Correction des exercices du 18/09/2023 (Structures algébriques)

Ex 1 : Soit A un anneau commutatif. Un idéal I de A est dit premier lorsque :
$\forall (a,b) \in A^2,\ ab \in I \Rightarrow (a \in I \ \text{ OU } \ b \in I)$.

1. On suppose $A \neq \{0\}$. Montrer que $\{0\}$ est premier si et seulement si A est intègre.

2. Trouver les idéaux premiers de $\mathbb{Z}$.

3. Soit $P \in \mathbb{K}[X]$ irréductible. Montrer que $P\mathbb{K}[X]$ est premier.

4. Soit I un idéal différent de A. Il est dit maximal lorsqu'on ne peut pas intercaler d'idéal strictement entre I et A. Montrer que $\{0\}$ est un idéal maximal si et seulement si A est un corps.

5. Déterminer les idéaux maximaux de $\mathbb{Z}$.

6. Montrer que tout idéal maximal de A est premier.

Correction :

1. • On suppose que $\{0\}$ est premier.
Soient $a, b \in A$ tels que $ab = 0$. Ainsi on a : $ab \in \{0\}$ et donc par hypothèse : $a \in \{0\}$ ou $b \in \{0\}$, soit $a = 0$ ou $b = 0$. Ainsi A est intègre.
• On suppose que A est intègre.
Soient $a, b \in A$ tel que $ab \in \{0\}$. On a donc $ab = 0$; puis $a = 0$ ou $b = 0$, car A est intègre. On a donc : $a \in \{0\}$ ou $b \in \{0\}$. Ainsi $\{0\}$ est un idéal premier.

2. Soit I un idéal de $\mathbb{Z}$ non nul et différent de $\mathbb{Z}$ et premier. Il existe donc $n \in \mathbb{N}$ avec $n \geq 2$ tel que $I = n\mathbb{Z}$ (si $n = 0$, on aurtait $I = \{0\}$ et si $n = 1$, on aurait $I = \mathbb{Z}$).
On suppose que $n = ab$, avec $1 < a, b < n$. Comme $ab = n$ est dans I, alors a est dans I ou b est dans I, ce qui implique que $n|a$ ou $n|b$. Cela est imposible, car $0 < a < n$ et $0 < b < n$. Ainsi n est premier.
Réciproquement on suppose que $I = n\mathbb{Z}$, avec n un nombre premier.
Soit $a, b \in \mathbb{Z}$ tels que : $ab \in I$. On a donc $n|ab$. Si $n|a$, alors a est dans I, sinon a est premier avec n, car n est un nombre premier et donc par le lemme de Gauss, on a : $n|b$, donc b est dans I. Ainsi I est un idéal premier.
Grâce à la première question $\{0\}$ est un idéal premier ($\mathbb{Z}$ est intègre) et $\mathbb{Z}$ est clairement premier.

$$\boxed{\text{Les idéaux premiers de } \mathbb{Z}, \text{ sont } \{0\}, \mathbb{Z} \text{ et } n\mathbb{Z}, \text{ avec } n \text{ un nombre premier}}$$

3. Soit $I = P\mathbb{K}[X]$. Soient $A, B \in \mathbb{K}[X]$ tel que $AB \in I$. On a donc $P|AB$. Si $P|A$, alors A est dans I, sinon A est premier avec P, car P est irréductible et donc par le lemme de Gauss, on a : $P|B$, donc B est dans I. Ainsi

$$\boxed{P\mathbb{K}[X] \text{ est un idéal premier}}$$

4. • On suppose que $\{0\}$ est un idéal maximal.
Soit $x \in A \setminus \{0\}$. Ainsi $I = xA$ est un idéal de A différent de $\{0\}$, avec $\{0\} \subset I \subset A$. Par maximalité de $\{0\}$, on a : $I = A$, soit $xA = A$. Ainsi 1 est dans xA, donc il existe y dans A tel que : $1 = xy$. Par commutativité de A, on a : $1 = xy = yx$, donc x est inversible dans A. Ainsi A est un corps.
• On suppose que A est un corps.
Soit I un idéal tel que : $\{0\} \subset I \subset A$. Si $I \neq \{0\}$, alors il existe x dans I non nul. Comme I est un idél, alors $x \times x^{-1}$ est dans I, donc 1 est dans I. On a donc : $\forall a \in A,\ a = \underbrace{1}_{\in I} \times \underbrace{a}_{\in A} \in I$, car I est un idéal. Ainsi $A \subset I \subset A$, donc $I = A$. Ainsi $\{0\}$ est un idéal maximal.

5. Soit $I = n\mathbb{Z}$ un idéal maximal de $\mathbb{Z}$.
On ne peut avoir $n = 0$, car dans ce cas $I = \{0\}$, puis $I \subset 2\mathbb{Z} \subset \mathbb{Z}$, ce qui contredit la maximalité de I. De plus on ne peut avoir $n = 1$, car : $I \neq \mathbb{Z}$. Ainsi on a $n \geq 2$.
On suppose que n n'est pas un nombre premier. On a donc : $n = ab$, avec $1 < a, b < n$. Ainsi $n\mathbb{Z} \subset a\mathbb{Z} \subset \mathbb{Z}$ et ces inclusions sont strictes, car n de divise pas a donc a n'est pas dans $n\mathbb{Z}$ et on a : $a > 1$, donc $a\mathbb{Z} \neq \mathbb{Z}$. Cela contredit la maximalité de I.
Ainsi n est premier.
Réciproquement on suppose que $I = n\mathbb{Z}$, avec n un nombre premier.
Soit $J = m\mathbb{Z}$ un idéal de $\mathbb{Z}$ tel que : $I \subset J \subset \mathbb{Z}$. On a $m \neq 0$, car J ne peut être $\{0\}$, car il contient I. On a donc : $n \in J = m\mathbb{Z}$, puis $m|n$. Comme n est premier, alors $m = 1$ ou $m = n$, ce qui implique que $J = \mathbb{Z}$ ou $J = I$. Ainsi I est bien maximal.

Les idéaux maximaux de $\mathbb{Z}$, sont les $n\mathbb{Z}$, avec n un nombre premier

6. Soit I un idéal maximal de A. Soient $a, b \in A$ tels que $ab \in I$. On a vu dans le cours que la somme de deux idéaux est un idéal. Voici la preuve pour rappel :
Soit I_1 et I_2 deux idéaux de A. On note$I_1 + I_2 = \{x + y,\ x \in I_1, y \in I_2\}$.

- $(I_1 + I_2, +)$ est un sous-groupe de $(A, +)$:
  - I_1 et I_2 étant des idéaux de A, ce sont des sous-groupes de $(A, +)$ et ils contiennent donc 0. Ainsi : $0 = \underbrace{0}_{\in I_1} + \underbrace{0}_{\in I_2} \in I_1 + I_2$.
  - Soit $x, y \in (I_1 + I_2)$. Il existe donc $a_1, b_1 \in I_1$ et $a_2 + b_2 \in I_2$ tels que $x = a_1 + a_2$ et $y = b_1 + b_2$. Ainsi $x - y = (a_1 - b_1) + (a_2 - b_2)$. Or $a_1 - b_1$ est dans I_1 et $a_2 - b_2$ est dans I_2, car $(I_1, +)$ et $(I_2, +)$ sont des sous-groupes de $(A, +)$ Donc $x - y$ est dans $I_1 + I_2$.
- Soit $z \in I_1 + I_2$. Il existe $a_1 \in I_1$ et $a_2 \in I_2$ tels que $z = a_1 + a_2$. Soit $a \in A$. On a $az = a_1a + a_2z$. Comme I_1 et I_2 sont des idéaux, alors a_1z et a_2z sont respectivement dans I_1 et I_2. Ainsi az est dans $I_1 + I_2$.

Ainsi $I_1 + I_2$ est un idéal de A.
Ainsi on a l'inclusion d'idéaux : $I \subset I + aA \subset A$. Par maximalité de I, on a $I = I + aA$ ou $A = I + aA$. Si $I = I + aA$, alors $a = 0 + a \times 1$ est dans I. Si $A = I + aA$, alors 1 est dans $I + aA$, puis il existe $u \in I$ et $v \in A$ tels que $1 = u + av$, puis $b = ub + abv$. Comme I est un idéal, alors ub et $(ab)v$ sont dans I (car u et ab le sont), puis b est dans I, car $(I, +)$ est un groupe. Par conséquent I est un idéal premier de A.

Tout idéal maximal de A est premier

Ex 2 : Résoudre dans $\mathbb{Z}/41\mathbb{Z}$ l'équation $x^3 - 21x^2 + 29x - 9 = 0$.
Correction : On constate que $\overline{1}$ est solution.
En posant la division euclidienne de $X^3 - 21X^2 + 29X - 9$ par $X - 1$, on a :
$X^3 - 21X^2 + 29X - 9 = (X - 1)(X^2 - 20X + 9)$.
Dans $\mathbb{Z}/41\mathbb{Z}$ qui est un corps car 41 est premier, on a :
$\overline{0} = (x - \overline{1})(x^2 - \overline{20}x + \overline{9}) \Leftrightarrow x = \overline{1}$ OU $x^2 - \overline{20}x + \overline{9} = \overline{0}$, car un corps est intègre.
Imitons la résolution d'une équation du second degré dans $\mathbb{R}$ ou $\mathbb{C}$ pour résoudre $x^2 - \overline{20}x + \overline{9} = \overline{0}$.
Le discriminant ici serait : $\overline{20}^2 - 4.\overline{9} = \overline{364} = \overline{36} = \overline{6}^2$ dans $\mathbb{Z}/41\mathbb{Z}$. On aurait envie de dire que les solutions sont $\overline{(20 - 6)/2} = \overline{7}$ et $\overline{(20 + 6)/2} = \overline{13}$.
On a : $(x - \overline{7})(x - \overline{13}) = x^2 - \overline{20}x + \overline{91} = x^2 - \overline{20}x + \overline{9}$.
On a donc : $x^2 - \overline{20}x + \overline{9} = \overline{0} \Leftrightarrow (x - \overline{7})(x - \overline{13}) = \overline{0} \Leftrightarrow x = \overline{7}$ OU $x = \overline{13}$, par intégrité de $\mathbb{Z}/41\mathbb{Z}$.

Ainsi

$$\boxed{\mathcal{S} = \{\overline{1}, \overline{7}, \overline{13}\}}$$