Théorie des nombres
FEUILLE DE TD No1

---

**Exercice 1** Considérons l'anneau $\mathbf{Z}[\sqrt{13}]$. À tout élément $x = a + b\sqrt{13}$ de $\mathbf{Z}[\sqrt{13}]$ on associe son conjugué $\overline{x} = a - b\sqrt{13}$.

1. Montrer que pour tous $x, y \in \mathbf{Z}[\sqrt{13}]$ on a
$$\overline{x+y} = \overline{x} + \overline{y} \quad \text{et} \quad \overline{xy} = \overline{xy}.$$
2. En considérant l'application $N : x \to x\overline{x}$, caractériser le groupe $U$ des éléments inversibles de $\mathbf{Z}[\sqrt{13}]$. Vérifier que $\pm 1$, $\pm 18 \pm 5\sqrt{13}$ sont dans $U$.
3. Montrer que les éléments 2, $3 + \sqrt{13}$, $-3 + \sqrt{13}$ sont irréductibles dans $\mathbf{Z}[\sqrt{13}]$.
4. Montrer que l'anneau $\mathbf{Z}[\sqrt{13}]$ n'est pas factoriel.

**Exercice 2** Quels sont les idéaux de l'anneau $\mathbf{Z}/3^3 7^2\mathbf{Z}$ ? Quelles sont les relations d'inclusions entre eux ? Lesquels sont premiers ?

**Exercice 3** Soit $P = X^3 - 2X^2 + 2$.

1. Montrer que $P$ est irréductible dans $\mathbf{Q}[X]$. En déduire que $\mathbf{Q}[\mathbf{X}]/(P)$ est un corps.
2. Soit $Q = X^4 - 3X^2 + 1$. Déterminer l'inverse de $Q$ dans $\mathbf{Q}[\mathbf{X}]/(P)$.

**Exercice 4** Soit $A$ un anneau commutatif intÃÍgre.

1. Soient $f$ et $g$ deux polynômes non constants à coefficients dans $A$. Dans l'anneau $A[X, Y]$, on considère l'idéal $I$ engendré par les polynômes $f(X)$ et $g(Y)$.
Montrer que l'on a
$$I \neq A[X, Y].$$
2. Montrer que pour tout entier $k$ tel que $1 \leq k \leq n$, l'idéal de $A[X_1, \ldots, X_n]$ engendré par $X_1, \ldots, X_k$ est premier. Ces $n$ idéaux sont-ils deux à deux distincts ?

**Exercice 5** Soit $A$ un anneau commutatif intÃÍgre. Soit $I$ l'idéal de $A[X, Y]$ engendré par $X + Y$.

1. Montrer que $A[X, Y]/I$ est isomorphe à l'anneau $A[X]$.
2. L'idéal $I$ est-il premier ? Est-il maximal ?

**Exercice 6**

1. Montrer que $(\mathbf{Z}/6\mathbf{Z})[X]$ n'est pas factoriel.
2. Montrer que $\mathbf{Z}[\sqrt{-3}]$ n'est pas factoriel.
3. Donner un idéal non principal de $A = \mathbf{Z}[\sqrt{-3}]$.
4. Montrer que le sous-anneau $A$ de $\mathbf{R}[X]$ engendré par $X^2$ et $X^3$ n'est pas factoriel.
5. Vérifier l'égalité $17 = (5 + 2\sqrt{2})(5 - 2\sqrt{2}) = (7 + 4\sqrt{2})(7 - 4\sqrt{2})$. Peut-on en déduire que $A = \mathbf{Z}[\sqrt{2}\,]$ n'est pas factoriel ?
6. Soit $A$ un anneau principal. Peut-on supposer que $A$ ne possède pas d'éléments irréductibles ?

**Exercice 7** Soit $A$ un anneau commutatif. On dit que $x \in A$ est nilpotent si il existe $n > 0$ tel que $x^n = 0$

1. Montrer que l'ensemble $N$ des éléments nilpotents de $A$ est un idéal de $A$.
2. Montrer que le quotient $A/N$ n'a pas d'élément nilpotent.
3. Trouver un exemple d'anneau $A$ avec deux éléments $x$ et $y$ nilpotents tels que $x + y$ n'est pas nilpotent.
4. Montrer que $A$ n'a pas d'élément nilpotent si et seulement si tout élément inversible de $A[X]$ est constant.

**Exercice 8** Infinité des nombres premiers.
On définit le $n$-ième nombre de Fermat par $F_n = 2^{2^n} + 1$.

1. Montrer par récurrence que pour tout $n \geq 1$

$$F_n = \prod_{i=0}^{n-1} F_i + 2.$$

2. En déduire que les nombres de Fermat sont deux à deux premiers entre eux et qu'il y a une infinité de nombres premiers.

**Exercice 9** Infinité des nombres premiers.
Pour $a$, $b$ dans $\mathbf{Z}$ avec $b \neq 0$, on définit l'ensemble $E_{a,b} = a + b\mathbf{Z} = \{a + bn \mid n \in \mathbf{Z}\}$. On munit $\mathbf{Z}$ de la topologie dont les $E_{a,b}$ forment une base d'ouvert.

1. Montrer que chacun des $E_{a,b}$ est un ensemble ouvert et fermé pour cette topologie.
2. Montrer que tout ouvert de $\mathbf{Z}$ est soit vide, soit infini.
3. On note $\mathcal{P}$ l'ensemble des nombres premiers. Montrer que

$$\bigcup_{p \in \mathcal{P}} E_{0,p} = \mathbf{Z} \setminus \{-1, 1\}.$$

4. En raisonnant par l'absurde, montrer que l'ensemble $\mathcal{P}$ est infini.

**Exercice 10** On appelle triplet pythagoricien un triplet $(a, b, c)$ d'entiers strictement positifs tels que $a^2 + b^2 = c^2$ ; autrement dit, $a, b, c$ sont les longueurs des côtés d'un triangle rectangle, $c$ étant la longueur de l'hypoténuse du triangle.

1) Soient $m > n$ des entiers naturels premiers entre eux et $k$ un entier naturel quelconque. Montrer que :

$$a = k(m^2 - n^2), \qquad b = 2kmn, \qquad c = k(m^2 + n^2)$$

est un triplet pythagoricien.

Dans la suite de ce problème, on propose de montrer la réciproque. Soit donc $(a, b, c)$ un triplet pythagoricien tel que $a, b$ et $c$ n'aient aucun diviseur premier commun.

2) Montrer que $(a, b), (b, c), (c, a)$ sont des couples d'entiers premiers entre eux.
3) Montrer que $a$ ou $b$ est pair (on pourra raisonner modulo 4).

On suppose désormais $b$ pair et on pose $b = 2b'$.

4) Montrer que $u = \dfrac{c + a}{2}$ et $v = \dfrac{c - a}{2}$ sont des entiers premiers entre eux.
5) Montrer que $u$ et $v$ sont des carrés d'entiers. Conclure.
6) Pour quelles valeurs de $m$ et $n$ obtient-on $a = 10441$ et $c = 20809$ ?