DM 31 : Autour des idéaux

Dans tout ce problème, A désigne un anneau, dont les lois sont selon l'usage notées "+" et ".". On note 0_A et 1_A les éléments neutres pour + et ..
Lorsque I est une partie de A, on dit que I est un idéal à droite de A si et seulement si

— I est non vide ;
— pour tout $x, y \in I$, $x + y \in I$;
— pour tout $i \in I$ et $a \in A$, $ia \in I$.

Lorsque A est commutatif, la notion d'idéal à droite correspond à la notion usuelle d'idéal, étudiée en cours.
Lorsque A est un anneau quelconque, la notion d'idéal à droite ne fait pas partie du cours et toute propriété relative à cette notion devra être démontrée.

Partie I : Idéaux à droite

1°) Montrer qu'une intersection de plusieurs idéaux à droite de A, même en quantité infinie, est un idéal à droite.

2°) On suppose que $(I_n)_{n\in\mathbb{N}}$ est une suite d'idéaux à droite de A, croissante au sens de l'inclusion. Montrer que $\bigcup_{n\in\mathbb{N}} I_n$ est un idéal à droite de A.

3°) Soit B une partie quelconque de A.
On pose $\mathrm{Id}(B) = \left\{ \sum_{i=1}^{n} b_i a_i \ / \ n \in \mathbb{N} \text{ et } \forall i \in \mathbb{N}_n, [b_i \in B \text{ et } a_i \in A] \right\}$.
Montrer que $\mathrm{Id}(B)$ est le plus petit idéal à droite de A contenant B.
On dira que $\mathrm{Id}(B)$ est l'idéal à droite engendré par B.

En particulier, lorsque B est fini, en notant $B = \{b_1, \dots, b_p\}$,
on a $\mathrm{Id}(\{b_1, \dots, b_p\}) = \{\sum_{i=1}^{p} b_i a_i / \ \forall i \in \mathbb{N}_p, a_i \in A\}$ (on ne demande pas de le démontrer).
Par la suite, cet ensemble sera également noté $b_1A + b_2A + \cdots + b_pA$.
En particulier, pour tout $b \in A$, $\mathrm{Id}(\{b\}) = \{ba \ / \ a \in A\} = bA$.

Partie II : Idéaux à droite de $L(E)$

On suppose que $\mathbb{K}$ est un corps et que E est un $\mathbb{K}$-espace vectoriel de dimension finie. On posera $n = \dim(E)$.
On rappelle que $L(E)$ est une $\mathbb{K}$-algèbre. En particulier, $L(E)$ est un anneau pour l'addition et la composition.
Pour tout sous-espace vectoriel F de E, on pose $I_F = \{u \in L(E) \ / \ \mathrm{Im}(u) \subset F\}$.

4°) Montrer que les idéaux à droite de $L(E)$ sont des sous-espaces vectoriels de $L(E)$.

5°) Pour tout sous-espace vectoriel F de E, montrer que I_F est un idéal à droite de $L(E)$.

Lorsque K est un ensemble quelconque, on note $E^{(K)}$ l'ensemble des familles $(x_k)_{k\in K}$ d'éléments de E telles que $\{k \in K \ / \ x_k \neq 0_E\}$ est fini. Ainsi, $E^{(K)}$ est l'ensemble des familles presque nulles de vecteurs de E.
Si de plus $(F_k)_{k\in K}$ est une famille de sous-espaces vectoriels de E, on note $\sum_{k\in K} F_k = \left\{ \sum_{k\in K} x_k \ / \ (x_k)_{k\in K} \in E^{(K)} \text{ et } \forall k \in K, x_k \in F_k \right\}$. Il s'agit du plus petit sous-espace vectoriel de E contenant $\bigcup_{k\in K} F_k$ (on ne demande pas de le démontrer).

Lorsque I est un idéal à droite de $L(E)$, on pose $F_I = \sum_{u\in I} Im(u)$.

6°) Lorsque I est un idéal à droite de $L(E)$, montrer qu'il existe $p \in \mathbb{N}$ et $v_1, \dots, v_p \in I$ tels que $F_I = \sum_{k=1}^{p} \mathrm{Im}(v_k)$.

7°) Lorsque F est un sous-espace vectoriel de E, montrer que $F = F_{(I_F)}$.

8°) Lorsque I est un idéal à droite de $L(E)$, montrer que $I \subset I_{(F_I)}$.

9°) Soit I un idéal à droite de $L(E)$. On sait d'après la question 6 qu'il existe $p \in \mathbb{N}$ et $v_1, \dots, v_p \in I$ tels que $F_I = \sum_{k=1}^{p} \mathrm{Im}(v_k)$. Notons $(e_1, \dots, e_n)$ une base de E.
Soit $u \in I_{(F_I)}$.
Montrer qu'il existe une famille $(x_{j,k})_{\substack{1\le j\le n \\ 1\le k\le p}}$ de vecteurs de E telle que, pour tout $j \in \mathbb{N}_n$, $u(e_j) = \sum_{k=1}^{p} v_k(x_{j,k})$. En déduire que $u = v \circ \varphi$, où v est l'application de E^p dans E définie par $v(x_1, \dots, x_p) = \sum_{k=1}^{p} v_k(x_k)$, pour tout $(x_1, \dots, x_p) \in E^p$, et où φ est l'unique application linéaire de E dans E^p telle que, pour tout $j \in \mathbb{N}_n$, $\varphi(e_j) = (x_{j,1}, \dots, x_{j,p})$.
En déduire que $I = I_{(F_I)}$.

Ceci établit que les idéaux à droite de $L(E)$ sont exactement les I_F, où F est un sous-espace vectoriel quelconque de E.

10°) Montrer que les idéaux à droite de $L(E)$ sont exactement les $\mathrm{Id}(\{p\})$, où $p \in L(E)$.

Partie III : Arithmétique sur un anneau principal

Pour toute la suite de ce problème, on suppose que A est un anneau intègre (donc commutatif). On notera $U(A)$ l'ensemble des éléments inversibles de A.

Lorsque $a, b \in A$, on dit que a divise b et on note $a|b$ si et seulement si il existe $k \in A$ tel que $b = ka$. On dit aussi que a est un diviseur de b et que b est un multiple de a. On dit que a et b sont associés si et seulement si a divise b et b divise a.

11°) Soit $a, b \in A$. On reprend la notation présentée en fin de première partie.
Montrer que $a|b$ si et seulement si $aA \supset bA$.

12°) Soit $a, b \in A$.
Montrer que a et b sont associés si et seulement si il existe $u \in U(A)$ tel que $a = ub$.
Montrer que la relation "être associé à" est une relation d'équivalence sur A.

On fixe $n \in \mathbb{N}$ avec $n \geq 1$. On pose $\mathbb{Z}[i\sqrt{n}] = \{a + ib\sqrt{n} \ / \ a, b \in \mathbb{Z}\}$.

13°) Montrer que $\mathbb{Z}[i\sqrt{n}]$ est un sous-anneau de $\mathbb{C}$.

14°) Déterminer les éléments inversibles de $\mathbb{Z}[i\sqrt{n}]$.

Lorsque $a \in A$, on dit que a est irréductible dans A si et seulement si a n'est pas inversible et si pour tout $u, v \in A$, $a = uv \Longrightarrow (u \in U(A)$ ou $v \in U(A))$.

15°) On suppose que p est un élément irréductible de A.
Montrer que tout élément associé à p est aussi irréductible.

16°) Quels sont les éléments irréductibles de $\mathbb{Z}$?

17°) Montrer que $2 + i\sqrt{5}$, $2 - i\sqrt{5}$ et 3 sont irréductibles dans $\mathbb{Z}[i\sqrt{5}]$.

Lorsque $a, b \in A$, on dit que a et b sont premiers entre eux si et seulement si les seuls diviseurs communs de a et b sont les éléments inversibles.

18°) Soit $p, q \in A$. On suppose que p et q sont irréductibles et que p et q ne sont pas associés. Montrer que p et q sont premiers entre eux.

On rappelle qu'un idéal I de A est principal si et seulement si il existe $b \in A$ tel que $I = \mathrm{Id}(\{b\}) = bA$. On rappelle également que l'anneau intègre A est principal si et seulement si tous ses idéaux sont principaux.

19°) Jusqu'à la fin de cette partie, on suppose que A est principal.

a) Soit $a, b \in A$. Montrer que les propriétés suivantes sont équivalentes :

— (1) : a et b sont premiers entre eux ;

— (2) : $\text{Id}(\{a, b\}) = A$;

— (3) : il existe $u, v \in A$ tel que $ua + vb = 1_A$ (identité de Bezout).

b) Soit $a, b, c \in A$ tels que a est premier avec b et avec c.
Montrer que a est premier avec bc.

c) Soit $a, b, c \in A$ tels que $a | bc$ et a est premier avec b. Montrer que $a | c$.

Partie IV : Anneaux noethériens

Lorsque I est un idéal de A, on dit que I est de type fini si et seulement si il existe une partie B de A telle que $I = \text{Id}(B)$ et telle que B est finie.
On dit que A est un anneau noethérien si et seulement si tous ses idéaux sont de type fini.

20°) Quel résultat du cours permet d'affirmer que $\mathbb{Z}$ est un anneau noethérien ?

21°) Montrer que les propriétés suivantes sont équivalentes :

— (1) : A est noethérien ;

— (2) : Toute suite croissante d'idéaux est stationnaire, c'est-à-dire plus précisément que, pour toute suite $(I_n)_{n \in \mathbb{N}}$ d'idéaux de A, croissante au sens de l'inclusion, il existe $N \in \mathbb{N}$ tel que, pour tout $n \geq N$, $I_n = I_N$.

— (3) : Tout ensemble non vide d'idéaux de A possède au moins un élément maximal au sens de l'inclusion.

22°) Pour tout idéal I de $\mathbb{Z}[i\sqrt{n}]$, on pose $d_0(I) = I \cap \mathbb{Z}$ et
$d_1(I) = \{b \in \mathbb{Z} \ / \ \exists a \in \mathbb{Z}, \ \ a + ib\sqrt{n} \in I\}$.

a) Lorsque I est un idéal de $\mathbb{Z}[i\sqrt{n}]$, montrer que $d_0(I)$ et $d_1(I)$ sont des idéaux de $\mathbb{Z}$ et que $d_0(I) \subset d_1(I)$.

b) Soit I et J deux idéaux de $\mathbb{Z}[i\sqrt{n}]$ tels que $I \subset J$, $d_0(I) = d_0(J)$ et $d_1(I) = d_1(J)$.
Montrer que $I = J$.

c) Montrer que $\mathbb{Z}[i\sqrt{n}]$ est noethérien.

23°) On suppose que A est noethérien. Montrer que tout élément non nul de A se décompose comme un produit d'éléments irréductibles de A, c'est-à-dire plus précisément que, pour tout $a \in A \setminus \{0_A\}$, il existe $u \in U(A)$, $r \in \mathbb{N}$ et des éléments irréductibles $p_1, \ldots, p_r$ de A tels que $a = u \prod_{i=1}^{r} p_i$. *Indication :* On pourra utiliser l'ensemble des idéaux principaux aA tels que $a \in A \setminus \{0\}$ et tels que a ne peut pas s'écrire sous la forme $u \prod_{i=1}^{r} p_i$, où $u \in U(A)$, $r \in \mathbb{N}$ et $p_1, \ldots, p_r$ sont des éléments irréductibles de A.

24°) On suppose que A est principal.
D'après la question 15, l'axiome du choix garantit l'existence d'un ensemble $\mathcal{P}$ d'éléments irréductibles de A tel que, pour tout $q \in A$, si q est irréductible, il est associé à un unique élément de $\mathcal{P}$ (on ne demande pas de démontrer cette affirmation).
Montrer que pour tout $a \in A \backslash \{0\}$, il existe une unique famille $(v_p)_{p \in \mathcal{P}}$ d'entiers naturels, presque nulle (c'est-à-dire que $\{p \in \mathcal{P} \ / \ v_p \neq 0\}$ est fini), et un unique $u \in U(A)$ tels que $a = u \displaystyle\prod_{p \in \mathcal{P}} p^{v_p}$.

25°) Montrer que $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.