

DM n° 16 : Anneaux

Suggestion de travail supplémentaire (à ne pas me rendre) : encore DS 6 de l'an dernier.

Problème 1 – Anneaux factoriels et anneaux noethériens

Le but de ce problème est l'étude de décompositions généralisant dans un anneau commutatif quelconque la décomposition primaire bien connue dans $\mathbb{Z}$. Pour cela, on introduit trois notions de primalité très voisines mais différentes en général : les éléments premiers, les éléments irréductibles et les éléments extrémaux d'un anneau intègre. On montre notamment que dans un anneau principal, ces trois notions coïncident, ce qui est à la base de la preuve d'un résultat classique affirmant qu'un anneau principal est factoriel (c'est-à-dire tel que tout élément se décompose de façon essentiellement unique en produit d'éléments irréductibles). Ce résultat fait l'objet de la partie III. Les deux dernières parties ont pour but de généraliser les décompositions obtenues dans des anneaux plus généraux, appelés anneaux noethériens, en se plaçant cette fois non plus sous l'angle des éléments, mais sous l'angle des idéaux. On démontre notamment dans la dernière partie le théorème de Lasker-Noether, stipulant que dans un anneau noethérien, tout idéal admet une décomposition primaire réduite.

Dans tout le problème, A est un anneau **commutatif**.

Définitions, notations et rappels :

- On désigne par $A^\times$ l'ensemble des éléments inversibles de A , et on rappelle que le produit de A induit sur $A^\times$ une structure de groupe multiplicatif.
- On rappelle qu'un idéal I de A est un sous-groupe additif de A tel que pour tout $a \in A$ et $i \in I$, $ai \in I$.
- Un idéal propre de A est un idéal distinct de $\{0\}$ et de A .
- Soit a dans A . L'idéal engendré par a est noté (a) . Il s'agit du plus petit idéal de A contenant a .
- Plus généralement, si X est une partie de A , on désignera par (X) l'idéal engendré par X , c'est-à-dire le plus petit idéal I tel que $X \subset I$. Par simplification de cette notation, si a et b sont deux éléments de A , on notera (a, b) , (ou $\mathcal{I}(a, b)$ en cas de confusion possible avec un couple) l'idéal engendré par $\{a, b\}$. Si X est une partie de A et $a \in A$, on notera également (a, X) (ou $\mathcal{I}(a, X)$) l'idéal engendré par $X \cup \{a\}$.
- Soit $a, b \in A$. On dit que a divise b , ou que b est un multiple de a (et on note $a \mid b$) s'il existe $c \in A$ tel que $ac = b$. De façon équivalente (d'après les questions préliminaires), $(b) \subset (a)$.
- Un idéal principal I est un idéal engendré par un unique élément, donc tel qu'il existe $a \in A$ tel que $I = (a)$.
- Un anneau principal est un anneau intègre dans lequel tous les idéaux sont principaux.
- Un idéal I de A est de type fini s'il admet un système générateur fini, donc s'il existe $a_1, \dots, a_n$ tel que $I = (a_1, \dots, a_n)$.
- Soit I un idéal de A . On rappelle que les lois de A passent au quotient dans A/I et définissent sur A/I une structure d'anneau.
- On rappelle que les idéaux de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$, $n \in \mathbb{N}$.
- $\mathbb{P}$ désigne l'ensemble des nombres premiers.

On rappelle que dans tout le problème, A est un anneau **commutatif**.

Questions préliminaires

1. Soit $a \in A$. Montrer que $(a) = aA = \{ab, b \in A\}$.
2. Soit I un idéal de A . Montrer que $(a, I) = aA + I = \{ab + i, b \in A, i \in I\}$.

Partie I – Opérations sur un idéal

Les questions de cette partie sont en grande partie indépendantes, et ont pour but de donner des outils qui seront utilisés plus tard.

1. Soit $f : A \longrightarrow B$ un morphisme entre deux anneaux.
 - (a) Soit J un idéal de B , montrer que $f^{-1}(J)$ est un idéal de A .
 - (b) On suppose de plus f surjective. Montrer que pour tout idéal I de A , $f(I)$ est un idéal de B .
2. (a) Soit I un idéal de A , et $\pi : A \rightarrow A/I$ la projection canonique, associant à tout $a \in A$ sa classe $\bar{a}$ dans le quotient A/I . Montrer que π induit (via l'image directe) une bijection de l'ensemble des idéaux de A contenant I dans l'ensemble des idéaux de A/I .
 - (b) Soit $n \in \mathbb{N} \setminus \{0, 1\}$. Décrire les idéaux de $\mathbb{Z}/n\mathbb{Z}$.
3. Soit $(I_k)_{k \in K}$ une famille d'idéaux de A . Montrer que $\bigcap_{k \in K} I_k$ est un idéal de A .
4. Soit $(I_n)_{n \in \mathbb{N}}$ une suite croissante (au sens de l'inclusion) d'idéaux de A . Montrer que $\bigcup_{n \in \mathbb{N}} I_n$ est un idéal de A .
5. Montrer que A est un corps si et seulement si les seuls idéaux de A sont $\{0\}$ et A .
6. On suppose dans cette question que A est intègre. Soit a et b dans A . Montrer que $(a) = (b)$ si et seulement s'il existe $u \in A^\times$ tel que $b = au$. On dit alors que a et b sont associés.

Partie II – Éléments irréductibles, premiers et extrémaux

Dans $\mathbb{Z}$, les nombres premiers (vérifiant le lemme d'Euclide) sont irréductibles, et inversement. Dans d'autres anneaux, les deux notions doivent en général être différenciées. Le but de cette partie est d'étudier un peu le rapport entre la primalité, l'irréductibilité, et une autre notion voisine, l'extrémalité.

On suppose dans cette partie que A est intègre. Soit $a \in A$. On dit que :

- a est premier s'il est non nul, non inversible, et vérifie la propriété d'Euclide : pour tout $(b, c) \in A^2$, si $a \mid bc$ et $a \nmid b$, alors $a \mid c$.
- a est irréductible s'il est non nul, non inversible, et ne peut pas s'écrire comme produit de deux éléments non inversibles.
- a est extrémal s'il est non nul, non inversible, et si pour tout $b \in A$ non divisible par a , $\mathcal{I}(a, b) = A$

Soit I un idéal de A . On dit que :

- I est premier si $I \neq A$ et si pour tout $(a, b) \in A^2$, $ab \in I$ et $a \notin I$ implique $b \in I$
- I est maximal s'il est distinct de A et s'il n'existe pas d'idéal J tel que $I \subsetneq J \subsetneq A$; autrement dit, I est maximal au sens de l'inclusion parmi les idéaux stricts de A .

1. Soit I un idéal de A .
 - (a) Montrer que I est premier si et seulement si A/I est intègre.
 - (b) Montrer que I est maximal si et seulement si A/I est un corps.
2. Décrire les idéaux premiers et les idéaux maximaux de $\mathbb{Z}$.
3. Soit a un élément de A .
 - (a) Montrer que a est premier si et seulement si (a) est un idéal premier non réduit à $\{0\}$.
 - (b) Montrer que a est extrémal si et seulement si $a \neq 0$ et (a) est un idéal maximal.
 - (c) Montrer que a est irréductible si et seulement si (a) est maximal (au sens de l'inclusion) parmi les idéaux principaux propres de A .
4. Soit a un élément de A .
 - (a) Montrer que si a est extrémal, alors a est premier.
 - (b) Montrer que si A est intègre et a est premier, alors a est irréductible.
 - (c) Trouver dans $\mathbb{Z}/6\mathbb{Z}$ un contre-exemple à la propriété précédente lorsque A n'est pas intègre.
5. Montrer que si A est un anneau principal, alors a est extrémal ssi a est premier ssi a est irréductible.
6. Contre-exemples.
 - (a) Soit $P = X$ dans $\mathbb{R}[X, Y]$ (anneau des polynômes à deux indéterminées, obtenues comme sommes de monômes $\alpha_{i,j} X^i Y^j$, $\alpha_{i,j} \in \mathbb{R}$). Montrer que P est premier mais non extrémal.
 - (b) Soit A le sous-ensemble de $\mathbb{R}[X, Y]$ formé des polynômes obtenus comme sommes de monômes $a_{i,j} X^i Y^j$ tels que $i + j$ soit pair.

- i. Montrer que A est un sous-anneau de $\mathbb{R}[X, Y]$.
- ii. Montrer que XY est un élément irréductible de A mais pas premier.

Partie III – Anneaux factoriel

Soit A un anneau.

- On dit que A est atomique s'il est intègre et si tout élément a non nul admet une décomposition en facteurs irréductibles, c'est-à-dire s'il existe $n \geq 0$, des éléments irréductibles $p_1, \dots, p_n$, et un élément inversible u tels que $a = up_1 \dots p_n$. En particulier, le cas $n = 0$ correspond aux éléments inversibles ($a = u$).
- On dit que A est factoriel s'il est atomique, et si de plus, pour tout $a \in A$, la décomposition de a en facteurs irréductibles est essentiellement unique, c'est-à-dire unique à permutation près et à inversibles près. On entend par là que si $a = up_1 \dots p_n = vq_1 \dots q_m$ sont deux décompositions en facteurs irréductibles (u et v étant inversibles), alors $n = m$, et quitte à réindexer les q_i , pour tout $i \in \llbracket 1, n \rrbracket$, p_i et q_i sont associés.

On considère les deux propriétés suivantes :

- $(\mathcal{H}_1)$: toute suite croissante d'idéaux est stationnaire : si $(I_n)_{n \in \mathbb{N}}$ est une suite d'idéaux telle que pour tout $n \in \mathbb{N}$, $I_n \subset I_{n+1}$, alors il existe n_0 tel que pour tout $n \geq n_0$, $I_n = I_{n_0}$.
- $(\mathcal{H}_2)$: tout élément irréductible est premier.

1. Soit A un anneau commutatif intègre vérifiant $(\mathcal{H}_1)$.
 - (a) On suppose qu'il existe $a_0 \in A \setminus \{0\}$ tel que a_0 ne soit pas produit d'éléments irréductibles. Montrer qu'il existe a_1 , qui n'est pas produit d'éléments irréductibles, et tel que $(a_0) \subsetneq (a_1)$.
 - (b) Montrer que A est atomique.
2. Soit A un anneau commutatif intègre vérifiant $(\mathcal{H}_2)$. Pour tout a admettant une décomposition en facteurs irréductibles, on note $n(a)$ le nombre minimal de facteurs irréductibles dans une décomposition de a . En raisonnant par récurrence sur $n(a)$, montrer que pour tout $a \in A$ admettant une décomposition en facteurs irréductibles, cette décomposition est essentiellement unique.
3. Montrer qu'un anneau A vérifie $(\mathcal{H}_1)$ si et seulement si tous ses idéaux sont de type fini.
4. Montrer que les anneaux principaux sont factoriels

Un anneau vérifiant la propriété $(\mathcal{H}_1)$ est appelé anneau noethérien, du nom de la mathématicienne allemande Emmy Noether (1882-1935). Un anneau noethérien est donc un anneau commutatif dont tous les idéaux sont de type fini. Le résultat qu'on a montré dans cette partie est le suivant : tout anneau noethérien intègre est atomique, et si de plus il vérifie $(\mathcal{H}_2)$, il est factoriel.

Partie IV – Idéaux premiers

Le but de la fin de ce problème est de généraliser aux idéaux d'un anneau noethérien A la décomposition primaire d'un entier n de $\mathbb{Z}$, vue sous l'angle des idéaux. Cette généralisation est remarquable parce qu'elle est valide sans hypothèses d'intégrité (contrairement à la propriété atomique de la partie précédente), et qu'elle est valide pour tous les idéaux de A et pas seulement les idéaux principaux. Dans cette partie, on explicite le cas de $\mathbb{Z}$, et on introduit des idéaux d'un type particulier, qui vont nous permettre de définir la décomposition primaire d'un idéal.

1. Soit $n \in \mathbb{N} \setminus \{0, 1\}$, et $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ sa décomposition primaire, les p_i étant des entiers premiers, 2 à 2 distincts, et les α_i étant des entiers strictement positifs.
 - (a) Montrer que

$$(n) = \bigcap_{i \in \llbracket 1, k \rrbracket} (p_i^{\alpha_i}).$$
 - (b) Soit $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$. Soit $I = (p^\alpha)$. Montrer que I vérifie la propriété suivante (avec $A = \mathbb{Z}$) :
 $(\mathcal{H}_3)$: pour tous $a, b \in A$ tels que $ab \in I$ et $b \notin I$, il existe $n \in \mathbb{N}^*$ tel que $a^n \in I$.
 - (c) Réciproquement, montrer que si I est un idéal propre de $\mathbb{Z}$ vérifiant cette propriété, il est de la forme (p^α) , $p \in \mathbb{P}$, $\alpha \in \mathbb{N}$. L'idéal nul vérifie-t-il $(\mathcal{H}_3)$?

Soit, dans toute la suite du problème, A un anneau noethérien.

Soit I un idéal de A . On dit que I est primaire s'il vérifie la propriété $(\mathcal{H}_3)$. Ainsi, on a montré que les idéaux primaires de $\mathbb{Z}$ sont exactement $\{0\}$, les (p^α) , et (trivialement) $\mathbb{Z}$ lui-même.

2. Montrer que $\{0\}$ est un idéal primaire de A si et seulement si les diviseurs de 0 sont nilpotents.

Pour $a \in A$ et I un idéal de A , on note $\varphi_{a,I}$ l'application de A/I dans lui-même définie par :

$$\varphi_{a,I}(\bar{b}) = \overline{ab}.$$

3. Montrer que I est un idéal primaire si et seulement si pour tout $a \in A$, $\varphi_{a,I}$ est soit injective, soit nilpotente (au sens de la composition itérée).

Pour tout idéal primaire I , on note $P_I = \{a \in A \mid \varphi_{a,I} \text{ est nilpotente}\}$.

4. (a) Soit I un idéal primaire. Montrer que P_I est un idéal premier de A .
(b) Déterminer P_I lorsque $A = \mathbb{Z}$ et $I = (p^\alpha)$, $p \in \mathbb{P}$, $\alpha \geq 1$.

Soit P un idéal premier, et I un idéal primaire. On dira que I est un idéal P -primaire si $P_I = P$.

5. Soit P un idéal premier. Montrer que si $I_1, \dots, I_n$ sont des idéaux P -primaires, alors $\bigcap_{k=1}^n I_k$ est un idéal P -primaire.
6. Soit J un idéal quelconque de A . Montrer que si J s'écrit comme intersection finie d'idéaux primaires, alors on peut trouver des idéaux primaires $I_1, \dots, I_n$ tels que les P_{I_k} soient 2 à 2 distincts, et tels que

$$J = \bigcap_{k=1}^n I_k.$$

Une décomposition $J = \bigcap_{k=1}^n I_k$ telle que dans la question 5(b) et minimale (dans le sens où l'égalité n'est plus vérifiée en enlevant l'un des I_k) est appelée décomposition primaire réduite de l'idéal J . Ainsi, en enlevant les éventuels I_k inutiles dans la décomposition de 5(b), on a montré que si J est une intersection finie d'idéaux primaires, alors J admet une décomposition primaire réduite.

Partie V – Décomposition primaire dans un anneau noethérien (théorème de Lasker-Noether).

On termine ce problème en montrant que tout idéal d'un anneau noethérien admet une décomposition primaire réduite (théorème de Lasker-Noether). On se donne donc un anneau noethérien A . Il suffit, d'après la partie précédente, de montrer que tout idéal J est une intersection d'idéaux primaires.

1. Soit J un idéal de A . Montrer que pour tout $a \in A$, l'application $\varphi_{a,J}$ définie dans la partie précédente est un morphisme de groupes additifs, et que $\text{Ker}(\varphi_{a,J})$ et $\text{Im}(\varphi_{a,J})$ sont des idéaux de A/J .
2. Soit $\varphi : (G, +) \rightarrow (G, +)$ un morphisme de groupe. Montrer que $\text{Ker}(\varphi) = \text{Ker}(\varphi^2)$ si et seulement si $\text{Ker}(\varphi) \cap \text{Im}(\varphi) = \{0\}$.
3. On suppose qu'il existe dans A des idéaux n'admettant pas de décomposition primaire.
 - (a) Montrer qu'il existe un idéal J maximal au sens de l'inclusion parmi les idéaux n'admettant pas de décomposition primaire.
 - (b) En considérant la suite $(\text{Ker}(\varphi_{a,J}^n))_{n \in \mathbb{N}^*}$ pour a convenablement choisi dans A (l'exposant étant à prendre au sens de la composition), trouver un morphisme de groupes additifs $\varphi : A/J \rightarrow A/J$ tel que $\text{Ker}(\varphi) \cap \text{Im}(\varphi) = \{\bar{0}\}$ et tel que $\text{Ker}(\varphi) \neq \{\bar{0}\}$ et $\text{Im}(\varphi) \neq \{\bar{0}\}$.
 - (c) Trouver une contradiction et conclure.

On peut montrer que la décomposition primaire réduite est unique, mais cela nécessite des techniques un peu plus fines.

4. (a) Soit $n \geq 2$. Justifier que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau noethérien.
(b) Exprimer, en fonction des facteurs de la décomposition primaire de n , la décomposition primaire réduite de l'idéal $\{0\}$ de $\mathbb{Z}/n\mathbb{Z}$.