

DM n° 16 : Anneaux

Corrigé du problème 1 – Anneaux factoriels et anneaux noethériens

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

Questions préliminaires

1. Par définition (a) est le plus petit idéal de A contenant a .
 - Par stabilité renforcée de l'idéal (a) , puisque $a \in (a)$, pour tout $b \in A$, $ab \in (a)$. Ainsi, $aA \subset (a)$.
 - Par ailleurs, aA est bien un idéal de A :
 - * $0 = a0 \in A$ et si x et y sont dans aA , on peut écrire $x = ab$ et $y = ac$, avec b et c dans A . Ainsi, $x - y = a(b - c) \in aA$. On en déduit que aA est un sous-groupe additif de A .
 - * Si $b \in aA$ et $c \in A$, on peut écrire $b = ad$, avec $d \in A$, et donc $bc = adc \in aA$. Ainsi, aA vérifie la propriété de stabilité multiplicative renforcée
 - Ainsi, par minimalité de (a) , on a bien $(a) = aA$.
2. Le raisonnement est le même :
 - La structure d'idéal (donc stabilité multiplicative renforcée et stabilité additive) nous assure que $aA + I \subset (a, I)$.
 - Montrons que $aA + I$ est un idéal :
 - * $0 = a0 + 0 \in aA + I$.
 - * Soit $x, y \in aA + I$. Il existe donc $b, c \in A$ et $i, j \in I$ tels que

$$x = ab + i \quad \text{et} \quad y = ac + j \quad \text{donc:} \quad x - y = a(b - c) + (i - j).$$

Or, $b - c \in A$, et I étant un idéal, $i - j \in I$. On a donc $x - y \in aA + I$. On déduit de ce point et du précédent que $aA + I$ est un sous-groupe additif de A .

- * Soit $x \in aA + I$, et $c \in A$. Il existe $b \in A$ et $i \in I$ tels que $x = ab + i$. On a alors

$$xc = abc + ic.$$

Or, $bc \in A$ et $ic \in I$ (car I est un idéal), donc $xc \in aA + I$.

- * Ainsi, $aA + I$ est un idéal de A .
- Comme $aA + I$ contient de toute évidence a et I , par minimalité de (a, I) , on obtient

$$(a, I) = aA + I$$

Partie I – Opérations sur un idéal

1. Soit $f : A \rightarrow B$ un morphisme entre deux anneaux.
 - (a) Soit J un idéal de B .
 - Puisque f est un morphisme de groupes additifs, d'après le cours, $f^{-1}(J)$ est un sous-groupe de $(B, +)$.
 - Soit $x \in f^{-1}(J)$ et $a \in A$. On a alors $f(x) \in J$, donc, puisque J est un idéal, $f(a)f(x) \in J$, soit $f(ax) \in J$, par propriété de morphisme. On en déduit que $ax \in f^{-1}(J)$, donc $f^{-1}(J)$ vérifie la propriété de stabilité renforcée.
 - Ainsi, $f^{-1}(J)$ est un idéal de A .
 - (b) On suppose de plus f surjective. Soit I un idéal de A .
 - Puisque f est un morphisme de groupes additifs, d'après le cours, $f(I)$ est un sous-groupe de $(A, +)$.

- Soit $x \in f(I)$ et $b \in B$. Il existe $i \in I$ tel que $x = f(i)$, et puisque f est surjective, on dispose également de $a \in A$ tel que $f(a) = B$. Or, I étant un idéal, $ai \in I$, donc $f(ai) \in f(I)$. Or

$$f(ai) = f(a)f(i) = bx,$$

donc $bx \in I$.

- Ainsi, $f(I)$ est un idéal de B .

2. (a) Notons $\mathcal{I}_{A,I}$ l'ensemble des idéaux de A contenant I et $\mathcal{I}_{A/I}$ l'ensemble de tous les idéaux de A/I .

- L'application π induit, via l'image directe, une application de $\mathcal{I}_{A,I}$ dans $\mathcal{I}_{A/I}$ d'après la question 1(b) (en effet, π est un morphisme d'anneaux surjectif).
- De même, l'image réciproque π^{-1} induit une application de $\mathcal{I}_{A/I}$ dans $\mathcal{I}_{A,I}$ (l'image réciproque d'un idéal J contient bien I puisque $0 \in J$ et $\pi^{-1}(0) = I$). On va montrer que l'image directe et l'image réciproque sont réciproques l'une de l'autre sur ces ensembles.
- Soit J un idéal de A tel que $I \subset J$. Alors

$$J \subset \pi^{-1}(\pi(J)).$$

De plus, soit $j \in \pi^{-1}(\pi(J))$. On a donc $\pi(j) \in \pi(J)$. Il existe donc $j' \in J$ tel que $\pi(j) = \pi(j')$, donc $\pi(j - j') = 0$, donc $j - j' = i$, puis $j = i + j'$. Puisque $I \subset J$, on en déduit que $j \in J$. Ainsi

$$\pi^{-1}(\pi(J)) \subset J, \quad \text{puis:} \quad J = \pi^{-1}(\pi(J)).$$

- Soit J un idéal de A/I . Puisque π est surjective, on a directement

$$\pi(\pi^{-1}(J)) = J.$$

- Ainsi, l'image directe et l'image réciproque de π induisent deux applications réciproques l'une de l'autre de $\mathcal{I}_{A,I}$ dans $\mathcal{I}_{A/I}$.

(b) Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont donc les images par la projection des idéaux de \mathbb{Z} contenant $n\mathbb{Z}$, c'est-à-dire des $d\mathbb{Z}$, pour tout $d \mid n$. Ainsi, les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$, $d \mid n$.

3. C'est une vérification facile.

- D'après le cours, $\bigcap_{k \in K} I_k$ est un sous-groupe de $(A, +)$ en tant qu'intersection de sous-groupes.
- Soit $a \in A$ et $i \in \bigcap_{k \in K} I_k$. Alors, pour tout $k \in K$, $i \in I_k$. Comme I_k est un idéal de A , $ai \in I_k$, donc

$$ai \in \bigcap_{k \in K} I_k.$$

- $\bigcap_{k \in K} I_k$ est donc bien un idéal de A .

4. Soit $(I_n)_{n \in \mathbb{N}}$ une suite croissante (au sens de l'inclusion) d'idéaux de A .

- D'après le cours, l'union d'une chaîne de sous-groupes est un sous-groupe. Or, la croissance de la suite nous assure la propriété de chaîne, donc $\bigcup_{n \in \mathbb{N}} I_n$ est un sous-groupe additif de $(A, +)$. En effet, pour étudier la stabilité par différence pour $x - y$, avec x et y dans l'union, la propriété de chaîne nous permet de nous placer dans un I_n contenant à la fois x et y (petite précision à donner à l'écrit, le résultat utilisé n'étant pas explicitement au programme).
- Soit $a \in A$ et $i \in \bigcup_{n \in \mathbb{N}} I_n$. Il existe $n \in \mathbb{N}$ tel que $i \in I_n$. On a alors $ai \in I_n$, donc

$$ai \in \bigcup_{n \in \mathbb{N}} I_n.$$

- Ainsi, $\bigcup_{n \in \mathbb{N}} I_n$ est un idéal de A .

5. • On suppose que A est un corps. Soit I un idéal non nul de A . Alors il existe $a \in I$ tel que $a \neq 0$. Comme A est un corps, a est inversible, et comme I est un idéal, $1 = aa^{-1} \in I$. Ainsi,

$$A = 1A = (1) \subset I \quad \text{donc:} \quad \boxed{I = A}$$

- Réciproquement, supposons que les seuls idéaux de A soit $\{0\}$ et A . Soit $a \neq 0$ dans A . Alors $(a) \neq \{0\}$, donc $(a) = A$. En particulier, $1 \in (a) = aA$, donc il existe $b \in A$ tel que $ab = 1$. On en déduit que a est inversible. Tous les éléments non nuls de A étant inversibles, $\boxed{A \text{ est un corps}}$.
6. C'est un résultat vu en cours, mais on le refait pour bien insister sur l'importance de l'intégrité.
- Supposons $(a) = (b)$. Si $a = 0$, $(a) = 0$, et nécessairement $b = 0$, et le résultat est prouvé. On peut supposer $a \neq 0$. Alors $aA = bA$. Ainsi, $a \in bA$, et on dispose de $c \in A$ tel que $a = bc$. De même, on dispose de d tel que $b = ad$. Par conséquent, en combinant les deux égalités, $a = acd$, et comme $a \neq 0$, il est régulier (par intégrité de A). On en déduit que $cd = 1$, donc c et d sont inversibles. On obtient le résultat en posant $u = d$.
 - Réciproquement, si $b = au$ avec u inversible, pour tout $x \in (b)$, on dispose de $c \in A$ tel que $x = bc = auc \in (a)$. Donc $(b) \subset (a)$. L'inversibilité de u permet d'échanger les rôles de a et b , et on a alors aussi $(a) \subset (b)$, d'où l'égalité.
- Ainsi, $\boxed{(a) = (b) \text{ si et seulement si il existe } u \in A^\times \text{ tel que } b = au}$.

Partie II – Éléments irréductibles, premiers et extrémaux

1. Soit I un idéal de A .

- (a) • Supposons I premier. Alors puisque $I \neq A$, A/I n'est pas l'anneau nul. De plus, soit $\bar{a}, \bar{b} \in A/I$ tels que $\bar{a}\bar{b} = 0$ et $\bar{a} \neq 0$. Ainsi, $ab \in I$ et $a \notin I$. Puisque I est premier, il en résulte que $b \in I$, donc $\bar{b} = 0$. Ainsi, $\boxed{A/I \text{ est intègre}}$.
- Supposons A/I intègre. Par convention, l'anneau A n'est pas intègre. Ainsi, $I \neq A$. Soit $a, b \in A$ tels que $a \notin I$ et $ab \in I$. Alors $\bar{a} \neq 0$ et $\bar{a}\bar{b} = 0$. Par intégrité de A/I , il en résulte que $\bar{b} = 0$, donc $b \in I$. Ainsi, $\boxed{I \text{ est un idéal premier}}$.
- (b) Les idéaux de A/I sont en bijection, d'après I-2a, avec les idéaux de A contenant I . Ainsi, d'après la question I-5, A est un corps ssi A/I possède uniquement deux idéaux, ssi A possède uniquement deux idéaux contenant I (qui sont I et A lui-même), ssi il n'existe pas d'idéal intermédiaire à I et A ssi I est un idéal maximal de A . Ainsi, $\boxed{I \text{ est maximal si et seulement si } A/I \text{ est un corps}}$.

2. Soit $n\mathbb{Z}$ un idéal de \mathbb{Z}

- $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier, donc $\boxed{\text{les idéaux maximaux de } \mathbb{Z} \text{ sont exactement les } n\mathbb{Z}, n \in \mathbb{P}}$.
 - * Si n est premier, $\mathbb{Z}/n\mathbb{Z}$ étant un corps, il est intègre, donc $n\mathbb{Z}$ est un idéal premier.
 - * Si n est composé, disons $n = ab$, $a, b > 1$, alors \bar{a} et \bar{b} sont non nuls dans $\mathbb{Z}/n\mathbb{Z}$, mais leur produit est nul. Ainsi, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.
 - * $1\mathbb{Z}$ n'est pas un idéal premier, car un idéal premier est strict par définition
 - * Enfin, $0\mathbb{Z} = \{0\}$ est bien un idéal premier, puisque $\mathbb{Z} = \mathbb{Z}/\{0\}$ est intègre.
- Ainsi, $\boxed{\text{les idéaux premiers de } \mathbb{Z} \text{ sont les } n\mathbb{Z}, \text{ avec } n = 0 \text{ ou } n \in \mathbb{P}}$.

3. Soit a un élément de A .

- (a) • Supposons a premier.
- * Il est alors non nul par définition, donc $(a) \neq \{0\}$.
 - * De plus, $(a) \neq A$, sinon, $(a) = (1)$ et a et 1 seraient associés. Comme l'anneau est intègre, cela contredit le fait que a n'est pas inversible.
 - * De plus, soit $b, c \in (a)$ tels que $b \notin (a)$ et $bc \in (a)$. Alors $a \mid bc$ et $a \nmid b$. Puisque a est premier, il en résulte que $a \mid c$, donc $c \in (a)$. Cela correspond bien à la définition d'un idéal premier.
- Supposons que l'idéal (a) est premier non nul.
 - * Alors $a \neq 0$, et a est non inversible (car $(a) \neq A$).
 - * Soit b, c tels que $a \mid bc$ et $a \nmid b$. Alors $bc \in (a)$ et $b \notin (a)$, donc $c \in (a)$ (car l'idéal est premier), d'où $a \mid c$.

* Donc a est premier.

Ainsi, a est premier si et seulement si (a) est un idéal premier non réduit à $\{0\}$.

- (b) • Supposons a extrémal. Puisque a est non nul non inversible, (a) est un idéal propre de A . Si (a) n'est pas maximal, il existe I tel que $(a) \subsetneq I \subsetneq A$. Ainsi, soit $b \in I \setminus (a)$, on a donc :

$$\mathcal{I}(a, b) \subset I \subsetneq A,$$

et puisque $b \notin (a)$, b n'est pas divisible par a . Cela contredit la définition d'un élément extrémal. Ainsi, (a) est maximal.

- Supposons (a) maximal et $a \neq 0$. Alors (a) est par définition un idéal propre de A . En particulier, cela implique que a est non inversible. De plus, soit b non divisible par a , c'est-à-dire $b \notin (a)$. Alors $(a) \subsetneq \mathcal{I}(a, b)$. La maximalité de (a) impose alors que $\mathcal{I}(a, b) = A$.

Ainsi, a est extrémal si et seulement si $a \neq 0$ et (a) est un idéal maximal.

- (c) • Supposons (a) non maximal parmi les idéaux principaux propres.
- * Si (a) n'est pas un idéal propre, a est nul ou inversible, donc a n'est pas irréductible.
 - * Sinon, (a) étant principal propre et non maximal parmi les idéaux principaux propres, il existe (b) tel que $(a) \subsetneq (b) \subsetneq A$. En particulier $b \mid a$, d'où l'existence de c tel que $a = bc$. De plus, a et b ne sont pas associés, (l'inclusion étant stricte), donc c n'est pas inversible. L'élément b non plus n'est pas inversible (sinon on aurait $(b) = A$). Ainsi, a n'est pas irréductible.
- Supposons a non irréductible.
- * Si a est nul ou inversible, $(a) = \{0\}$ ou $(a) = A$, donc (a) n'est pas un idéal propre.
 - * Sinon, il existe b et c non inversibles tels que $a = bc$. Ainsi, $(a) \subset (b)$. Si l'inclusion est une égalité, a et b sont associés, donc, l'anneau étant intègre, il existe $u \in A^\times$ tel que $a = bu$. Ainsi, $bu = bc$, et l'intégrité amène $u = c$ (b étant non nul, puisque $a \neq 0$). Or c est non inversible, d'où une contradiction. Par conséquent, $(a) \subsetneq (b)$, et (a) n'est pas maximal parmi les idéaux principaux propres.

Ainsi, a est irréductible si et seulement si (a) est maximal parmi les idéaux principaux propres de A .

4. Soit a un élément de A .

- (a) Si a est extrémal, alors, d'après 3(b), $(a) \neq \{0\}$ et (a) est maximal. On déduit de la question 1(b) que $A/(a)$ est un corps, donc intègre. On déduit de la question 1(a) que (a) est un idéal premier (et non nul), donc d'après 3a, a est premier.
- (b) On suppose A intègre et a premier. Alors a est non nul et non inversible. Supposons que a ne soit pas irréductible. Il existe alors b et c non inversibles tels que $a = bc$. En particulier, a divise bc . Puisque a est premier, a divise b ou a divise c . Disons a divise b . On a donc $(b) \subset (a)$. Mais on a également $(a) \subset (b)$ puisque $a = bc$. Ainsi, a et b sont associés, ce qui, comme dans la question 3c implique que c est inversible du fait de l'intégrité de A , d'où une contradiction. Ainsi, a est irréductible.
- (c) Dans $A = \mathbb{Z}/6\mathbb{Z}$, 2 est premier. En effet,

$$(2) = 2\mathbb{Z}/6\mathbb{Z}, \quad \text{et} \quad A/(2) \simeq \mathbb{Z}/2\mathbb{Z},$$

qui est un corps, donc intègre. En revanche, il n'est pas irréductible, puisque $3 = 2 \times 4$, et 2 et 4 ne sont pas inversibles (puisque non premiers avec 6).

5. Soit A un anneau principal. Alors la maximalité parmi les idéaux principaux stricts équivaut à la maximalité parmi tous les idéaux stricts (puisque les idéaux sont tous principaux). On déduit alors de 3(a) et 3(c) que a est extrémal ssi a est irréductible. Par ailleurs, les deux implications démontrées en 4(a) et 4(b) sont vraies, puisqu'un anneau principal est intègre. Donc, dans un anneau principal,

$$a \text{ est extrémal ssi } a \text{ est premier ssi } a \text{ est irréductible.}$$

6. Contre-exemples.

- (a) • $P = X$ n'est pas extrémal, car (X) n'est pas un idéal maximal. On peut considérer par exemple (X, Y) , qui inclut strictement (X) , mais n'est pas égal à $\mathbb{R}[X]$ tout entier (les polynômes constants ne sont pas dans (X, Y)).

- En revanche, P est premier. En effet, supposons que X ne divise ni $Q(X, Y)$ ni $R(X, Y)$. On peut alors regrouper tous les monômes divisibles par X et factoriser par X . Les autres monômes ne dépendent que de Y et définissent donc un polynôme d'une seule indéterminée Y . Ainsi, on peut écrire :

$$Q(X, Y) = X\tilde{Q}(X, Y) + S(Y) \quad \text{et} \quad R(X, Y) = X\tilde{R}(X, Y) + T(Y).$$

En effectuant le produit,

$$Q(X, Y)R(X, Y) = X(X\tilde{Q}(X, Y)\tilde{R}(X, Y) + \tilde{Q}(X, Y)T(Y) + \tilde{R}(X, Y)S(Y)) + S(Y)T(Y).$$

Or, puisque S et T sont non nuls (car Q et R non divisibles par X), ST est non nul (son degré étant la somme des degrés de S et T). Ainsi, QR n'est pas divisible par X .

Cela montre bien que $\boxed{P \text{ est premier}}$.

- (b) Soit A le sous-ensemble de $\mathbb{R}[X, Y]$ formé des polynômes obtenus comme sommes de monômes $a_{i,j}X^iY^j$ tels que $i + j$ soit pair.

- Le polynôme constant 1 (neutre multiplicatif) est dans A (somme vide de tels monômes)
- Si P et Q sont dans A , leur différence aussi, puisque constituée uniquement de monômes $a_{i,j}X^iY^j$ (provenant de P) et $-b_{i,j}X^iY^j$ (provenant de Q), avec $i + j$ pair.
- Si P et Q sont dans A , PQ est formé de monômes $a_{i,j}b_{k,\ell}X^iY^jX^kY^\ell$, avec $i + j$ et $k + \ell$ pairs (obtenus en formant le produit des monômes de P et des monômes de Q). Ces monômes se réécrivent $a_{i,j}b_{k,\ell}X^{i+k}Y^{j+\ell}$, et R

$$(i + k) + (j + \ell) = (i + j) + (k + \ell)$$

est pair en tant que somme de deux entiers pairs. Ainsi, PQ est encore dans A .

- On en déduit que $\boxed{A \text{ est un sous-anneau de } \mathbb{R}[X, Y]}$.
- On commence par une remarque sur les degrés des polynômes de 2 indéterminées. On remarque que si P est un polynôme de $\mathbb{R}[X]$, on peut regrouper les monômes suivant leur degré en Y , et obtenir une représentation :

$$P(X, Y) = \sum_{k=0}^d a_k(X)Y^k,$$

les coefficients $a_k(X)$ étant eux-mêmes des polynômes en X uniquement. C'est en fait ainsi qu'on définit, par récurrence, les polynômes à plusieurs indéterminées :

$$\mathbb{R}[X_1, \dots, X_{n+1}] = \mathbb{R}[X_1, \dots, X_n][X_{n+1}],$$

et pour deux variables, en particulier :

$$\mathbb{R}[X, Y] = \mathbb{R}[X][Y].$$

Ainsi, $\mathbb{R}[X, Y]$ peut être vu comme l'anneau des polynômes en Y , à coefficients dans $\mathbb{R}[X]$. Cette construction est valide plus généralement sur tout anneau A , pas seulement \mathbb{R} .

Ainsi, on peut considérer le degré $\deg_Y(P)$ de P par rapport à Y , comme étant le degré de ce polynôme en Y à coefficients dans $\mathbb{R}[X]$. Les règles usuelles pour le produit s'appliquent alors, du fait de l'intégrité des anneaux de polynômes (car \mathbb{R} lui-même est intègre, et cette propriété se propage lorsqu'on ajoute des indéterminées). En effet, l'intégrité nous assure que le produit des monômes dominants (en Y) de P et Q n'est pas nul. Ainsi

$$\deg_Y(PQ) = \deg_Y(P) + \deg_Y(Q).$$

Évidemment, on peut intervertir le rôle de X et Y et définir de même $\deg_X(P)$, qui vérifie les mêmes propriétés relatives au produit.

- Montrons maintenant que XY est irréductible. En effet, si XY s'écrit $XY = PQ$, avec P et Q non inversibles, alors

$$\deg_Y(PQ) = 1 \quad \text{et} \quad \deg_X(PQ) = 1,$$

donc

$$\deg_Y(P) + \deg_Y(Q) = 1 \quad \text{et} \quad \deg_X(P) + \deg_X(Q) = 1.$$

Quitte à intervertir P et Q , on peut supposer que $\deg_Y(P) = 1$ et $\deg_Y(Q) = 0$. Puisque les monômes ont tous un degré total pair, P doit faire intervenir l'indéterminée X . Ainsi, on a aussi $\deg_X(P) = 1$ et par conséquent $\deg_X(Q) = 0$.

On en déduit que Q est un polynôme constant non nul. C'est donc un élément inversible de $\mathbb{R}[X, Y]$.

Cela montre bien que XY est irréductible.

- Il n'est pas premier, car XY divise X^2Y^2 , mais il ne divise ni X^2 ni Y^2 .

Partie III – Anneaux factoriel

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. En particulier, il n'est pas lui-même irréductible (sinon il serait produit à un terme), ni inversible (produit à 0 terme). Ainsi, il peut s'écrire sous la forme $a_0 = b_0 c_0$, avec b_0 et c_0 non inversibles. Puisque a_0 n'est pas produit d'irréductibles, au moins un des deux éléments b_0 et c_0 ne peut pas s'écrire comme produit d'irréductible, disons b_0 . On pose $a_1 = b_0$. Comme a_1 divise a_0 , $(a_0) \subset (a_1)$. Comme c_0 n'est pas inversible, puisque A est intègre, l'argument donné en question II-3(c) montre que $(a_0) \subsetneq (a_1)$.

- (b) Avec les mêmes hypothèses que dans la question précédente, puisque a_1 n'admet pas de décomposition en produit d'éléments irréductibles, on peut itérer la construction de la question 1(a), et définir une suite $(a_n)_{n \in \mathbb{N}}$ strictement croissante d'idéaux tels que pour tout $n \in \mathbb{N}$, a_n ne soit pas décomposable en produit de facteurs irréductibles.

Cela contredit l'hypothèse (\mathcal{H}_1) . Ainsi, l'hypothèse faite en début de question 1(a), à savoir l'existence de a_0 , est fautive. On en déduit que A est atomique.

Remarque : l'hypothèse (\mathcal{H}_1) est un peu plus forte que nécessaire. On peut se contenter de l'hypothèse : (\mathcal{H}'_1) : toute suite croissante d'idéaux principaux est stationnaire.

2. On montre l'unicité de la décomposition en raisonnant par récurrence sur $n(a)$, le nombre minimal de facteurs irréductibles dans une décomposition de a .

- Soit a tel que $n(a) = 0$. Ceci équivaut à dire que a est inversible. S'il existe une autre décomposition que la décomposition triviale, elle s'écrit $a = up_1 \dots p_n$, avec $n > 0$. On aurait alors :

$$p_1(p_2 \dots p_n u a^{-1}) = 1,$$

et donc p_1 est inversible, ce qui contredit l'irréductibilité.

Ainsi, la décomposition de a est unique.

- Soit $n \in \mathbb{N}^*$. On suppose que pour tout $a \in A$ admettant au moins une décomposition en facteur irréductible et tel que $n(a) < n$, cette décomposition est essentiellement unique. Soit a tel que $n(a) = n$. Considérons une décomposition minimale

$$a = up_1 \dots p_n$$

avec $n = n(a)$, et

$$a = vq_1 \dots q_m,$$

une autre décomposition, u et v étant inversibles, les p_i et les q_j étant irréductibles. Puisque p_1 est irréductible, d'après (\mathcal{H}_2) , p_1 est premier. Or, p_1 divise a , et v est inversible, donc p_1 divise $q_1 \dots q_m$. Par définition d'un élément premier (propriété d'Euclide, étendue à m termes par récurrence triviale), il existe $j \in \llbracket 1, m \rrbracket$

tel que $p_1 \mid q_j$. Il existe donc $r \in A$ tel que $p_1 r = q_j$. Puisque q_j est irréductible, ceci n'est possible que si $r \in A^\times$, donc p_1 et q_j sont associés

Quitte à réindexer les q_j , on peut supposer que $q_j = 1$. L'intégrité de A nous permet alors de simplifier par $p_1 = q_1$, et on obtient l'égalité :

$$up_2 \dots p_n = vq_2 \dots q_m$$

Soit $b = up_2 \dots p_n$. Ainsi, $n(b) \leq n - 1$, donc on peut lui appliquer l'hypothèse de récurrence, qui amène $m = n$, et le fait que quitte à réindexer les q_i , pour tout $i \in \llbracket 2, n \rrbracket$, p_i et q_i sont associés. Comme on l'avait aussi obtenu pour $i = 1$, les deux décompositions considérées de a sont essentiellement les mêmes.

Ainsi, toute décomposition de a est essentiellement la même que la décomposition minimale qu'on s'est donnée et donc, si elle existe, la décomposition de a en facteurs irréductibles est essentiellement unique.

3. • Soit A un anneau dont tous les idéaux sont de type fini. Soit $(I_n)_{n \in \mathbb{N}}$ une suite croissante d'idéaux, et

$$I = \bigcup_{n \in \mathbb{N}} I_n.$$

D'après la question I-4, I est un idéal. Par hypothèse, il est de type fini. Soit (x_1, \dots, x_m) un système de générateurs de I . Par définition de I , pour tout $k \in \llbracket 1, m \rrbracket$, il existe n_k tel que $x_k \in I_{n_k}$. On pose

$$N = \max\{n_k, k \in \llbracket 1, m \rrbracket\}.$$

Ainsi, par croissance de la suite (I_n) , pour tout $n \geq N$, et tout $k \in \llbracket 1, m \rrbracket$, $x_k \in I$. Par minimalité de l'idéal engendré, pour tout $n \geq N$, on obtient donc :

$$I = \mathcal{I}(x_1, \dots, x_n) \subset I_n.$$

L'inclusion réciproque étant une conséquence directe de la définition de I , on en déduit que pour tout $n \geq N$, $I_n = I$, et la suite (I_n) est stationnaire. On en déduit que A vérifie (\mathcal{H}_1) .

- Soit A un anneau ayant au moins un idéal I qui ne soit pas de type fini. On construit une suite (x_n) d'éléments de I de la manière suivante :

* x_0 est un élément quelconque non nul de I . Un tel élément existe, sinon $I = \{0\}$ qui est de type fini.

* Si x_0, \dots, x_n sont construits, on définit x_{n+1} en choisissant un élément quelconque de $I \setminus \mathcal{I}(x_0, \dots, x_n)$.

Un tel élément existe, car sinon $I = \mathcal{I}(x_0, \dots, x_n)$ qui est de type fini.

On définit alors pour tout $n \in \mathbb{N}$, $I_n = \mathcal{I}(x_0, \dots, x_n)$. Par définition, (I_n) est croissante. De plus, pour tout $n \in \mathbb{N}$, $x_{n+1} \in I_{n+1} \setminus I_n$, donc (I_n) est strictement croissante.

Ainsi, A ne vérifie pas (\mathcal{H}_1) .

On en conclut que A vérifie (\mathcal{H}_1) si et seulement si tous ses idéaux sont de type fini.

4. Un anneau principal est intègre, et vérifie (\mathcal{H}_1) d'après la question précédente (tous ses idéaux étant de type fini, puisqu'engendrés par un unique élément), ainsi que (\mathcal{H}_2) , d'après II-5. On déduit alors des questions III-1 et III-2 que tout anneau principal est factoriel.

Un anneau vérifiant la propriété (\mathcal{H}_1) est appelé anneau noethérien, du nom de la mathématicienne allemande Emmy Noether (1882-1935).

Partie IV – Idéaux primaires

1. Soit $n \in \mathbb{N}^*$, 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) • Puisque pour tout $i \in \llbracket 1, k \rrbracket$, $p_i^{\alpha_i} \mid n$, on en déduit que $(n) \subset (p_i^{\alpha_i})$, donc

$$(n) \subset \bigcap_{i \in \llbracket 1, k \rrbracket} (p_i^{\alpha_i}).$$

- Soit $a \in \bigcap_{i \in [1, k]} (p_i^{\alpha_i})$. Alors pour tout $i \in [1, k]$, $p_i^{\alpha_i}$ divise a . Comme les $p_i^{\alpha_i}$ sont deux à deux premiers entre eux, il en résulte que $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ divise a , donc $a \in (n)$. Ainsi

$$\bigcap_{i \in [1, k]} (p_i^{\alpha_i}) \subset (n).$$

En conclusion, $(n) = \bigcap_{i \in [1, k]} (p_i^{\alpha_i})$.

Il s'agit en fait de la description du ppcm par les idéaux de \mathbb{Z} .

- (b) Soit $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}$. Soit $I = (p^\alpha)$. Soit a et b dans A tels que $ab \in I$ et $b \notin I$. Ainsi, b n'est pas divisible par p^α . On en déduit que $v_p(b) < \alpha$. Comme p^α divise ab , $v_p(ab) \geq \alpha$. Il en résulte que

$$v_p(a) = v_p(ab) - v_p(b) > 0,$$

donc p divise a , puis p^α divise a^α . En posant $n = \alpha$, on a bien trouvé n tel que $a^n \in I$. Ainsi (p^α) vérifie (\mathcal{H}_3) . Avec la terminologie introduite juste après, cela signifie que (p^α) est un idéal primaire de \mathbb{Z} .

- (c) Réciproquement, soit I un idéal propre de \mathbb{Z} qui ne soit pas de la forme (p^α) , $p \in \mathbb{P}$. Puisque \mathbb{Z} est principal, il existe n tel que $I = (n)$. Soit

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

la décomposition primaire de n . Pr hypothèse, $k > 1$, et on peut poser $a = p_1^{\alpha_1}$ et $b = p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. On a bien $ab \in (n)$, et pour tout $n \in \mathbb{N}$, $p_1 \nmid b^n$, donc $b^n \notin (n)$. On en déduit que I ne vérifie pas (\mathcal{H}_3) .

On en déduit que les idéaux propres de \mathbb{Z} vérifiant (\mathcal{H}_3) sont exactement les idéaux (p^α) , $p \in \mathbb{P}$, $\alpha \geq 1$.

Soit $a, b \in \mathbb{Z}$ tels que $ab \in \{0\}$ et $a \notin \{0\}$, c'est-à-dire $ab = 0$ et $a \neq 0$. Puisque \mathbb{Z} est intègre, $b = 0$, i.e. $b \in \{0\}$.

On en déduit que $\{0\}$ vérifie (\mathcal{H}_3) .

Puisque \mathbb{Z} vérifie aussi trivialement (\mathcal{H}_3) , on en déduit (avec la terminologie introduite en dessous) que les idéaux primaires de \mathbb{Z} sont $\{0\}$, \mathbb{Z} et les (p^α) . La question 1(a) montre alors que tout idéal de \mathbb{Z} est intersection finie d'idéaux primaires, le cas particulier de (0) et (1) provenant du fait que (0) et (1) = \mathbb{Z} sont eux-mêmes primaires. C'est cette propriété que l'on cherche à généraliser dans la partie V.

2. • Supposons que les diviseurs de 0 sont nilpotents. Soit $a, b \in A$ tels que $ab \in \{0\}$ et $a \notin \{0\}$. Alors $ab = 0$, et $a \neq 0$, donc b est un diviseur de 0, et par hypothèse b est nilpotent. il existe donc $n \geq 1$ tel que $b^n = 0$, donc $b^n \in \{0\}$. Ainsi, $\{0\}$ est un idéal primaire. Le cas d'un anneau intègre est un cas particulier de cette situation.
- Supposons que $\{0\}$ soit un idéal primaire. Soit b un diviseur de 0. On dispose donc de $a \neq 0$ tel que $ab = 0$ et $a \neq 0$. Alors $ab \in \{0\}$ et $a \notin \{0\}$. Puisque $\{0\}$ est primaire, il existe $n \in \mathbb{N}^*$ tel que $b^n = 0$. Ainsi, b est nilpotent.

Ainsi $\{0\}$ est un idéal primaire de A si et seulement si tout diviseur de 0 est nilpotent.

3. • Supposons I primaire. Soit $a \in A$ tel que $\varphi_{a,I}$ ne soit pas injective. Comme $\varphi_{a,I}$ est un morphisme de groupe (mais pas d'anneau), ceci équivaut à dire que $\text{Ker}(\varphi_{a,I}) \neq \{\bar{0}\}$. Il existe donc $b \in A$ tel que $\bar{b} \neq \bar{0}$, et $\overline{ab} = \bar{0}$, donc $b \notin I$ et $ab \in I$. Puisque I est primaire, il existe $n \in \mathbb{N}^*$ tel que $a^n \in I$ (désolé pour la petite maladresse de l'énoncé qui inverse le rôle de a et de b entre la définition et l'utilisation). Or, pour tout $b \in A$,

$$\varphi_{a,I}^n(\bar{b}) = \overline{a^n b} = \overline{a^n} \bar{b} = \bar{0},$$

puisque $a^n \in I$. On en déduit que $\varphi_{a,I}$ est nilpotente.

Ainsi, $\varphi_{a,I}$ est injective ou nilpotente

- Réciproquement, supposons que pour tout $a \in A$, $\varphi_{a,I}$ est injective ou nilpotente. Soit $a, b \in A$ tels que $ab \in I$ et $b \notin I$. Ainsi, $\varphi_{a,I}(\bar{b}) = \{\bar{0}\}$, et $\bar{b} \neq \bar{0}$. Par conséquent, $\text{Ker}(\varphi_{a,I})$ n'est pas réduit à $\{\bar{0}\}$, et $\varphi_{a,I}$ n'est donc pas injective. Par hypothèse, on en déduit qu'elle est nilpotente ; Il existe $n \in \mathbb{N}^*$ tel que $\varphi_{a,I}^n$ soit l'application nulle. En particulier,

$$\overline{a^n} = \varphi_{a,I}^n(\bar{1}) = \bar{0},$$

donc $a^n \in I$.

En conclusion, I est primaire.

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,

- Montrons d'abord que P_I est un idéal.

- * $\varphi_{0,I}$ est nilpotente donc $\bar{0} \in P_I$;

- * Soit a et b dans P_I . Ainsi, $\varphi_{a,I}$ et $\varphi_{b,I}$ sont nilpotentes. Soit n et m tels que $\varphi_{a,I}^n = 0$ et $\varphi_{b,I}^m = 0$. Alors pour tout $c \in A$, d'après la formule du binôme (valide puisque A est commutatif) :

$$\varphi_{(a-b),I}^{m+n}(c) = \overline{(a-b)^{m+n}c} = \sum_{i=0}^{m+n} \binom{m+n}{i} \overline{(-1)^{m+n-i} a^i b^{m+n-i} c}.$$

Or, pour tout les indices i de la somme on a soit $i \geq n$, soit $m+n-i \geq m$, et on déduit de la définition de m et n que $\overline{a^i b^{m+n-i} c} = \bar{0}$. Ainsi, pour tout c de A ,

$$\varphi_{(a-b),I}^{m+n}(c) = \bar{0},$$

donc $\varphi_{(a-b),I}$ est nilpotente, et $a-b \in P_I$.

- * Soit $a \in P_I$ et $b \in A$, et n tel que $\varphi_{a,I}^n = 0$. Pour tout $c \in A$,

$$\varphi_{ab,I}(c) = \overline{(ab)^n c} = \bar{b}^n \varphi_{a,I}^n(c) = \bar{0}.$$

Ainsi, $\varphi_{ab,I}$ est nilpotente, donc $ab \in P_I$.

- * On en déduit que P_I est bien un idéal de A .

- Soit a et b dans P_I tels que $ab \in P_I$ et $a \notin P_I$. Ainsi, $\varphi_{a,I}$ n'est pas nilpotente (elle est donc injective puisque I est primaire), et $\varphi_{ab,I}$ est nilpotente. Soit $n \in \mathbb{N}^*$ tel que $\varphi_{ab,I}^n = 0$. En évaluant en $\bar{1}$, $\overline{ab^n} = \bar{0}$, donc $a^n b^n = 0$, puis $\varphi_{a,I}^n(\overline{b^n}) = \bar{0}$. Puisque $\varphi_{a,I}^n$ est injective en tant que composée de fonctions injectives, $\text{Ker}(\varphi_{a,I}^n) = \{\bar{0}\}$, et donc $\overline{b^n} = 0$. Ainsi, pour tout $c \in A$,

$$\varphi_{b,I}^n(\bar{c}) = \overline{b^n c} = \bar{0}.$$

Ainsi, $\varphi_{b,I}$ est nilpotente, et par conséquent $b \in P_I$.

Cela prouve bien que P_I est un idéal premier de A .

(b) Soit $A = \mathbb{Z}$ et $I = (p^\alpha)$, $p \in \mathbb{P}$, $\alpha \geq 1$. Soit $a \in \mathbb{Z}$. Pour tout $b \in \mathbb{Z}$ et tout $n \in \mathbb{N}^*$,

$$\varphi_{a,I}^n(b) = \overline{a^n b}.$$

Ainsi, $\varphi_{a,I}^n$ est nulle si et seulement si pour tout $b \in \mathbb{Z}$, $v_p(a^n b) \geq \alpha$. Comme il existe des entiers b tels que $v_p(b) = 0$, ceci est vrai si et seulement si $v_p(a^n) \geq \alpha$, donc $nv_p(a) \geq \alpha$.

Une telle valeur de n existe si et seulement si $v_p(a) > 0$, donc si et seulement si $p \mid a$, i.e. $a \in (p)$.

Ainsi, $P_I = (p)$, qui est bien un idéal premier.

5. Soit P un idéal premier et I_1, \dots, I_n des idéaux P -primaires. Soit $I = \bigcap_{k=1}^n I_k$. D'après I-3, I est un idéal.

- Soit $a \in P$. Alors pour tout $k \in \llbracket 1, n \rrbracket$, φ_{a,I_k} est nilpotente. On dispose donc de n_k tel que $\varphi_{a,I_k}^{n_k} = 0$. Soit

$$n = \max\{n_k, k \in \llbracket 1, n \rrbracket\}.$$

On a alors, pour tout $k \in \llbracket 1, n \rrbracket$, $\varphi_{a,I_k}^n = 0$. Soit alors $b \in A$. Pour tout $k \in \llbracket 1, n \rrbracket$,

$$\overline{a^n b} = \bar{0} \text{ dans } A/I_k,$$

c'est-à-dire $a^n b \in I_k$. Ceci étant vrai pour tout $k \in \llbracket 1, n \rrbracket$,

$$a^n b \in \bigcap_{k=1}^n I_k = I.$$

Ainsi, $\varphi_{a,I}^n = 0$, donc $\varphi_{a,I}$ est nilpotente.

- Soit $a \in A \setminus P$. Alors pour tout $k \in \llbracket 1, n \rrbracket$, φ_{a, I_k} est injective, donc de noyau nul. Soit $b \in A$ tel que $\varphi_{a, I}(b) = \bar{0}$, donc $ab \in I$. On en déduit que pour tout $k \in \llbracket 1, n \rrbracket$, $ab \in I_k$, donc la classe de b dans A/I_k est dans $\text{Ker}(\varphi_{a, I_k})$ et est donc nulle. Ainsi, $b \in I_k$. On en déduit que

$$b \in \bigcap_{k=1}^n I_k = I,$$

donc que $\bar{b} = \bar{0}$ (classe dans A/I). Par conséquent, $\text{Ker}(\varphi_{a, I}) = \{\bar{0}\}$, puis $\text{Ker}(\varphi_{a, I})$ est injective.

- Des deux points précédents, il découle :

- * d'une part que pour tout $a \in A$, $\varphi_{a, I}$ est soit nilpotente soit injective ; ainsi I est bien un idéal primaire d'après la question IV-3 ;

- * d'autre part que l'ensemble des éléments $a \in A$ tels que $\varphi_{a, I}$ est nilpotente est l'idéal P ; ainsi, $P_I = P$ est un idéal P -primaire.

6. Si on part d'une décomposition quelconque de J comme intersection finie d'idéaux primaires, on peut définir les I_k comme les intersections des idéaux primaires de cette décomposition dont l'idéal premier associé est le même. Ainsi, les I_k seront encore primaires, d'idéaux premiers associés 2 à 2 distincts, et on aura toujours

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

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

1. • On a déjà utilisé le fait que $\varphi_{a, J}$ est un morphisme de groupe additif, mais sans le justifier explicitement. C'est l'occasion de le faire : si b et c sont dans A ,

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

Ainsi, $\varphi_{a, I}$ est un morphisme de groupes.

- $\text{Ker}(\varphi_{a, I})$ est donc un sous-groupe additif de A/J . Par ailleurs, soit $b \in \text{Ker}(\varphi_{a, I})$ et $\bar{c} \in A/J$. Alors

$$\varphi_{a, I}(\overline{bc}) = \overline{abc} = \varphi_{a, I}(b)\bar{c} = \bar{0}\bar{c} = \bar{0}.$$

Donc $\overline{bc} \in \text{Ker}(\varphi_{a, I})$.

On en conclut que $\text{Ker}(\varphi_{a, I})$ est un idéal de A/J .

- De même, $\text{Im}(\varphi_{a, I})$ est un sous-groupe de A/J , d'après le cours. Par ailleurs, si $\bar{b} \in \text{Im}(\varphi_{a, I})$ et $\bar{c} \in A/J$, il existe $\bar{b}' \in A/J$ tel que $\bar{b} = \varphi_{a, I}(\bar{b}')$, et donc

$$\overline{bc} = \varphi_{a, I}(\bar{b}')\bar{c} = \overline{ab'c} = \varphi_{a, I}(b')\bar{c} \in \text{Im}(\varphi_{a, I}).$$

Donc $\text{Im}(\varphi_{a, I})$ est un idéal de A/J .

2. Soit $\varphi : (G, +) \rightarrow (G, +)$ un morphisme de groupe.

- Si $\text{Ker}(\varphi) = \text{Ker}(\varphi^2)$, soit $g \in \text{Ker}(\varphi) \cap \text{Im}(\varphi)$. On dispose alors de $h \in G$ tel que $g = \varphi(h)$, et d'autre part $\varphi(g) = 0$. Ainsi,

$$\varphi^2(h) = \varphi(\varphi(h)) = \varphi(g) = 0.$$

On en déduit que $h \in \text{Ker}(\varphi^2) = \text{Ker}(\varphi)$, donc $g = \varphi(h) = 0$. Ainsi

$$\text{Ker}(\varphi) \cap \text{Im}(\varphi) = \{0\}$$

(l'inclusion réciproque étant trivial, 0 étant dans tout sous-groupe de G).

- Supposons que $\text{Ker}(\varphi) \cap \text{Im}(\varphi) = \{0\}$.

- * Soit $g \in \text{Ker}(\varphi)$. On a alors $\varphi(g) = 0$, donc $\varphi^2(g) = \varphi(0) = 0$. Ainsi, $\text{Ker}(\varphi) \subset \text{Ker}(\varphi^2)$.

- * Soit $g \in \text{Ker}(\varphi^2)$. Alors $\varphi(\varphi(g)) = 0$. On en déduit que

$$\varphi(g) \in \text{Ker}(\varphi) \cap \text{Im}(\varphi) = \{0\},$$

d'où $g \in \text{Ker}(\varphi)$.

Ainsi, on a bien l'égalité $\boxed{\text{Ker}(\varphi) = \text{Ker}(\varphi^2)}$

3. On suppose qu'il existe dans A des idéaux n'admettant pas de décomposition primaire.

- (a) Soit I_0 un idéal n'admettant pas de décomposition primaire. On suppose par l'absurde qu'il n'existe pas d'idéal maximal parmi les idéaux n'admettant pas de décomposition primaire. Ainsi, I_0 n'est pas maximal dans ce sens, et il existe un idéal I_1 n'admettant pas de décomposition primaire, et tel que $I_0 \subsetneq I_1$.

En itérant cette construction, on obtient une suite strictement croissante d'idéaux, qui contredit le fait que A est noethérien.

Ainsi, $\boxed{\text{il existe un idéal } J \text{ maximal parmi les idéaux n'ayant pas de décomposition primaire}}$.

- (b) • Soit un tel idéal J . Puisqu'il n'admet pas de décomposition primaire, il n'est lui-même pas primaire. Ainsi, il existe $a \in A$ tel que $\varphi_{a,J}$ n'est ni injective, ni nilpotente. On se donne un tel a .
- Avant de poursuivre, on montre que A/J est également noethérien. En effet, soit $(I_n)_{n \in \mathbb{N}}$ une suite croissante d'idéaux de A/J . D'après I-1(a), en notant π la projection canonique, $(\pi^{-1}(I_n))_{n \in \mathbb{N}}$ est une suite croissante d'idéaux de A , donc stationnaire. La question I-2a nous assure alors que (I_n) est également stationnaire, donc que A/J est noethérien.
- Par un argument similaire à celui donné dans la question précédente, la suite $(\text{Ker}(\varphi_{a,J}^n))_{n \in \mathbb{N}^*}$ est croissante. Puisque A/J est noethérien, elle est donc stationnaire. On en déduit qu'il existe un entier r tel que pour tout $n \geq r$, $\text{Ker}(\varphi_{a,J}^n) = \text{Ker}(\varphi_{a,J}^r)$.
- On pose alors $\varphi = \varphi_{a,J}^r$. On a donc en particulier $\text{Ker}(\varphi^2) = \text{Ker}(\varphi)$. La question précédente amène donc $\text{Ker}(\varphi) \cap \text{Im}(\varphi) = \{0\}$.
- Or, $\varphi_{a,J}^r$ n'est pas injective, sinon $\varphi_{a,J}^r$ le serait, et $\varphi_{a,J}^r$ n'est pas nulle car $\varphi_{a,J}$ n'est pas nilpotente. On en déduit que $\text{Ker}(\varphi) \neq \{0\}$ et $\text{Im}(\varphi) \neq \{0\}$.

(c) Soit

$$K = \pi^{-1}(\text{Ker}(\varphi)) \quad \text{et} \quad L = \pi^{-1}(\text{Im}(\varphi)).$$

Puisque $\text{Ker}(\varphi) \neq \{0\}$ et $\text{Im}(\varphi) \neq \{0\}$, on obtient $J \subsetneq K$ et $J \subsetneq L$. De plus K et L sont des idéaux d'après I-1(a). Par maximalité de J , on en déduit que K et L admettent des décompositions primaires.

Soit $K = \bigcap_{i=1}^n Q_i$ et $L = \bigcap_{j=1}^m R_j$ des décompositions primaires de K et L . On obtient alors :

$$\begin{aligned} J &= \pi^{-1}(\{0\}) \\ &= \pi^{-1}(\text{Ker}(\varphi) \cap \text{Im}(\varphi)) \\ &= \pi^{-1}(\text{Ker}(\varphi)) \cap \pi^{-1}(\text{Im}(\varphi)) \\ &= K \cap L \\ &= \bigcap_{i=1}^n Q_i \cap \bigcap_{j=1}^m R_j \end{aligned}$$

Ainsi J est une intersection finie d'idéaux primaires donc admet une décomposition primaire, ce qui contredit sa définition.

Ainsi, $\boxed{\text{tout idéal de } A \text{ admet une décomposition primaire}}$ qu'on peut réduire ensuite comme expliqué dans la partie IV.

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

4. (a) Soit $n \geq 2$. Puisque $\mathbb{Z}/n\mathbb{Z}$ est fini, tout idéal est fini, donc aussi de type fini. On a même montré un peu plus haut qu'ils sont principaux (mais $\mathbb{Z}/n\mathbb{Z}$ n'en est pas pour autant un anneau principal car il n'est pas intègre).

Ainsi, $\boxed{(\mathbb{Z}/n\mathbb{Z}, +, \times) \text{ est un anneau noethérien.}}$

- (b) • Soit $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Puisque $(n) = \bigcap_{i=1}^k (p_i^{\alpha_i})$ (question IV-1(a)), on obtient, en réduisant modulo n :

$$\boxed{\{\bar{0}\} = \bigcap_{i=1}^k p_i^{\alpha_i} \mathbb{Z}/n\mathbb{Z}.$$

Il reste à montrer que ce sont bien des idéaux primaires.

- Soit $A = \mathbb{Z}/n\mathbb{Z}$, $I = p_i^{\alpha_i}\mathbb{Z}/n\mathbb{Z}$ et $P = p_i\mathbb{Z}/p\mathbb{Z}$. On désigne par \tilde{x} la classe d'un entier x dans $\mathbb{Z}/n\mathbb{Z}$, et par \bar{x} la classe de \tilde{x} dans A/I .
 - * Soit $\tilde{a} \in P$, représenté par $a \in \mathbb{Z}$. Alors $p_i \mid a$, donc $a^{\alpha_i} \in p_i^{\alpha_i}\mathbb{Z}$, et donc $\tilde{a}^{\alpha_i} \in I$. On en déduit que $\varphi_{\tilde{a},I}^{\alpha_i} = 0$, donc $\varphi_{\tilde{a},I}$ est nilpotente.
 - * Soit $\tilde{a} \in A \setminus P$. Ainsi, $p_i \nmid a$, donc $p_i^{\alpha_i} \nmid a$. On en déduit que a est inversible modulo $p_i^{\alpha_i}$, donc \tilde{a} est inversible. Ainsi, \bar{a} est aussi inversible (réduire modulo I une relation d'inversibilité de \tilde{a}). La multiplication par \bar{a} est donc bijective (de réciproque la multiplication par \bar{a}^{-1}). On en déduit que $\varphi_{\tilde{a},I}$ est injective.
 - * On déduit des 2 points précédents que I est un idéal primaire, d'idéal premier associé P .
- Les idéaux premiers associés étant 2 à 2 distincts, la décomposition primaire réduite de $\{0\}$ est donc bien

$$\{\bar{0}\} = \bigcap_{i=1}^k p_i^{\alpha_i}\mathbb{Z}/n\mathbb{Z}.$$