Plus grand diviseur

Marc Lorenzi

7 novembre 2026

Résumé

Tout le monde sait ce qu'est le pgcd de deux entiers, ou 3, ou 4, etc. Cet article vise à définir le plus grand diviseur d'un ensemble (vide, fini ou infini, bref quelconque) d'éléments d'un anneau principal. On montre dans la dernière partie que, moyennant l'axiome du choix, on peut toujours se ramener à un nombre fini d'éléments.

1 Introduction

Dans tout l'article, $\mathbb{A}$ désigne un anneau *commutatif* et *intègre*. On note $\mathbb{U}$ le groupe des éléments inversibles de l'anneau $\mathbb{A}$. Un *idéal* de $\mathbb{A}$ est une partie I de $\mathbb{A}$ vérifiant les deux propriétés suivantes.

- I est un sous-groupe du groupe additif $(\mathbb{A}, +)$.
- Pour tout $\lambda \in \mathbb{A}$ et tout $a \in I$, $\lambda a \in I$.

On montre facilement qu'une partie I de $\mathbb{A}$ est un idéal si et seulement si

- $I \neq \emptyset$.
- Pour tous $a, b \in I$, $a + b \in I$.
- Pour tout $\lambda \in \mathbb{A}$ et tout $a \in I$, $\lambda a \in I$.

Étant donnés deux éléments a et b de l'anneau $\mathbb{A}$, a *divise* b lorsqu'il existe $c \in \mathbb{A}$ tel que $b = ac$. On note alors $a|b$. La relation « divise » est un *préordre*, c'est à dire qu'elle est réflexive et transitive. En revanche, elle n'est pas antisymétrique. Plus précisément, on a le résultat suivant.

Proposition 1. *Soient $a, b \in \mathbb{A}$. On a $a|b$ et $b|a$ si et seulement si il existe $u \in \mathbb{U}$ tel que $b = au$.*

Démonstration. Si $b = 0$, le résultat est immédiat. Prenons dans la suite $b \neq 0$.

Supposons que $a|b$ et $b|a$. Il existe $u, v \in \mathbb{A}$ tels que $b = au$ et $a = bv$. On a donc $b = buv$. Comme $b \neq 0$ et $\mathbb{A}$ est intègre, $uv = 1$. Ainsi, $u \in \mathbb{U}$. Inversement, supposons qu'il existe $u \in \mathbb{U}$ tel que $b = au$. De $b = au$ on déduit $a|b$. Mais aussi, $a = bu^{-1}$, donc $b|a$. □

2 Plus grand diviseur d'une partie de $\mathbb{A}$

N.B. Nous supposerons dans toute la suite que $\mathbb{A}$ est un anneau *principal*, c'est à dire que les

idéaux de $\mathbb{A}$ sont de la forme $d\mathbb{A}$ où $d \in \mathbb{A}$.

2.1 Introduction

Définition 1. Soit $E \subseteq \mathbb{A}$. Un plus grand diviseur de E est un élément δ de $\mathbb{A}$ tel que pour tout $d \in \mathbb{A}$,

$$(\forall a \in E, d|a) \iff d|\delta$$

Notation. Pour toute partie E de $\mathbb{A}$, nous noterons $\wedge E$ l'ensemble des plus grands diviseurs de E. Cet ensemble peut très bien, à ce stade de notre étude, être vide ! Notons cependant le résultat suivant.

Proposition 2. *Soit $E \subseteq A$. On suppose que $\wedge E \neq \emptyset$. Soit $\delta \in \wedge E$. On a alors*

$$\wedge E = \delta\mathbb{U}$$

Démonstration. ($\subseteq$) Soit $\delta' \in \wedge E$. On a $\delta'|\delta'$, donc pour tout $a \in E$, $\delta'|a$. Mais $\delta \in \wedge E$. La caractérisation d'un plus grand diviseur de E nous dit que $\delta'|\delta$. De même, $\delta|\delta'$. Il existe donc $u \in \mathbb{U}$ tel que $\delta' = \delta u$. Nous avons donc $\wedge E \subseteq \delta\mathbb{U}$.

($\supseteq$) Soit $\delta' \in \delta\mathbb{U}$. Soit $u \in \mathbb{U}$ tel que $\delta' = \delta u$. Soit $d \in \mathbb{A}$. Supposons que pour tout $a \in E$, $d|a$. Alors, $d|\delta$. Comme $\delta|\delta'$, on a aussi $d|\delta'$. Inversement, supposons que $d|\delta'$. Comme $\delta = \delta' u^{-1}$, $\delta'|\delta$ et donc $d|\delta$. Comme δ est un plus grand diviseur de E, on a donc, pour tout $a \in E$, $d|a$. Ainsi, $\delta' \in \wedge E$. Nous avons donc $\delta\mathbb{U} \subseteq \wedge E$. □

Regardons deux exemples extrêmes.

Exemple. Quel est le plus grand diviseur du vide ? Prenons $E = \emptyset$. La condition du membre de gauche de l'équivalence est vraie pour tout $d \in \mathbb{A}$. Un plus grand diviseur de $\emptyset$ est donc un $\delta \in \mathbb{A}$ tel que pour tout $d \in \mathbb{A}$, d divise δ. Il en existe un et un seul, qui est $\delta = 0$. Ainsi, $\wedge\emptyset = \{0\}$.

Exemple. Prenons $E = \mathbb{A}$. Soit $d \in \mathbb{A}$. Si d divise tous les éléments de $\mathbb{A}$, alors d divise 1, donc $d \in \mathbb{U}$. Inversement, si $d \in \mathbb{U}$, alors il divise tous les éléments de $\mathbb{A}$. Ainsi, $\wedge\mathbb{A} = \mathbb{U}$.

2.2 Caractérisation

Soit $E \subseteq \mathbb{A}$. L'intersection des idéaux de $\mathbb{A}$ contenant E est un idéal de $\mathbb{A}$ contenant E. C'est clairement le plus petit idéal de $\mathbb{A}$ contenant E. Nous le noterons $\langle E \rangle$.

Appelons *combinaison linéaire d'éléments de E* tout $x \in \mathbb{A}$ de la forme

$$x = \sum_{a \in E} \lambda_a a$$

où les $\lambda_a \in \mathbb{A}$ sont presque tous nuls. L'appellation « combinaison linéaire » peut paraître osée. En fait, il n'en est rien : l'anneau $\mathbb{A}$ est muni de façon canonique d'une structure de $\mathbb{A}$-module (un module est l'analogue d'un espace vectoriel, sauf que l'ensemble des scalaires est un anneau

et pas un corps) et ce que nous appelons combinaison linaire en est bien une dans le $\mathbb{A}$-module $\mathbb{A}$. Les idéaux de $\mathbb{A}$ ne sont finalement rien d'autre que les sous-modules de $\mathbb{A}$.

Proposition 3. *Soit E une partie de $\mathbb{A}$. L'idéal engendré par E est l'ensemble des combinaisons linéaires d'éléments de E.*

Démonstration. Notons I l'ensemble des combinaisons linéaires d'éléments de E. L'ensemble I est clairement un idéal de $\mathbb{A}$ contenant E. Soit J un idéal de $\mathbb{A}$ contenant E. Soit $x \in I$. On a

$$x = \sum_{a \in E} \lambda_a a$$

où les $\lambda_a \in \mathbb{A}$ sont presque tous nuls. Pour tout $a \in E$, $a \in J$ donc, puisque J est un idéal, $x \in J$. Ainsi, $I \subseteq J$. L'idéal I est ainsi le plus petit idéal de $\mathbb{A}$ contenant E, d'où $I = \langle E \rangle$. □

Proposition 4. *Soit $E \subseteq \mathbb{A}$. Soit $\delta \in \mathbb{A}$ tel que $\langle E \rangle = \delta\mathbb{A}$. On a alors $\wedge E = \delta\mathbb{U}$.*

Démonstration. Notons que l'existence de δ résulte du fait que $\mathbb{A}$ est un anneau principal.

Soit $d \in \mathbb{A}$.

($\Rightarrow$) Supposons que pour tout $a \in A$, d divise a. δ appartient à $\delta\mathbb{A} = \langle E \rangle$. Il existe donc une famille presque nulle $(\lambda_a)_{a \in A}$ d'éléments de $\mathbb{A}$ telle que

$$\delta = \sum_{a \in E} \lambda_a a$$

Comme d divise tous les termes de la somme, il divise δ.

($\Leftarrow$) Supposons que d divise δ. Soit $a \in E$. a appartient à $\langle E \rangle = \delta\mathbb{A}$, donc δ divise a. Par transitivité de la relation « divise », d divise a.

Ainsi, $\delta \in \wedge E$ et donc, par la proposition 2, $\wedge E = \delta\mathbb{U}$. □

Corollaire 5. *Pour tout $E \subseteq \mathbb{A}$, $\wedge E \neq \emptyset$.*

2.3 Un exemple

Plaçons nous dans l'anneau $\mathbb{A} = \mathbb{Z}$. Soit

$$E = \{16^n + 10^n - 1 : n \in \mathbb{N}^*\}$$

Nous allons montrer que $\wedge E = \{\pm 5\}$. Posons, pour tout $n \in \mathbb{N}^*$,

$$a_n = 16^n + 10^n - 1$$

Soit $\delta \in \wedge E$. On a $a_1 = 25$ donc δ divise 25. Ainsi, $\delta = \pm 1$, $\delta = \pm 5$ ou $\delta = \pm 25$. Par ailleurs, $a_2 = 355$. Or, 25 ne divise pas 355, donc $\delta \neq \pm 25$.

Soit $n \in \mathbb{N}^*$. On a

$$a_n \equiv 1^n + 0^n - 1 = 0 \bmod 5$$

et donc 5 divise a_n. Comme 5 divise tous les a_n, 5 divise δ. Ainsi, $\wedge E = \{-5, 5\}$.

3 L'infini se ramène au fini

3.1 Introduction

Le but de ce qui précède était de montrer que, dans un anneau principal, on peut définir non seulement le plus grand diviseur commun de 2, 3 ou 4 éléments de l'anneau, mais aussi celui d'une infinité d'éléments. Nous avons en apparence gagné en généralité, mais pas autant que nous aurions pu l'espérer : nous allons en effet montrer le résultat suivant.

Proposition 6. *Soit $E \subseteq \mathbb{A}$. Il existe un ensemble fini $E' \subseteq E$ tel que $\wedge E = \wedge E'$.*

Nous allons décomposer la preuve en plusieurs étapes.

3.2 Suites croissantes d'idéaux

Commençons par montrer deux résultats sur les suites croissantes d'idéaux de $\mathbb{A}$.

Proposition 7. *La réunion d'une suite croissante d'idéaux de $\mathbb{A}$ est un idéal de $\mathbb{A}$.*

Démonstration. Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de $\mathbb{A}$. Posons

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

On a $0 \in I_0$, donc $0 \in I$, d'où $I \neq \emptyset$. Soient $x, y \in I$. Il existe $m, n \in \mathbb{N}$ tels que $x \in I_m$ et $y \in I_n$. En posant $p = \max(m, n)$, on a par la croissance de la suite $(I_n)_{n\in\mathbb{N}}$, $x, y \in I_p$. De là, $x + y \in I_p$ d'où $x + y \in I$. Soient enfin $\lambda \in \mathbb{A}$ et $x \in I$. Soit $n \in \mathbb{N}$ tel que $x \in I_n$. Comme I_n est un idéal de $\mathbb{A}$, $\lambda x \in I_n$, d'où $\lambda x \in I$. □

Proposition 8. *Une suite croissante d'idéaux de $\mathbb{A}$ est stationnaire.*

Démonstration. Comme dans la preuve précédente, soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de $\mathbb{A}$. Posons

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

Comme l'anneau $\mathbb{A}$ est principal, il existe $d \in \mathbb{A}$ tel que $I = d\mathbb{A}$. Or, $d \in I$, donc il existe $n_0 \in \mathbb{N}$ tel que $d \in I_{n_0}$. Pour tout $n \geq n_0$, on a $d \in I_n$ (croissance). De là, $I = d\mathbb{A} \subseteq I_n \subseteq I$, d'où $I_n = I$. La suite $(I_n)_{n\in\mathbb{N}}$ est donc stationnaire à partir du rang n_0. □

Remarque. Cette propriété est essentielle, elle s'appelle la *condition de chaîne ascendante*. Un anneau qui vérifie la condition de chaîne ascendante s'appelle un *anneau nœthérien*. Tout anneau principal est nœthérien, mais il existe des anneaux nœthériens qui ne sont pas principaux, comme par exemple l'anneau $\mathbb{K}[X, Y]$ des polynômes à deux indéterminées sur un corps $\mathbb{K}$.

3.3 La preuve de la proposition

Soit $E \subseteq \mathbb{A}$. Définissons par récurrence sur n une suite $(E_n)_{n\in\mathbb{N}}$ de parties finies de E. Posons $E_0 = \emptyset$. Soit $n \in \mathbb{N}$. Supposons construit E_n. Deux cas se présentent.

Premier cas, $\langle E_n\rangle \neq \langle E\rangle$. Comme $E_n \subseteq E$, on a aussi $\langle E_n\rangle \subseteq \langle E\rangle$. Supposons un instant que $E \subseteq \langle E_n\rangle$. On a alors $\langle E\rangle \subseteq \langle E_n\rangle$, d'où $\langle E_n\rangle = \langle E\rangle$, contradiction. Ainsi, l'ensemble $E \setminus \langle E_n\rangle$ n'est pas vide. Choisissons $x \in E \setminus \langle E_n\rangle$ et posons $E_{n+1} = E_n \cup \{x\}$.

Second cas, $\langle E_n\rangle = \langle E\rangle$. Posons alors $E_{n+1} = E_n$.

Remarquons que l'axiome du choix intervient dans la définition de notre suite.

Exemple. Reprenons l'exemple du paragraphe 2.3. On a $E_0 = \emptyset$. On peut ensuite prendre, par exemple, $E_1 = \{a_1\} = \{25\}$ puis $E_2 = \{a_1, a_2\} = \{25, 355\}$. On a alors $\langle E_2\rangle = \langle E\rangle = 5\mathbb{Z}$ d'où $E_2 = E_3 = E_4 = \ldots$.

Posons, pour tout $n \in \mathbb{N}$, $I_n = \langle E_n\rangle$.

Lemme 9. *La suite $(I_n)_{n\in\mathbb{N}}$ est une suite croissante d'idéaux de $\mathbb{A}$.*

Démonstration. Soit $n \in \mathbb{N}$. Par construction, on a $E_n \subseteq E_{n+1}$ et donc

$$I_n = \langle E_n\rangle \subseteq \langle E_{n+1}\rangle = I_{n+1}$$

□

Lemme 10. *Il existe $n_0 \in \mathbb{N}$ tel que $\langle E\rangle = \langle E_{n_0}\rangle$.*

Démonstration. La suite $(I_n)_{n\in\mathbb{N}}$ est une suite croissante d'idéaux de l'anneau principal $\mathbb{A}$, elle est donc stationnaire. Donnons-nous $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$, $I_n = I_{n_0}$. On a $E_{n_0} \subseteq E$ et donc $I_{n_0} = \langle E_{n_0}\rangle \subseteq \langle E\rangle$. Inversement, soit $x \in \langle E\rangle$. Écrivons

$$x = \sum_{a\in E} \lambda_a a$$

où les $\lambda_a \in \mathbb{A}$ sont presque tous nuls. Supposons que $x \notin I_{n_0}$. Soit $F = E_{n_0} \cup \{x\}$. Comme $x \in \langle F\rangle$, $I_{n_0} = \langle E_{n_0}\rangle \subsetneq \langle F\rangle$. Cependant,

$$\langle E_{n_0+1}\rangle = I_{n_0+1} = I_{n_0} = \langle E_{n_0}\rangle$$

Ceci contredit notre définition de la suite $(E_n)_{n\in\mathbb{N}}$. Ainsi, $x \in I_{n_0}$. □

Nous avons ainsi prouvé la proposition 6. L'ensemble $E' = E_{n_0}$ est fini et inclus dans E. Par le lemme 10, $\langle E\rangle = \langle E'\rangle$, donc $\wedge E = \wedge E'$.