TD 6

Anneaux et idéaux

Exercice 1. Soit $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

(a) Montrer que $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$ est un anneau avec les opérations classiques d'addition et multiplication dans $\mathbb{R}$.

(b) On considère la fonction

$$\begin{array}{rccc} f: & \mathbb{Z}[\sqrt{2}] & \to & \mathbb{Z}[\sqrt{2}] \\ & a + b\sqrt{2} & \mapsto & a - b\sqrt{2} \end{array}$$

Montrer que f est un automorphisme de $\mathbb{Z}[\sqrt{2}]$ d'ordre 2.

(c) Pour $x \in \mathbb{Z}[\sqrt{2}]$, on pose $N(x) = x \cdot f(x)$. Montrer que pour tout x, $y \in \mathbb{Z}[\sqrt{2}]$, $N(x) \in \mathbb{Z}$ et $N(xy) = N(x)N(y)$.

(d) Montrer que x est inversible dans $\mathbb{Z}[\sqrt{2}]$ si et seulement si $N(x) = \pm 1$. Donner des exemples d'éléments inversibles dans $\mathbb{Z}[\sqrt{2}]$.

Exercice 2. Soient I et J deux idéaux d'un anneau commutatif A. On définit :

$$\begin{aligned} I + J &:= \{\, x + y \mid x \in I,\ y \in J \,\}, \\ I \cap J &:= \{\, x \in A \mid x \in I \text{ et } x \in J \,\}, \\ IJ &:= \left\{ \sum_{k=1}^{n} x_k y_k \;\middle|\; n \geq 1,\ x_k \in I,\ y_k \in J \right\}. \end{aligned}$$

(a) Montrer que $I + J$, $I \cap J$ et IJ sont des idéaux de A.

(b) On considère dans $\mathbb{Z}$ les idéaux $I = 126\mathbb{Z}$ et $J = 84\mathbb{Z}$. Déterminer explicitement les idéaux $I + J$, $I \cap J$ et IJ.

(c) Plus généralement, dans $\mathbb{Z}$, si $I = a\mathbb{Z}$ et $J = b\mathbb{Z}$ avec $a, b \in \mathbb{Z}$, déterminer les générateurs respectifs de $I + J$, $I \cap J$ et IJ.

Exercice 3.

(a) Soit K un corps et $A, P \in K[X]$. Montrer que la classe $[A]$ est inversible dans $\frac{K[X]}{(P)}$ si et seulement si $\text{pgcd}(A, P) = 1$.

(b) Déterminer pour quelles valeurs du paramètre $a \in \mathbb{F}_5$ l'anneau quotient

$$A = \frac{\mathbb{F}_5[X]}{(X^2 + aX + 1)},$$

est un corps. Pour ces valeurs, quelle est la cardinalité de A.

Exercice 4. On rappelle que pour p un nombre premier, on note $\mathbb{F}_p := \frac{\mathbb{Z}}{p\mathbb{Z}}$. On considère l'ensemble $A = \mathbb{F}_5 \times \mathbb{F}_5$ dans lequel sont définies les opérations suivantes :

$$(a,b) + (a',b') := (a+a',\, b+b'), \qquad (a,b)(a',b') := (aa' + 3bb',\, ab' + a'b).$$

(a) Montrer que A est un anneau commutatif, dont on déterminéra les éléments neutres par rapport à l'addition et à la multiplication.

(b) Montrer que l'application

$$\varphi : \mathbb{F}_5[X] \longrightarrow A, \qquad \sum_i a_i X^i \longmapsto \sum_i (a_i, 0) \cdot (0,1)^i,$$

est un homomorphisme d'anneaux.

(c) Déterminer le noyau $\ker \varphi$ et l'image $\operatorname{Im} \varphi$ et définir l'application canonique

$$\overline{\varphi} : \frac{\mathbb{F}_5[X]}{\ker \varphi} \longrightarrow \operatorname{Im} \varphi$$

donnée par le théorème d'isomorphisme.

Exercice 5. Le but de cet exercice est de montrer l'existence d'un anneau où la décomposition en facteurs irréductibles n'est pas unique (contrairement à ce qui se passe dans $\mathbb{Z}$ ou dans $K[X]$), afin de voir que cette propriété n'est pas une évidence en soi.

On désigne par $A = \mathbb{Z}[i\sqrt{5}] \subseteq \mathbb{C}$ l'ensemble des nombres complexes de la forme $z = a + b\,i\sqrt{5}$ avec $a, b \in \mathbb{Z}$.

(a) Soient $+$ et $\cdot$ respectivement l'addition et la multiplication dans $\mathbb{C}$. Montrer que $(A, +, \cdot)$ est un anneau intègre et que si on définit $N(z) = |z|^2$, où $|z|$ dénote le module d'un nombre complexe, alors N définit une application $A \to \mathbb{N}$ telle que $N(zz') = N(z)N(z')$.

(b) Déterminer les éléments inversibles z de A (en montrant d'abord qu'un tel élément z vérifie nécessairement $N(z) = 1$).

(c) Déterminer explicitement tous les éléments $z \in A$ tels que $N(z) = p$ avec $p \in \{2, 3, 4, 6, 9, 12, 18\}$ (à savoir les diviseurs entiers de 36 autres que 1 et 36).

(d) Montrer que l'élément 6 admet dans A les deux décompositions en éléments irréductibles

$$6 = 2 \times 3 = (1 + i\sqrt{5}) \times (1 - i\sqrt{5}),$$

que ces décompositions ne sont pas équivalentes (aux inversibles près), et qu'il n'y a pas d'autres décompositions de 6 dans A (à l'ordre près des facteurs, et à éléments inversibles près).

(e) On considère l'ensemble $I := \{a + b\,i\sqrt{5} : a \equiv b \pmod 2\}$. Montrer que I est un idéal de A et que $I = (2,\, 1 + i\sqrt{5})$. Montrer que I n'est pas un idéal *principal*, c'est-à-dire il n'existe pas $g \in I$ tel que $I = (g)$.