# TD3 : Idéaux premiers et maximaux ; polynômes ; approximation

Diego Izquierdo

*Les exercices 1, 4, 5, 11 et 12 ont été traités pendant la séance de TD.*

**Exercice 2 : Vrai ou faux ? Le retour**

Soit $A$ un anneau.

**1.** Si $A$ est intègre, tout élément irréductible engendre un idéal premier.

> **Indications :** FAUX : Dans $A = \mathbb{C}[T^2, T^3]$, l'élément $T^2$ est irréductible mais n'engendre pas un idéal premier car $T^3 \cdot T^3 \in (T^2)$. L'assertion serait vraie si $A$ était factoriel.

**2.** Si $A$ est factoriel et si $a$ et $b$ sont deux éléments de $A$ premiers entre eux, alors il existe un isomorphisme $A/(ab) \cong A/(a) \times A/(b)$.

> **Indications :** FAUX : Il suffit de prendre $A = \mathbb{C}[X, Y]$, $a = X$ et $b = Y$. L'assertion serait vraie si $A$ était principal.

**3.** L'idéal (89) est premier dans $\mathbb{Z}[i]$.

> **Indications :** FAUX : On a $89 = 5^2 + 8^2 = (5 + 8i)(5 - 8i)$, donc 89 n'est pas irréductible dans $\mathbb{Z}[i]$.

**4.** Si $P \in \mathbb{C}[X, Y]$ est tel que $P(X, 0)$ et $P(0, Y)$ sont irréductibles, alors $P$ est irréductible.

> **Indications :** FAUX : Prendre $P(X, Y) = (X + 1)(Y + 1)$.

**5.** L'anneau des nombres décimaux est isomorphe à $\mathbb{Z}[X]/(10X - 1)$.

> **Indications :** VRAI : Soit $\mathbb{D}$ l'anneau des nombres dédimaux. Soit $\phi : \mathbb{Z}[X] \to \mathbb{D}, X \mapsto \frac{1}{10}$. C'est un morphisme surjectif. Soit $K$ son noyau. Il est évident que $K$ contient $(10X - 1)$. Réciproquement, soit $P \in K$. En écrivant la division euclidienne de $P$ par $10X - 1$, on voit qu'il existe $R \in \mathbb{Q}[X]$ tel que $P = (10X - 1)R$. Comme $ct(P) = ct(R)$, on a $R \in \mathbb{Z}[X]$. On en déduit que $K = (10X - 1)$, ce qui achève la preuve.

**6.** On a un isomorphisme d'anneaux $(\mathbb{R}[X]/(X^5(X^4 - 1)))^{\text{red}} \cong \mathbb{R}^3 \times \mathbb{C}$.

> **Indications :** VRAI : On a $\left(\mathbb{R}[X]/(X^5(X^4 - 1))\right)^{\text{red}} \cong \mathbb{R}[X]/\sqrt{(X^5(X^4 - 1))} \cong \mathbb{R}[X]/(X(X-1)(X+1)(X^2+1)) \cong \mathbb{R}[X]/(X) \times \mathbb{R}[X]/(X-1) \times \mathbb{R}[X]/(X+1) \times \mathbb{R}[X]/(X^2+1) \cong \mathbb{R}^3 \times \mathbb{C}$.

**Exercice 3 : Corps et idéaux**

Soit $A$ un anneau commutatif unitaire.

**1.** On suppose $A$ intègre et que $A$ possède un nombre fini d'idéaux. Montrer que $A$ est un corps.

> **Indications :** Soit $x \in A \setminus \{0\}$. Pour chaque entier naturel $n$, notons $I_n = (x^n)$. Par hypothèse, il existe $n < m$ tels que $I_n = I_m$. Comme $A$ est intègre, on en déduit qu'il existe $u \in A^\times$ tel que $x^n u = x^m$. On en déduit que $u = x^{m-n}$, et donc que $x \in A^\times$.

**2.** On suppose que $A$ possède un nombre fini d'idéaux. Montrer que tout idéal premier de $A$ est maximal.

> **Indications :** Soit $I$ un idéal premier de $A$. L'anneau $A/I$ possède un nombre fini d'idéaux et est intègre. Donc c'est un corps, et $I$ est maximal.

**3.** On suppose que tout idéal propre de $A$ est premier. Montrer que $A$ est un corps.

> **Indications :** Soit $x \in A \setminus \{0\}$. Si $(x^2) = A$, alors $x^2$ est inversible et donc $x$ l'est aussi. Supposons maintenant que $(x^2) \neq A$. Alors $(x^2)$ est un idéal premier, et donc $x \in (x^2)$ : il existe $u \in A$ tel que $x = ux^2$. Or $A$ est intègre, puisque l'idéal (0) est premier. On en déduit que $ux = 1$, c'est-à-dire que $x$ est inversible : absurde ! On en déduit que $x$ est inversible et que $A$ est un corps.

**Exercice 6 : Idéaux premiers d'un anneau de polynômes**

Soit $A$ un anneau principal de corps des fractions $K$. Nous allons caractériser les idéaux premiers et maximaux de $A[X]$.

**1.** Soit $I$ un idéal premier non nul de $A[X]$.

(a) Montrer que $I \cap A$ est un idéal maximal de $A$.

> **Indications :** Le morphisme $A/(A \cap I) \to A[X]/I$ est injectif. Comme $I$ est premier, on en déduit que $A/(A \cap I)$ est intègre, autrement dit que $A \cap I$ est un idéal premier de $A$. L'anneau $A$ étant principal, c'est même un idéal maximal.

(b) On suppose $I \cap A = 0$.

(i) Soit $J$ l'idéal de $K[X]$ engendré par $I$. Montrer que $I = J \cap A[X]$.

> **Indications :** L'inclusion $I \subseteq J \cap A[X]$ est évidente. Soit $P \in J \cap A[X]$ non nul. Il existe $a \in A \setminus \{0\}$ tel que $aP \in I$. Or $a \notin I$ car $I \cap A = 0$. Donc, comme $I$ est premier, on déduit que $P \in I$.

(ii) Montrer que $I$ est principal, engendré par un polynôme non constant, irréductible et primitif.

> **Indications :** L'anneau $K[X]$ est principal, donc il existe $P \in K[X]$ tel que $J = (P)$. Soit $c$ le contenu de $P$. On a alors $I = A[X] \cap (c^{-1}P)K[X] = (c^{-1}P)A[X]$ car $c^{-1}P$ est primitif. On en déduit que $I$ est principal, engendré par le polynôme $c^{-1}P$. De plus, comme $I$ est premier, $c^{-1}P$ est irréductible et comme $I \cap A = 0$, $c^{-1}P$ est non constant.

(c) On suppose que $I \cap A$ est non nul, et on pose $k = A/(I \cap A)$. Montrer que soit $I$ est engendré par $I \cap A$, soit $I$ est engendré par $I \cap A$ et par un polynôme $P \in A[X]$ dont l'image dans $k[X]$ est irréductible.

> **Indications :** L'anneau $A$ étant principal, il existe $a \in A$ non nul tel que $A \cap I = (a)$. On remarque que l'idéal $I$ contient $aA[X]$. Comme $A[X]/aA[X] = k[X]$ est principal, il existe $P \in k[X]$ irréductible ou nul tel que $I/J = Pk[X]$. On en déduit que $I = aA[X]$ si $P = 0$ et que $I = (a, \tilde{P})$ où $\tilde{P} \in A[X]$ est un relèvement de $P$ si $P \neq 0$.

(d) Déduire de ce qui précède que les idéaux premiers de $A[X]$ sont : (0) ; les idéaux principaux engendrés par un polynôme non constant, irréductible et primitif ; les idéaux engendrés par un idéal maximal de

$A$ ; les idéaux engendrés par un idéal maximal $\mathfrak{m}$ de $A$ et un polynôme de $A[X]$ dont la réduction modulo $\mathfrak{m}$ est irréductible. Lesquels sont maximaux ?

> **Indications :** La liste des idéaux premiers est immédiate à partir des questions précédentes. Les idéaux engendrés par un idéal maximal de $A$ et $(0)$ ne sont jamais maximaux, alors que les idéaux engendrés par un idéal maximal $\mathfrak{m}$ de $A$ et un polynôme de $A[X]$ dont la réduction modulo $\mathfrak{m}$ est irréductible sont toujours maximaux. Les idéaux principaux engendrés par un polynôme non constant, irréductible et primitif peuvent être maximaux ou non.

**2.** Quels sont les idéaux premiers (resp. maximaux) de $\mathbb{C}[X,Y]$ ?

> **Indications :** Les idéaux premiers sont $(0)$, les idéaux principaux engendrés par des éléments irréductibles, et les idéaux $(X-a, Y-b)$ avec $a, b \in \mathbb{C}$. Ces derniers sont les idéaux maximaux.

**3.** Quels sont les idéaux premiers (resp. maximaux) de $\mathbb{Z}[X]$ ?

> **Indications :** Les idéaux premiers sont $(0)$, les idéaux principaux engendrés par des éléments irréductibles de $\mathbb{Z}[X]$, et les idéaux $(p, P)$ où $p \in \mathbb{Z}$ est un nombre premier et $P \in \mathbb{Z}[X]$ un polynôme dont la réduction modulo $p$ est irréductible. Ces derniers sont les idéaux maximaux.

**4.** Soit $\alpha$ un entier algébrique, c'est-à-dire un élément de $\mathbb{C}$ racine d'un polynôme unitaire irréductible à coefficients dans $\mathbb{Z}$. Montrer que tout idéal premier non nul de $\mathbb{Z}[\alpha]$ est maximal.

> **Indications :** Soit $P$ un polynôme unitaire irréductible à coefficients dans $\mathbb{Z}$ annulant $\alpha$. On a alors un isomorphisme $\mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/(P)$. Donc les idéaux premiers non nuls de $\mathbb{Z}[\alpha]$ correspondent aux idéaux premiers de $\mathbb{Z}[X]$ contenant strictement $(P)$. Ce sont donc les $(p, P)$ pour $p$ un nombre premier tel que la réduction de $P$ modulo $p$ est irréductible : ils sont bien maximaux.

**Exercice 7 : Idéaux premiers de $\mathcal{C}([0,1], \mathbb{R})$**

**1.** Soient $A$ un anneau et $I$ un idéal de $A$. Notons $J$ l'intersection des idéaux premiers de $A$ contenant $I$. Le but de cette question est de montrer que $\sqrt{I} = J$.

(a) Montrer que $\sqrt{I}$ est contenu dans $J$.

> **Indications :** Soit $x \in \sqrt{I}$. Il existe $n \in \mathbb{N} \setminus \{0\}$ tel que $x^n \in I$. Soit $\mathfrak{p}$ un idéal premier de $A$ contenant $I$. Alors $x^n \in \mathfrak{p}$, et donc $x \in \mathfrak{p}$. Cela étant vrai pour tout $\mathfrak{p}$, on en déduit que $x \in J$, et donc que $\sqrt{I} \subseteq J$.

(b) Réciproquement, soit $a \in A \setminus \sqrt{I}$, et considérons $\mathcal{E}$ la famille constituée des idéaux qui contiennent $I$ mais qui ne contiennent aucune puissance de $a$. Montrer que $\mathcal{E}$ possède un élément maximal (pour l'inclusion), qui est un idéal premier de $A$. En déduire que $a \notin J$.

**Indications :** La famille $\mathcal{E}$ est non vide puisqu'elle contient $I$. De plus, l'inclusion est un ordre inductif sur $\mathcal{E}$ : en effet, si $(I_i)$ est une famille totalement ordonnée d'éléments de $\mathcal{E}$, alors $\bigcup_i I_i$ est dans $\mathcal{E}$. Le lemme de Zorn permet donc de conclure que $\mathcal{E}$ possède un élément maximal $I_0$. Supposons que $I_0$ ne soit pas premier. Soient $b, c \in A$ tels que $bc \in I_0$ mais $b \notin I_0$ et $c \notin I_0$. Alors il existe $n$ et $m$ des entiers naturels tels que $a^n \in I_0 + (b)$ et $a^m \in I_0 + (c)$. On en déduit que $a^{n+m} \in I_0$ : absurde ! Donc $I_0$ est premier. De plus, $a \notin I_0$ et $I \subseteq I_0$. Donc $a \notin J$.

(c) Conclure.

**Indications :** On a $\sqrt{I} = J$.

Soit $\mathcal{C}$ l'anneau des fonctions continues de $[0,1]$ dans $\mathbb{R}$.

**2.** Quels sont les idéaux maximaux de $\mathcal{C}$ ? Sont-ils principaux ?

**Indications :** Notons $M_x = \{f \in \mathcal{C} \mid f(x) = 0\}$ pour tout $x \in [0,1]$. C'est un idéal de $\mathcal{C}$. Et le morphisme d'anneaux $\mathcal{C} \to \mathbb{R}, f \mapsto f(x)$ est surjectif, de noyau $M_x$ ; donc $M_x$ est maximal. Réciproquement, soit $M$ un idéal maximal de $\mathcal{C}$. Supposons $\bigcap_{f \in M} \{x \in X | f(x) = 0\} = \varnothing$. Dit autrement, les $f^{-1}(\mathbb{R} \setminus \{0\})$ pour $f \in M$ sont des ouverts qui recouvrent $[0,1]$. Par compacité on extrait une famille finie $f_1, \ldots, f_n \in M$ vérifiant

$$f_1^{-1}(\mathbb{R} \setminus \{0\}) \cup f_2^{-1}(\mathbb{R} \setminus \{0\}) \cup \cdots \cup f_n^{-1}(\mathbb{R} \setminus \{0\}) = [0,1].$$

De ce fait, la fonction $\sum_i f_i^2$ est un élément de $M$ qui ne s'annule nulle part et est donc inversible dans $\mathcal{C}$. Mais alors, $M$ est égal à $\mathcal{C}$, ce qui est absurde. En conclusion, il existe $x \in [0,1]$ tel que l'on ait $M \subseteq M_x$ ; et on a égalité par maximalité de $M$.

**3.** Soit $I = \{f : [0,1] \to \mathbb{R} \mid \forall m \in \mathbb{N}, \lim_{x \to 0} \frac{f(x)}{x^m} = 0\}$. Montrer que $I = \sqrt{I}$ (on dit que $I$ est un idéal radical). L'idéal $I$ est-il premier ?

**Indications :** Soient $f \in \mathcal{C}$ et $n \in \mathbb{N} \setminus \{0\}$ tels que $f^n \in I$. Alors $\lim_{x \to 0} \left(\frac{f(x)}{x^m}\right)^n = 0$ pour tout $m$. Donc $f \in I$ et $I = \sqrt{I}$. L'idéal $I$ n'est pas premier, puisqu'il est possible de construire $f, g \in \mathcal{C}$ telles que $fg = 0$ et $\frac{f(x)}{x}$ et $\frac{g(x)}{x}$ n'ont pas de limite en 0 (faire un dessin !).

**4.** En déduire que $\mathcal{C}$ possède des idéaux premiers non maximaux.

**Indications :** Supposons que tous les idéaux premiers de $A$ soient maximaux. Alors d'après la question 1., $I$ serait une intersection d'idéaux maximaux. Mais le seul idéal maximal contenant $I$ est $M_0$, et $I \neq M_0$. Absurde !

## Exercice 8 : Points en géométrie algébrique

**1.** On considère les anneaux :

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

Déterminer les morphismes de $\mathbb{R}$-algèbres de ces anneaux à valeurs dans $\mathbb{R}$ (resp. $\mathbb{C}$).

**Indications :** Il n'y a pas de morphismes de $\mathbb{C}[X]$ à valeurs dans $\mathbb{R}$ car $\mathbb{R}$ ne possède pas d'élément de carré -1. Les morphismes de $\mathbb{C}[X]$ à valeurs dans $\mathbb{C}$ sont donnés par l'évaluation en un certain $x \in \mathbb{C}$. Il n'y a pas de morphismes de $\mathbb{R}[X]/(X^2+X+1)$ à valeurs dans $\mathbb{R}$. Les morphismes de $\mathbb{R}[X]/(X^2+X+1)$ à valeurs dans $\mathbb{C}$ sont l'évaluation en $j$ et l'évaluation en $j^2$. Les morphismes de $\mathbb{R}[X]/(X^3-6X^2+11X-6)$ à valeurs dans $\mathbb{R}$ (resp. $\mathbb{C}$) sont l'évaluation en 1, l'évaluation en 2 et l'évaluation en 3 (resp. l'évaluation en 1, l'évaluation en 2 et l'évaluation en 3). Les morphismes de $\mathbb{R}[X]/(X^4-1)$ à valeurs dans $\mathbb{R}$ (resp. $\mathbb{C}$) sont l'évaluation en 1 et l'évaluation en -1 (resp. l'évaluation en 1, l'évaluation en -1, l'évaluation en $i$ et l'évaluation en $-i$).

**2.** On considère l'anneau $\mathbb{R}[X]/(X^5)$. Déterminer les morphismes de $\mathbb{R}$-algèbres de cet anneau à valeurs dans $\mathbb{R}$ (resp. $\mathbb{C}$, resp. $\mathbb{R}[\varepsilon]$).

**Indications :** Le seul morphisme de $\mathbb{R}[X]/(X^5)$ dans $\mathbb{R}$ (resp. $\mathbb{C}$) est celui qui envoie $X$ sur 0. Les morphismes de $\mathbb{R}[X]/(X^5)$ dans $\mathbb{R}[\varepsilon]$ sont ceux qui envoient $X$ sur $a\epsilon$ pour un certain $a \in \mathbb{R}$.

**3.** (a) Soit $k$ un corps. Montrer qu'il existe une $k$-algèbre $A$ définissant une "variété" $X$ telle que, pour chaque $k$-algèbre $B$, on ait une bijection $X(B) \cong B^\times$. Calculer $X(k[\varepsilon])$.

**Indications :** On prend $A = k[X,Y]/(XY-1)$. On a alors $X(k[\varepsilon]) = k[\epsilon]^\times = \{a+b\epsilon | a \in k^\times, b \in k\}$.

(b) Même question pour $X(B) \cong GL_n(B)$.

**Indications :** On prend $A = k[(X_{ij})_{1\leq i,j\leq n}, Y]/(\det(X_{ij}Y-1)$. On a alors $X(k[\varepsilon]) = GL_n(k[\epsilon]) = \{A+B\epsilon | A \in GL_n(k), B \in \mathcal{M}_n(k)\}$.

(c) Même question pour $X(B) \cong \mu_n(B)$ où $\mu_n(B)$ désigne l'ensemble des racines $n$-ièmes de l'unité dans $B$.

**Indications :** On prend $A = k[X]/(X^n-1)$. On a alors $X(k[\varepsilon]) = \mu_n(k[\epsilon])$ est $\mu_n(k)$ si $\mathrm{car}(k) \nmid n$, $\{a+b\epsilon | a \in \mu_n(k), b \in k\}$ si $\mathrm{car}(k)|n$.

**Exercice 9 : L'anneau $\hat{\mathbb{Z}}$**

Pour $n$ et $m$ deux entiers naturels non nuls tels que $n|m$, on note $\pi_{m,n}$ la projection naturelle $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. On pose :

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \{(x_n)_n \in \prod_n \mathbb{Z}/n\mathbb{Z} \mid \forall (n,m) \in (\mathbb{N}^*)^2, n|m \Rightarrow \pi_{m,n}(x_m) = x_n\}.$$

En notant $\mathcal{P}$ l'ensemble des nombres premiers, montrer que $\hat{\mathbb{Z}} \cong \prod_{p\in\mathcal{P}} \mathbb{Z}_p$.

**Indications :** On définit $\varphi : \hat{\mathbb{Z}} \to \prod_p \mathbb{Z}_p, (x_n)_n \mapsto ((x_{p^m})_m)_p$. Montrons que c'est un isomorphisme d'anneaux. Soit $x = (x_n) \in \mathrm{Ker}(\varphi)$. Pour tout premier $p$, pour tout $m > 0$, on a $x_{p^m} = 0$. Soit $n$ un entier naturel quelconque, et écrivons sa décomposition en produit de facteurs premiers : $n = \prod_{i=1}^r p_i^{m_i}$. L'image de $x_n$ par le morphisme $\mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^r \mathbb{Z}/p_i^{m_i}\mathbb{Z}$ est $(x_{p_1^{m_1}}, ..., x_{p_r^{m_r}}) = 0$. Mais ce morphisme est un isomorphisme d'après le lemme chinois. Donc $x_n = 0$ et $\varphi$ est injectif.
Soit maintenant $y = ((y_{p,m})_m)_p \in \prod_p \mathbb{Z}_p$. Soit $n \in \mathbb{N}$ non nul et écrivons sa décomposition en produit de facteurs premiers : $n = \prod_{i=1}^r p_i^{m_i}$. Soit $x_n$ l'image réciproque de $(y_{p_1,m_1}, ..., y_{p_r,m_r})$ par l'isomorphisme $\mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^r \mathbb{Z}/p_i^{m_i}\mathbb{Z}$ donné par le lemme chinois. On vérifie alors aisément que la suite $(x_n)$ est dans $\hat{\mathbb{Z}}$ et que $\varphi((x_n)) = y$. On en déduit que $\varphi$ est surjectif.

## Exercice 10 : Racines de l'unité dans $\mathbb{Z}_p$

Soit $p$ un nombre premier impair. Sans utiliser le lemme de Hensel, montrer que le groupe des racines de l'unité dans $\mathbb{Z}_p$ est cyclique d'ordre $p-1$. Après avoir remarqué que $\mathbb{Z}_p$ est intègre, en déduire que, si $p$ et $l$ sont deux nombres premiers impairs distincts, alors les corps des fractions de $\mathbb{Z}_p$ et $\mathbb{Z}_l$ ne sont pas isomorphes.

**Indications :** L'anneau $\mathbb{Z}_p$ étant intègre, il possède au plus $m$ racines $m$-ièmes de l'unité pour chaque $m$. Pour tout entier naturel $n$, on a un isomorphisme :

$$f_n : \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z} \to (\mathbb{Z}/p^n\mathbb{Z})^\times,$$

qui envoie $(0,1)$ sur $1+p$. Par conséquent, les racines de l'unité dans $\mathbb{Z}_p$ sont chacune d'ordre divisant $(p-1)p^s$ pour un certain $s$. Soit $x = (x_n)$ une racine $p$-ième de l'unité dans $\mathbb{Z}_p$. Alors pour chaque $n > 0$, il existe $k_n \in \mathbb{N}$ tel que $x_n = (1+p)^{k_n}$ et $p^{n-2}|k_n$. De plus, comme $x \in \mathbb{Z}_p$, on a $k_{n+1} \equiv k_n \mod p^{n-1}$, donc $p^{n-1}|k_n$, et $x_n = 1$. On en déduit que la seule racine $p$-ième de l'unité dans $\mathbb{Z}_p$ est 1, et donc que toute racine de l'unité dans $\mathbb{Z}_p$ est d'ordre divisant $p-1$.
Montrons maintenant qu'il existe une racine primitive $p-1$-ième de l'unité dans $\mathbb{Z}_p$. Soit $x_1$ un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. On sait que, pour tout entier naturel $n$, il existe un unique $x_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ d'ordre $p-1$ relevant $x_1$. On a alors $x_{n+1} \equiv x_n \mod p^n$ pour tout $n$, et donc $(x_n) \in \mathbb{Z}_p$ est une racine de l'unité d'ordre exactement $p-1$. Cela prouve que le groupe des racines de l'unité dans $\mathbb{Z}_p$ est cyclique d'ordre $p-1$.
Soient $p$ et $l$ deux nombres premiers impairs. Si les corps des fractions de $\mathbb{Z}_p$ et $\mathbb{Z}_l$ étaient isomorphes, ils auraient le même nombre de racines de l'unité. Or on peut vérifier que toute racine de l'unité du corps des fractions de $\mathbb{Z}_p$ (resp. $\mathbb{Z}_l$) est dans $\mathbb{Z}_p$ (resp. $\mathbb{Z}_l$). Donc $p-1 = l-1$, c'est-à-dire $p = l$.

## Exercice 13 : Approximations plus subtiles

**1.** Montrer que 28 est un cube dans $\mathbb{Z}_3$.

**Indications :** Soit $n \geq 2$ tel qu'il existe $x \in \mathbb{Z}$ tel que $x^3 \equiv 28 \mod 3^n$. Cherchons $y \in \mathbb{Z}$ tel que $y^3 \equiv 28 \mod 3^{n+1}$. Pour ce faire, cherchons $y$ sous la forme $x + 3^{n-1}t$. On calcule $y^3 = (x + 3^{n-1}t)^3 \equiv x^3 + 3^n x^2 t \mod 3^{n+1}$. En choisissant $t \in \mathbb{Z}$ tel que $x^2 t \equiv \frac{28-x^3}{3^n} \mod 3$, on obtient $y^3 \equiv x^3 + 28 - x^3 \equiv 28 \mod 3^{n+1}$. On a donc trouvé $y \in \mathbb{Z}$ tel que $y^3 \equiv 28 \mod 3^{n+1}$. Comme $1^3 \equiv 28 \mod 9$, une récurrence simple montre que 28 est un cube dans $\mathbb{Z}/3^n\mathbb{Z}$ pour tout $n$. Donc 28 est un cube dans $\mathbb{Z}_3$.

**2.** Montrer qu'il existe $f(T) \in \mathbb{Q}[[T]]$ tel que $f(T)^5 + Tf(T) + T^3 = 0$.

**Indications :** Soit $n \geq 3$ tel qu'il existe $P \in \mathbb{Q}[T]$ tel que $P(T)^5 + TP(T) + T^3 \equiv 0 \mod T^n$ et $P \equiv 0 \mod T^2$. Écrivons $P(T)^5 + TP(T) + T^3 = T^n S$, et cherchons $Q \in \mathbb{Q}[T]$ tel que $Q(T)^5 + TQ(T) + T^3 \equiv 0 \mod T^{n+1}$ et $Q \equiv P \mod T^{n-1}$. Pour ce faire, cherchons $Q$ sous la forme $P + T^{n-1}R$. On calcule $Q^5 + TQ + T^3 \equiv P^5 + TP + T^n R + T^3 \equiv T^n(S + R) \mod T^{n+1}$. On choisit $R = -S$, de sorte que $Q^5 + TQ + T^3 \equiv 0 \mod T^{n+1}$. Comme $0^5 + T0 + T^3 \equiv 0 \mod T^3$, on construit par récurrence une suite $(P_n)_{n\geq 3}$ à valeurs dans $\mathbb{Q}[T]$ telle que $P_n(T)^5 + TP_n(T) + T^3 \equiv 0 \mod T^n$, $P_3 = 0$ et $P_{n+1} \equiv P_n \mod T^{n-1}$, ce qui achève la preuve.

## Exercice 14 : Approximation dans $\mathbb{Z}[i]$

Existe-t'il $z \in \mathbb{Z}[i]/(51^{100})$ tel que $z^2 = 2$ ?

**Indications :** On a :

$$\begin{aligned}\mathbb{Z}[i]/(51) &\cong \mathbb{Z}[i]/(3) \times \mathbb{Z}[i]/(17) \\ &\cong \mathbb{Z}/3\mathbb{Z}[X]/(X^2+1) \times \mathbb{Z}/17\mathbb{Z}[X]/(X^2+1) \\ &\cong \mathbb{Z}/3\mathbb{Z}[X]/(X^2+1) \times (\mathbb{Z}/17\mathbb{Z})^2\end{aligned}$$

Or $\mathbb{Z}/3\mathbb{Z}[X]/(X^2+1)$ et $\mathbb{Z}/17\mathbb{Z}$ sont des corps de cardinaux respectifs 9 et 17. Leurs groupes multiplicatifs sont donc isomorphes à $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{Z}/16\mathbb{Z}$. L'isomorphisme $\mathbb{Z}/3\mathbb{Z}[X]/(X^2+1)^\times \cong \mathbb{Z}/8\mathbb{Z}$ envoie 2 sur un élément d'ordre 2, donc sur 4. L'isomorphisme $\mathbb{Z}/17\mathbb{Z}^\times \cong \mathbb{Z}/16\mathbb{Z}$ envoie 2 sur un élément d'ordre 8, donc sur $2, 6, 10$ ou 14. On en déduit que 2 possède une racine carrée dans $\mathbb{Z}[i]/(51)$. Le lemme de Hensel permet de conlure que 2 possède une racine carrée dans $\mathbb{Z}[i]/(51^{100})$.

## Exercice 15 : Partiel 2013

Soit $n \geq 1$ un entier. Montrer que :

**1.** Il existe $u_n \in \mathbb{R}[X]$ tel que $u_n \equiv X \mod (X^2+1)$ et $u_n^2 + 1 \equiv 0 \mod (X^2+1)^n$.

**Indications :** Soit $f = Y^2 + 1 \in \mathbb{R}[X][Y]$. On a $f(X) \equiv 0 \mod (X^2+1)$. De plus, $f'(X) \equiv 2X \mod (X^2+1)$, donc $f'(X)$ est inversible dans $\mathbb{R}[X]/(X^2+1)$, d'inverse $-\frac{X}{2}$. Le lemme de Hensel montre alors qu'il existe $u_n \in \mathbb{R}[X]$ tel que $u_n \equiv X \mod (X^2+1)$ et $u_n^2 + 1 \equiv 0 \mod (X^2+1)^n$.

**2.** La classe de $u_n$ modulo $(X^2+1)^n$ est unique. Donner une formule pour la classe de $u_{n+1}$ modulo $(X^2+1)^{n+1}$ en fonction de $u_n$.

**Indications :** On raisonne par l'absurde. Soit $n$ le plus petit entier tel qu'il existe $u_n$ et $u'_n$ tels que $(X^2+1)^n \nmid u_n - u'_n$, $u_n \equiv X \mod (X^2+1)$, $u'_n \equiv X \mod (X^2+1)$, $u_n^2 + 1 \equiv 0 \mod (X^2+1)^n$ et $u_n'^2 + 1 \equiv 0 \mod (X^2+1)^n$. Il est évident que $n > 1$. On a alors $u_n \equiv u'_n \mod (X^2+1)^{n-1}$. L'unicité dans le lemme de Hensel montre donc que $u_n \equiv u'_n \mod (X^2+1)^n$ : absurde. Cela achève la preuve de l'unicité. D'après la preuve du lemme de Hensel, on a $u_{n+1} = u_n + \frac{X}{2}(u_n^2+1) \mod (X^2+1)^{n+1}$.

**3.** Les formules :

$$\alpha_n : \mathbb{C}[Y] \to \mathbb{R}[X]/(X^2+1)^n, a+bi \mapsto a+bu_n, Y \mapsto X - u_n,$$

définissent un morphisme surjectif de $\mathbb{R}$-algèbres.

**Indications :** On vérifie aisément que $\alpha_n$ est un morphisme de $\mathbb{R}$-algèbres. Reste à vérifier la surjectivité. Pour ce faire, il suffit de voir que $X \in \mathrm{Im}(\alpha_n)$ car $\mathbb{R}[X]/(X^2+1)^n$ est engendré par $X$ comme $\mathbb{R}$-algèbre. Mais $X = \alpha_n(Y+i)$.

**4.** $\alpha_n$ définit un isomorphisme de $\mathbb{R}$-algèbres :

$$\mathbb{C}[Y]/(Y^n) \to \mathbb{R}[X]/(X^2+1)^n.$$

**Indications :** Par une récurrence simple et en utilisant la question 2., on voit que $u_n(i) = i$. Par conséquent, $i$ est racine de $(X-u_n)^n$ de multiplicité au moins $n$. Il en est donc de même de $-i$, et $(X^2+1)^n$ divise $(X-u_n)^n$. On en déduit que $\alpha_n(Y^n) = 0$, c'est-à-dire que $Y^n \in \mathrm{Ker}(\alpha_n)$. Par conséquent, $\alpha_n$ induit une surjection $\mathbb{C}[Y]/(Y^n) \to \mathbb{R}[X]/(X^2+1)^n$. Mais comme espaces vectoriels, $\mathbb{C}[Y]/(Y^n)$ et $\mathbb{R}[X]/(X^2+1)^n$ sont de même dimension finie. Donc $\alpha_n$ définit un isomorphisme de $\mathbb{R}$-algèbres :

$$\mathbb{C}[Y]/(Y^n) \to \mathbb{R}[X]/(X^2+1)^n.$$

**5.** Pour tout polynôme non constant $f \in \mathbb{R}[X]$, il existe un isomorphisme :

$$\mathbb{R}[X]/(f) \cong \prod_{j=1}^{N} \mathbb{R}[X]/(X^{a_j}) \times \prod_{k=1}^{M} \mathbb{C}[Y]/(Y^{b_k}).$$

**Indications :** On écrit $f = \lambda \prod_{j=1}^{N}(X-x_j)^{a_j} \prod_{k=1}^{M}(X^2+y_kX+z_k)^{b_k}$, où $\lambda, x_j, y_k, z_k \in \mathbb{R}$ et $X^2+y_kX+z_k$ est irréductible dans $\mathbb{R}[X]$ pour tout $k$. On suppose que les $x_j$ (resp. les $X^2+y_kX+z_k$) sont deux à deux distincts. On utilise le lemme chinois :

$$\mathbb{R}[X]/(f) \cong \prod_{j=1}^{N} \mathbb{R}[X]/(X-x_j)^{a_j} \times \prod_{k=1}^{M} \mathbb{R}[X]/(X^2+y_kX+z_k)^{b_k}.$$

On remarque maintenant que $\mathbb{R}[X]/(X-x_j)^{a_j} \cong \mathbb{R}[X]/(X^{a_j}), X \mapsto X+x_j$ et :

$$\mathbb{R}[X]/(X^2+y_kX+z_k)^{b_k} = \mathbb{R}[X]/((X+\frac{y_k}{2})^2+z_k-\frac{y_k^2}{4})^{b_k} \cong \mathbb{R}[X]/(X^2+1)^{b_k},$$
$$X \mapsto \sqrt{z_k-\frac{y_k^2}{4}}X-\frac{y_k}{2}.$$

A l'aide de la question précédente, on obtient :

$$\mathbb{R}[X]/(f) \cong \prod_{j=1}^{N} \mathbb{R}[X]/(X^{a_j}) \times \prod_{k=1}^{M} \mathbb{C}[Y]/(Y^{b_k}).$$

**Exercice 16 : Anneau des séries formelles**

**1.** Soit $k$ un corps. Montrer que $k[[T]]$ est un anneau euclidien possédant exactement un idéal premier.

**Indications :** Un stathme possible est donné par $\phi : k[[T]] \to \mathbb{N}, \sum a_iX^i \mapsto \min\{i|a_i \neq 0\}+1$.

**2.** Exhiber un élément de $\mathbb{Z}[X]$ qui n'est pas irréductible, mais qui est irréductible dans $\mathbb{Z}[[X]]$.

**Indications :** Choisissons $P = X(X+1)$. Il est clair que $P$ n'est pas irréductible dans $\mathbb{Z}[X]$. Par contre, $1+X$ est inversible dans $\mathbb{Z}[[X]]$ et $X$ est irréductible dans $\mathbb{Z}[[X]]$ puisque $\mathbb{Z}[[X]]/(X) \cong \mathbb{Z}$ est intègre, donc $P$ est irréductible dans $\mathbb{Z}[[X]]$.

**3.** Exhiber un élément irréductible de $\mathbb{Z}[X]$, qui n'est pas irréductible dans $\mathbb{Z}[[X]]$.

**Indications :** Considérons $P = 6+X$. Il est évident que $P$ est irréductible dans $\mathbb{Z}[X]$. Montrons par récurrence que pour tout $n \in \mathbb{N}\setminus\{0\}$ il existe $Q_n$ et $R_n$ dans $\mathbb{Z}[[X]]$ tels que $Q_1 = 2$, $R_1 = 3$, $Q_{n+1} \equiv Q_n \mod X^n$, $R_{n+1} \equiv R_n \mod X^n$ et $Q_nR_n \equiv P \mod X^n$. Pour $n = 1$, l'assertion est évidente. Supposons la propriété prouvée pour un certain entier naturel $n$. Soit $a \in \mathbb{Z}$ tel que $Q_nR_n - P \equiv aX^n \mod X^{n+1}$. Soient $Q_{n+1} = Q_n - aX^n$ et $R_{n+1} = R_n + aX^n$. On a alors :

$$Q_{n+1}R_{n+1} \equiv Q_nR_n - aX^nR_n + aX^nQ_n \equiv P + aX^n - 3aX^n + 2aX^n \equiv P \mod X^{n+1},$$

ce qui achève la récurrence. Soient $Q$ et $R$ les uniques éléments de $\mathbb{Z}[[X]]$ tels que $Q \equiv Q_n \mod X^n$ et $R \equiv R_n \mod X^n$ pour tout $n$. On a alors $QR = P$. Mais $Q$ et $R$ ne sont pas inversibles dans $\mathbb{Z}[[X]]$, donc $P$ n'est pas irréductible.

**4.** Les questions concernant la factorialité de $A[[T]]$ sont difficiles. Pierre Samuel a montré en 1960 les faits suivants :

- Si $A$ est un anneau principal et $n$ un entier naturel, alors l'anneau $A[[T_1, T_2, ..., T_n]]$ est factoriel ;
- Il existe des anneaux factoriels $A$ tels que $A[[T]]$ n'est pas factoriel : par exemple, $A = \mathbb{Z}/2\mathbb{Z}[X, Y, Z]/(Z^2 - X^3 - Y^7)$.

**Exercice 17 (difficile [1]) : Produit de deux sous-anneaux**
Soient $A$ un anneau et $I$ un idéal. Montrer que, si $A/I$ est un produit non trivial de deux sous-anneaux, il en est de même pour $\hat{A} = \varprojlim_n A/I^n$.

> **Indications :** Soit $n \in \mathbb{N} \setminus \{0\}$. Soit $e \in A$ tel que $e^2 \equiv e \mod I^n$. On note $f = e^2 - e$ et on calcule alors $(3e^2 - 2e^3)^2 - 3e^2 + 2e^3 \equiv -8e^3 - 12e^2 f + 11e^2 + 20ef - 3e - 3f \equiv 0 \mod I^{n+1}$. De plus, $3e^2 - 2e^3 \equiv 3e - 2e \equiv e \mod I^n$. On a donc construit $e' \in A$ tel que $e' \equiv e \mod I^n$ et $e'^2 \equiv e' \mod I^{n+1}$.
> Soit maintenant $e_1 \in A$ non congru à 0 ou 1 modulo $I$ tel que $e^2 \equiv e \mod I$. Par récurrence, on construit $e_n \in A$ tel que $e_n^2 \equiv e_n \mod I^n$ et $e_{n+1} \equiv e_n \mod I^n$. On en déduit que l'élément $(e_n)$ de $\varprojlim_n A/I^n$ est un idempotent différent de 0 et 1, ce qui achève la preuve.

**Exercice 18 : Lemme de Hensel bis**

**1.** Soit $p$ un nombre premier. Soient $f_1, ..., f_n$ des éléments de $\mathbb{Z}[X_1, ..., X_m]$. Considérons le système d'équations (S) :

$$\begin{cases} f_1(x_1, ..., x_m) &= 0 \\ f_2(x_1, ..., x_m) &= 0 \\ & ... \\ f_n(x_1, ..., x_m) &= 0 \end{cases}$$

Soit $x \in (\mathbb{Z}/p\mathbb{Z})^m$ une solution de (S). On suppose que le rang de la matrice jacobienne $J(x) = \left(\frac{\partial f_i}{\partial x_j}(x)\right)_{i,j} \in \mathcal{M}_{n,m}(\mathbb{Z}/p\mathbb{Z})$ est égal à $n$. Montrer que le système (S) possède une unique solution dans $\mathbb{Z}_p$ qui relève $x$.

1. Pour une version plus facile de l'exercice, on pourra aller voir l'exercice I.3.11 dans le polycopié.

**Indications :** Soit $k \in \mathbb{N} \setminus \{0\}$ tel qu'il existe une solution $x^{(k)}$ de (S) modulo $p^k$. On écrit $\begin{pmatrix} f_1(x^{(k)}) \\ f_2(x^{(k)}) \\ \vdots \\ f_n(x^{(k)}) \end{pmatrix} = p^k w^{(k)}$. On cherche à trouver $x^{(k+1)}$ solution de (S) modulo $p^{k+1}$, congrue à $x^{(k)}$ modulo $p^k$. Pour ce faire, on cherche $x^{(k+1)}$ sous la forme $x^{(k)} + p^k v^{(k)}$ avec $v^{(k)} \in \mathbb{Z}^m$. On a :

$$\begin{pmatrix} f_1(x^{(k+1)}) \\ f_2(x^{(k+1)}) \\ \vdots \\ f_n(x^{(k+1)}) \end{pmatrix} \equiv \begin{pmatrix} f_1(x^{(k)}) \\ f_2(x^{(k)}) \\ \vdots \\ f_n(x^{(k)}) \end{pmatrix} + p^k J(x) v^{(k)} \mod p^{k+1}.$$

Comme $J(x)$ est de rang $n$, on peut choisir $v_k$ tel que $J(x)v^{(k)} \equiv -w^{(k)} \mod p$. Avec ce choix, on voit que $x^{(k+1)} = x^{(k)} + p^k v^{(k)}$ est l'unique solution de (S) modulo $p^{k+1}$, congrue à $x^{(k)}$ modulo $p^k$. Une récurrence simple permet de conclure.

**2.** Trouver tous les nombres premiers $p$ tels que l'équation $x^2 + 1 = 3y^2$ a des solutions dans $\mathbb{Z}_p$.

**Indications :** Supposons d'abord $p > 3$. Comme $|\{x^2+1 | x \in \mathbb{Z}/p\mathbb{Z}\}| = |\{3y^2 | y \in \mathbb{Z}/p\mathbb{Z}\}| = \frac{p+1}{2}$, on déduit que l'équation $x^2+1 = 3y^2$ admet au moins une solution $(x_0, y_0)$ dans $\mathbb{Z}/p\mathbb{Z}$. De plus, $(x_0, y_0)$ n'est pas nul dans $(\mathbb{Z}/p\mathbb{Z})^2$. Donc d'après la question précédente, l'équation possède au moins une solution dans $\mathbb{Z}_p$.
Si $p = 3$, l'équation n'a pas de solutions dans $\mathbb{Z}_3$ car elle n'en a pas dans $\mathbb{Z}/3\mathbb{Z}$.
Si $p = 2$, l'équation n'a pas de solutions dans $\mathbb{Z}_2$ car elle n'en a pas dans $\mathbb{Z}/4\mathbb{Z}$.

**3.** Combien de solutions possède le système d'équations :

$$\begin{cases} x^2 + 1 &= 3y^2 \\ x^3 + 3y^5 + y &= 2 \end{cases}$$

dans $\mathbb{Z}_5$ ?

**Indications :** Dans $\mathbb{Z}/5\mathbb{Z}$, les solutions sont $(3, 0)$ et $(4, 2)$. De plus, les matrices jecobiennes correspondantes sont inversibles dans $\mathcal{M}_2(\mathbb{Z}/5\mathbb{Z})$. Le lemme de Hensel montre donc que le système d'équations possède 2 solutions dans $\mathbb{Z}_5$.

**Exercice 19 (culturel) : Topologie sur les entiers $p$-adiques**

Soit $p$ un nombre premier. Comme dans l'exercice 11, on munit $\mathbb{Z}_p$ de la topologie induite par la topologie produit sur $\prod_n \mathbb{Z}/p^n\mathbb{Z}$. Ainsi $\mathbb{Z}_p$ est un anneau topologique.

**1.** Pour $x = (x_n)_n \in \mathbb{Z}_p$, on pose $v_p(x) = \max\{n \in \mathbb{N} / x_n = 0\}$. Montrer que :

$$d_p(x, y) = p^{-v_p(x-y)}$$

définit une distance sur $\mathbb{Z}_p$.

**2.** En déduire que $\mathbb{Z}_p$ est métrisable, puis que $\mathbb{Z}_p$ est complet.

**3.** Montrer que $\mathbb{Z}$ s'injecte dans $\mathbb{Z}_p$. Quelle fonction induit $v_p$ sur $\mathbb{Z}$ ?

**4.** Montrer que $\mathbb{Z}_p$ est le complété de $\mathbb{Z}$ (où $\mathbb{Z}$ est bien sûr muni de la distance $d_p$) ?

**Exercice 20 (culturel) : L'anneau des entiers $p$-adiques**

On garde les notations de l'exercice précédent.

**1.** Rappeler pourquoi $\mathbb{Z}_p$ est un anneau intègre.

Soit $\mathbb{Q}_p$ le corps des fractions de $\mathbb{Z}_p$.

**2.** Montrer que la fonction $v_p : \mathbb{Z}_p \to \mathbb{N}$ s'étend en un morphisme de groupes surjectif $v_p : \mathbb{Q}_p \to \mathbb{Z}$. Montrer que $\mathbb{Z}_p = \{x \in \mathbb{Q}_p / v_p(x) \geq 0\}$ et que $\mathbb{Z}_p^\times = \mathrm{Ker}(v_p)$.

**3.** En déduire que l'anneau $\mathbb{Z}_p$ est principal. Quels sont ses idéaux ? Montrer que, pour chaque $x \in \mathbb{Z}_p$, on a $\mathbb{Z}_p/(x) \cong \mathbb{Z}/p^{v_p(x)}\mathbb{Z}$.

**4.** On rappelle qu'un idéal $J$ de $A$ est dit premier (resp. maximal) si $A/J$ est un anneau intègre (resp. un corps). Quels sont les idéaux premiers (resp. maximaux) de $\mathbb{Z}_p$ ?

**5.** La surjection $\pi : \mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ induit par restriction un morphisme de groupes surjectif $\pi : \mathbb{Z}_p^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$. Montrer qu'il possède une section, c'est-à-dire qu'il existe un morphisme de groupes $s : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ tel que $\pi \circ s = Id$.

**6.** On pose $s(0) = 0$. Montrer que la fonction :

$$\phi : (\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}} \to \mathbb{Z}_p, (x_n)_n \mapsto \sum_n s(x_n)p^n$$

est une bijection. S'agit-il d'un isomorphisme d'anneaux ?

**7.** Il est intéressant de comprendre quelle structure d'anneau il faut mettre sur $(\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}}$ pour que $\phi$ soit un isomorphisme. C'est la théorie des vecteurs de Witt qui y répond, mais elle dépasse très largement le cadre de ce cours.

**Exercice 21 (culturel) : Séries formelles**

Soit $k$ un corps. Pour $x \in k[[T]]$ et $y \in k[[T]]$, on pose $v(x) = \max\{n \in \mathbb{N} / x \in (T^n)\}$ et $d(x, y) = e^{-v(x-y)}$. En procédant comme dans l'exercice 19, montrer que $d$ définit une distance sur $k[[T]]$ et que $k[[T]]$ est alors un anneau qui s'identifie au complété de $k[T]$ pour la distance $d$. Quand $k[[T]]$ est-il compact ?