# TD2 : Anneaux, idéaux, anneaux principaux et factoriels

Diego Izquierdo

*Les exercices 1, 2, 4 et 5 sont à préparer avant le TD. Pendant la séance de TD, les exercices seront traités dans l'ordre suivant : 1, 2, 4, 5, 6, 11. Si le temps le permet, nous traiterons ensuite les exercices 9 et 13. Les exercices 5 et 6 sont fondamentaux : il faut les retenir.*

**Exercice 1 (à préparer) : Idéaux principaux, idéaux de type fini**

**1.** Soit $k$ un corps. Rappeler pourquoi tout idéal de $k[X]$ est principal.
**2.** Exhiber des idéaux non principaux dans $k[X,Y]$, $k[T^2,T^3]$ et $\mathbb{Z}[X]$.
**3.** Montrer que $\mathbb{Z}[i\sqrt{5}]$ possède des idéaux non principaux.
**4.** Soit $k$ un corps. Montrer que la sous-$k$-algèbre de $k[X,Y]$ engendrée par les $X^nY$ pour $n>0$ possède un idéal qui n'est pas de type fini.

**Exercice 2 (à préparer) : Vrai ou faux ?**
Soit $A$ un anneau.

**1.** Pour tout couple d'idéaux $(I,J)$ de $A$, on a $\sqrt{I+J}=\sqrt{I}+\sqrt{J}$.
**2.** Si $a$, $b$ et $u$ sont trois éléments $A$ tels que $(a)=(b)$ et $a=bu$, alors $u\in A^\times$.
**3.** Un sous-anneau d'un anneau euclidien est factoriel.
**4.** L'anneau des nombres décimaux est euclidien.
**5.** Les groupes $\mathbb{Q}^\times$ et $(\mathbb{Z}/3\mathbb{Z}(X))^\times$ sont isomorphes.

**Exercice 3 : Vrai ou faux ? Le retour**
Soit $A$ un anneau.

**1.** Pour tout idéal $I$ de $A$, on a $\sqrt{\sqrt{I}}=\sqrt{I}$.
**2.** Tout idéal du quotient d'un anneau principal par un idéal est principal.
**3.** Si $A$ est intègre, $I$ est un idéal principal et $A/I$ est un anneau principal, alors $A$ est principal.
**4.** La somme de deux idéaux non principaux d'un anneau est soit un idéal non principal soit l'anneau tout entier.
**5.** S'il existe une suite croissante $(A_n)_{n\in\mathbb{N}}$ de sous-anneaux factoriels de $A$ telle que $A=\bigcup_{n\in\mathbb{N}}A_n$, alors $A$ est factoriel.

**Exercice 4 (à préparer) : Quotients d'anneaux**
Soit $k$ un corps.

**1.** Montrer que la $k$-algèbre $k[X,Y]/(X^2-Y^3)$ est isomorphe à $k[T^2,T^3]$.
**2.** Montrer que la $k$-algèbre $k[X,Y]/(X^2-Y)$ est isomorphe à $k[T]$.

**3.** Plus généralement, soient $a$ et $b$ deux entiers naturels non nuls. Réaliser l'anneau $k[T^a, T^b]$ comme quotient de $k[X,Y]$.
**4.** Montrer que la $k$-algèbre $k[X,Y]/(XY-1)$ n'est pas isomorphe à $k[T]$.
**5.** Réaliser les anneaux $\mathbb{Z}[i\sqrt{7}]$ et $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ comme quotients de $\mathbb{Z}[X]$.

**Exercice 5 (à préparer) : Idéaux dans un anneau principal**
Soient $A$ un anneau principal et $x \in A$ non nul. Montrer que les assertions suivantes sont équivalentes :
(i) l'élément $x$ est irréductible ;
(ii) l'idéal $(x)$ est premier, c'est-à-dire que $A/(x)$ est un anneau intègre ;
(iii) l'idéal $(x)$ est maximal, c'est-à-dire que $A/(x)$ est un corps.

**Exercice 6 : Idéaux d'un quotient**
Soient $A$ un anneau commutatif unitaire et $I$ un idéal.
**1.** Montrer que les idéaux de $A/I$ sont en bijection avec les idéaux de $A$ contenant $I$.
**2.** Soit $J \supseteq I$ un idéal de $A$. Montrer que $A/J$ est canoniquement isomorphe au quotient de $A/I$ par $J/I$.
**3.** On dit que $I$ est un idéal premier (resp. maximal) si $A/I$ est intègre (resp. un corps). Montrer que les idéaux premiers (resp. maximaux) de $A/I$ sont en bijection avec les idéaux premiers (resp. maximaux) de $A$ contenant $I$.
**4.** Déterminer les idéaux des anneaux suivants :

$$\mathbb{R}[X]/(X^2+X+1), \mathbb{R}[X]/(X^3-6X^2+11X-6), \mathbb{R}[X]/(X^4-1), \mathbb{R}[X]/(X^5).$$

Lesquels sont premiers ? Et maximaux ?
**5.** Combien l'anneau $\mathbb{R}[X]/(X^5(X^4-1))$ possède-t'il d'idéaux ? d'idéaux premiers ? d'idéaux maximaux ?

**Exercice 7 : Anneau de polynômes**
Soit $A$ un anneau commutatif unitaire. Montrer que si $A$ n'est pas un corps, alors $A[X]$ n'est pas principal.

**Exercice 8 : Un contre-exemple**
Soit $A$ un anneau.
**1.** Supposons $A$ intègre. Rappeler pourquoi, si $a$ et $b$ sont deux éléments de $A$ tels que $(a) = (b)$, alors il existe $u \in A^\times$ tel que $a = bu$.
Prenons maintenant $A = \mathbb{Q}[X,Y,Z]/(X - XYZ)$. On note $x$, $y$ et $z$ les classes de $X$, $Y$ et $Z$ dans $A$.
**2.** Vérifier que $A$ n'est pas intègre.

3. Montrer que $(x) = (xy)$.
4. Montrer qu'il n'existe pas d'élément $u \in A^\times$ tel que $xu = xy$.

**Exercice 9 : Exemples d'anneaux non factoriels**

1. Montrer que l'anneau $A = \mathbb{C}[X, Y, Z, T]/(XY - ZT)$ est intègre mais pas factoriel.
2. Montrer que l'anneau $B = \mathbb{Z}[\sqrt{10}]$ n'est pas factoriel, mais que tout élément non nul de $B$ s'écrit sous la forme $up_1 ... p_n$ avec $u \in B^\times$ et $p_i$ irréductible pour chaque $i$.
3. Plus généralement, est-il vrai que, si $p$ et $q$ sont deux nombres premiers distincts, alors l'anneau $\mathbb{Z}[\sqrt{pq}]$ n'est pas factoriel ?

**Exercice 10 : Un anneau principal non euclidien**

Soit $R$ un anneau euclidien qui n'est pas un corps.

1. Montrer que l'on peut trouver un élément non inversible $x$ de $R$ tel que la restriction à $R^\times \cup \{0\}$ de la projection canonique de $R$ sur $R/(x)$ soit surjective. On pourra choisir $x$ tel que $\phi(x)$ soit minimal parmi les éléments $x \notin R^\times$, où $\phi$ désigne le stathme d'une division euclidienne de $R$.

Soient $\alpha = \frac{1+i\sqrt{19}}{2}$ et $A = \mathbb{Z}[\alpha]$.

2. Déterminer $A^\times$.
3. Montrer que $A$ n'est pas euclidien.
4. Si $a, b \in A \setminus \{0\}$, montrer qu'il existe $q, r \in A$ tels que $r = 0$ ou $|r| < |b|$ et qui vérifient, soit $a = bq + r$, soit $2a = bq + r$.
5. Montrer que $A/(2)$ est un corps. On pourra utiliser l'exercice 5.
6. Montrer que $A$ est un anneau principal.

**Exercice 11 : Une équation diophantienne**

1. Montrer que $\mathbb{Z}[\frac{1+i\sqrt{11}}{2}]$ est un anneau euclidien. Quelles sont ses unités ?
2. Trouver tous les couples $(x, y) \in \mathbb{Z}^2$ tels que $y^2 + 11 = x^3$.

**Exercice 12 : Autres équations diophantiennes**

1. Trouver tous les couples d'entiers impairs $(x, y)$ tels que $y^2 + 28 = x^3$.
2. Trouver tous les couples $(x, y) \in \mathbb{C}[T]^2$ tels que $y^2 + T = x^3$.

**Exercice 13 : Sommes de deux carrés**

On cherche à déterminer $S = \{a^2 + b^2 | (a, b) \in \mathbb{Z}^2\}$.

1. (a) Quels sont les nombres premiers $p$ tels que $-1$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ ?
   (b) En déduire que, si $p$ est un nombre premier congru à 3 modulo 4 et $n$ un élément non nul de $S$, alors $v_p(n)$ est pair.

**2.** Rappeler pourquoi l'anneau $\mathbb{Z}[i]$ est principal. Quelles sont ses unités ?

**3.** (a) Montrer qu'un nombre premier $p$ est dans $S$ si, et seulement si, il n'est pas irréductible dans $\mathbb{Z}[i]$.

(b) En déduire qu'un nombre premier impair $p$ est dans $S$ si, et seulement si, il est congru à 1 modulo 4. On pourra utiliser le résultat de l'exercice 5.

**4.** Montrer qu'un entier naturel $n$ est dans $S$ si, et seulement si, pour tout premier $p$ congru à 3 modulo 4, la valuation $v_p(n)$ est paire.

**Exercice 14 : Entiers de la forme** $a^2 + ab + b^2$
S'inspirer de l'exercice précédent pour déterminer l'ensemble $T = \{a^2 + ab + b^2 \mid (a, b) \in \mathbb{Z}^2\}$.

**Exercice 15 : Les entiers de la forme** $a^2 - 2b^2$
On cherche à déterminer $S = \{a^2 - 2b^2 \mid (a, b) \in \mathbb{Z}^2\}$. Pour ce faire, on pose $A = \mathbb{Z}[\sqrt{2}]$.

**1.** Dans cette question, nous allons déterminer les nombres premiers $p$ tels que 2 est un carré modulo $p$.

(a) On suppose que $p \equiv 1 \mod 8$. Montrer que $-1$ est une puissance quatrième dans $\mathbb{Z}/p\mathbb{Z}$. En déduire que 2 est bien un carré modulo $p$.

Dans la suite de cette question, on supposera que $p$ est impair.

(b) Soit $P \in \mathbb{Z}/p\mathbb{Z}[X]$ un polynôme irréductible divisant $X^4 + 1$. Montrer que l'anneau $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ est un corps contenant $\mathbb{Z}/p\mathbb{Z}$ comme sous-corps et possédant une racine quatrième de $-1$. On notera $k = \mathbb{Z}/p\mathbb{Z}[X]/(P)$ et $\alpha$ une racine quatrième de $-1$ dans $k$.

(c) Vérifier que les éléments $x$ de $k$ vérifiant $x^2 = 2$ sont $\alpha + \alpha^{-1}$ et $-\alpha - \alpha^{-1}$.

(d) Montrer qu'un élément $x$ de $k$ est dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $x^p = x$.

(e) Déduire des deux questions précédentes que 2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $p$ est congru à 1 ou 7 modulo 8.

**2.** Montrer que l'anneau $A$ est euclidien.

**3.** Soit $n$ un entier. Montrer que, si $n \in S$, alors $-n \in S$.

**4.** Quels sont les nombres premiers impairs $p$ qui sont irréductibles dans $A$ ?

**5.** En déduire qu'un nombre premier impair $p$ est dans $S$ si, et seulement si, il est congru à 1 ou 7 modulo 8.

**6.** Caractériser $S$.

**7.** Soit $n \in S$. Montrer qu'il existe une infinité de couples $(a, b) \in \mathbb{Z}^2$ tels que $n = a^2 - 2b^2$.