Correction du contrôle continu du 21 octobre 2022
"Algèbre 1 - HAX708X"

Exercice 1

Soit A un anneau commutatif intègre et soit M un A-module. Soit M_{tor} l'ensemble des éléments de torsion de M, c'est-à-dire l'ensemble des $m \in M$ tels qu'il existe $a \in A - \{0\}$ tel que $am = 0$.

(1) Montrer que M_{tor} est un sous-module de M.
(2) Montrer que le module quotient M/M_{tor} est sans torsion *(i.e. 0 est le seul élément de torsion)*.

Si $am = 0$ et $bn = 0$ alors $ab(m+n) = 0$ et $a(cm) = 0$ pour tout $c \in A$. Comme A est intègre, on remarque que si $a \neq 0$ et $b \neq 0$ alors $ab \neq 0$. On voit ainsi que M_{tor} est stable pour l'addition et la multiplication externe, c'est donc un sous-module de M.

Soit $\overline{m} \in M/M_{tor}$ et $a \neq 0$ tel que $a\overline{m} = \overline{am} = 0$. Cela signifie que $am \in M_{tor}$: il existe donc $b \neq 0$ tel que $b(am) = bam = 0$. Comme $ba \neq 0$ on obtient $m \in M_{tor}$, soit $\overline{m} = 0$. On a montré que M/M_{tor} est sans torsion.

Exercice 2

On considère le polynôme $P = X^4 + X^3 + X^2 + X + 1$.

(1) Déterminer la décomposition en facteur premier de P dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$. *On calculera le produit $P(1-X)$.*
(2) Montrer que P est irréductible dans $\mathbb{Z}[X]$.
(3) En déduire que $\cos(\frac{2\pi}{5}) \notin \mathbb{Q}$.

Point (1)

On remarque que $P(1-X) = 1 - X^5$. Ainsi les racines complexes de P sont les racines 5-ième de l'unité différentes de 1. On obtient ainsi la factorisation en facteur premier de P dans $\mathbb{C}[X]$: $P = \prod_{k=1}^{4}(X - e^{i\frac{2k\pi}{5}})$.

On remarque que $\overline{e^{i\frac{2\pi}{5}}} = e^{i\frac{8\pi}{5}}$ et $\overline{e^{i\frac{4\pi}{5}}} = e^{i\frac{6\pi}{5}}$, ainsi $P = (X - e^{i\frac{2\pi}{5}})(X - \overline{e^{i\frac{2\pi}{5}}})(X - e^{i\frac{4\pi}{5}})(X - \overline{e^{i\frac{4\pi}{5}}})$ et donc

$$P = \underbrace{\left(X^2 - 2\cos(\tfrac{2\pi}{5})X + 1\right)}_{Q_1}\underbrace{\left(X^2 - 2\cos(\tfrac{4\pi}{5})X + 1\right)}_{Q_2}$$

est la décomposition en facteur premier de P dans $\mathbb{R}[X]$.

Point (2)

On remarque que le contenu de P est 1 (P est primitif). Ainsi, si P n'est pas irréductible dans $\mathbb{Z}[X]$, il existe $P_1, P_2 \in \mathbb{Z}[X]$, de degré ≥ 1, tels que $P = P_1P_2$. Ces polynômes sont de degré égal à 2 car P ne possède pas de racine rationelle. Ils sont aussi unitaires car P est unitaire. Sachant que $P = Q_1Q_2$ avec Q_1, Q_2 irréductibles dans $\mathbb{R}[X]$, on voit que les P_i coincident avec les Q_j. Cela est contradictoire avec le fait que $2\cos(\frac{2\pi}{5}) \notin \mathbb{Z}$.

Point (3)

Comme P est irréductible dans $\mathbb{Z}[X]$ (et P n'est pas une constante), on sait que P est aussi irréductible dans $\mathbb{Q}[X]$. Cela implique que les Q_j n'appartiennent pas à $\mathbb{Q}[X]$: en particulier, $\cos(\frac{2\pi}{5}) \notin \mathbb{Q}$.

Exercice 3

On considère l'anneau $A = \mathbb{R}[X,Y]/(1+Y-YX^2)$.

(1) Montrer que A est isomorphe à la localisation $S^{-1}\mathbb{R}[X]$ pour une certaine partie multiplicative $S \subset \mathbb{R}[X]$.

(2) Montrer que A est un anneau principal.

(3) Déterminer les éléments inversibles de A.

(4) Déterminer les morphismes d'anneaux $\varphi : A \to \mathbb{R}$ tels que $\varphi(\lambda) = \lambda, \forall \lambda \in \mathbb{R}$.

Point (1)

On considère la partie multiplicative $S = \{(X^2-1)^n, n \in \mathbb{N}\}$ de $\mathbb{R}[X]$. Considérons maintenant le morphisme $\phi : \mathbb{R}[X,Y] \to S^{-1}\mathbb{R}[X]$ défini par le relation

$$\phi(P(X,Y)) = P(X, \tfrac{1}{X^2-1}), \qquad \forall P \in \mathbb{R}[X,Y].$$

On voit facilement que ϕ est surjective et que $\ker(\phi)$ contient l'idéal engendré par $1 - Y(X^2-1)$. Ainsi ϕ induit un morphisme $\bar{\phi} : \mathbb{R}[X,Y]/(1+Y-YX^2) \to S^{-1}\mathbb{R}[X]$ surjectif. Pour montrer que $\bar{\phi}$ est bijective, on vérifie que l'application $\psi : S^{-1}\mathbb{R}[X] \to \mathbb{R}[X,Y]/(1+Y-YX^2), \psi(\frac{P(X)}{(X^2-1)^n}) = \mathrm{cl}(P(X)Y^n)$ est bien définie. Alors on a $\psi \circ \bar{\phi} = Id$ et donc $\bar{\phi}$ est injective.

Point (2)

Soit I un idéal de $S^{-1}\mathbb{R}[X]$. On considère $I_0 = I \cap \mathbb{R}[X]$. On remarque que I_0 est un idéal de $\mathbb{R}[X]$ tel que $\forall T \in S^{-1}\mathbb{R}[X], \exists n \in \mathbb{N}$ tel que $(X^2-1)^n T \in I_0$. Soit $P_0 \in \mathbb{R}[X]$ tel que $I_0 = (P_0)$. On remarque alors que P_0 engendre l'idéal I. Comme $A \simeq S^{-1}\mathbb{R}[X]$ est un anneau intègre, on a montré que $A \simeq S^{-1}\mathbb{R}[X]$ est un anneau principal.

Point (3)

Tout élément $T \in S^{-1}\mathbb{R}[X]$ est de la forme $T = (X^2-1)^{-n}P(X) = (X-1)^{-n}(X+1)^{-n}P(X)$ avec $P(X) \in \mathbb{R}[X]$ et $n \in \mathbb{N}$. En écrivant $P(X) = (X-1)^a(X+1)^b Q(X)$ avec $\mathrm{pgcd}(Q, X^2-1) = 1$ et $a, b \in \mathbb{N}$, on obtient

$$T = (X-1)^k (X+1)^\ell Q(X)$$

avec $k, \ell \in \mathbb{Z}$ et $\mathrm{pgcd}(Q, X^2-1) = 1$. On voit aisément que cette dernière écriture est unique. L'élément T est inversible s'il existe $T_1 = (X-1)^{k_1}(X+1)^{\ell_1}Q_1(X)$ tel que

$$1 = TT_1 = T = (X-1)^{k+k_1}(X+1)^{\ell+\ell_1}Q(X)Q_1(X)$$

Sachant que $\mathrm{pgcd}(QQ_1, X^2-1) = 1$, cela implique que $k + k_1 = \ell + \ell_1 = 0$ et $Q(X)Q_1(X) = 1$. On voit alors que les éléments inversibles de $S^{-1}\mathbb{R}[X]$ sont de la forme $\lambda(X-1)^k(X+1)^\ell$ avec $\lambda \in \mathbb{R} - \{0\}$ et $k, \ell \in \mathbb{Z}$.

Point (4)

Considérons un morphisme d'anneaux $\varphi : \mathbb{R}[X,Y]/(1+Y-YX^2) \to \mathbb{R}$ tel que $\varphi(\lambda) = \lambda, \forall \lambda \in \mathbb{R}$. Si $\pi : \mathbb{R}[X,Y] \to \mathbb{R}[X,Y]/(1+Y-YX^2)$ est la projection, alors $\varphi \circ \pi : \mathbb{R}[X,Y] \to \mathbb{R}$ est un morphisme d'anneaux tel que $\varphi \circ \pi(\lambda) = \lambda, \forall \lambda \in \mathbb{R}$, et vérifiant

$$(\star) \qquad (1+Y-YX^2) \subset \ker(\varphi \circ \pi(\lambda)).$$

Il existe $(a,b) \in \mathbb{R}^2$ tel que $\varphi \circ \pi(P) = P(a,b), \forall P \in \mathbb{R}[X,Y]$. La condition $(\star)$ est équivalente à la relation $b(a^2-1) = 1$.

Conclusion : $\varphi : \mathbb{R}[X,Y]/(1+Y-YX^2) \to \mathbb{R}$ est entièrement déterminé par le choix d'un réel $a \neq \pm 1$, en considérant la relation $\varphi(\overline{P}) = P(a, \frac{1}{a^2-1})$.

Exercice 4

On considère l'anneau $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$. Pour tout entier $n \geq 2$, on considère l'anneau quotient $A_n := \mathbb{Z}[i]/(n)$ et l'anneau de polynômes $\mathbb{Z}/n\mathbb{Z}[X]$.

(1) Quels sont les éléments inversibles de $\mathbb{Z}[i]$?

(2) Montrer que A_n est isomorphe au quotient $\mathbb{Z}/n\mathbb{Z}[X]/(X^2 + 1)$.

(3) En déduire qu'un entier $n \geq 2$ est irréductible dans $\mathbb{Z}[i]$ si et seulement si n est un nombre premier, et si -1 n'est pas un carré de $\mathbb{Z}/n\mathbb{Z}$.

Point (1)

Si $z = x + iy \in \mathbb{Z}[i]$, alors $\bar{z} = x - iy \in \mathbb{Z}[i]$ et $|z|^2 = z\bar{z} \in \mathbb{N}$. Si $z \in \mathbb{Z}[i]$ est inversible, alors $\exists z' \in \mathbb{Z}[i]$ tel que $zz' = 1$. Sachant que que $1 = |zz'|^2 = |z|^2|z'|^2$, on obtient $|z|^2 = 1$, soit $z \in \{\pm 1, \pm i\}$. Réciproquement tous les éléments de $\{\pm 1, \pm i\}$ sont inversibles.

Point (2)

La classe de $x + iy \in \mathbb{Z}[i]$ dans $A_n := \mathbb{Z}[i]/(n)$ est nulle ssi n divise x et y dans $\mathbb{Z}$. Ainsi l'application $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to A_n$, qui associe $x + iy + (n)$ à $(x + n\mathbb{Z}, b + n\mathbb{Z})$ est un isomorphisme de groupes additifs.

Le noyau du morphisme $\mathbb{Z} \to \mathbb{Z}[i]/(n), x \mapsto x + (n)$ est égal à $n\mathbb{Z}$. Ainsi $\mathbb{Z}/n\mathbb{Z}$ est naturellement un sous anneau de $A_n = \mathbb{Z}[i]/(n)$. Considérons le morphisme d'anneaux $\mathrm{ev}_i : \mathbb{Z}/n\mathbb{Z}[X] \to A_n$ défini par la relation $\mathrm{ev}_i(P) = P(i)$. On vérifie tout d'abord que ev_i est surjectif. Pour calculer le noyau de ev_i, on effectue la division euclidienne de $P \in \mathbb{Z}/n\mathbb{Z}[X]$ par le polynôme unitaire $X^2 + 1$, soit $P = (X^2 + 1)Q + aX + b$ avec $a, b \in \mathbb{Z}/n\mathbb{Z}$. Alors $\mathrm{ev}_i(P) = 0$ si et seulement si $a = b = 0$. Ainsi $\ker(\mathrm{ev}_i) = (X^2 + 1)$. Conclusion : ev_i induit un isomorphisme d'anneaux entre $\mathbb{Z}/n\mathbb{Z}[X]/(X^2 + 1)$ et A_n.

Point (2), deuxième preuve

On utilise ici le fait que si $I \subset J$ sont deux idéaux d'un anneau A, alors J/I est un idéal de A/I et le quotient $(A/I)/(J/I)$ est isomorphe à A/J. Ici on travaille avec $A = \mathbb{Z}[X]$ et l'idéal $J = (n, X^2 + 1)$.

<u>1er cas :</u> on prend $I_1 = (n)$, alors $A/I_1 \simeq \mathbb{Z}/n\mathbb{Z}[X]$ et l'idéal J/I_1 est égal à $(X^2 + 1) \subset \mathbb{Z}/n\mathbb{Z}[X]$. Donc $A/J \simeq \mathbb{Z}/n\mathbb{Z}[X]/(X^2 + 1)$.

<u>2ème cas :</u> on prend $I_2 = (X^2 + 1)$, alors $A/I_2 \simeq \mathbb{Z}[i]$ et l'idéal est J/I_2 est égal à $(n) = n\mathbb{Z}[i]$. Donc $A/J \simeq \mathbb{Z}[i]/(n)$.

On a bien démontré que les trois anneaux A/J, $\mathbb{Z}/n\mathbb{Z}[X]/(X^2 + 1)$ et $\mathbb{Z}[i]/(n)$ sont isomorphes.

Point (3)

Un entier $n \geq 2$ est irréductible dans $\mathbb{Z}[i]$ ssi l'anneau quotient $A_n := \mathbb{Z}[i]/(n) \simeq \mathbb{Z}/n\mathbb{Z}[X]/(X^2 + 1)$ est un corps. Il faut tout d'abord que $\mathbb{Z}/n\mathbb{Z}[X]/(X^2 + 1)$ soit intègre : c'est le cas ssi n est un nombre premier. Dans ce cas $\mathbb{Z}/n\mathbb{Z}$ est un corps, et le quotient $\mathbb{Z}/n\mathbb{Z}[X]/(X^2 + 1)$ est un corps ssi $X^2 + 1$ est irréductible dans $\mathbb{Z}/n\mathbb{Z}[X]$. C'est le cas ssi $X^2 + 1$ n'admet pas de racines dans $\mathbb{Z}/n\mathbb{Z}$, c'est à dire si -1 n'est pas un carré de $\mathbb{Z}/n\mathbb{Z}$.