7. ANNEAUX, CORPS ET POLYNÔMES (SUITE)

Exercice 1 — Soit A un anneau commutatif intègre.

1. Démontrer qu'un polynôme $P \in A[T]$ est inversible si et seulement si $P = a$ avec $a \in A^\times$. (*Indication : raisonner par l'absurde en supposant que* P *de degré* ≥ 1 *est inversible, d'inverse* Q*, et considérer le terme dominant du polynôme* PQ.)

2. En déduire que l'on a $A[X_1, \ldots, X_n]^\times = A^\times$ pour tout $n \geq 1$.

Exercice 2 — Soit k un corps commutatif. Étudier l'irréductibilité des polynômes

$$X^3 - Y^2 - X \quad \text{et} \quad XY^3 - X^2Y - Y^2 + X.$$

(*Indiation : travailler d'abord dans l'anneau* $k(X)[Y]$ *puis utiliser le théorème de Gauss.*)

Exercice 3 — Soit A un anneau commutatif.

1. Soit I un idéal de A et soit $p : A \to A/I$ la projection canonique. Démontrer que l'application $J \mapsto p^{-1}(J)$ réalise une bijection entre l'ensemble des idéaux de A/I et l'ensemble des idéaux de A contenant I, puis vérifier que J est premier (resp. maximal) si et seulement si $p^{-1}(J)$ est premier (resp. maximal).

En guise d'application, déterminer tous les idéaux premiers (resp. maximaux) de l'anneau $\mathbb{Z}/6\mathbb{Z}$.

2. Étant donnés deux éléments f, g de A, on pose $A' = A/(f)$ et on note $a \mapsto \overline{a}$ la projection canonique $A \to A'$. Démontrer que l'application $A \to A'$, $a \mapsto \overline{a} \pmod{\overline{g}}$ induit un isomorphisme d'anneaux entre $A/(f,g)$ et $A'/(\overline{g})$.

Exercice 4 (*L'anneau des entiers de Gauss*) — On étudie dans cet exercice l'anneau $\mathbb{Z}[i]$ des entiers de Gauss.

On désigne par N l'application $\mathbb{Z}[i] \to \mathbb{N}$, $z = a + ib \mapsto N(z) = z\overline{z} = a^2 + b^2$.

1. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?

2. Comment démontre-t-on que cet anneau est principal ? En guise d'illustration, déterminer un générateur de l'idéal engendré par $5 + 5i$ et $3 - 4i$.

3. Soit p un nombre premier. Démontrer que l'anneau $\mathbb{Z}[i]/(p)$ est isomorphe à $\mathbb{F}_p[X]/(X^2 + 1)$. (*Indication : utiliser la question 2 de l'exercice 3.*)

4. Soit p un nombre premier.

(i) Si $p \geq 2$, démontrer que -1 est un carré dans $\mathbb{F}_p$ si et seulement s'il existe un élément d'ordre 4 dans le groupe $\mathbb{F}_p^\times$. En déduire que tel est le cas si et seulement si $p \equiv 1 \pmod 4$. (*Indication : utiliser le fait que le groupe* $\mathbb{F}_p^\times$ *est cyclique, cf. fiche 3, exercice 12.*)

(ii) En déduire que p est un élément irréductible de $\mathbb{Z}[i]$ si et seulement si $p \equiv 3 \pmod 4$.

(iii) Si $p = 2$ ou si $p \equiv 1 \pmod 4$, démontrer qu'il existe un élément irréductible π de $\mathbb{Z}[i]$ tel que $\pi\overline{\pi} = p$.

4. En utilisant la question précédente, démontrer que les éléments irréductibles de $\mathbb{Z}[i]$ sont, aux éléments inversibles près,

– les nombres premiers $p \in \mathbb{N}$ avec $p \equiv 3 \pmod 4$,
– les entiers de Gauss $a + ib$ dont la norme est un nombre premier.

Vérifier enfin que, parmi ces éléments, seuls $1 + i$ et $1 - i$ sont associés.

Exercice 5 (*L'anneau des entiers de Gauss : applications*) — Voici deux applications arithmétiques de l'étude de l'anneau $\mathbb{Z}[i]$ conduite à l'exercice précédent.

1. *Première application : un nombre entier naturel* $n \geq 2$ *peut s'écrire sous la forme* $a^2 + b^2$ *avec* $a, b \in \mathbb{N}$ *si et seulement si, dans sa décomposition en facteurs premiers, tout nombre premier* $p \equiv 3 \pmod 4$ *intervient avec une multiplicité paire.*

Soit Σ l'ensemble des nombres entiers $n \geq 2$ que l'on peut écrire sous la forme $a^2 + b^2$ avec $a, b \in \mathbb{N}$ et soit $n \geq 2$ un nombre entier.

(i) Vérifier que $n \in \Sigma$ si et seulement s'il existe $z \in \mathbb{Z}[i]$ tel que $n = z\overline{z}$.

(ii) On rappelle que l'anneau $\mathbb{Z}[i]$ est factoriel (car principal, cf. cours). Démontrer que n s'écrit sous la forme $z\overline{z}$ dans $\mathbb{Z}[i]$ si et seulement si sa décomposition en facteurs premiers dans $\mathbb{Z}$ est de la forme $n = \prod_p p^{v_p(n)}$ avec $v_p(n)$ pair pour tout $p \equiv 3 \pmod 4$.

2. *Seconde application : détermination des solutions entières de l'équation de Pythagore* $x^2+y^2=z^2$.

On cherche à déterminer l'ensemble $\mathscr{E}$ de tous les triplets $(x,y,z)\in\mathbb{Z}^3$ tels que $x^2+y^2=z^2$ et $xyz\neq 0$.

(i) Justifier que tout élément (x,y,z) de $\mathscr{E}$ s'écrit sous la forme (dx',dy',dz') avec $d\in\mathbb{N}$, $(x',y',z')\in\mathscr{E}$ et $\mathrm{pgcd}(x',y')=1$.

Soit $(x,y,z)\in\mathscr{E}$ avec $\mathrm{pgcd}(x,y)=1$; l'identité $x^2+y^2=z^2$ s'écrit également sous la forme

$$(x+iy)(x-iy)=z^2.$$

(ii) Justifier que, pour tout élément irréductible $\pi\in\mathbb{Z}[i]$ non associé à $1+i$, la multiplicité de π dans $x+iy$ est paire.

(iii) Justifier que la multiplicité de $1+i$ est la même dans $x+iy$ et dans $x-iy$. En utilisant le fait que z est un nombre réel, vérifier par ailleurs que la multiplicité de $1+i$ dans z est paire. En déduire finalement que la multiplicité de $1+i$ dans $x+iy$ est paire.

(iv) Déduire des questions précédentes que l'on a $x+iy=u\lambda^2$ et $z=\pm\lambda\overline{\lambda}$ avec $u\in\mathbb{Z}[i]^\times$ et $\lambda\in\mathbb{Z}[i]$. En conclusion, démontrer qu'il existe $a,b\in\mathbb{Z}$ tels que $(x,y,z)=(a^2-b^2,2ab,a^2+b^2)$ ou $(x,y,z)=(2ab,a^2-b^2,a^2+b^2)$.

Exercice 6 — Soit ϑ une racine carrée de -5 dans $\mathbb{C}$ et soit $\mathbb{Z}[\vartheta]$ le plus petit sous-anneau de $\mathbb{C}$ contenant ϑ.

1. Démontrer que l'application

$$\mathbb{Z}[\mathrm{X}]\to\mathbb{C},\ \ \mathrm{P}\mapsto\mathrm{P}(\vartheta)$$

induit un isomorphisme d'anneaux entre $\mathbb{Z}[\mathrm{X}]/(\mathrm{X}^2+5)$ et $\mathbb{Z}[\vartheta]$. En déduire que tout élément de $\mathbb{Z}[\vartheta]$ s'écrit d'une manière et d'une seule sous la forme $a+b\vartheta$ avec $a,\ b\in\mathbb{Z}$ et que l'on a

$$(a+b\vartheta)-(a'+b'\vartheta)=(a-a')+(b-b')\vartheta,\ \ (a+b\vartheta)(a'+b'\vartheta)=(aa'-5bb')+(ab'+a'b)\vartheta.$$

2. Montrer que l'application

$$\mathrm{N}:\mathbb{Z}[\vartheta]\to\mathbb{N},\ a+b\vartheta\mapsto a^2+5b^2$$

est multiplicative, c'est-à-dire vérifie $\mathrm{N}(zz')=\mathrm{N}(z)\mathrm{N}(z')$. En déduire que les seuls éléments inversibles de $\mathbb{Z}[\vartheta]$ sont 1 et -1.

3. Vérifier que les éléments 2, 3, $1+\vartheta$, $1-\vartheta$ sont irréductibles et deux à deux non associés. En utilisant l'identité $6=2.3=(1+\vartheta)(1-\vartheta)$, en déduire que l'anneau $\mathbb{Z}[\vartheta]$ n'est pas factoriel.

4. Soient $\mathfrak{p}=(2,1+\vartheta)$, $\mathfrak{q}=(3,1+\vartheta)$ et $\mathfrak{q}'=(3,1-\vartheta)$ les idéaux de $\mathbb{Z}[\vartheta]$ respectivement engendrés par 2 et $1+\vartheta$, par 3 et $1+\vartheta$ et par 3 et $1-\vartheta$.

(i) Montrer que ces idéaux ne sont pas principaux.

(*Indication : raisonner par l'absurde en observant que, si* $\mathfrak{p}$ *était engendré par un élément* z *de* $\mathbb{Z}[\vartheta]$, *alors* $\mathrm{N}(z)\geq 2$ *et* $\mathrm{N}(z)|\mathrm{pgcd}(\mathrm{N}(2),\mathrm{N}(1+\vartheta))=\mathrm{pgcd}(4,6)=2$, *donc* $\mathrm{N}(z)=2$, *ce qui est impossible...*)

(ii) En utilisant l'exercice 3, prouver que l'on a $\mathbb{Z}[\vartheta]/\mathfrak{p}\simeq\mathbb{F}_2$ et $\mathbb{Z}[\vartheta]/\mathfrak{q},\ \mathbb{Z}[\vartheta]/\mathfrak{q}'\simeq\mathbb{F}_3$. En déduire que les idéaux $\mathfrak{p},\mathfrak{q}$ et $\mathfrak{q}'$ de $\mathbb{Z}[\vartheta]$ sont maximaux.

(iii) Vérifier que l'on a $\mathfrak{p}^2=(2)$ et $\mathfrak{q}\mathfrak{q}'=(3)$. En déduire que l'on a $(6)=\mathfrak{p}^2\mathfrak{q}\mathfrak{q}'$.

Exercice 7 — Soit X un espace topologique compact et soit $\mathrm{C}(\mathrm{X})=\mathrm{C}^0(\mathrm{X},\mathbb{R})$ le $\mathbb{R}$-espace vectoriel des fonctions réelles continues sur X ; muni de l'addition et de la multiplication usuelle des fonctions, $\mathrm{C}(\mathrm{X})$ est un anneau commutatif.

L'objet de cet exercice est de montrer que l'on peut reconstituer l'espace topologique X *à partir de l'anneau* $\mathrm{C}(\mathrm{X})$.

On désigne par $\mathrm{M}(\mathrm{X})$ l'ensemble de tous les idéaux maximaux de l'anneau $\mathrm{C}(\mathrm{X})$.

1. Soit x un point de X. Vérifier que l'application

$$\mathrm{ev}_x:\mathrm{C}(\mathrm{X})\to\mathbb{R},\ \ f\mapsto f(x)$$

est un homomorphisme d'anneaux surjectif. En déduire que son noyau

$$\mathfrak{m}_x=\{f\in\mathrm{C}(\mathrm{X})\mid f(x)=0\}$$

est un idéal maximal de $\mathrm{C}(\mathrm{X})$.

2. On rappelle la conséquence suivante du *lemme d'Urysohn* en Topologie générale : quels que soient les sous-espaces fermés disjoints F et F′ dans un espace topologique compact X, il existe une fonction continue $f\in\mathrm{C}(\mathrm{X})$ telle que $f_{|\mathrm{F}}=0$ et $f_{|\mathrm{F}'}=1$.

En utilisant ce résultat, démontrer que l'application

$$j : \mathrm{X} \to \mathrm{M}(\mathrm{X}), \;\; x \mapsto \mathfrak{m}_x$$

est injective.

3. On va démontrer que l'application j est surjective, et donc bijective, en raisonnant par l'absurde. Supposons qu'il existe un idéal maximal $\mathfrak{m}$ de $\mathrm{C}(\mathrm{X})$ qui ne soit pas de la forme $\mathfrak{m}_x$ pour un certain point x dans X.

(i) On choisit pour tout point $x \in \mathrm{X}$ une fonction f_x appartenant à $\mathfrak{m}$ mais non à $\mathfrak{m}_x$. Justifier que f_x ne s'annule pas sur tout un voisinage ouvert de x.

(ii) En déduire qu'il existe un nombre fini de points $x_1, \ldots, x_n$ de X tels que la fonction $g = f_{x_1}^2 + \ldots + f_{x_n}^2$ ne s'annule en aucun point de X.

(iii) En conclure à une contradiction, ce qui prouve la surjectivité de l'application j. (*Indication : observer que, par construction,* $g \in \mathfrak{m}$ *; or* g *est inversible dans* $\mathrm{C}(\mathrm{X})$...)

4. Étant donnée une fonction $f \in \mathrm{C}(\mathrm{X})$, on pose

$$\mathrm{D}(f) = \{\mathfrak{m} \in \mathrm{M}(\mathrm{X}) \mid f \notin \mathfrak{m}\}.$$

Vérifier que les ensembles $\mathrm{D}(f)$ constituent une base d'ouverts pour une topologie sur $\mathrm{M}(\mathrm{X})$, c'est-à-dire que les réunions quelconques d'ensembles de cette forme vérifient les axiomes caractérisant les ouverts d'un espace topologique.

5. Si l'on munit $\mathrm{M}(\mathrm{X})$ de la topologie que l'on vient de définir, vérifier que l'application j est un homéomorphisme.