Algèbre – Interrogation II

*Vous disposez d'**une heure** pour résoudre quatre des cinq exercices suivants qui sont tous indépendants. Vous pouvez admettre le résultat d'une question pour résoudre une question ultérieure même sans l'avoir traitée. Vous pouvez utiliser librement tous les résultats du cours. Ce qui a été vu uniquement en TD est à redémontrer. En cas de questions ou si vous repérez ce qui vous semble être une erreur d'énoncé, n'hésitez pas à me solliciter. Une rédaction propre et rigoureuse sera valorisée.*

Exercice 1. Soit A un anneau principal.

1. Donner deux exemples de tels anneaux.
2. Démontrer que tout anneau euclidien est principal.
3. Soit $\mathfrak{P}$ un idéal premier de A. Montrer que $A/\mathfrak{P}$ est principal. Que se passe-t-il lorsque l'idéal n'est plus supposé premier ?
4. Le résultat est-il vrai pour un anneau factoriel ?
5. Montrer que $\mathbf{Z}[X]$ n'est pas principal. On pourra considérer l'idéal $(2, X)$.

Solution.

1. D'après le cours, les anneaux $k[X]$ avec k corps et $\mathbf{Z}$ sont euclidiens donc principaux. On renvoie au TD pour un exemple d'anneau principal non euclidien.
2. Soit A un anneau euclidien de stathme v et I un idéal de A non nul. On a alors que l'ensemble $\{v(x) \ : \ x \in I \setminus \{0\}\}$ est une partie non vide de $\mathbf{N}$. Elle admet donc un plus petit élément et on peut trouver $a \in I \setminus \{0\}$ de stathme niminal parmi les éléments non nuls de I. On a alors $(a) \subseteq I$ et établissons l'inlusion réciproque. Soit $x \in I$. Comme A est euclidien, il existe q, r dans A tels que $x = aq + r$ avec $r = 0$ ou $v(r) < v(q)$. Or, $r = x - aq \in I$ donc par minimalité de a, $r = 0$ et $x = aq \in (a)$. On a donc bien que $I = (a)$ et que A est principal.
3. Soit $\mathfrak{P}$ un idéal premier de A. On a alors que $A/\mathfrak{P}$ est intègre. Montrons alors que tout idéal de $A/\mathfrak{P}$ est principal. Soit $\pi : A \to A/\mathfrak{P}$ la surjection canonique. On sait que les idéaux de $A/\mathfrak{P}$ sont de la forme $\pi(J)$ avec J un idéal de A contenant $\mathfrak{P}$. Mais puisque A est principal, il existe a dans A tel que $J = (a)$. On a alors que $\pi(J) = (\pi(a))$, ce qui permet de conclure.
   Lorsque l'idéal n'est plus supposé premier, on a bien que tous les idéaux sont principaux mais l'anneau quotient n'est pas intègre, ce qui es requis pour être un anneau principal.
4. Non puisque d'après le cours, $\mathbf{Z}[X]$ est factoriel (car $\mathbf{Z}$ l'est) mais $\mathbf{Z}[i\sqrt{5}] \cong \mathbf{Z}[X]/(X^2 + 5)$ ne l'est pas[1].
5. On raisonne par l'absurde en supposant que l'idéal $(2, X) = (P)$ est principal avec $P \in \mathbf{Z}[X]$. On a alors que $2 \in (P)$ soit que $P \mid 2$, ce qui implique pour des raisons de degré que P est constant et vaut ± 1 ou ± 2. Mais de même $P \mid X$ dans $\mathbf{Z}[X]$ de sorte que $P = \pm 1$. Ainsi, $P \in \mathbf{Z}[X]^\times = \mathbf{Z}^\times$ (car $\mathbf{Z}$ est intègre). On aurait alors $(2, X) = (P) = \mathbf{Z}[X]$. Mais alors $1 \in (2, X)$ de sorte qu'il existe deux polynômes $P, Q \in \mathbf{Z}[X]$ tels que $1 = PX + 2Q$. En évaluant en 0, il viendrait $1 = 2Q(0)$ dans $\mathbf{Z}$, ce qui est absurde. Ainsi $(2, X)$, et par conséquent $\mathbf{Z}[X]$ n'est pas principal !

Exercice 2. Pour $d \in \mathbf{N}$, on pose $A_d = \left\{(x, y) \in \mathbf{Z}^2 \ : \ y - x \in d\mathbf{Z}\right\}$.

1. Montrer que, pour tout $d \in \mathbf{Z}$, A_d est un sous-anneau de $\mathbf{Z}^2$.
2. Réciproquement, soit A un sous-anneau de $\mathbf{Z}^2$. Montrer que
$$H = \{x \in \mathbf{Z} \ : \ (x, 0) \in A\}$$
est un sous-groupe de $\mathbf{Z}$. En déduire qu'il existe un $d \in \mathbf{N}$ tel que $A = A_d$.

Solution.

1. On a clairement que $(1, 1) \in A_d$. Soient $(x, y), (x', y') \in A_d$. On a alors
$$(x, y) - (x', y') = (x - x', y - y') \quad \text{et} \quad (y - y') - (x - x') = (y - x) - (y' - x').$$
Or, comme $(x, y), (x', y') \in A_d$, $y - x, y' - x' \in d\mathbf{Z}$ qui est un sous-groupe de $\mathbf{Z}$ donc $(y - x) - (y' - x') \in d\mathbf{Z}$ et $(x, y) - (x', y') \in A_d$. Reste à vérifier la stabilité par produit. On a alors
$$(x, y) \cdot (x', y') = (xx', yy').$$
On a alors $y = x + dk$ et $y' = x + d\ell$ pour $k, \ell \in \mathbf{Z}$. On a alors
$$yy' = xx' + d(\ell x + kx' + dk\ell) \quad \text{donc} \quad yy' - xx' \in d\mathbf{Z}$$
de sorte que $(x, y) \cdot (x', y') \in A_d$. On pouvait aussi écrire $yy' - xx' = yy' - xy' + xy' - xx' = (y - x)y' - x(y' - x')$.
Noter qu'on a que $(x, y) \in A_d$ si, et seulement si, $x \equiv y \pmod{d}$ et on a alors redémontré la compatibilité de la congruence modulo d avec la somme et le produit, ce qui est bien connu !

1. Car $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ et que ces quatre éléments sont tous irréductibles non associés deux à deux.

2. On a clairement que $0 \in H$ car A est un sous-anneau de $\mathbf{Z}^2$ et contient donc $(0,0)$. Soient $x, x' \in H$, alors $x - x' \in H$ car

$$(x - x', 0) = (x, 0) - (x', 0) \in A \quad \text{car} \quad A \text{ sous-anneau de } \mathbf{Z}^2.$$

On a par conséquent bien que H est un sous-groupe de $\mathbf{Z}$. On sait alors qu'il existe $d \in \mathbf{N}$ tel que $H = d\mathbf{Z}$.
Montrons alors que $A = A_d$. Soit $(x, y) \in A$, alors comme A est un sous-anneau de $\mathbf{Z}^2$, il contient $(1,1)$ et

$$(x - y, 0) = (x, y) - y(1,1) \in A$$

de sorte que $x - y \in H = d\mathbf{Z}$. Réciproquement, si $(x, y) \in A_d$, alors $y - x \in d\mathbf{Z}$ et donc $y - x \in H$ ce qui implique que $(y - x, 0) \in A$. On a donc

$$(x, y) = (y - x, 0) + y(1,1) \in A.$$

Les sous-anneaux de $\mathbf{Z}^2$ sont donc exactement les A_d.

Exercice 3.

1. Soit A un anneau possédant un unique idéal maximal $\mathfrak{M}$. Montrer que $\mathfrak{M} = A \setminus A^\times$.

2. Réciproquement, on suppose que $\mathfrak{M} = A \setminus A^\times$ est un idéal de A. Montrer que tout idéal I de A distinct de A est contenu dans $\mathfrak{M}$.

3. Montrer que A posséde un unique idéal maximal si, et seulement si, pour tout $x \in A$, x ou $1 - x$ est inversible.

4. Soit A un anneau possédant un unique idéal maximal. Montrer que l'équation $x^2 = x$ n'a que deux solutions dans A, à savoir 0 et 1.

5. Soit k un corps et n un entier. Décrire les idéaux de $A = k[X]/(X^n)$ et montrer que A posséde un unique idéal maximal que l'on précisera.

Solution.

1. Notons $I = \{x \in A \mid x \notin A^\times\}$. Soit $\mathfrak{M}$ l'idéal maximal de A, il est contenu dans I car tous les éléments de $\mathfrak{M}$ sont non inversibles. Soient $x, y \in I$ et montrons que $x - y \in I$. Comme $\mathfrak{M}$ est le seul idéal maximal de A on a que l'idéal engendré par $x - y$ est contenu dans $\mathfrak{M}$ qui est contenu dan s I donc $x - y \in I$. Comme I est non vide car $0 \in I$ on a bien que $(I, +)$ est un sous-groupe de $(A, +)$. En plus, si $x \in I$, on a que l'idéal engendré par x est forcément contenu dans $\mathfrak{M}$, donc pour tout $a \in A$, $ax \in M \subset I$.

2. Supposons que I est un idéal. Soit $\mathfrak{M}$ l'unique idéal maximal de A. Alors pour tout $y \in \mathfrak{M}$, $y \notin A^\times$ car sinon $\mathfrak{M} = A$, donc $\mathfrak{M} \subset I$ et $I \neq A$ donc par maximalité, $\mathfrak{M} = I$.

3. Supposons que $x \notin A^\times$. Alors $x \in I = A \backslash A^\times$ qui est l'unique idéal maximal. Si $1 - x \in I$, alors $1 = 1 - x + x \in I$ mais $1 \in A^\times$ donc $1 - x \notin I$ et donc $1 - x \in A^\times$. De même, si $1 - x \notin A^\times$ alors $1 - x \in I$ et si $x \in I$ alors $1 \in I$, donc $x \notin I$ et $x \in A^\times$.
Réciproquement, supposons pour tout $x \in A$, $x \in A^\times$ ou $1 - x \in A^\times$. Soit $\mathfrak{M}$ un idéal maximal de A et soit $y \in A \backslash \mathfrak{M}$ alors $(y, \mathfrak{M}) = A$ et il existe $a \in A$, $m \in \mathfrak{M}$ tels que $1 = ay + m$ donc $ay = 1 - m \in A^\times$ car $m \in \mathfrak{M} \neq A$ donc $m \notin A^\times$. On a donc montré que (y) contenait un élément inversible, donc $(y) = A$. On a alors que $y \in A^\times$. On a montré que $A \backslash \mathfrak{M} = A^\times$ donc $A \backslash A^\times = M$ est un idéal et donc A possède un unique idéal maximal par **2.**.

4. Soit $x \in A$ tel que $x^2 = x$, alors $x^2 - x = x(x - 1) = 0$ et x et $x - 1$ sont des diviseurs de zéro. Par la question précédente, on a que : soit $x \in A \in A^\times$ et dans ce cas $x = 1$, soit $x - 1 \in A^\times$ et dans ce cas $x = 0$.
Si $A = \mathbf{Z}$ alors il est intègre donc si $x^2 = x$ on a que $x = 1$ ou $x = 0$, donc les seuls solutions de $x^2 = x$ sont 1 et 0 mais $\mathbf{Z}$ admet plusieurs idéaux maximaux car pour tout nombre premier p, l'idéal $p\mathbf{Z}$ est maximal.

5. Les idéaux de $k[x]/(x^n)$ sont en bijection avec les idéaux de $k[x]$ qui contiennent (x^n) ; comme $k[x]$ est principal, ils sont engendrés par un $P \in k[x]$ tel que $(x^n) \subseteq (P)$, c'est-à-dire tels que P divise (x^n), ce qui implique que $P = x^k$ avec $k \leq n$. Le seul idéal maximal est alors (x) car pour tout $k \leq n - 1$, on a que les idéaux de $k[x]/(x^n)$ sont donnés par

$$(x^n) \subseteq (x^{n-1}) \subseteq \cdots \subseteq (x^k) \subseteq \cdots \subseteq (x).$$

Exercice 4. On considère l'application

$$\varphi : \begin{cases} \mathbf{Z}[X] & \longrightarrow & \mathbf{Z}/2\mathbf{Z} \\ P & \longmapsto & \overline{P(0)}, \end{cases}$$

où $\overline{k}$ désigne la classe modulo 2 d'un entier k.

1. Justifier que φ est un morphisme d'anneaux surjectif.

2. Soit $P \in \mathbf{Z}[X]$. Établir qu'il existe $Q \in \mathbf{Z}[X]$ et $k \in \mathbf{Z}$ tels que $P = QX + k$.

3. Établir que $\mathrm{Ker}(\varphi) = (2, X)$ puis que $\mathbf{Z}[X]/(2, X) \cong \mathbf{Z}/2\mathbf{Z}$. Qu'en déduisez-vous quant à l'idéal $(2, X)$?

Solution.

1. On a bien $\varphi(1) = \overline{1}$ et pour tous $P, Q \in \mathbf{Z}[X]$. On a alors que
$$\varphi(P+Q) = \overline{(P+Q)(0)} = \overline{P(0)+Q(0)} = \overline{P(0)} + \overline{Q(0)}$$
car la réduction modulo 2 est un morphisme d'anneaux. De même,
$$\varphi(PQ) = \overline{(PQ)(0)} = \overline{P(0)Q(0)} = \overline{P(0)} \cdot \overline{Q(0)}$$
et φ est un morphisme d'anneaux.
2. Comme X est unitaire, on peut effectuer une division euclidienne dans $\mathbf{Z}[X]$ de P par X et obtenir qu'il existe $Q \in \mathbf{Z}[X]$ et $k \in \mathbf{Z}$ tels que $P = QX + k$. On pouvait aussi simplement ici écrire pour un entier naturel d et des entiers $a_0, a_1, \ldots, a_d$:
$$P = \sum_{k=0}^{d} a_k X^k = X\left(\sum_{k=1}^{d} a_k X^{k-1}\right) + a_0.$$
3. On voit clairement que $(2, X) \subseteq \mathrm{Ker}(\varphi)$ car tout élément de $(2, X)$ est de la forme $P = 2S + XT$ avec $S, T \in \mathbf{Z}[X]$ et $P(0) = 2S(0)$ qui est bien nul modulo 2. Réciproquement, si $P \in \mathrm{Ker}(\varphi)$, alors $P(0)$ est pair. Par ailleurs, par la question précédente, il existe $Q \in \mathbf{Z}[X]$ et $k \in \mathbf{Z}$ tels que $P = QX + k$. On a alors $P(0) = k$ pair et $k = 2k'$ pour $k' \in \mathbf{Z}$ et $P = QX + 2k' \in (2, X)$, ce qui permet de conclure !
Le morphisme φ est surjectif ($P = 1$ et $P = 0$ ont pour image $\overline{1}$ et $\overline{0}$) et le théorème de factorisation implique que
$$\mathbf{Z}[X]/(2, X) \cong \mathbf{Z}/2\mathbf{Z}$$
qui est un corps si bien que $(2, X)$ est un idéal maximal de $\mathbf{Z}[X]$.

Exercice 5. Soit $A = \left\{a + b\sqrt{10} \ : \ (a, b) \in \mathbf{Z}^2\right\}$.

1. Montrer que A est un anneau isomorphe à $\mathbf{Z}[X]/(X^2 - 10)$.
2. On pose $N(a + b\sqrt{10}) = (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$. Justifier que $a + b\sqrt{10} \in A^\times$ si, et seulement si, $N(a + b\sqrt{10}) = \pm 1$.
3. Montrer que l'équation $x^2 - 10y^2 = \pm 2$ n'a pas de solution entière.
4. Montrer que 2 est irréductible. On pourra penser à utiliser l'application N.
5. L'idéal (2) est-il premier dans A ? Que pouvez-vous en conclure ?

Solution.

1. Comme dans le cas de $\mathbf{Z}[i]$ en TD, on voit que
$$A = \left\{P(\sqrt{10}) \ : \ P \in \mathbf{Z}[X]\right\}.$$
L'inclusion de gauche à droite est immédiate car si $z \in A$, il existe deux entiers a et b tels que $z = a + b\sqrt{10}$ de sorte qu'en prenant $P = a + bX$, $z = P(\sqrt{10})$. Pour l'inclusion réciproque, soit $z = P(\sqrt{10})$ avec $P \in \mathbf{Z}[X]$. On effectue une division euclidienne dans $\mathbf{Z}[X]$ de P par $X^2 - 10$ (qui est licite car ce dernier est unitaire) qui fournit l'existence de $Q, R \in \mathbf{Z}[X]$ tels que $P = Q(X^2 - 10) + R$ avec R de degré au plus 1. Ainsi, il existe deux entiers a et b tels que $R(X) = a + bX$ et en évaluant en $\sqrt{10}$, il vient $P(\sqrt{10}) = R(\sqrt{10}) = a + b\sqrt{10}$. Ainsi, le morphisme d'évaluation
$$\varphi : \left\{ \begin{array}{ccc} \mathbf{Z}[X] & \longrightarrow & A \\ P & \longmapsto & P(\sqrt{10}), \end{array} \right.$$
est un morphisme d'anneaux surjectif. Son noyau est donné par $(X^2 - 10)$. En effet, cet idéal est clairement inclus dans le noyau et si P est dans le noyau, alors $P(\sqrt{10}) = 0$ et on effectue une division euclidienne dans $\mathbf{Z}[X]$ de P par $X^2 - 10$ (qui est licite car ce dernier est unitaire) qui fournit l'existence de $Q, R \in \mathbf{Z}[X]$ tels que $P = Q(X^2 - 10) + R$ avec R de degré au plus 1. Ainsi, il existe deux entiers a et b tels que $R(X) = a + bX$ et en évaluant en $\sqrt{10}$, il vient $a + b\sqrt{1} = 0$. Or, la famille $(1, \sqrt{10})$ est $\mathbf{Q}$-libre car $\sqrt{10}$ n'est pas rationnel et on en déduit que $a = b = 0$ et que $P = Q(X^2 - 10) \in (X^2 - 10)$. Cela fournit au quotient l'isomorphisme cherché
$$A \cong \mathbf{Z}[X]/(X^2 - 10).$$
2. Supposons que $z = a + b\sqrt{10} \in A^\times$. Il existe alors $z' = a' + b'\sqrt{10}$ dans A tel que $zz' = 1$. On constate alors que
$$N(zz') = N(aa' + 10bb' + \sqrt{10}(ab' + a'b)) = (aa' + 10bb')^2 - 10(ab' + a'b)^2 = (aa')^2 + 100(bb')^2 - 10((ab')^2 + (a'b)^2)$$
tandis que
$$N(z)N(z') = (a^2 - 10b^2)(a'^2 - 10b'^2) = (aa')^2 + 100(bb')^2 - 10((ab')^2 + (a'b)^2) = N(zz').$$
On a donc $N(z)N(z') = N(1) = 1$. Or, on voit que si $z \in A$, $N(z) \in \mathbf{Z}$ de sorte que $N(z) \in \{\pm 1\}$.
Réciproquement, si $N(z) = \pm 1$ avec $z = a + b\sqrt{10}$ avec a, b entiers, alors $z(a - b\sqrt{10}) = \pm 1$. On a $zz' = 1$ avec $z' = \pm(a - b\sqrt{10}) \in A$ et donc $z \in A^\times$.

3. Raisonnons par l'absurde en supposant qu'il existe deux entiers x et y tels que $x^2 - 10y^2 = \pm 2$. On a alors modulo 5 que $x^2 \equiv \pm 2 \pmod 5$. Mais les carrés modulo 5 sont

$$0^2 \equiv 0 \pmod 5, \quad 1^2 \equiv 4^2 \equiv 1 \pmod 5, \quad 2^2 \equiv 3^2 \equiv -1 \pmod 5.$$

Ainsi, ± 2 n'est pas un carré modulo 5 et on aboutit à une contradiction !

4. Si 2 n'est pas irréductible, alors il existe $u, v \notin A$ tels que $2 = uv$. On a alors en prenant la norme $4 = N(2) = N(uv) = N(u)N(v)$. On a donc puisque $N(u), N(v) \in \mathbf{Z}$ que $N(u) \in \{\pm 1, \pm 2, \pm 4\}$. Mais u non inversible donc d'après la question **2.**, $N(u) \neq \pm 1$ et de même $N(u) \neq \pm 4$ car sinon $N(v) = \pm 1$ mais v est non inversible. On a donc $N(u) = \pm 2$. Mais, $u = x + y\sqrt{10}$ avec x, y entiers de sorte que $N(u) = x^2 - 10y^2 = \pm 2$, ce qui est absurde par la question précédente. Dans tous les cas, on a une contradiction donc 2 est irréductible.

5. L'idéal (2) est premier dans A si, et seulement si, $A/(2)$ est intègre. Or, par **1.**, $A \cong \mathbf{Z}[X]/(X^2 - 10)$ de sorte que (2) est premier si, et seulement si, $\left(\mathbf{Z}[X]/(X^2 - 10)\right)/(2)$ est intègre. Comme on l'a vu en TD,

$$\left(\mathbf{Z}[X]/(X^2 - 10)\right)/(2) \cong (\mathbf{Z}[X]/(2))/(X^2 - 10) \quad \text{et} \quad (\mathbf{Z}[X]/(2) \cong \mathbf{Z}/2\mathbf{Z}[X]$$

de sorte que (2) est premier si, et seulement si, $\mathbf{Z}/2\mathbf{Z}[X]/(X^2 - 10) = \mathbf{Z}/2\mathbf{Z}[X]/(X^2)$ est intègre. Cela arrive, puisque $\mathbf{Z}/2\mathbf{Z}$ est un corps si, et seulement si, (X^2) est premier. Or les idéaux premiers de $\mathbf{Z}/2\mathbf{Z}[X]$ sont (0) et (P) avec P irréductible. Or, X^2 n'est pas irréductible donc $\mathbf{Z}/2\mathbf{Z}[X]/(X^2)$ n'est pas intègre [2] et (2) n'est pas premier.
D'après le cours, A n'est pas factoriel car dans un anneau factoriel, tout élément p irréductible donne lieu à un idéal (p) premier !

2. On peut aussi le voir ici car si on note $\overline{X}$ la classe de X dans le quotient $\mathbf{Z}/2\mathbf{Z}[X]/(X^2)$, alors $\overline{X} \neq 0$ et $\overline{X}^2 = 0$ donc le quotient n'est pas intègre !