Chap. 4

Factorisation en nombres premiers

a) Le théorème :

Théorème (théorème fondamental de l'arithmétique).

Soit $a \in \mathbb{N}$, $a \geq 2$. On peut écrire de manière unique :

$$a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_n^{\alpha_n}$$

où :

i) $n \in \mathbb{N}^*$

ii) $p_1, \dots, p_n$ sont des nombres premiers, et

$$p_1 < p_2 < \dots < p_n$$

iii) $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$.

Remarque : "De manière unique", signifie que :

Si $a = p_1^{\alpha_1} \times \cdots \times p_n^{\alpha_n}$
$= q_1^{\beta_1} \times \cdots \times q_m^{\beta_m}$

où i) $n, m \in \mathbb{N}^*$

ii) $p_1, \dots, p_n, q_1, \dots, q_m$ sont des nombres premiers tels que $p_1 < \dots < p_n$
et $q_1 < \dots < q_m$

iii) $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m \in \mathbb{N}^*$

Alors on a :

i) $n = m$.

ii) $p_i = q_i \quad \forall i \in [\![1, n]\!]$

iii) $\alpha_i = \beta_i \quad \forall i \in [\![1, n]\!]$.

Exemple : $396 = 2^2 \times 3^2 \times 11^1$

$n = 3$

$p_1 = 2 < p_2 = 3 < p_3 = 11$

$\alpha_1 = 2, \ \alpha_2 = 2, \ \alpha_3 = 1$

Preuve :

i) **Existence :**

Procédons par récurrence sur a.

Si $a = 2 = 2^1$, c'est vrai.

Supposons qu'on puisse trouver une telle écriture pour tout entier inférieur ou égal à a. Montrons qu'elle existe aussi pour $a+1$:

Puisque $a+1 \geqslant 2$, $a+1$ est divisible par un nombre premier p.

Ecrivons $(a+1) = p\, b$. $b \in \mathbb{N}$.

Puisque $p \geqslant 2$, on a :

$$1 \leqslant b \leqslant a.$$

Si $b = 1$, alors $a = p^1$, on a fini.

Si $b \geqslant 2$, d'après l'hypothèse de récurrence,

$$b = q_1^{\beta_1} \cdots q_m^{\beta_m}$$

où les q_i sont des nombres

premiers.

Donc $\quad a = p \times q_1^{\beta_1} \times \dots \times q_m^{\beta_m}$

Quitte à réorganiser les facteurs premiers, l'ecistence d'une décomposition est prouvée.

ii) Unicité :

Supposons que l'on puisse écrire :

$$a = p_1^{\alpha_1} \times \dots \times p_n^{\alpha_n} = q_1^{\beta_1} \times \dots \times q_m^{\beta_m}$$

où les entiers $m, n, p_i, q_i, \alpha_i, \beta_i$ satisfont les hypothèses déjà énoncées.

Montrons que $\quad p_1 \in \{q_1, \dots, q_m\}$

puisque $a = p_1 \times (p_1^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_n^{\alpha_n})$

$$= q_1^{\beta_1} \times \dots \times q_m^{\beta_m},$$

on observe que $p_1 \mid q_1^{\beta_1} \times \dots \times q_m^{\beta_m}$

donc p_1 divise $q_1 \times (q_1^{\beta_1 - 1} \times \dots \times q_m^{\beta_m})$.
On peut utiliser le lemme suivant :

Lemme : Soit p, q deux nombres premiers.
Soit $p \wedge q = 1$, soit $p = q$.

Preuve : Soit $d = p \wedge q$.
$d \mid p$. si $d = 1$ c'est terminé.
Sinon $d = p$. Donc $d = p$ est un diviseur de q distinct de 1.
Forcément, $p = q$. $\square$

On a donc : $p_1 \mid q_1 \times (q_1^{\beta_1 - 1} \times q_2^{\beta_2} \times \dots \times q_m^{\beta_m})$.
Si $p_1 = q_1$, on a bien :
$$p_1 \in \{q_1, \dots, q_m\}.$$

Sinon, d'après le lemme de Gauss,

$$p_1 \mid q_1^{\beta_1 - 1} q_2^{\beta_2} \cdots q_m^{\beta_m}.$$

Puisque $p_1 \wedge q_1 = 1$, $p_1 \wedge q_1^{\beta_1 - 1} = 1$.
Le lemme de Gauss nous dit que :

$$p_1 \mid q_2^{\beta_2} \cdots q_m^{\beta_m}.$$

On recommence autant de fois que nécessaire, pour obtenir

$$p_1 \in \{q_2, \dots, q_m\}.$$

$$\{p_1, \dots, p_n\} = \{q_2, \dots, q_m\}$$

Le raisonnement effectué pour p_1 peut être appliqué à chacun des p_i pour prouver que

$$\{p_1, \dots, p_n\} \subset \{q_1, \dots, q_m\};$$

De même avec les q_i pour l'inclusion inverse.

L'égalité des cardinaux de ces ensembles donne $m = n$.

Puisque les p_i et q_i sont ordonnés, $p_i = q_i$ pour tout $i \in [\![1, n]\!]$.

Montrons que $\alpha_i = \beta_i$.

Supposons que $\alpha_1 > \beta_1$.

On a :

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$$

$$\Rightarrow p_1^{\alpha_1 - \beta_1} \times \left(p_2^{\alpha_2} \cdots p_n^{\alpha_n} \right) = p_2^{\beta_2} \cdots p_n^{\beta_n}$$

Donc p_1 divise $p_2^{\beta_2} \cdots p_n^{\beta_n}$, ce qui est impossible.

Ainsi, $\alpha_1 \leq \beta_1$.

De même, $\beta_1 \geq \alpha_1$, et $\alpha_i = \beta_i$ pour tout i.

$\square$

Autre écriture du théorème.
La décomposition en facteur premier peut aussi s'écrire ainsi :

Notons $\mathcal{P}$ l'ensemble des nombres premiers.
Soit $a \in \mathbb{N}$.
Il existe une unique application

$$\begin{aligned} \alpha : \mathcal{P} &\longrightarrow \mathbb{N} \\ p &\longmapsto \alpha_p \end{aligned}$$

telle que seul un nombre fini des α_p est nul et :

$$a = \prod_{p \in \mathcal{P}} p^{\alpha_p}.$$

Pour tout entier premier p, l'exposant α_p est appelé valuation p-adique de a, et parfois noté $v_p(a)$.

Exemple :

$$396 = 2^2 . 3^2 . 5^0 . 7^0 . 11^1 . 13^0 . 17^0 \ldots$$

Donc $\alpha_2 = v_2(396) = 2$

$\alpha_3 = 2$, $\alpha_5 = 0$, etc ...

b) Applications.

Les applications sont nombreuses.
Montrons par exemple le résultat classique suivant :

$\boxed{\text{Proposition: } \sqrt{2} \text{ est irrationnel.}}$

Preuve :

Supposons que $\sqrt{2}$ soit rationnel.
On peut écrire :

$$\sqrt{2} = \frac{a}{b} \quad \text{avec} \quad a \in \mathbb{N}^*, \ b \in \mathbb{N}^*.$$

$$\Rightarrow a = b\sqrt{2}$$

$$\Rightarrow a^2 = 2b.$$

Décomposons a et b en facteurs premiers :

$$a = \prod_{p \in \mathcal{P}} p^{\alpha_p} \quad , \quad b = \prod_{p \in \mathcal{P}} p^{\beta_p}$$

L'équation $a^2 = 2b^2$ devient :

$$\left(\prod p^{\alpha_p}\right)^2 = 2\left(\prod p^{\beta_p}\right)^2$$

$$\Rightarrow \prod p^{2\alpha_p} = 2 \times \prod p^{2\beta_p}$$

$$\Rightarrow 2^{2\alpha_2} \times \prod_{\substack{p \in \mathcal{P} \\ p \neq 2}} p^{2\alpha_p} = 2^{2\beta_2 + 1} \prod_{\substack{p \in \mathcal{P} \\ p \neq 2}} p^{2\beta_p}$$

L'unicité de la valuation 2-adique nous donne :

$$\underbrace{2\alpha_2}_{\text{pair}} = \underbrace{2\beta_2 + 1}_{\text{impair}}.$$

Ce n'est pas possible. $\square$

Beaucoup d'applications reposent sur le lemme suivant :

Lemme : Soit $(a, b) \in (\mathbb{N}^*)^2$ dont la décomposition en facteurs premiers s'écrit :

$$a = \prod_{p \in \mathcal{J}} p^{\alpha_p} \quad , \quad b = \prod_{p \in \mathcal{J}} p^{\beta_p}$$

Alors $a \mid b$ si et seulement si :

$$\forall p \in \mathcal{J}, \quad \alpha_p \leq \beta_p .$$

Preuve :

* si $\alpha_p \leq \beta_p$ pour tout p, on peut écrire $b = a \times \left(\prod p^{\beta_p - \alpha_p}\right)$.

* Dans l'autre sens, écrivons $b = ac$ et $c = \prod p^{\gamma_p}$.
L'unicité de la valuation p-adique donne :

$\forall p \in \mathcal{J}, \quad \beta_p = \alpha_p + \gamma_p \Rightarrow \alpha_p \leq \beta_p.$ $\square$

Proposition :

Soit $a = \prod_{p \in \mathcal{J}} p^{\alpha_p}$, $b = \prod_{p \in \mathcal{J}} p^{\beta_p}$

deux entiers décomposés en facteurs premiers. On a :

$$\text{pgcd}(a, b) = \prod_{p \in \mathcal{J}} p^{\min(\alpha_p, \beta_p)}$$

$$\text{ppcm}(a, b) = \prod_{p \in \mathcal{J}} p^{\max(\alpha_p, \beta_p)}$$

Preuve (pour le pgcd ; ppcm en exercice).

Pour tout nombre premier p, posons
$\delta_p = \min(\alpha_p, \beta_p)$.

Posons $d = \prod p^{\delta_p}$.

Puisque, pour tout p, $\delta_p \leqslant \alpha_p$,

d divise a.

De même, d divise b.

Soit maintenant $d' \in \mathbb{N}^*$, un diviseur commun à a et b.

Ecrivons $d' = \prod p^{\delta'_p}$.

Puisque $d' \mid a$, $\delta'_p \leq \alpha_p$ pour tout nombre premier p.

De même, $\delta'_p \leq \beta_p$.

Ainsi

$$\delta'_p \leq \min(\alpha_p, \beta_p)$$
$$\delta'_p \leq \delta_p.$$

Donc d' divise d. $\square$