IX

Exercice 1

a) Soit p un nombre premier $= 1 \bmod 4$. Montrer que dans $\mathbb{Z}[i]$, p est le produit de deux nombres premiers. En déduire que p est somme de 2 carrés.

b) Si m, n sont des entiers sommes de 2 carrés d'entiers, montrer que mn aussi.

c) Soit $n \in \mathbb{N}$. Montrer que n est somme de deux carrés si et seulement si les nombres premiers $= 3 \bmod 4$ apparaissent dans la décomposition de n avec un exposant pair.

Exercice 2

Soit A un anneau principal.

a) Soit P un idéal premier de $A[X]$. Montrer que $P = 0$, P est principal ou P est de la forme $P = (p, f)$ où $p \in A$ est irréductible et f est irréductible dans $A/p[X]$ *(indication : considérer $P \cap A$)*. Dans ce dernier cas, montrer que P est maximal.

b) Si $A = \mathbb{C}[[t]]$ et $f = tX - 1$, montrer que (f) est un idéal maximal de A.

c) Si A contient une infinité d'éléments irréductibles (deux à deux non associés), montrer qu'aucun idéal maximal $\mathfrak{m}$ de A n'est principal *(indication : si $\mathfrak{m} = (f)$, considérer un élément irréductible de A qui ne divise aucun coefficient de f)*.

Exercice 3 Soit A l'ensemble des polynômes de la forme

$$\sum_n \frac{a_n}{n!} X^n$$

avec $\forall\, n,\ a_n \in \mathbb{Z}$.

a) Vérifier que A est un sous-anneau de $\mathbb{Q}[X]$.

b) Montrer que la suite d'idéaux de A :

$$(X) \subseteq (X, \frac{X^2}{2}) \subseteq ... \subseteq (X, \frac{X^2}{2}, ..., \frac{X^n}{n!}) \subseteq ...$$

est strictement croissante.

c) En déduire un idéal de A qui n'est pas de type fini.

Exercice 4 a) Soit I un idéal de $\mathbb{C}[X, Y]$ tel que $\mathbb{C}[X, Y]/I$ est de dimension finie. Montrer qu'il existe un nombre fini d'idéaux maximaux de $\mathbb{C}[X, Y]$ qui contiennent I.

b) En déduire qu'il existe un nombre fini $\leqslant \dim \mathbb{C}[X, Y]/I$ de points $(x, y) \in \mathbb{C}^2$ tels que $p(x, y) = 0$ pour tout $p \in I$.

Exercice 5 Soient p, q deux nombres premiers distincts impairs. L'objectif de cet exercice est de montrer la *loi de réciprocité quadratique de Gauss* :

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Soit ζ une racine primitive q-ième d'unité dans une clôture algébrique de $\mathbb{F}_p$. On pose

$$\tau := \sum_{x \in \mathbb{F}_q^\times} \left(\frac{x}{q}\right) \zeta^x.$$

Cette somme est appelée la *somme de Gauss*.

a) Montrer que

$$\tau^2 = \sum_{u \in \mathbb{F}_q} \zeta^u \left(\sum_{t \in \mathbb{F}_q} \left(\frac{t(u-t)}{q}\right)\right).$$

b) Montrer que, si $t \neq 0$, on a

$$\left(\frac{t(u-t)}{q}\right) = (-1)^{\frac{q-1}{2}} \left(\frac{1-ut^{-1}}{q}\right).$$

c) On pose $C_u := \sum_{t \in \mathbb{F}_q^\times} \left(\frac{1-ut^{-1}}{q}\right)$.

(a) Montrer que $C_0 = q-1$ et que $C_u = -1$ pour $u \neq 0$.

(b) En déduire que $\tau^2 = (-1)^{\frac{q-1}{2}} q$.

(c) Montrer que

$$\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = \left(\frac{q}{p}\right) (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

d) En utilisant la définition de τ, calculer τ^p. En déduire que $\tau^{p-1} = \left(\frac{p}{q}\right)$.

e) Conclure.

Par exemple, si p est un nombre premier impair $\neq 5$, 5 est un carré $\bmod p \Leftrightarrow p$ *est un carré* $\bmod 5$.

Exercice 6 On considère l'équation $x^2 \equiv 59\ [103]$ dans $\mathbb{Z}$.

a) À l'aide de la loi de réciprocité quadratique, montrer que l'équation admet une solution.

b) Trouver tous les solutions de l'équation.

c) Montrer que $59^{51} - 1$ est divisible par 103.

Exercice 7 Soit $y \in \mathbb{C}$ une racine primitive 8−ième de l'unité.

a) Montrer que $(y + y^{-1})^2 = 2$.

b) En déduire que :

$$(y + y^{-1}) 2^{(p-1)/2} = (y^p + y^{-p}) \bmod p$$

dans $\mathbb{Z}[y]$.

c) Retrouver la loi de réciprocité complémentaire :

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p = \pm 1 \bmod 8, \\ -1 & \text{si } p = \pm 3 \bmod 8. \end{cases}$$