U2LG35 L3 Algèbre 2014-2015 **Université Paris-Diderot**

Feuille d'exercices numéro 5 bis

☞ **Exercice 1.** Parmi les anneaux de la forme $\mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{N}$), lesquels sont principaux ?

☞ **Exercice 2.** Soit $D(X)$ un polynôme à coefficents réels du second degré sans racine réelle. Montrer que l'anneau quotient $\mathbb{R}[X]/D(X)$ est isomorphe au corps $\mathbb{C}$ des nombres complexes.

☞ **Exercice 3.** *On note $\mathscr{A}$ l'anneau des série entières à coefficients réels.*

(a) Quels sont les éléments inversibles de $\mathscr{A}$?

(b) Montrer que $\mathscr{A}$ a un unique idéal maximal $\mathscr{I}$.

(c) Pour tout $p \in \mathbb{N}$, décrire les éléments de l'idéal $\mathscr{I}^p$.

(d) Montrer que $\mathscr{A}$ est un anneau principal.

(e) Montrer que $\mathscr{A}$ n'a pas d'autre idéal non trivial (i.e. distinct de $\mathscr{A}$ et de 0) que les $\mathscr{I}^p$.

☞ **Exercice 4.** *Soit $\mathscr{A}$ un anneau commutatif unitaire et soit $\mathscr{M}$ un idéal maximal de $\mathscr{A}$.*

(a) Montrer que si tout élément de $\mathscr{A} - \mathscr{M}$ est inversible, alors $\mathscr{A}$ n'a pas d'autre idéal maximal que $\mathscr{M}$.

On admettra que tout idéal distinct de $\mathscr{A}$ est inclus dans un idéal maximal de $\mathscr{A}$.([1])

(b) Montrer réciproquement que si $\mathscr{M}$ est l'unique idéal maximal de $\mathscr{A}$ alors tout élément de $\mathscr{A} - \mathscr{M}$ est inversible.

(c) Montrer que si tout élément de la forme $1 + x$ avec $x \in \mathscr{M}$ est inversible, alors $\mathscr{A}$ n'a pas d'autre idéal maximal que $\mathscr{M}$.

☞ **Exercice 5.** Montrer que dans un anneau principal, tout idéal premier est maximal.

☞ **Exercice 6.** **(a)** Montrer que l'ensemble des éléments nilpotents d'un anneau commutatif $\mathscr{A}$ est un idéal $\mathscr{N}$ et que le quotient $\mathscr{A}/\mathscr{N}$ n'a pas d'élément nilpotent non nul.

(b) Montrer que l'idéal $\mathscr{N}$ de la question précédente est inclus dans l'intersection de tous les idéaux premiers de $\mathscr{A}$.([2])

---

1. Ce théorème se démontre en utilisant le lemme de Zorn.
2. Il lui est en fait égal, mais ceci requiert l'utilisation du lemme de Zorn.

Solutions des exercices de la feuille 5 bis

☞ **Exercice 1.** Par définition, un anneau principal est intègre. Or, si $n \neq 0, 1$ n'est pas premier on a $n = ab$ avec $1 < a < n$ et $1 < b < n$, et les éléments a et b de $\mathbb{Z}/n\mathbb{Z}$ sont non nuls alors que leur produit est nul. $\mathbb{Z}/n\mathbb{Z}$ n'est donc pas intègre dans ce cas. Par ailleurs, $\mathbb{Z}/n\mathbb{Z}$ étant un corps pour n premier, il est commutatif intègre et tous ses idéaux, à savoir lui-même et 0 sont principaux (engendrés respectivement par 1 et 0). C'est donc un anneau principal. Enfin, $\mathbb{Z}/1\mathbb{Z} = 0$ est principal et $\mathbb{Z}/0\mathbb{Z}$ est isomorphe à $\mathbb{Z}$ qui est principal.

☞ **Exercice 2.** On a $D(X) = \alpha X^2 + \beta X + \gamma$ avec $\alpha \neq 0$. Comme $D(X)$ et $D(X)/\alpha$ engendrent le même idéal, on peut supposer que $\alpha = 1$. On peut mettre ce trinôme sous « forme canonique » :

$$D(X) = \left(X + \frac{\beta}{2}\right)^2 + \frac{4\gamma - \beta^2}{4}$$

On a $M = \dfrac{4\gamma - \beta^2}{4} > 0$ puisque $D(X)$ n'a pas de racine réelle. Dans le quotient $\mathbb{R}[X]/D(X)$, on a donc

$$\left(\frac{X + \frac{\beta}{2}}{\sqrt{M}}\right)^2 = -1$$

On pose donc $i = \dfrac{X + \frac{\beta}{2}}{\sqrt{M}}$, et on a $i^2 = -1$. Il reste à montrer que tout élément $P(X)$ de $\mathbb{R}[X]/D(X)$ se met de manière unique sous la forme $a + ib$ avec a et b réels. Notons que dans le quotient on a $X^2 = -bX - c$, puisque $D(X) = 0$. Ainsi, tout élément du quotient est représenté par un polynôme $P(X)$ de degré au plus 1. On fait la division euclidienne de ce $P(X)$ par i, et comme i est de degré 1, on obtient $P(X) = Q(X)i + R(X)$ avec $R(X)$ de degré 0, autrement-dit de la forme $R(X) = a \in \mathbb{R}$. Comme $P(X)$ est de degré 1, on voit que $Q(X)$ doit être lui aussi de degré 0 et s'écrit donc b avec $b \in \mathbb{R}$. On a donc $P(X) = a + ib$ avec a et b réels.

L'unicité résulte du fait que si $a + ib = c + id$, alors $(a - c) + (b - d)i$ est multiple de $D(X)$ dans $\mathbb{R}[X]$. Comme i est de degré 1 ceci ne peut arriver que si $a = c$ et $b = d$.

☞ **Exercice 3.** **(a)** Une série entière $f(x)$ s'écrit $f(x) = a_0 + a_1 x + a_2 x^2 + \dots$. Si $a_0 \neq 0$, c'est un élément inversible de $\mathscr{A}$. On obtient son inverse en divisant 1 par $f(x)$ « selon les puissances croissantes ». Formellement, il s'agit de trouver une série entière $g(x)$ telle que $f(x)g(x) = 1$. On doit avoir :

$$\begin{array}{rcl} a_0 b_0 & = & 1 \\ a_0 b_1 + a_1 b_0 & = & 0 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 & = & 0 \\ & \dots & \end{array}$$

Si $a_0 \neq 0$, on obtient donc $b_0 = 1/a_0$, puis $b_1 = -a_1 b_0/a_0$ etc... puisqu'on n'est jamais amené à diviser par autre chose que a_0.

Par ailleurs, si $a_0 = 0$, sur tout produit de la forme $f(x)g(x)$ on peut mettre x en facteur ce qui interdit qu'il soit égal à 1. Les inversibles de $\mathscr{A}$ sont donc les séries formelles dont le « terme constant » n'est pas nul.

(b) Il résulte de la solution de **(a)** que les éléments non inversibles de $\mathscr{A}$ sont ceux qui peuvent s'écrire $xf(x)$, autrement-dit les multiples de x, c'est-à-dire les éléments de l'idéal principal engendré par x, qui se trouve donc être l'unique idéal maximal $\mathscr{I}$ de $\mathscr{A}$.

(c) Un produit de p éléments de $\mathscr{I}$ est une série entière de la forme $x^p f(x)$. L'idéal $\mathscr{I}^p$ est donc l'idéal principal engendré par x^p.

(d) $\mathscr{A}$ est bien sûr commutatif, unitaire et il est intègre, car deux series non nulles $f(x)$ et $g(x)$ s'écrivent ax^p+(termes de plus haut degré) et bx^q+(termes de plus haut degré) avec a et b non nuls. Le produit $f(x)g(x)$ s'écrit alors abx^{p+q}+(termes de plus haut degré) et est donc non nul car $ab \neq 0$. Il reste à voir que tout idéal de $\mathscr{A}$ est principal.

Pour tout $f(x) \in \mathscr{A}$, $f(x) \neq 0$, appelons « valuation » de $f(x)$ le plus grand entier n tel que $f(x) \notin \mathscr{I}^{n+1}$. Il est équivalent de dire que n est le plus grand entier tel que x^n divise $f(x)$. cet entier existe toujours pour $f(x) \neq 0$.

Soit $\mathscr{K}$ un idéal non réduit à 0 de $\mathscr{A}$, et soit $f(x) = x^n f_1(x) \in \mathscr{K}$ de valuation minimale n (ce qui signifie que $f_1(x)$ est inversible). Tout élément $g(x)$ de $\mathscr{K}$ s'écrit $g(x) = x^n g_1(x)$ puisque sa valuation est au moins n. Comme $f_1(x)$ est inversible, on peut écrire $g_1(x) = f_1(x)f_1(x)^{-1}g_1(x)$, et donc $g(x) = f(x)\left(f_1(x)^{-1}g_1(x)\right)$. Ainsi, $\mathscr{K}$ est l'idéal principal engendré par $f(x)$.

(e) Soit $\mathscr{K}$ un idéal non trivial. D'après la question précédente, il est engendré par une série $f(x)$ distincte de 0 et non inversible. On peut donc écrire $f(x) = x^n f_1(x)$ avec $f_1(x)$ inversible, ce qui montre que $\mathscr{K}$ est engendré par x^n et donc égal à $\mathscr{I}^n$.

☞ **Exercice 4.** **(a)** Tout idéal qui contient un élément inversible contient ses multiples donc contient 1 et est donc égal à $\mathscr{A}$. Ainsi, si tous les éléments de $\mathscr{A} - \mathscr{M}$ sont inversibles, tout idéal de $\mathscr{A}$ distinct de $\mathscr{A}$ est inclus dans $\mathscr{M}$ et $\mathscr{M}$ est alors l'unique idéal maximal de $\mathscr{A}$.

(b) Si $x \in \mathscr{A} - \mathscr{M}$ n'était pas inversible, il engendrerait un idéal $\mathscr{I}$ distinct de $\mathscr{A}$. Il existerait alors un idéal maximal $\mathscr{N}$ tel que $\mathscr{I} \subset \mathscr{N}$, et on aurait $\mathscr{N} = \mathscr{M}$. Mais c'est impossible puisque $x \notin \mathscr{M}$.

(c) D'après **(a)**, il suffit de montrer que tout élément a qui n'est pas dans $\mathscr{M}$ est inversible. Commme $\mathscr{M}$ est maximal, l'idéal engendré par a et $\mathscr{M}$ est $\mathscr{A}$. On a donc $1 = ay + m$ avec $m \in \mathscr{M}$. Donc $ay = 1 - m$ est inversible par hypothèse, et a est alors inversible.

☞ **Exercice 5.** Comme l'anneau $\mathscr{A}$ est principal, tout idéal s'écrit (x) pour un certain x. Soit (x) un ideal premier distinct de $\mathscr{A}$ et non nul. Soit (y) un idéal distinct de (x) tel que $(x) \subset (y)$. On a $x \in (y)$, donc $x = yz$, donc $yz \in (x)$, donc $z \in (x)$ car (x) est premier et $y \notin (x)$. Donc $z = xt$, et enfin $x = yz = ytx$, donc $x(1 - yt) = 0$, et comme l'anneau est intègre $1 = yt$, et donc $(y) = \mathscr{A}$.

☞ **Exercice 6.** **(a)** Si $x^n = 0$ alors $(xy)^n = x^n y^n = 0$. Par ailleurs, si $x^n = 0$ et $y^m = 0$, alors tous les termes du développement du binôme de $(x+y)^{n+m}$ contiennent une puissance de x ou de y qui est nulle. $\mathscr{N}$ est donc un idéal.

(b) Notons $\mathscr{N}'$ l'intersection des idéaux premiers de $\mathscr{A}$. Si $x^n = 0 \in \mathscr{I}$ pour tout idéal premier $\mathscr{I}$, on a $x \in \mathscr{I}$ (par récurrence sur n en utilisant le fait que $\mathscr{I}$ est premier). On a donc $\mathscr{N} \subset \mathscr{N}'$.