

Sur l'unicité de la décomposition en facteurs premiers

KUKITA Eishi

Mots-clefs : histoire des mathématiques, mathématiques, arithmétique, nombres entiers, nombres premiers

Avant-propos *De l'immense monde des nombres celui des entiers n'est qu'une partie minuscule, dont la profondeur est pourtant tellement insondable que l'on mit plus de trois siècles, par exemple, pour démontrer une proposition apparemment très simple, formulée par Pierre de Fermat, mathématicien du XVII^e siècle, sans rien de plus en guise de commentaire sur un livre de Diophante^{*1}, selon laquelle, étant donné n un entier quelconque supérieur ou égal à 3, aucuns entiers x, y, z ne satisfont l'équation $x^n + y^n = z^n$. Intéressé au développement de l'arithmétique en Europe au début du temps moderne, dont l'inventeur de la proposition énigmatique est l'une des figures les plus éminentes, nous avons cru incontournable de nous rendre compte à fond de la proposition, dite « théorème fondamental de l'arithmétique », qui se rapporte à la nature la plus élémentaire des entiers les plus élémentaires, à savoir des premiers. Pour imiter Descartes, une autre grande figure mathématique contemporaine de Fermat, la méthode, chemin à suivre, exige que l'on se rende clair et distinct ce qu'il y a du plus simple, qui serve désormais d'appui inébranlable de la raison. Si nous, loin d'être versé dans la*

*1. « Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duas ejusdem nominis fas est dividere : cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet. » P. Fermat, *Précis des Œuvres mathématiques et de l'Arithmétique de Diophante*, Éd. Jacques Gabay, Paris, p.128. Pour l'histoire qui va de l'origine jusqu'à la solution finale du problème, voir Simon Singh, *Fermat's Last Theorem*, Conville & Walsh Limited, 1997.

matière, avons osé un tel sujet, c'est simplement que la fascination de ce champ fécond et mystérieux nous a profondément touché.

* * *

Soit a un nombre entier quelconque strictement supérieur à 1 ; il se divise par 1 et par lui-même. On l'appelle *premier* s'il n'est divisible par d'autres entiers (positifs) que 1 et lui-même. Un entier supérieur ou égal à 2, non-premier, est *composé*. Les composés peuvent être mis sous la forme de produits de premiers au nombre fini, tels que ;

$$\begin{aligned}4 &= 2^2 \\24381 &= 3^4 \cdot 7 \cdot 43 \\4294967297 &= 641 \cdot 6700417\end{aligned}$$

(la dernière formule est du nombre $2^{32} + 1$, dont Fermat prévit qu'il serait premier, tandis que plus d'un siècle après un autre génie, Euler, montra qu'il était en fait décomposable comme on le voit ici.)

Ces produits se nomment *décompositions en facteurs premiers*.

La décomposition de chaque entier est unique, abstraction faite de l'ordre des facteurs. Par exemple le nombre 24381 a pour décomposition $3^4 \cdot 7 \cdot 43$, et uniquement cela (il est pourtant vrai que cette décomposition s'écrit de plusieurs manières : « $43 \cdot 3^4 \cdot 7$ », « $43 \cdot 7 \cdot 3 \cdot 3 \cdot 3 \cdot 3$ », etc.)

Les premiers ne sont pas décomposables par définition. Cependant, étant donné a un premier, si l'on considère la formule de l'identité

$$a = a$$

comme celle de la décomposition, en d'autres termes que l'on admet que l'expression « produit de premiers » comprend le premier lui-mêmes, on peut alors avancer la proposition suivante :

Un entier quelconque, supérieur ou égal à 2, se décompose uniquement en produit de facteurs premiers au nombre fini.

Ce fait apparemment évident, que l'on appelle « théorème fondamental de l'arithmétique », n'est pas vérifiable extensivement, étant donnée une infinité

de premiers. En effet, soient A le plus grand de tous les premiers, et $B = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots A) + 1$. B n'est divisible par aucun des premiers nommés ici, donc il l'est lui-même. D'autre part B est évidemment plus grand que A , ce qui est contradictoire avec l'hypothèse sur A . Ainsi le nombre des premiers est-il illimité^{*2}. Dans les pages qui suivent on lira une démonstration du théorème axiomatiquement établie. La compréhension n'en requiert que la connaissance des notions élémentaires telles que l'égalité et l'inégalité des nombres, les quatre opérations arithmétiques : addition, soustraction, multiplication et division, etc. Nous signalons pourtant que, pour la commodité de l'exposé, nous nous sommes permis d'employer certaines expressions propres aux mathématiques postérieures à la théorie des ensembles^{*3}.

1. Raisonnement par récurrence

Axiome Chaque partie non-vide de \mathbb{N} , ensemble de tous les entiers naturels, a son élément minimal.

Théorème 1a (1^{ère} forme du raisonnement) Soit A une partie quelconque de \mathbb{N} ; $A = \mathbb{N}$, si elle satisfait les conditions suivantes ;

- [1] $0 \in A$
- [2] $\forall n \in \mathbb{N} : n \in A \Rightarrow n + 1 \in A$

Démonstration Soit B le complémentaire de A . Si l'on suppose que $B \neq \emptyset$, il existe n_0 , élément minimal de B (par Axiome). $n_0 \neq 0$ (Par [1]), c'est-à-dire $n_0 \geq 1$, donc $n_0 - 1 \geq 0$. $n_0 - 1 \in A$ (par la définition de n_0), d'où (par [2])

$$n_0 = (n_0 - 1) + 1 \in A$$

ce qui est contradictoire avec l'hypothèse : $n_0 \in B$. Ainsi faut-il que $B = \emptyset$, c'est-à-dire $A = \mathbb{N}$. CQFD

*2. Ce que l'on savait depuis l'Antiquité grecque. Voir Euclide, *Éléments*, livre 9, théorème 20.

*3. Voici quelques-unes que l'on verra ci-dessous. $a \in A$ se lit : « a est un élément de l'ensemble A », « a appartient à A », « A inclut a », etc. $A' \subset A$: « A' est une partie / un sous-ensemble de A », « A inclut A' », etc. $\forall a$: « un a quelconque », « n'importe quel a ». $\exists a$: « un certain a ». $\mathbb{N}, \mathbb{Z}^+, \mathbb{Z}, \mathbb{Q}$: ensembles de tous les entiers naturels ($\{0, 1, 2, \dots\}$), de tous les entiers positifs ($\{1, 2, \dots\}$), de tous les entiers ($\{0, \pm 1, \pm 2, \dots\}$) et de tous les rationnels.

Théorème 1b (2^e forme du raisonnement) Soit A une partie quelconque de \mathbb{N} ;
 $A = \mathbb{N}$, si elle satisfait les conditions suivantes ;

[1] $0 \in A$

[2] $\forall n \in \mathbb{N}, \forall i \in \{0, 1, \dots, n-1\} : i \in A \Rightarrow n \in A$

Démonstration Étant donnés B et n_0 de la démonstration du théorème précédent, $n_0 - 1 \in A$, alors (par [2]) $n_0 \in A$, ce qui est contradictoire avec l'hypothèse : $n_0 \in B$, etc. CQFD

Théorème 2a Soit $P(n)$ une proposition sur $n \in \mathbb{N}$; elle est vraie pour $\forall n \in \mathbb{N}$, s'il se démontre que

[1] $P(0)$ est vraie.

[2] $P(n+1)$ est vraie, supposé que $P(n)$ soit vraie.

Démonstration Soit $A = \{n \mid n \in \mathbb{N}, P(n) \text{ est vraie}\}$. A satisfait [1] et [2] de Théorème 1a, donc $A = \mathbb{N}$. CQFD

Théorème 2b Soit $P(n)$ une proposition sur $n \in \mathbb{N}$; elle est vraie pour $\forall n \in \mathbb{N}$, s'il se démontre que

[1] $P(0)$ est vraie.

[2] $P(n)$ est vraie, supposé que $P(i)$ soit vraie pour $\forall i \in \{0, 1, \dots, n-1\}$.

Démonstration Soit $A = \{n \mid n \in \mathbb{N}, P(n) \text{ est vraie}\}$. A satisfait [1] et [2] de Théorème 1b, donc $A = \mathbb{N}$. CQFD

Remarque Dans l'axiome et les théorèmes précédents, on peut remplacer, si besoin est, \mathbb{N} , ensemble de tous les entiers naturels, par \mathbb{Z}^+ , celui des tous les entiers positifs, ou prendre pour point de départ un entier quelconque au lieu de 0 ou 1.

2. Théorème de la division

Théorème 3 Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^+$; il existe uniquement $q, r \in \mathbb{Z}$ tels que

$$a = qb + r, \quad 0 \leq r < b \quad (1)$$

Démonstration Fixez b à un entier quelconque ; nous démontrons l'existence unique de q, r pour $\forall a \in \mathbb{Z}$.

Lorsque $a \geq 0$, si $0 \leq a < b$, alors $q = 0$ et $r = a$ satisfont (1). Si $a \geq b$, supposez que le thèse soit vraie pour $\forall n \in \mathbb{Z}^+$ strictement inférieur à a . Étant donné que $0 \leq a - b < a$, il existe (par l'hypothèse de récurrence) $q_1, r_1 \in \mathbb{Z}$ tels que

$$a - b = q_1 b + r_1, \quad 0 \leq r_1 < b$$

Alors on a

$$a = (q_1 + 1)b + r_1$$

donc $q = q_1 + 1$ et $r = r_1$ satisfont (1). Ainsi (par Théorème 2b) la thèse est-elle vraie pour $\forall a \in \mathbb{N}$.

Lorsque $a < 0$, autrement dit $-a > 0$, il existe $q_2, r_2 \in \mathbb{Z}$ tels que

$$-a = q_2 b + r_2, \quad 0 \leq r_2 < b$$

Si $r_2 = 0$, alors

$$a = (-q_2)b$$

donc $q = -q_2$ et $r = 0$ satisfont (1). Si $0 < r_2 < b$, alors

$$a = -q_2 b - r_2 = (-q_2 - 1)b + (b - r_2), \quad 0 < b - r_2 < b$$

donc $q = -q_2 - 1$ et $r = b - r_2$ satisfont (1).

Pour voir l'unicité de q, r , supposez que

$$a = q_1 b + r_1 = q_2 b + r_2, \quad \begin{cases} 0 \leq r_1 < b \\ 0 \leq r_2 < b \end{cases}$$

Alors on a

$$(q_1 - q_2)b = r_2 - r_1$$

Si $q_1 > q_2$, alors $q_1 - q_2 > 0$. Il s'ensuit que le membre gauche de cette formule est supérieur à b . D'autre part $r_2 - r_1 \leq r_2 < b$, donc le membre droit y est inférieur, ce qui est contradictoire. L'hypothèse $q_1 < q_2$ mène elle aussi à une contradiction de la même nature. Ainsi faut-il que $q_1 = q_2$, donc $r_1 = r_2$. CQFD

Remarque Parallèlement à ce théorème, on peut en avancer un autre, non pas sur les entiers, mais sur les polynômes.

Soient A l'ensemble de tous les polynômes de x et $F(x), G(x) \in A$; il existe uniquement $Q(x), R(x) \in A$ tels que

$$F(x) = Q(x)G(x) + R(x), \quad \deg R(x) < \deg G(x) \quad (1)$$

Démonstration Fixez $G(x)$ à un polynôme quelconque ; nous démontrons l'existence unique de $Q(x), R(x)$ pour $\forall F(x) \in A$.

Lorsque $\deg F(x) < \deg G(x)$, $Q(x) = 0$ et $R(x) = F(x)$ satisfont (1).

Lorsque $\deg F(x) = \deg G(x)$, avec une constante c_0 (1) s'écrit sous la forme de

$$F(x) = c_0 G(x) + R_0(x), \quad \deg R_0(x) < \deg G(x)$$

alors $Q(x) = c_0$ et $R(x) = R_0(x)$ satisfont (1).

Lorsque $\deg F(x) > \deg G(x)$, supposez que $\deg F(x) = n$ et la thèse soit vraie pour $\forall F'(x) \in A$ tel que $\deg F'(x) \leq n - 1$. (Par le théorème fondamental de l'algèbre) $F(x)$ se décompose en produit de binômes de x au nombre de n . Soient $x - a$ un de ces facteurs et

$$F(x) = (x - a)F_a(x)$$

Étant donné que $\deg F_a(x) = n - 1$, il existe (par l'hypothèse de récurrence) $Q_1(x), R_1(x) \in A$ tels que

$$F_a(x) = Q_1(x)G(x) + R_1(x), \quad \deg R_1(x) < \deg G(x)$$

Alors on a

$$F(x) = (x - a)Q_1(x)G(x) + (x - a)R_1(x)$$

Si $\deg (x - a)R_1(x) < \deg G(x)$, alors

$$Q(x) = (x - a)Q_1(x), \quad R(x) = (x - a)R_1(x)$$

satisfont (1). Si $\deg (x - a)R_1(x) = \deg G(x)$, alors avec une constante c_1 on a

$$(x - a)R_1(x) = c_1 G(x) + R_2(x), \quad \deg R_2(x) < \deg G(x)$$

et (1) s'écrit sous la forme

$$F(x) = ((x - a)Q_1(x) + c_1)G(x) + R_2(x)$$

donc

$$Q(x) = (x - a)Q_1(x) + c_1, \quad R(x) = R_2(x)$$

satisfont (1).

Pour voir l'unicité de $Q(x), R(x)$, supposez que

$$F(x) = Q_1(x)G(x) + R_1(x) = Q_2(x)G(x) + R_2(x), \quad \begin{cases} \deg R_1(x) < \deg G(x) \\ \deg R_2(x) < \deg G(x) \end{cases}$$

Alors on a

$$(Q_1(x) - Q_2(x))G(x) = R_2(x) - R_1(x)$$

Si $Q_1(x) \neq Q_2(x)$, alors

$$\begin{aligned} \deg G(x) &\leq \deg (Q_1(x) - Q_2(x))G(x) = \deg (R_2(x) - R_1(x)) \\ &\leq \deg R_2(x) \end{aligned}$$

ce qui est contradictoire avec l'hypothèse sur $R_2(x)$. Ainsi faut-il que $Q_1(x) = Q_2(x)$, donc $R_1(x) = R_2(x)$. CQFD

3. Idéal et PGCD (plus grand commun diviseur)

Définition Soient $a_1, \dots, a_r \in \mathbb{Z}$. La partie de \mathbb{Z}

$$I = \{x_1a_1 + \dots + x_ra_r \mid x_1, \dots, x_r \in \mathbb{Z}\}$$

s'appelle *idéal*, engendré par a_1, \dots, a_r .

Remarque Voici quelques caractéristiques de l'idéal :

- $0 \in I$. $\pm a_1, \dots, \pm a_r \in I$ aussi, donc si au moins un des a_1, \dots, a_r est non-nul, il existe des entiers positifs qui appartiennent à I .
- La somme de deux éléments quelconques de I y appartient.
- Un multiple quelconque d'un élément quelconque de I y appartient.
- L'idéal engendré par un seul $d \in \mathbb{Z}$ est l'ensemble de tous les multiples de d .

Théorème 4 Soient $a_1, \dots, a_r \in \mathbb{Z}$ dont au moins un est non-nul, et d leur PGCD; l'idéal engendré par a_1, \dots, a_r est égal à celui engendré par d , et il existe $k_1, \dots, k_r \in \mathbb{Z}$ tels que

$$k_1 a_1 + \dots + k_r a_r = d \quad (1)$$

Démonstration Soit I_1 l'idéal engendré par a_1, \dots, a_r . I_1 a pour éléments des entiers positifs, et (par Axiome) il existe d , le plus petit de ces derniers. Soit I_2 l'idéal engendré par d .

Un multiple quelconque de d appartient à I_1 , donc

$$I_2 \subset I_1 \quad (2)$$

D'autre part pour $\forall a \in I_1$ il existe (par Théorème 3) $q, s \in \mathbb{Z}$ tels que

$$a = qd + s, \quad 0 \leq s < d$$

c'est-à-dire

$$s = a + (-q)d \in I_1$$

s ne peut être un entier positif strictement inférieur à d , étant donné que d est le plus petit des éléments positifs de I_1 . Alors $s = 0$ et $a = qd \in I_2$, donc

$$I_1 \subset I_2 \quad (3)$$

Avec (2) et (3) on obtient que $I_1 = I_2$.

$a_1, \dots, a_r \in I_1$ étant tous multiples de d , d en est un diviseur commun. D'autre part $d \in I_1$, donc il existe k_1, \dots, k_r qui satisfont (1). Soit e un diviseur commun quelconque de a_1, \dots, a_r . Chaque $k_i a_i$ ($i = 1, \dots, r$) est divisible par e , et d , leur somme, l'est lui aussi. Il s'ensuit que $e \leq d$, donc d est le PGCD de a_1, \dots, a_r . CQFD

Remarque 1 Ici aussi, comme pour le théorème précédent, on peut en avancer un parallèle sur les polynômes.

Soient A l'ensemble de tous les polynômes de x , et $A_1(x), \dots, A_r(x) \in A$, n'ayant pour diviseurs communs que des constantes; il existe $M_1(x), \dots, M_r(x) \in A$ tels que

$$M_1(x)A_1(x) + \dots + M_r(x)A_r(x) = 1$$

Démonstration Soient $\forall U_1(x), \dots, U_r(x) \in A$, et B l'ensemble de tous les polynômes tels que

$$U_1(x)A_1(x) + \dots + U_r(x)A_r(x)$$

[1] Soit $F(x), F'(x) \in B$ tels que

$$\begin{aligned} F(x) &= F_1(x)A_1(x) + \dots + F_r(x)A_r(x), \\ F'(x) &= F_1'(x)A_1(x) + \dots + F_r'(x)A_r(x) \end{aligned}$$

Alors

$$F(x) \pm F'(x) = (F_1(x) \pm F_1'(x))A_1(x) + \dots + (F_r(x) \pm F_r'(x))A_r(x)$$

donc $F(x) \pm F'(x) \in B$.

[2] Pour $\forall Q(x) \in A$

$$Q(x)F(x) = (Q(x)F_1(x))A_1(x) + \dots + (Q(x)F_r(x))A_r(x)$$

donc $Q(x)F(x) \in B$.

Soit $G(x)$ un des éléments non-nuls de B dont le degré est le plus bas du B . (Par l'hypothèse) $G(x) \in B$, donc il existe $M_1(x), \dots, M_r(x) \in A$ tels que

$$G(x) = M_1(x)A_1(x) + \dots + M_r(x)A_r(x)$$

Pour $\forall F(x) \in B$ il existe (par la Remarque du Théorème 3) $Q(x), R(x) \in A$ tels que

$$F(x) = Q(x)G(x) + R(x), \quad \deg R(x) < \deg G(x)$$

Alors (par [1] et [2])

$$R(x) = F(x) - Q(x)G(x) \in B$$

(Par l'hypothèse) il n'existe aucun élément non-nul de B dont le degré est plus bas que celui de $G(x)$, donc $R(x) = 0$, ce qui signifie qu'un élément quelconque de B se divise par $G(x)$.

$A_1(x), \dots, A_r(x) \in B$, donc $G(x)$ est leur diviseur commun. (Par l'hypothèse) ils n'ont pour diviseurs communs que des constantes, donc $G(x)$ en est une. Un multiple quelconque d'un élément de B y appartenant lui aussi, on peut poser que $G(x) = 1$. CQFD

Remarque 2 Nous signalerons désormais par (a_1, \dots, a_r) le PGCD de a_1, \dots, a_r .

4. Nature des premiers

Théorème 5 Soient $n, a_1, a_2 \in \mathbb{Z}$. Si $a_1 a_2$ se divise par n et $(a_1, n) = 1$, alors a_2 se divise par n .

Démonstration Il existe (par Théorème 4) $k_1, k_2 \in \mathbb{Z}$ tels que

$$k_1 a_1 + k_2 n = 1$$

c'est-à-dire

$$k_1 a_1 a_2 + k_2 n a_2 = a_2$$

Par l'hypothèse $a_1 a_2$ est un multiple de n , donc $k_1 a_1 a_2$ en est un lui aussi.

D'autre part $k_2 n a_2$ l'est naturellement. Ainsi leur somme $a_2 = k_1 a_1 a_2 + k_2 n a_2$ l'est-elle elle aussi. CQFD

Théorème 6 Soient $a_1, a_2 \in \mathbb{Z}$ et p un premier. Si $a_1 a_2$ se divise par p , alors au moins un des a_1 ou a_2 se divise par p .

Démonstration p n'a pour diviseurs positifs que p et 1, donc pour $\forall a \in \mathbb{Z}$ (a, p) est soit p , soit 1. Si $(a_1, p) = p$, alors a_1 est divisible par p . Si $(a_1, p) = 1$, alors (par Théorème 5) a_2 est divisible par p . CQFD

Corollaire 1 Soient $a_1, \dots, a_r \in \mathbb{Z}$ et p un premier. Si $a_1 \cdots a_r$ se divise par p , alors au moins un des a_1, \dots, a_r se divise par p .

Démonstration Le cas de $r = 2$ est Théorème 6. Lorsque $r \geq 3$, supposez que la thèse soit vraie pour les produits d'entiers au nombre de $n - 1$. Si

$$a_1 \cdots a_r = (a_1 \cdots a_{r-1}) a_r$$

se divise par p , alors (par Théorème 6) au moins un des $a_1 \cdots a_{r-1}$ ou a_r se divise par p . Dans le premier cas (par l'hypothèse de récurrence) au moins un des a_1, \dots, a_{r-1} se divise par p . Donc la thèse est vraie (par Théorème 2a) pour $\forall r$ supérieur ou égal à 2. CQFD

Corollaire 2 Soient $a \in \mathbb{Z}$, $r \in \mathbb{Z}^+$ et p un premier. Si a^r se divise par p , alors a se divise lui-même par p .

Démonstration Il suffit de poser que $a_1 = \dots = a_r = a$ dans Corollaire 1.
CQFD

5. Démonstration du théorème fondamental

Théorème 7a (possibilité de la décomposition) Un entier quelconque supérieur ou égal à 2 se décompose en produit de facteurs premiers au nombre fini, tel que

$$a = p_1 \cdots p_r$$

Démonstration La thèse est vraie pour $a = 2$. Lorsque $a \geq 3$, supposez que la thèse soit vraie pour $\forall a' \in \mathbb{Z}$ tel que $2 \leq a' < a$. Si a est premier, alors la thèse est vraie. Sinon il existe a_1 , diviseur de a tel que $1 < a_1 < a$, avec lequel a se décompose en

$$a = a_1 a_2$$

Étant donné que $2 \leq a_1 < a$ et $2 \leq a_2 < a$, chacun des a_1, a_2 se décompose (par l'hypothèse de récurrence) en produit de facteurs premiers au nombre fini. a est le produit de ces deux produits, dont le nombre des facteurs est la somme de ceux des deux derniers, c'est-à-dire fini. Donc la thèse est vraie (par Théorème 2b) pour $\forall r$ supérieur ou égal à 2. **CQFD**

Théorème 7b (unicité de la décomposition) Si $p_1, \dots, p_r, q_1, \dots, q_s \in \mathbb{Z}^+$ sont tous premiers et

$$p_1 \cdots p_r = q_1 \cdots q_s \quad (1)$$

alors $r = s$ et $p_i = q_i$ ($i = 1, \dots, r$), q_1, \dots, q_s étant rangés en ordre approprié.

Démonstration Lorsque $r = 1$, le membre gauche de (1) est un premier, donc le membre droit l'est lui aussi. Alors $s = 1$ et $q_1 = p_1$.

Lorsque $r \geq 2$, supposez que la thèse soit vraie pour les premiers au nombre de $r - 1$. Si (1) est vrai, alors $q_1 \cdots q_s$ se divise par p_1 , donc (par Corollaire 1 de Théorème 6) au moins un d'eux se divise par p_1 . Soit q_1 , par

exemple, divisible par p_1 . q_1 est un premier comme l'est p_1 , donc $q_1 = p_1$. Alors les deux membres de (1) se divisent par p_1 et on a

$$p_2 \cdots p_r = q_2 \cdots q_s \quad (2)$$

Le membre gauche de (2) est produit de premiers au nombre de $r - 1$, donc (par l'hypothèse de récurrence) $r - 1 = s - 1$, c'est-à-dire $r = s$, et $p_i = q_i$ ($i = 2, \dots, r$), q_2, \dots, q_s étant rangés en ordre approprié. Donc (par Théorème 2a) la thèse est vraie pour $\forall r$ supérieur ou égal à 1. CQFD

6. Quelques applications des théorèmes démontrés

Remarque 1 Il est possible qu'un même facteur premier apparaisse à plusieurs reprises dans la décomposition d'un entier. Soient a entier supérieur ou égal à 2, $\alpha_1, \dots, \alpha_r \in \mathbb{Z}^+$ et p_1, \dots, p_r facteurs premiers de a qui se diffèrent l'un de l'autre, apparaissant dans la décomposition de a respectivement α_i ($i = 1, \dots, r$) fois. Avec la puissance, a s'écrit sous la forme

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

Cette forme-ci, que nous nommons *décomposition normale*, peut inclure, si besoin est, des premiers qui ne soient pas facteurs de a . Leurs exposants sont alors 0.

Remarque 2 Soient p_1, \dots, p_r l'ensemble de tous les facteurs premiers de $a, b \in \mathbb{Z}^+$, et $\alpha_i, \beta_i \in \mathbb{N}$ ($i = 1, \dots, r$) tels que

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \quad b = p_1^{\beta_1} \cdots p_r^{\beta_r}$$

Pour que b soit diviseur de a , il est nécessaire et suffisant que

$$\beta_i \leq \alpha_i \quad (i = 1, \dots, r)$$

Si $d = (a, b)$ et $\min\{\alpha_i, \beta_i\} = \delta_i$, alors

$$d = p_1^{\delta_1} \cdots p_r^{\delta_r}$$

Lorsque a, b sont premiers entre eux, c'est-à-dire $(a, b) = 1$, alors $\delta_1 = \dots = \delta_r = 0$.

Remarque 3 Soit $q = b/a$ ($a, b \in \mathbb{Z}$) rationnel non-nul tel que $d = (a, b) > 1$. En posant que $a = da'$ et $b = db'$, on a $q = b'/a'$, (a', b') étant 1. Cela signifie qu'un rationnel quelconque non-nul équivaut à une fraction irréductible.

Exemple 1 $\sqrt{2}$ est irrationnel.

Démonstration Si $\sqrt{2} \in \mathbb{Q}$, alors, avec $\exists a, b \in \mathbb{Z}$ tel que $(a, b) = 1$, $\sqrt{2}$ s'écrit sous la forme

$$\sqrt{2} = \frac{b}{a} \quad (1)$$

Évidemment $\sqrt{2} \notin \mathbb{Z}$, donc $a > 1$. En multipliant les deux membres de (1) par a et les élevant à la deuxième puissance, on a

$$2a^2 = b^2 \quad (2)$$

Soit p un facteur premier de a . (Par (2)) b^2 est divisible par p , et (par Corollaire 2 de Théorème 6) b l'est lui aussi. Alors $(a, b) = p$, ce qui est contradictoire avec l'hypothèse $(a, b) = 1$. Ainsi faut-il que $\sqrt{2} \notin \mathbb{Q}$. **CQFD**

Remarque La proposition de l'Exemple 1 se démontre autrement :

Démonstration Soit x entier positif. Si x est impair, c'est-à-dire si, avec $\exists k \in \mathbb{Z}$, x s'écrit : $x = 2k + 1$, alors $x^2 = 2(2k^2 + 2k) + 1$, c'est-à-dire x^2 est impair. Donc si x^2 est pair, alors x l'est lui aussi.

Si $\sqrt{2} \in \mathbb{Q}$, alors, étant donnés a, b de la démonstration précédente, on a $2a^2 = b^2$, donc b^2 est pair, et b l'est lui aussi. Donc avec $\exists k \in \mathbb{Z}$ b s'écrit : $b = 2k$. Il s'ensuit que $2a^2 = (2k)^2$, c'est-à-dire $a^2 = 2k^2$. a^2 est donc pair, et a l'est lui aussi. Alors $(a, b) = 2$, ce qui est contradictoire avec l'hypothèse $(a, b) = 1$, etc. **CQFD**

Cette démonstration-ci dépend pourtant d'une propriété spécifique du nombre 2, tandis que celle-là, d'une nature moins spécifique, se généralise comme on le verra ci-dessous.

Exemple 2 Soit $n, k \in \mathbb{Z}^+$. S'il n'existe pas $x \in \mathbb{Z}$ qui satisfasse l'équation

$$x^n = k$$

alors $\sqrt[n]{k}$ est irrationnel.

Démonstration Si $\sqrt[n]{k} \in \mathbb{Q}$, alors, avec $\exists a, b \in \mathbb{Z}$ tel que $(a, b) = 1$, $\sqrt[n]{k}$ s'écrit sous la forme

$$\sqrt[n]{k} = \frac{b}{a} \quad (1)$$

Évidemment $\sqrt[n]{k} \notin \mathbb{Z}$, donc $a > 1$. En multipliant par a les deux membres de (1) et les élevant à la $n^{\text{ième}}$ puissance, on a

$$ka^n = b^n \quad (2)$$

Soit p un facteur premier de a . (Par (2)) b^n est divisible par p , et (par Corollaire 2 de Théorème 6) b l'est lui aussi. Alors $(a, b) = p$, ce qui est contradictoire avec l'hypothèse $(a, b) = 1$. Ainsi faut-il que $\sqrt[n]{k} \notin \mathbb{Q}$. CQFD

Exemple 3 Soient $c_0, \dots, c_n \in \mathbb{Z}$ dont c_0, c_n sont non-nuls. Si l'équation de x

$$c_0x^n + c_1x^{n-1} + \dots + c_{n-1}x + c_n = 0$$

a pour solution une valeur rationnelle (en fait entière) $x = b/a$ telle que $a \in \mathbb{Z}^+$, $b \in \mathbb{Z}$ et $(a, b) = 1$, alors a est diviseur de c_0 , et b de c_n .

Démonstration Par l'hypothèse

$$c_0 \left(\frac{b}{a}\right)^n + c_1 \left(\frac{b}{a}\right)^{n-1} + \dots + c_{n-1} \left(\frac{b}{a}\right) + c_n = 0$$

En multipliant par a^n les deux membres, on a

$$c_0b^n + c_1ab^{n-1} + \dots + c_{n-1}a^{n-1}b + c_na^n = 0 \quad (1)$$

d'où

$$c_0b^n = a(-c_1b^{n-1} - \dots - c_{n-1}a^{n-2}b - c_na^{n-1})$$

donc c_0b^n se divise par a . Soient $d = (a, b^n) > 1$ et p un facteur quelconque de d . a est divisible par p . b^n l'est lui aussi, alors (par Corollaire 2 de Théorème 6) b se divise par p . Il s'ensuit que $(a, b) = p$, ce qui est contradictoire avec l'hypothèse $(a, b) = 1$. Ainsi faut-il que $(a, b^n) = 1$, et (par Théorème 5) c_0 se divise par a .

(1) s'écrit aussi sous la forme

$$c_na^n = b(-c_0b^{n-1} - c_1ab^{n-2} - \dots - c_{n-1}a^{n-1})$$

d'où vient parallèlement que c_n se divise par b . CQFD

Remarque 1 Soit $c_0 = 1$. Pour savoir si l'équation de x

$$x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n = 0$$

a pour solution des valeurs rationnelles (en fait entières) ou non, il suffit de remplacer, dans le membre gauche, x par les diviseurs positifs et négatifs de c_0 , et de voir si les résultats en sont 0 ou non.

Remarque 2 Exemple 1 et Exemple 2 sont des cas spéciaux de Exemple 3. Si, par exemple, l'équation de x

$$x^2 - 2 = 0$$

a pour solution une valeur rationnelle, il faut que ce soit un entier diviseur de 2, c'est-à-dire un des $\pm 1, \pm 2$, qui tous ne satisfont évidemment pas l'équation. Donc $\sqrt{2}$ est irrationnel.

Remarque 3 Pour revenir à $\forall c_0 \in \mathbb{Z}$ non-nul, on peut avancer la proposition de Exemple 3 en termes suivants :

Étant donnés c_0, \dots, c_n de Exemple 3, si le polynôme

$$P(x) = c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n$$

a pour facteur un binôme $ax - b$ tel que $a \in \mathbb{Z}^+$, $b \in \mathbb{Z}$ et $(a, b) = 1$, alors a est diviseur de c_0 , et b de c_n .

Exemple 4 Soient $a_1, \dots, a_r \in \mathbb{Z}$ non-nuls. S'ils sont tous premiers entre eux, autrement dit que $(a_i, a_j) = 1$ pour $\forall i, j \in \{1, \dots, r\}$ tels que $i \neq j$, alors il existe $k_1, \dots, k_r \in \mathbb{Z}$ tels que

$$\frac{1}{a_1 \cdots a_r} = \frac{k_1}{a_1} + \cdots + \frac{k_r}{a_r} \quad (1)$$

Démonstration Soient $A = a_1 \cdots a_r$ et

$$A = a_i A_i \quad (i = 1, \dots, r)$$

Si A_1, \dots, A_r ont p pour facteur premier commun, alors p est un facteur premier de A , et (par Corollaire 1 de Théorème 6) au moins un des a_1, \dots, a_r se divise par p . Soit a_1 , par exemple, divisible par p . (Par l'hypothèse

$(a_i, a_j) = 1$) aucun des a_2, \dots, a_r ne se divise par p , ce qui est contradictoire avec l'hypothèse selon laquelle

$$A_1 = a_2 \cdots a_r$$

ait p pour facteur premier. Donc A_1, \dots, A_r sont tous premiers entre eux, c'est-à-dire $(A_1, \dots, A_r) = 1$. Il s'ensuit (par Théorème 4) qu'il existe $k_1, \dots, k_r \in \mathbb{Z}$ tels que

$$1 = k_1 A_1 \cdots k_r A_r \quad (2)$$

En divisant par A les deux membres de (2), on obtient (1). CQFD

Exemple 5 Soient $a \in \mathbb{Q}$ non-nul, et

$$p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

décomposition normale du dénominateur de la fraction irréductible équivalente à a . Alors il existe $k_1, \dots, k_r \in \mathbb{Z}$ tels que

$$a = \frac{k_1}{p_1^{\alpha_1}} + \cdots + \frac{k_r}{p_r^{\alpha_r}} \quad (1)$$

Démonstration Soient $P = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, et

$$P = p_i^{\alpha_i} P_i \quad (i = 1, \dots, r)$$

Si P_1, \dots, P_r ont p pour facteur premier commun, alors p est un facteur premier de P , et (par Corollaire 1 de Théorème 6) au moins un des $p_1^{\alpha_1}, \dots, p_r^{\alpha_r}$ se divise par p . Soit $p_1^{\alpha_1}$, par exemple, divisible par p . (Par l'hypothèse $(p_i, \dots, p_j) = 1$) aucun des $p_2^{\alpha_2}, \dots, p_r^{\alpha_r}$ ne se divise par p , ce qui est contradictoire avec l'hypothèse selon laquelle

$$P_1 = p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

ait p pour facteur premier. Donc P_1, \dots, P_r sont tous premiers entre eux, c'est-à-dire $(P_1, \dots, P_r) = 1$. Il s'ensuit (par Théorème 4) qu'il existe $k_1, \dots, k_r \in \mathbb{Z}$ tels que

$$1 = k_1 P_1 \cdots k_r P_r \quad (2)$$

En divisant par A les deux membres de (2), on obtient (1). CQFD