Université de Poitiers, Année 2023-2024

3^{e} année de Licence de Mathématiques, Anneaux

Corrigé du Contrôle continu du mercredi 6 mars 2024

Questions de cours (5 points)

Soit A un anneau commutatif.

1. Donner la définition d'un polynôme sur A.

   Il fallait donner la définition 1.1 du chapitre "Anneaux de polynômes".

   Un *polynôme sur* A (ou *à coefficients dans* A) est une suite presque nulle $P = (a_i)_{i\in\mathbb{N}} = (a_0, a_1, a_2, ..., a_i, ...)$ d'éléments de A. *Autrement dit, la suite n'a qu'un nombre fini de termes non nuls : il existe un entier $n \in \mathbb{N}$ tel que $a_i = 0_A$ pour tout $i > n$.*

2. On considère la suite $X = (\delta_{1i})_{i\in\mathbb{N}}$ d'éléments de A où δ_{ij} désigne le symbole de Kronecker. Démontrer par récurrence sur n que $X^n = (\delta_{ni})_{i\in\mathbb{N}}$ pour tout $n \in \mathbb{N}$.

   On rappelle que le symbole de Kronecker δ_{mn} *est défini pour tous entiers naturels m et n par $\delta_{mn} = 1_A$ si $m = n$ et $\delta_{mn} = 0_A$ si $m \neq n$. Il s'agissait donc de retrouver la démonstration du lemme 1.9 du chapitre "Anneaux de polynômes".*

   On procède par récurrence sur $n \in \mathbb{N}$ en considérant la proposition $\mathscr{P}(n)$: "$X^n = (\delta_{ni})_{i\in\mathbb{N}}$."

   Initialisation : par définition de la puissance 0, on a $X^0 = 1$ où 1 désigne l'élément neutre pour $\times$ de l'anneau des polynômes sur A, d'où $X^0 = (\delta_{0i})_{i\in\mathbb{N}}$. Ainsi $\mathscr{P}(0)$ est vraie.

   Hérédité : on suppose $\mathscr{P}(n)$ vraie pour $n \in \mathbb{N}$. Alors on a

   $$X^{n+1} = X^n X = (\delta_{ni})_{i\in\mathbb{N}}(\delta_{1i})_{i\in\mathbb{N}} = (\sum_{i+j=k} \delta_{ni}\delta_{1j})_{k\in\mathbb{N}}.$$

   Or on a $\delta_{ni}\delta_{1j} = 1_A$ lorsque $(i, j) = (n, 1)$ et $\delta_{ni}\delta_{1j} = 0_A$ lorsque $(i, j) \neq (n, 1)$, donc on obtient $\sum_{i+j=k} \delta_{ni}\delta_{1j} = \delta_{nn}\delta_{11} = 1_A$ lorsque $k = n + 1$ et $\sum_{i+j=k} \delta_{ni}\delta_{1j} = 0_A$ sinon. On en déduit que $X^{n+1} = (\delta_{(n+1)i})_{i\in\mathbb{N}}$, d'où $\mathscr{P}(n + 1)$.

   Conclusion : $\mathscr{P}(n)$ est vraie pour tout $n \in \mathbb{N}$.

3. Démontrer que, si I est un idéal premier de A, alors A/I est un anneau intègre.

   Il s'agissait de démontrer l'implication de la proposition 3.2 du chapitre "Anneaux intègres".

   Si I est un idéal premier de A, alors I est propre dans A, donc A/I est non nul. Aussi, si pour deux éléments a et b de A, on a $\overline{a}\overline{b} = 0_{A/I}$, alors le produit ab appartient à I, et comme I est premier dans A, l'un des facteurs a ou b appartient à I. On a alors soit $\overline{a} = 0_{A/I}$, soit $\overline{b} = 0_{A/I}$, ce qui montre que A/I est sans diviseur de zéro et que A/I est intègre.

Exercices

Exercice 1 – exercice sur les *Entiers de Gauss* issu du TD (7 points)

Voir la correction faite en TD : il s'agit d'une combinaison des exercices 10 de la fiche "Anneaux, Morphismes" et 9 de la fiche "Idéaux".

Exercice 2 (4,5 points)

Un *anneau local* est un anneau commutatif qui n'a qu'un seul idéal maximal.

1. Soit $m \in \mathbb{N}$. Démontrer que l'anneau $\mathbb{Z}/m\mathbb{Z}$ est local si et seulement si m est de la forme $m = p^n$ pour un nombre premier p et un entier $n \in \mathbb{N}^*$.

   On rappelle que les idéaux maximaux de $\mathbb{Z}$ sont les idéaux de la forme $p\mathbb{Z}$ pour un entier premier p (c'est la proposition 5.3 de chapitre "Anneaux intègres").

   Si m est divisible par deux nombres premiers distincts p et q, alors $m\mathbb{Z}$ est contenu dans $p\mathbb{Z}$ et dans $q\mathbb{Z}$ qui sont des idéaux maximaux de $\mathbb{Z}$. On en déduit que $p\mathbb{Z}/m\mathbb{Z}$ et $q\mathbb{Z}/m\mathbb{Z}$ sont deux idéaux maximaux de l'anneau $\mathbb{Z}/m\mathbb{Z}$, donc $\mathbb{Z}/m\mathbb{Z}$ n'est pas un anneau local.

   Si m n'est divisible par aucun nombre premier, alors on a $m = 1$ et $\mathbb{Z}/m\mathbb{Z}$ est l'anneau nul. Ainsi l'anneau $\mathbb{Z}/m\mathbb{Z}$ n'a pas d'idéal maximal et il n'est donc pas local.

   Il reste le cas où m est divisible par un seul nombre premier. On a alors $m = p^n$ pour un nombre premier p et un entier $n \in \mathbb{N}^*$. Les idéaux de $\mathbb{Z}$ contenant $m\mathbb{Z}$ sont donc ceux de la forme $p^i\mathbb{Z}$ pour $0 \leqslant i \leqslant n$ et $p\mathbb{Z}$ est donc le seul idéal maximal de $\mathbb{Z}$ contenant $m\mathbb{Z}$. On en déduit que $p\mathbb{Z}/m\mathbb{Z}$ est le seul idéal maximal de $\mathbb{Z}/m\mathbb{Z}$, ce qui démontre que l'anneau $\mathbb{Z}/m\mathbb{Z}$ est local.

   À ce stade, on peut conclure que l'anneau $\mathbb{Z}/m\mathbb{Z}$ est local si et seulement si m est de la forme $m = p^n$ pour un nombre premier p et un entier $n \in \mathbb{N}^*$.

2. Soit A un anneau commutatif. Démontrer que ses éléments non inversibles sont ceux qui appartiennent à un idéal maximal de A.

   Si un élément a de A est inversible, alors $1_A = aa^{-1}$ appartient à (a), donc on a $A = (a)$. Ainsi l'élément a n'appartient à aucun idéal propre de A, et il ne peut donc pas appartenir à un idéal maximal de A.

   Si un élément a de A n'est pas inversible, alors 1_A n'appartient pas à $aA = (a)$, et (a) est donc un idéal propre de A. Le théorème de Krull affirme qu'il existe un idéal maximal M de A contenant (a), et donc aussi a.

   Ceci démontre que les éléments non inversibles de A sont ceux qui appartiennent à un idéal maximal de A.

3. En déduire qu'un anneau commutatif est local si et seulement si l'ensemble de ses éléments non inversibles est un idéal.

   Supposons d'abord que A est un anneau local. Soit M le seul idéal maximal de A. D'après la question précédente, les éléments de M sont les éléments non inversibles de A, ils forment donc un idéal de A.

   Réciproquement, supposons que les éléments non inversibles de A forment un idéal de A. Notons I cet idéal. Comme 1_A est un élément inversible de A, l'idéal I est propre dans A. Soit J un idéal propre de A contenant I. Comme J est propre dans A, aucun de ses éléments n'est inversible, ce qui donne $J \subseteq I$, d'où $J = I$ et I est un idéal maximal de A De plus, si M est un idéal maximal de A, alors M est propre dans A et aucun de ses éléments n'est donc inversible, d'où $M \subseteq I$ et, par maximalité de M, on obtient $I = M$. Ainsi I est le seul idéal maximal de A.

Exercice 3 (3,5 points)

Soit $n \in \mathbb{N}^*$. On considère l'anneau $\mathscr{M}_n(K)$ des matrices carrées à coefficients dans K, où K désigne un corps commutatif. Pour tous entiers i et j compris entre 1 et n, on note E_{ij} la matrice, dite *élémentaire*, ayant tous ses coefficients nuls, sauf celui de la i^e ligne et j^e colonne qui vaut 1.

1. Soit $M = (a_{ij})_{1 \leq i,j \leq n} \in \mathscr{M}_n(K)$. Calculer $E_{ij}ME_{kl}$ où $1 \leq i, j, k, l \leq n$.

   La matrice $E_{ij}M$ est la matrice ayant toutes ses lignes nulles, sauf la i^e ligne qui est égale à la j^e ligne de M. La matrice $E_{ij}ME_{kl} = (E_{ij}M)E_{kl}$ a donc aussi toutes ses lignes nulles sauf la i^e ligne. De plus, seul le l^e coefficient de cette ligne est non nul et il vaut a_{jk}. On a donc $E_{ij}ME_{kl} = a_{jk}E_{il}$.

2. Montrer que, si $M \in \mathscr{M}_n(K)$ est une matrice non nulle, alors pour tous i et j tels que $1 \leq i, j \leq n$, il existe des matrices A et B de $\mathscr{M}_n(K)$ telles que $E_{ij} = AMB$.

   Comme $M = (a_{ij})_{1 \leq i,j \leq n}$ est non nulle, il existe des entiers k et l tels que a_{kl} est non nul. D'après la question précédente, on a $E_{ik}ME_{lj} = a_{kl}E_{ij}$, donc $E_{ij} = (\frac{1}{a_{kl}}E_{ik})ME_{lj}$. On a donc $E_{ij} = AMB$ pour $A = \frac{1}{a_{kl}}E_{ik}$ et $B = E_{lj}$.

3. Soit $M \in \mathscr{M}_n(K)$ une matrice non nulle. Montrer que, pour tout $N \in \mathscr{M}_n(K)$, il existe des matrices $(P_{ij})_{1 \leq i,j \leq n}$ et $(Q_{ij})_{1 \leq i,j \leq n}$ dans $\mathscr{M}_n(K)$ telles que $N = \sum_{1 \leq i,j \leq n} P_{ij}MQ_{ij}$.

   Comme M est non nulle, la question précédente dit que, pour tous entiers i et j compris entre 1 et n, il existe des matrices A_{ij} et B_{ij} de $\mathscr{M}_n(K)$ telles que $E_{ij} = A_{ij}MB_{ij}$. Soit $N = (b_{ij})_{1 \leq i,j \leq n}$ une matrice de $\mathscr{M}_n(K)$. Alors on obtient

   $$N = \sum_{1 \leq i,j \leq n} b_{ij}E_{ij} = \sum_{1 \leq i,j \leq n} b_{ij}A_{ij}MB_{ij}.$$

   On en déduit qu'en notant $P_{ij} = b_{ij}A_{ij}$ et $Q_{ij} = B_{ij}$ pour tous entiers i et j compris entre 1 et n, on a bien $N = \sum_{1 \leq i,j \leq n} P_{ij}MQ_{ij}$.

4. En déduire que les seuls idéaux de $\mathscr{M}_n(K)$ sont l'idéal nul et $\mathscr{M}_n(K)$.

   Soit I un idéal non nul de $\mathscr{M}_n(K)$. Alors il y a une matrice non nulle M appartenant à I. Soit $N \in \mathscr{M}_n(K)$. D'après la question précédente, il existe des matrices $(P_{ij})_{1 \leq i,j \leq n}$ et $(Q_{ij})_{1 \leq i,j \leq n}$ dans $\mathscr{M}_n(K)$ telles que $N = \sum_{1 \leq i,j \leq n} P_{ij}MQ_{ij}$.

   Comme I est un idéal de $\mathscr{M}_n(K)$ contenant M, alors on a $P_{ij}MQ_{ij} \in I$ pour tous i et j. Or les idéaux d'un anneau A sont des sous-groupes de $(A, +)$, donc $N = \sum_{1 \leq i,j \leq n} P_{ij}MQ_{ij}$ appartient à I. Ceci montre que toutes les matrices de $\mathscr{M}_n(K)$ appartiennent à I, d'où $I = \mathscr{M}_n(K)$. Ainsi, les seuls idéaux de $\mathscr{M}_n(K)$ sont l'idéal nul et $\mathscr{M}_n(K)$.

5. Si on remplace K par $\mathbb{Z}$, le résultat ci-dessus devient faux. Sans justification, décrire un idéal propre et non nul de $\mathscr{M}_n(\mathbb{Z})$.

   Il suffit de considérer l'ensemble I des matrices de $\mathscr{M}_n(\mathbb{Z})$ ayant tous leurs coefficients pairs. Autrement dit, c'est l'ensemble des matrices M de la forme $M = 2N$ pour $N \in \mathscr{M}_n(\mathbb{Z})$. Il s'agit bien d'un idéal propre et non nul de $\mathscr{M}_n(\mathbb{Z})$.

6. Que peut-on dire d'un anneau *commutatif* A ayant pour seuls idéaux l'idéal nul et A ?

   L'anneau nul a cette propriété. Aussi, d'après la remarque 4.2 du chapitre "Anneaux : généralités", les corps commutatifs ont cette propriété. Réciproquement, si un tel anneau A non nul a pour seuls idéaux l'idéal nul et A, alors l'idéal nul $\{0_A\}$ est un idéal maximal de A, et $A \simeq A/\{0_A\}$ est un corps d'après la proposition 4.2 du chapitre "Anneaux intègres". En conclusion, les anneaux commutatifs ayant cette propriété sont l'anneau nul et les corps commutatifs.