est un nombre entier divisant $\mathrm{P}(0)$. (*Indication : écrire* $r = \frac{a}{b}$ *avec* $a,\ b \in \mathbb{Z}$ *premiers entre eux et montrer que* $b = 1$.)
2. Soit $\mathrm{Q} \in \mathbb{Z}[\mathrm{X}]$ un polynôme à coefficients entiers et de degré $d \geq 1$, écrit sous la forme $\mathrm{Q} = a_d\mathrm{X}^d + a_{d-1}\mathrm{X}^{d-1} + \ldots + a_0$ avec $a_d \neq 0$. Supposons que le nombre rationnel $\alpha \in \mathbb{Q}$ soit une racine de Q.

(i) En utilisant la question précédente, montrer que $a_d\alpha$ est un nombre entier divisant $a_d^{d-1}a_0$.

(ii) En déduire qu'un nombre fini de vérifications permet de déterminer si un polynôme $\mathrm{Q} \in \mathbb{Q}[\mathrm{X}]$ donné admet ou non une racine dans $\mathbb{Q}$.

3. En guise d'application de ce qui précède, déterminer si les polynômes suivants sont ou non irréductibles dans $\mathbb{Q}[X]$:

$$X^3-5X^2+11X-4, \quad 3X^3+2X^2+X+4, \quad X^3-3X-\frac{1}{2}.$$

Exercice 8. Soit A un anneau commutatif.

1. Démontrer qu'il existe un unique homomorphisme d'anneaux de $\mathbb{Z}$ dans A.

2. Soit n un nombre entier strictement positif. Démontrer que l'application

$$\mathrm{Hom}_{\mathbf{Ann}}(\mathbb{Z}[X_1,\dots,X_n],A) \to A^n, \quad f \mapsto (f(X_1),\dots,f(X_n))$$

réalise une bijection entre l'ensemble $\mathrm{Hom}_{\mathbf{Ann}}(\mathbb{Z}[X_1,\dots,X_n],A)$ des homomorphismes d'anneaux $\mathbb{Z}[X_1,\dots,X_n] \to A$ et l'ensemble des n-uplets d'éléments de A.

Exercice 9. Soit k un corps commutatif et soit n un nombre entier strictement positif. Un polynôme $P \in k[X_1,\dots,X_n]$ est *homogène de degré d* s'il s'exprime comme une combinaison linéaire des seuls monômes $X_1^{\nu_1}\dots X_n^{\nu_n}$ tels que $\nu_1+\dots+\nu_n=d$. L'ensemble des polynômes homogènes de degré $d \in \mathbb{N}$ est un sous-espace vectoriel de $k[X_1,\dots,X_n]$, noté $k[X_1,\dots,X_n](d)$.

Prouver la formule : $\dim_k k[X_1,\dots,X_n](d) = \frac{(n+d)!}{n!\,d!}$.

(*Indication : raisonner par récurrence sur n et d en justifiant que l'application k-linéaire*

$$k[X_1,\dots,X_{n-1}](d) \oplus k[X_1,\dots,X_n](d-1) \to k[X_1,\dots,X_n](d), \quad (P,Q) \mapsto P+X_nQ$$

est un isomorphisme.)

Exercice 10. (*Polynômes symétriques*) Soit A un anneau commutatif et soit $n \geq 1$ un nombre entier. Un polynôme $P \in A[X_1,\dots,X_n]$ est dit *symétrique* si, pour toute permutation $\sigma \in \mathfrak{S}_n$, $P(X_{\sigma(1)},\dots,X_{\sigma(n)}) = P(X_1,\dots,X_n)$.

Étant donné un nombre entier $p \in \{1,\dots,n\}$, le *p-ème polynôme symétrique élémentaire* est défini par

$$\Sigma_p = \sum_{1\leq i_1<\dots<i_p\leq n} X_{i_1}\dots X_{i_p}.$$

On a donc

$$\Sigma_1 = X_1+X_2+\dots+X_n, \quad \Sigma_2 = X_1X_2+X_1X_3+\dots+X_{n-1}X_n, \quad \dots, \quad \Sigma_n = X_1\dots X_n.$$

1. Vérifier l'identité

$$(T-X_1)(T-X_2)\dots(T-X_n) = T^n-\Sigma_1T^{n-1}+\Sigma_2T^{n-2}+\dots+(-1)^n\Sigma_n$$

dans l'anneau de polynômes $A[X_1,\dots,X_n,T]$.

2. Nous allons maintenant démontrer le théorème suivant : *pour tout polynôme symétrique $P \in A[X_1,\dots,X_n]$, il existe un unique polynôme $Q \in A[Y_1,\dots,Y_n]$ tel que $P(X_1,\dots,X_n) = Q(\Sigma_1,\dots,\Sigma_n)$.*

On raisonne par récurrence sur n puis sur le degré total de P (c'est-à-dire le maximum des degrés des monômes non nuls de P). Soit $P \in A[X_1,\dots,X_n]$ un polynôme symétrique.

(i) Vérifier que le théorème est vrai si $n=1$ ou si $\deg(P)=0$.

(ii) Supposons $n\geq 2$ et $\deg(P)\geq 1$. Démontrer qu'il existe un unique polynôme $Q_1 \in A[Y_1,\dots,Y_{n-1}]$ tel que

$$P(X_1,\dots,X_{n-1},0) = Q_1(\widetilde{\Sigma}_1,\dots,\widetilde{\Sigma}_{n-1}),$$

où l'on a posé $\widetilde{\Sigma}_d = \Sigma_d(X_1,\dots,X_{n-1},0)$.

(iii) Vérifier que le polynôme $P-Q(\Sigma_1,\dots,\Sigma_{n-1}) \in A[X_1,\dots,X_n]$ est symétrique et que c'est un multiple de X_n. En déduire que P s'écrit sous la forme

$$P = Q_1(\Sigma_1,\dots,\Sigma_{n-1})+\Sigma_nQ_2$$

avec $Q_2 \in A[X_1,\dots,X_n]$ symétrique et tel que $\deg(Q_2)<\deg(P)$.

(iv) Achever la preuve du théorème.

3. En appliquant la méthode utilisée pour démontrer le théorème précédent, exprimer les deux polynômes symétriques suivants à l'aide des polynômes symétriques élémentaires :

$$X_1^2X_2+X_1X_2^2+X_1^2X_3+X_1X_3^2+X_2^2X_3+X_2X_3^2 \qquad (n=3)$$

et

$$(X_1X_2+X_3X_4)(X_1X_3+X_2X_4)(X_1X_4+X_2X_3) \qquad (n=4).$$