Université Paris Diderot
Master de Mathématiques

Algèbre
Année 2019-20

E. Letellier, L. Merel

CORRiGÉ du CONTRÔLE du 29 novembre 2019

I

Soit i une racine carrée de -1 dans $\mathbf{C}$. On rappelle que l'anneau $\mathbf{Z}[i] = \{a + ib/a, b \in \mathbf{Z}\}$ est un anneau euclidien. On rappelle qu'on a une application $\mathrm{N} : \mathbf{Z}[i] \to \mathbf{Z}$ qui à $a + ib$ associe $a^2 + b^2 = (a + ib)(a - ib)$. Tout $\mathbf{Z}[i]$-module est un groupe et donc un $\mathbf{Z}$-module.

1. Montrer que l'anneau $\mathbf{Z}[X]/(X^2 + 1)$ est isomorphe à $\mathbf{Z}[i]$.

Le morphisme $\mathbf{Z}[X] \to \mathbf{Z}[i]$ donné par $P \mapsto P(i)$ est surjectif de noyau $(X^2 + 1)$.

2. L'idéal de $\mathbf{Z}[X]$ engendré par 2 et X est-il principal ?

Si cet idéal était engendré par $P \in \mathbf{Z}[X]$, on aurait $P|X$ et $P|2$ et donc $P = 1$ ou $P = -1$. Donc l'idéal contiendrait 1. Mais il n'existe pas A, $B \in \mathbf{Z}[X]$ tels que $1 = 2A + XB$. En effet, en spécialisant en $X = 0$, trouve que $2|1$.

3. Donner un exemple de $\mathbf{Z}[X]$-module de type fini et sans torsion qui n'est pas libre.

L'idéal engendré par 2 et X est de type fini, sans torsion (puisque $\mathbf{Z}[X]$ est intègre et donc sans torsion) et n'est pas libre (sinon ce serait un idéal principal).

4. L'anneau $\mathbf{Z}[X]/(X^2 + 1)$ est-il principal ?

Oui puisqu'il est isomorphe à $\mathbf{Z}[i]$, qui est euclidien et donc principal.

5. Tout $\mathbf{Z}[X]$-module de torsion est-il un $\mathbf{Z}$-module de torsion ?

Le module quotient $\mathbf{Z}[X]/(X)$ est de torsion sur $\mathbf{Z}[X]$ (tous les éléments sont annulés par X). Il est isomorphe comme $\mathbf{Z}$-module à $\mathbf{Z}$, qui n'est pas de torsion sur $\mathbf{Z}$.

6. Tout $\mathbf{Z}[i]$-module de torsion est-il un $\mathbf{Z}$-module de torsion ?

Soit m un élément d'un $\mathbf{Z}[i]$-module de torsion. Il existe $a + ib \in \mathbf{Z}[i]$ non nul tel que $(a + ib)m = 0$. On a alors $N(a + ib)m = 0$ et $N(a + ib) = a^2 + b^2 \in \mathbf{Z}$ et non nul. Donc m est de torsion sur $\mathbf{Z}$. Réponse : oui.

7. Tout $\mathbf{Z}[i]$-module de torsion comme $\mathbf{Z}$-module est-il de torsion comme $\mathbf{Z}[i]$-module ?

Soit m un élément de torsion sur $\mathbf{Z}$ d'un $\mathbf{Z}[i]$-module. Il est annulé par un élément non nul de $\mathbf{Z}$, et donc par un élément non nul de $\mathbf{Z}[i]$. Il est donc de torsion sur $\mathbf{Z}[i]$.

8. Tout $\mathbf{Z}[i]$-module libre est-il un $\mathbf{Z}$-module libre ?

Soit $(b_j)_{j\in J}$ une base de d'un $\mathbf{Z}[i]$-module libre M. Alors une base de M comme $\mathbf{Z}$-module est obtenue en réunissant les familles $(b_j)_{j\in J}$ et $(ib_j)_{j\in J}$.

9. Tout $\mathbf{Z}[i]$-module libre de rang fini comme $\mathbf{Z}$-module est-il libre comme $\mathbf{Z}[i]$-module ?

Un $\mathbf{Z}[i]$-module libre comme $\mathbf{Z}$-module est sans torsion. Il est de type fini comme $\mathbf{Z}$-module et donc comme $\mathbf{Z}[i]$-module. Il est donc libre, puisque $\mathbf{Z}[i]$ est principal.

10. Soit $a + ib \in \mathbf{Z}[i]$ un élément irréductible. Montrer que les facteurs invariants de $\mathbf{Z}[i]/(a + ib)$ comme $\mathbf{Z}$-module sont p ou (p, p), avec p nombre premier.

L'anneau quotient $\mathbf{Z}[i]/(a + ib)$ est un corps fini. Notons p sa caractéristique. Il est engendré par l'image de $(1, i)$ et est donc de dimension au plus 2 sur le corps $\mathbf{Z}/p\mathbf{Z}$. Il est donc isomorphe, comme groupe, à $\mathbf{Z}/p\mathbf{Z}$ ou à $(\mathbf{Z}/p\mathbf{Z})^2$.

II

Soit E un $\mathbf{R}$-espace vectoriel de dimension finie $n > 0$. Soit $u \in \operatorname{End}(E)$ tel que $u^2 = -\operatorname{Id}_E$.
11. Montrer que l'anneau $\mathbf{R}[X]/(X^2+1)$ est isomorphe à $\mathbf{C}$.

C'est évident en spécialisant les polynômes en i.

12. Quel est le polynôme minimal de u ?

Comme $u^2 + \operatorname{Id}_E = 0$, ce polynôme divise X^2+1. Le polynôme X^2+1 est irréductible sur $\mathbf{R}$. Donc le polynôme minimal est X^2+1.

13. Que vaut le déterminant de u^2 ? En déduire que n est pair.

On a $\det(u^2) = \det(-\operatorname{Id}_E) = (-1)^n$. Donc $\det(u)^2 = (-1)^n$. Donc n est pair.

14. Montrer que l'application $(P, v) \mapsto P(u)(v)$ fait de E un $\mathbf{R}[X]$-module, puis un $\mathbf{R}[X]/(X^2+1)$-module.

La structure de $\mathbf{R}[X]$-module passe au quotient car X^2+1 annule u.

15. Quels sont les facteurs invariants de E comme $\mathbf{R}[X]$-module ?

Notons $(d_1, ..., d_s)$ ces facteurs invariants. Comme X^2+1 est le polynôme minimal de u, ils divisent tous X^2+1. Ils sont donc tous égaux à X^2+1, puisque ce polynôme est irréductible. Un calcul de dimension donne que $s = n/2$.

16. Munir E d'une structure de $\mathbf{C}$-espace vectoriel de dimension $n/2$.

Puisque E est un $\mathbf{R}[X]/(X^2+1)$-module, c'est un $\mathbf{C}$-espace vectoriel. On vient de voir qu'il est isomorphe à $(\mathbf{R}[X]/(X^2+1))^{n/2}$ et donc à $\mathbf{C}^{n/2}$.

17. Montrer que u agit sur le $\mathbf{C}$-espace vectoriel E par multiplication par i ou par $-i$.

Sur le $\mathbf{R}[X]/(X^2+1)$-module E, u agit par multiplication par X. L'identification entre $\mathbf{R}[X]/(X^2+1)$ et $\mathbf{C}$ associe à X au choix i ou $-i$.

18. Quels sont les facteurs invariants de E comme $\mathbf{C}[T]$-module ?

L'action de u sur le $\mathbf{C}$-espace vectoriel E se traduit par la multiplication par i (ou $-i$, suivant le choix fait). Donc E est isomorphe à $(\mathbf{C}[T]/(T-i))^{n/2}$. Ainsi les $n/2$ facteurs invariants sont tous égaux à $T-i$ ou $T+i$.

19. Soit w un endomorphisme $\mathbf{C}$-linéaire de E. Montrer que cela revient à dire que w est $\mathbf{R}$-linéaire et commute à u.

Pour que w soit $\mathbf{C}$-linéaire il faut et il suffit que w soit $\mathbf{R}$-linéaire et que $w(iv) = iw(v)$. Comme l'action de i (ou $-i$) coïncide avec u, cela revient à dire que w et u commutent.

20. On voit E comme un $\mathbf{C}[T]$-module (et comme un $\mathbf{R}[T]$-module) par l'application $(P, v) \mapsto P(w)(v)$. Supposons que E est isomorphe à $\mathbf{C}[T]/(T-z)$, avec $z \in \mathbf{C}$ non réel de conjugué $\bar{z}$. Montrer que E est ainsi isomorphe à $\mathbf{R}[T]/((T-z)(T-\bar{z}))$ comme $\mathbf{R}[T]$-module.

Le $\mathbf{C}[T]$-module $\mathbf{C}[T]/(T-z)$ est isomorphe à $\mathbf{C}$ par spécialisation des polynômes en z. Donc E est isomorphe, comme $\mathbf{R}[T]$-module, à $\mathbf{C}$ muni de l'endomorphisme multiplication par z. Le polynôme minimal de la multiplication par z est $(T-z)(T-\bar{z}))$ qui est irréductible sur $\mathbf{R}$. Ainsi les facteurs invariants de E comme $\mathbf{R}[T]$-module sont tous $(T-z)(T-\bar{z})$. Comme E est de dimension 2 sur $\mathbf{R}$, il n'y en a qu'un seul. Donc E est ainsi isomorphe à $\mathbf{R}[T]/((T-z)(T-\bar{z}))$ comme $\mathbf{R}[T]$-module.